LUISS

Dipartimento
di Giurisprudenza

Cattedra Diritto Penale 2

Intelligenza artificiale, riconoscimento facciale e pubblica sicurezza. La sorveglianza di massa tra diritto e procedura penale.

Prof. Antonino Gullo
RELATORE

Prof. Maria Lucia Di Bitonto
CORRELATORE

Matr. 132293
CANDIDATO

Anno Accademico 2021/2022

INTELLIGENZA ARTIFICIALE, RICONOSCIMENTO FACCIALE E PUBBLICA SICUREZZA.

LA SORVEGLIANZA DI MASSA TRA DIRITTO E PROCEDURA PENALE

SOMMARIO GENERALE:

INTRODUZIONE

Lo sviluppo tecnologico ha sempre rappresentato un elemento cardine nel progresso umano e della società, anche se alcuni traguardi raggiunti non sempre hanno destato un unanime consenso tra i potenziali beneficiari. Se poi la tecnologia di cui si parla ha come ambizioso obiettivo quello di emulare, se non superare, l'agire dell'essere umano nella sua dimensione logica e nella capacità di analisi, sintesi e decisione, il percorso che si delinea diventa insidioso.

L'intelligenza artificiale è molto di più di uno stadio evolutivo del progresso tecnologico, poiché rappresenta una sfida che mette in discussione l'intero agire umano, la sua onestà e la sua etica. Così facendo, tale tecnologia pone l'essere umano davanti al riflesso dei limiti e continui errori del suo agire. L'intelligenza artificiale, però, può anche rappresentare un'opportunità per il genere umano, per porsi interrogativi cruciali e risolvere atavici pregiudizi, garantendo così un futuro migliore e un rapporto con la "macchina intelligente" di benefica cooperazione e non di contrapposizione, come, più o meno consapevolmente, taluni temono.

Nella sua multiforme capacità di applicazione, l'intelligenza artificiale incontra il delicato dominio della pubblica sicurezza, un ambito già di per sé critico poiché situato sul difficile confine tra protezione del cittadino e intrusione nei suoi diritti e libertà. Un bilanciamento che è complesso in molte circostanze. Se, poi, un ulteriore elemento, dirompente e contraddittorio come l'intelligenza artificiale, entra nella dicotomia tra diritti e sicurezza, l'equilibrio potrebbe diventare ancora più ambizioso da raggiungere. Potrebbe però accadere che, invece, tale equilibrio sia più raggiungibile grazie a questo ausilio tecnologico, sebbene con imponenti sforzi concettuali, progettuali, operativi e normativi. La questione diventa ancora più delicata quando gli algoritmi, interpretabili come l'espressione del ragionamento logico dell'intelligenza artificiale, vengono applicati per identificare le persone. Dal momento che il riconoscimento avviene attraverso tecniche che "catturano" le informazioni personali, anche da un punto di vista biologico con i rilevamenti cosiddetti biometrici, è possibile creare un vero e proprio "documento di identità" della persona.

Il riconoscimento facciale rientra nell'alveo di tali tecniche e può essere impiegato per finalità "buone" o "cattive", in quanto, nella neutralità che ogni tecnologia intrinsecamente possiede nei confronti del suo impiego, essa è mero strumento nelle mani degli esseri umani. L'applicazione del riconoscimento facciale basato su intelligenza artificiale per sorvegliare le persone in modo specifico o in massa può essere di ausilio alle attività di pubblica sicurezza, ed è giustificabile o meno a seconda di talune circostanze. Tale applicazione, collocandosi sul citato confine tra diritti e sicurezza, necessita di un inquadramento normativo e di una chiara visione sulle responsabilità, in particolare penali, dei soggetti coinvolti. Tra l'altro, l'evoluzione delle tecniche basate sull'intelligenza artificiale è connotata da velocità ed ecletticità,

le quali richiedono strumenti giuridici idonei per poterne trarre beneficio ed essere al contempo protetti dagli aspetti potenzialmente pericolosi.

La tesi si incentra proprio sulla ricerca di un equilibrio giuridico tra diritti, pubblica sicurezza e possibile impiego diffuso della intelligenza artificiale, nello specifico nell'ambito penale. Il tema della ricerca, muovendo dall'intelligenza artificiale nel suo complesso, si focalizza, specificatamente, sugli algoritmi e sui sistemi per la identificazione attraverso il riconoscimento facciale, oltre al suo eventuale e discusso impiego per la sorveglianza di massa. Per poter individuare aree propositive nell'attuale scenario, il percorso del lavoro ha richiesto di affacciarsi anche in ambiti multidisciplinari, per comprendere la tecnologia dell'intelligenza artificiale e le opzioni che essa offre, le applicazioni presenti e future e, quindi, esaminarne l'impatto sullo scenario normativo. È stato altresì necessario guardare ai benefici, alle potenzialità, agli aspetti critici fino agli abusi dell'impiego del riconoscimento facciale nella sorveglianza di massa, non solo in ambito nazionale e dell'Unione Europea, ma anche in varie parti del mondo ritenute significative per la trattazione. Si è rivelato, altresì, utile per una valutazione compiuta, rapportare quanto rilevato nei diversi scenari normativi all'ambito europeo attuale e alla sua possibile evoluzione.

Nel corso della trattazione, sono emersi una serie di aspetti rilevanti circa la responsabilità dell'algoritmo in caso di reati e l'impiego di quest'ultimo quale strumento di ausilio per le attività di pubblica sicurezza e per il processo penale. Alcuni elementi chiave riguardano l'apprezzamento della prova legata all'algoritmo, l'autoria, il ruolo degli esperti a supporto delle autorità preposte alla pubblica sicurezza e dei tribunali, l'impiego di algoritmi autovalutativi e la dimensione progettuale di alcuni aspetti del trattamento dei dati personali di ausilio al bilanciamento tra diritti e sicurezza.

La tesi è organizzata in tre parti che concernono, rispettivamente, l'inquadramento della intelligenza artificiale (Capitolo I), la intelligenza artificiale nella pubblica sicurezza, con particolare riferimento al riconoscimento facciale e alla sorveglianza di massa (Capitolo II) nonché, infine, gli aspetti comparatistici, le proposte e le prospettive del riconoscimento facciale e della sorveglianza di massa (Capitolo III). In particolare, nel Capitolo I sono presentate le caratteristiche dell'intelligenza artificiale, degli algoritmi e i relativi domini applicativi, nonché il suo inquadramento nelle normative europee. Si è altresì affrontato il delicato tema della responsabilità legata ai sistemi di intelligenza artificiale e al loro impiego per coadiuvare le attività del giudice penale, nonché i problemi di autoria.

Nel Capitolo II, dopo aver introdotto le tecniche di riconoscimento biometrico e, specificatamente il riconoscimento facciale e la sorveglianza di massa, sono stati affrontati i complessi temi della relazione tra diritti, pubblica sicurezza, protezione dei dati e aspettativa di privacy. Sono altresì affrontati gli aspetti legati all'impiego dei dati per finalità di contrasto, nello scenario normativo europeo e nazionale, nell'attività del

Garante e in quelle dell'European Data Protection Board. Vengono poi approfonditi utili elementi legati all'ammissibilità, compiutezza e termine di conservazione dei dati che, unitamente ai contenuti di alcune sentenze della Corte di Giustizia dell'Unione europea, forniscono riflessioni per ulteriori proposte.

Nel Capitolo III, infine, viene dapprima completato il quadro sull'impiego di intelligenza artificiale, riconoscimento facciale e sorveglianza di massa con un approfondimento in aree geografiche extra-UE nonché una comparazione con il contesto europeo. Il fine è quello di predisporre una visione sistemica sull'accoglimento della tecnologia, sull'uso e l'abuso della stessa. Sull'analisi condotta nei capitoli precedenti, da cui sono emerse le potenzialità di queste nuove tecnologie, presenteremo una serie di proposte operative per il loro corretto impiego.

CAPITOLO I – INQUADRAMENTO DELL'INTELLIGENZA ARTIFICIALE

SOMMARIO: 1. IA: machine learning, software intelligenti e apprendimenti automatici. – 2. Ambiti applicativi della IA. – 2.1. *(Segue):* applicazioni in ulteriori ambiti. – 3. La definizione contenuta nella proposta di Regolamento sull'Intelligenza artificiale. – 3.1. *(Segue):* pratiche di IA e sistemi ad alto rischio. – 3.2. *(Segue):* esemplificazioni e sistema di gestione dei sistemi di IA ad alto rischio. – 4. Problematiche. – 4.1. *(Segue):* aspetti etici e di privacy. – 5. Sfide presenti e future nell'attribuzione di responsabilità dell'IA. – 5.1. *(Segue):* responsabilità del progettista e del programmatore. – 5.2. *(Segue):* responsabilità di venditore e produttore. – 5.3. *(Segue):* responsabilità dell'utilizzatore. – 5.4. *(Segue):* considerazioni conclusive sulla responsabilità da IA. – 6. Algoritmi predittivi nell'ambito penale. – 6.1. *(Segue):* l'*evidence-based sentencing* e le criticità collegate all'impiego dell'IA nelle decisioni giudiziarie. – 7. Autoria in caso di scelta di computer e software.

1. IA: software intelligenti, machine learning e apprendimenti automatici.

Nell'attuale mondo iperconnesso, si parla sempre più spesso dell'utilizzo dell'Intelligenza Artificiale (IA) in diversi ambiti del vivere civile. Pur essendo ormai penetrato diffusamente nella vita quotidiana dell'essere umano, si avverte l'esigenza di definire in modo condiviso, se non univoco, questa forma di intelligenza che si pone a diretto contatto con quella umana.

Vi sono similarità fra la struttura dell'intelligenza umana e quella della struttura fisica dell'IA, in quanto concepito sulla base del modello celebrale e sensoriale dell'essere umano. Cercando di stabilire che cosa sia l'intelligenza e l'emulazione di questa da parte della tecnologia, si pone la problematica di definire in modo chiaro la IA. La radice della definizione nasce nel 1950, quando il matematico Alan Turing[1] pose il principio delle questioni sul tema della intelligenza delle macchine chiedendosi se le macchine potessero pensare. Successivamente, nel cercare di paragonare i tipi di intelligenza umana e artificiale, concepì il cosiddetto "*Test di Turing*"[2] il quale si riteneva superato dalla macchina qualora, a seguito delle risposte poste da un esaminatore umano, questi non sarebbe stato in grado di distinguere la provenienza umana o meccanica delle risposte.[3]

La prima definizione di *intelligenza artificiale* è attribuita all'informatico John McCarthy nel 1956. Attraverso successive integrazioni si giunge alla seguente formulazione: «[l'IA è] la scienza e l'ingegneria del fare macchine intelligenti, specialmente programmi intelligenti per computer. è connessa al compito simile di

[1] TURING A. M., "On computable numbers, with an application to the entscheidungs problem", Princeton, 1936
[2] noto anche come il gioco dell'imitazione o "*the imitation game*"
[3] RUSSELL J. - NORVIG P., "*Artificial Intelligence. A Modern Approach*", New Jersey, 2010, 5, 6

usare i computer per comprendere l'intelligenza umana, ma l'IA non ha la necessità di limitarsi a metodi che sono biologicamente osservabili». [4]

È evidente, quindi, per il giurista la necessità di una definizione precisa ai fini di una migliore comprensione delle implicazioni nell'ambito giuridico, dal momento che per sua natura l'IA non sembra poter essere confinata in una descrizione univoca. L'esigenza di un inquadramento e una regolamentazione a livello europeo ha condotto alla presentazione del documento "*L'intelligenza artificiale per l'Europa*" da parte della Commissione europea per la quale l'IA *«*indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi*».*[5] Proseguendo nella descrizione la Commissione sottolinea come i sistemi imperniati sull'IA *«*possono consistere solo in software che agiscono nel mondo virtuale[6]; oppure incorporare l'IA in dispositivi hardware[7]*».*

Per giungere a una descrizione mirata della tecnologia IA è opportuno sottolineare che essa è un complesso sistema informatico composto da l'*hardware*, che definisce le parti tangibili del sistema, e *software*, il quale indica l'insieme di programmi che consentono allo stesso sistema di svolgere le proprie funzioni.

L'hardware dell'IA, in particolare, progettato tenendo conto delle specificità della stessa, consente l'incremento, il training e l'efficienza delle reti neurali artificiali, le quali simulano interconnessioni tra input e output e in base agli stessi modificano la loro struttura «non-lineare».[8] Gli acceleratori hardware in questo "sistema adattivo", si ispirano ed emulano le reti neurali cerebrali umane nella percezione ed elaborazione dei dati interni e esterni, con una realizzazione a carattere bio-mimetico con diversi modelli di neuroni e sinapsi, o sono finalizzati ad elaborare dati detratti da eventi reali filmati.[9]

Il training, quindi il processo tramite il quale le reti neurali apprendono come affrontare un problema quando questo si pone, è ricollegato al *Machine Learning* (ML)[10]. Quest'ultimo permette il cosiddetto *apprendimento automatico* e adattivo con

[4] MCCARTHY J., "*What Is Artificial Intelligence*", Standford, 2007

[5] Commissione Europea, Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni - *L'intelligenza artificiale per l'Europa*, COM (2018) 237 final.

[6] per esempio: assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale

[7] per esempio, in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose

[8] BOLDRINI N., *Reti neurali: cosa sono e a cosa servono*, in *AI4business*, 2022

[9] ABDERRAHMANE N. – LEMAIRE E. – MIRAMOND B., *Design Space Exploration of Hardware Spiking Neurons for Embedded Artificial Intelligence*, in *Elsevier*, vol. 121, 366 e ss., 2020

[10] risulta necessaria la sua distinzione rispetto all'intelligenza artificiale, essendo un sottoinsieme di questa e costituendo una modalità di apprendimento a sé stante

l'impiego di *algoritmi*[11] atti ad acquisire dati dall'esperienza e la cui evoluzione migliora l'impatto all'aumentare della mole di dati, che a sua volta consente lo sviluppo di modelli e di tecniche di deduzione logica di grande efficacia.[12] Vi sono tre modelli di apprendimento distinti con le quali il ML può agire. L'utilizzo di una di queste modalità dipende dalla presenza o meno di un soggetto atto all'addestramento, ad esempio un data scientist, il quale istruisce l'algoritmo sui dati da generare fornendogli input e output desiderati al fine di identificare una regola generale di collegamento tra gli stessi.

In questo caso si parla di ML "supervisionato", modello largamente utilizzato e che permette la riutilizzazione della regola appresa ad altri simili incognite; al contrario quando il ML è più indipendente, lo si definisce "non supervisionato" in quanto nell'apprendimento non vi è un output definito e l'obiettivo è l'identificazione di una struttura logica nei dati forniti ma non "etichettato".[13] L'utilizzo del modello supervisionato o meno del ML, dipende da quale sia l'esigenza a cui si deve rispondere: il modello supervisionato è, ad esempio, impiegato nell'ambito del riconoscimento vocale, mentre quello non supervisionato trova applicazione nell'impiego dei motori di ricerca. Una categoria ibrida fra le due precedenti è basata sull'apprendimento cosiddetto "semi-supervisionato" in cui solo una parte degli input ha il corrispondente output partendo da un insieme di dati parziali, sulla base dei quali costruire la regola necessaria. Nella classificazione è anche possibile identificare una ulteriore categoria, detta "per rinforzo", la quale opera imparando dinamicamente dagli errori commessi e dall'ottenimento di un riconoscimento quando l'obiettivo viene raggiunto.

Avendo ora presentato un quadro sul machine learning, risulta opportuno ai fini di una maggiore chiarezza e più ampia comprensione del concetto di IA, evidenziare la distinzione con una specifica branca del ML, in quanto spesso i due termini vengono erroneamente utilizzati come sinonimi. Quando il meccanismo di apprendimento "emula" i meccanismi del cervello umano si parla di *Deep learning* (DL).

Il ML è «un'insieme di metodi per consentire al software di adattarsi» e dunque alla macchina di apprendere in modo automatico, il cosiddetto "*autoapprendimento*", per svolgere specifici compiti o attività in base ai diversi algoritmi utilizzati. Si può dunque parlare di "*training*" dell'IA il quale impara, si corregge e si esercita in funzione di un autonomo compimento dell'attività, e dunque decide, un esempio di questo è il riconoscimento di immagini e vocale.[14]

[11] l'algoritmo è una procedura di calcolo che fornisce determinati valori in uscita, dati specifici valori in ingresso.
[12] HANNACHI A., *Patterns identification and Data mining in weather and climate*, in *Springer*, 2021
[13] MARMO R., *Algoritmi per l'intelligenza artificiale*, Milano, 2020, 8
[14] il training dell'IA sarà oggetto di approfondimento trattando degli algoritmi predittivi. – *infra*, § 6.1

Il DL è una particolare componente del ML, che a sua volta è ricompreso all'interno dell'IA[15]: la denominazione "deep" nasce dalla metodica dell'approccio con cui elabora e utilizza i dati, ai fini dell'impiego degli stessi per la creazione di un modello «*data-driven*» attraverso una articolata fase di costruzione.[16] Una importante caratteristica da considerare del DL è la capacità di ricreare attraverso un approccio emulativo le connessioni della mente umana a livello neurale: attraverso degli algoritmi specifici esso genera una "*rete neurale artificiale*" [17]. La ricerca su questo tipo di rete è partita dall'idea che la riproduzione del neurone umano fosse in grado di creare una *intelligenza* e che un comportamento intelligente non sia dettato tanto dal ragionamento quanto dall'adattabilità all'ambiente[18].

La rete neurale, ispirandosi alla struttura del cervello umano, si compone di elementi software o "*neuroni*" e dei collegamenti tra essi e ogni neurone, ricevendo come *input* determinati dati, può fornire *output*[19] agli altri neuroni ad esso collegati. Affinché la rete possa operare è necessaria una fase di addestramento nella quale si forniscano alla rete degli esempi attraverso l'inserimento di input e corrispondenti output. In questo modo, la rete diviene in grado di apprendere e decidere autonomamente, richiedendo un ridotto intervento da parte della componente umana. La rete neurale addestrata apprende, quindi, un comportamento, come accade, ad esempio, per il riconoscimento di un volto umano[20], dominio applicativo nel quale confronta i volti memorizzati nel database e acquisisce autonomamente nuove informazioni utili per successive elaborazioni. Un ulteriore esemplificazione è la creazione di una rete neurale che possa prevedere l'esito di casi giudiziari e che viene addestrata su casi reali e ipotetici fino al momento in cui non giunga a un risultato corretto.[21]

I sopraelencati elementi dell'IA permettono, ad avviso di chi scrive, un migliore inquadramento delle componenti dell'IA, ma non risolvono la necessità di una definizione che possa ricomprendere ogni ambito in cui l'IA si trova attualmente ad operare. Risulta quasi diabolico il ricercare una tale definizione, dato l'ampio spettro di domini applicativi in cui tale tecnologia si espande, per cui ritengo che, possa essere utile un approccio flessibile ma, al contempo, risulta problematica l'assenza di chiarezza quando si tratti dell'inquadramento normativo.

In questo senso, una approfondita analisi delle principali problematiche potrebbe essere di ausilio nel favorire un lavoro graduale ma sistematico nella direzione di garanzia e

---

[15] LOVERGINE S., *Breve disamina degli algoritmi di intelligenza artificiale. Aspetti tecnologici e metodologici*, Rapporto dell'Istituto Nazionale per Analisi Politiche Pubbliche (INAPP), 2022, 7

[16] ZSARKER I.H., *Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions,* in *SN COMPUT. SCI.,* 2, 420, 2021

[17] l'utilizzo del termine *artificiale* evidenzia la differenza con le connessioni neurali umane

[18] SARTOR G., *L'intelligenza artificiale e il diritto*, Torino, 2022, 56

[19] l'output indica il risultato corretto per l'input fornito

[20] *infra*, Capitolo II

[21] *infra* § 6

maggiore protezione dell'utente, anche, e soprattutto, in vista dell'evoluzione nella IA che continuerà a cambiarne il volto e le prestazioni.

2. Ambiti applicativi della IA.

Per poter comprendere le ricadute giuridiche, in particolare quelle penali, che scaturiscono dal mondo della IA è necessario entrare negli ambiti applicativi in cui la tecnologia è già diffusa e quelli che in futuro verranno "conquistati" dalla IA, grazie alla sua versatilità e al continuo progresso di cui siamo testimoni.

L'applicazione è intrinsecamente collegata con il fulcro si un sistema di IA che è rappresentato dai suoi algoritmi[22] e dalle sue capacità e prestazioni, i quali, come si vedrà[23], presentano aspetti vantaggiosi ma anche a volte contraddittori e, dunque, potenzialmente problematici nel loro funzionamento nei diversi domini applicativi. Al fine di comprendere gli algoritmi, attraverso una visione sistemica, verranno qui anticipati i punti cruciali[24] che concernono gli ambiti applicativi.

Un algoritmo di IA per essere efficace ma rispettoso dell'ambito in cui è inserito, è auspicabile che possieda *trasparenza*, *equità* e muova da una base *dati* "affidabile", garantendo, allo stesso tempo, accuratezza e velocità di esecuzione. L'importanza della caratteristica di trasparenza della IA risiede nella necessità degli operatori umani di comprendere il risultato prodotto dall'algoritmo, vista la complessità del sistema e spesso dell'"*opacità*" [25] del suo funzionamento, nonostante le operazioni siano eseguite su computer conformi alla teoria della calcolabilità di Turing[26]. La mancanza di trasparenza potrebbe generare, tra l'altro, diffidenza negli utenti, essendo essa garanzia della comprensibilità da parte dell'operatore e dell'utente del meccanismo decisionale dell'algoritmo. L'origine della diffidenza e della necessità di trasparenza deriva anche dal fatto che i risultati forniti dall'algoritmo potrebbero mancare di equità.

Da questo origina una parte del problema legata ai cosiddetti "*bias cognitivi*"[27] in quanto l'impronta conferita dal suo sviluppatore e, dunque, dalle sue opinioni personali conferirebbero al risultato un'assenza di neutralità. Il bias, tuttavia, può non risiedere solo nell'algoritmo ma anche nell'insieme dei dati che l'algoritmo utilizza per il suo

[22] LOVERGINE, *Breve disamina degli algoritmi di intelligenza artificiale*, cit., 8
[23] *infra* § 4, 5, 6
[24] *infra* § 4
[25] UBERTIS G.*, Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Diritto Penale Contemporaneo* 2020, 78
[26] *supra* § 1
[27] ROBERTS L. A. – RICHARDSON B. et al., *General Perspectives Toward the Impact of AI on Race and Society*, in *Social Justice and Education in the 21st Century*, 2021, 347-363

funzionamento e addestramento. Un esempio di come il bias possa inficiare la neutralità del risultato è il progettista, o i dati da cui esso attinge, che nasconda una discriminazione a carattere etnico, la quale a sua volta si trasferirà sugli output e dunque sull'ambito applicativo. Tanto più la mole di dati da cui algoritmo attinge è vasta, i cosiddetti "*big data*"[28], tanto più risulta difficile governarne la qualità e la neutralità, considerando che gli stereotipi e i pregiudizi caratterizzanti i comportamenti sociali potrebbero non solo riflettere ma persino ampliare la polarizzazione nella previsione dell'IA basata su questi dati.

Come verrà illustrato in seguito[29], l'importanza dell'assenza di polarizzazione assume cruciale rilevanza nelle applicazioni della IA nell'ambito giudiziario. Infatti, la capacità di analisi di una grande quantità di informazioni dell'IA e la sua capacità di previsione possono estendersi anche al riconoscimento di modelli comportamentali, come accade nella "*predictive policing*" (PP) [30], la quale si fonda sull'assunto della prevedibilità della commissione dei crimini e dell'intervento sull'ambiente sociale e fisico, ritenuto causa scatenante dei reati. In tal senso si ritiene che tale intervento potrebbe costituire un deterrente per reati futuri [31], come verrà approfondito successivamente[32], oltre a comportare potenziali benefici in termini di efficacia e riduzione di costi, da soppesare, tuttavia, col rischio di una non corretta previsione dell'avvenimento di un reato in una determinata area o ad opera di un determinato soggetto.[33] Inoltre, l'adozione effettiva da parte della polizia è un ulteriore elemento di cautela, poiché potrebbe differire in attenzione etica, effettività e tecniche.

La capacità di previsione dell'IA è riscontrabile anche in quella relativa al possibile esito di un giudizio, la cosiddetta "*giustizia predittiva*". La finalità della sua utilizzazione sarebbe quella di agevolare il compito dei soggetti giudiziari quali il giudice, difensori e accusa, sulla base delle informazioni costituite dai provvedimenti di legge e dalle pronunce giurisprudenziali, oltre ad essere centrale nella digitalizzazione della giustizia.[34] Nel caso di utilizzo di algoritmi basati sul DL, i meccanismi di autoapprendimento potrebbero condurre a una evoluzione autonoma dei

[28] AGATA C. – MANGIAMELI A., *Algoritmi e big data. Dalla carta sulla robotica* in Riv. fil. dir., 2019, 107, 124
[29] *infra* § 6
[30] FONSEKA T. M. – BHAT V. – KENNEDY S. H., *The utility of artificial intelligence in suicide risk prediction and the management of suicidal behaviours*, in *Sage*, 2019, 53 (10)
[31] FERGUSON A., *2017 a. Policing Predictive Policing*, in *Washington University Law Review*, 2017, 1148
[32] *infra* § 6
[33] BARRETT L., *Reasonably Suspicious Algorithms: Predictive Policing at the United States Border*, in *N.Y.U. Review of Law & Social Change*, 2017, 41 (3)
[34] MAESTRI E., *Giustizia digitale Tecnologia giudiziaria e accesso alla giustizia nell'era della digitalizzazione*, in *Archivio Penale*, 2020

risultati e dunque ad una quota di *imprevedibilità*[35] nei risultati di previsione dell'esito giudiziario.

L'utilizzo della IA quale supporto nell'ambito giuridico ha origine negli anni Ottanta quando si iniziò a impiegarla con i sistemi esperti basati sul paradigma "if-then"[36], per poi subire una estensione del suo impiego con l'avvento del ML e l'aumento della mole dei dati disponibili. In tal senso si può vedere come l'ausilio degli algoritmi nello svolgimento dell'attività legale generi un vantaggio da un punto di vista di celerità e sicurezza, pur con gli impliciti rischi che esso comporta, anche grazie all'analisi, elaborazione, rappresentazione e dunque comprensione del linguaggio naturale, attraverso il cosiddetto "*Natural Language Processing*" (NLP)[37], che permette ad esempio la disponibilità di un assistente virtuale per domande e risposte. Sono altresì disponibili software applicativi di supporto per gli studi legali, in particolare sviluppati e utilizzati negli Stati Uniti, quali ad esempio il Contract intelligence (COiN) e gli strumenti Genie AI e Rocket Lawyer, alternativi all'ormai inattivo strumento open source Docracy. Questi software consentono la gestione sicura della documentazione, della firma sia fisica che digitale, dello sviluppo di collaborazione interna e con terze parti.

Per quanto concerne la documentazione l'IA può essere utilmente impiegata nella revisione e nell'individuazione di elementi utili allo sviluppo processuale, oltre che nell'analisi contrattuale, con lo scopo di individuare ed estrarre informazioni di specifica rilevanza o per mettere in risalto le parti rilevanti di uno specifico contratto. In particolare, il training dell'algoritmo dell'IA su processi o contratti passati è ciò che permette l'individuazione di elementi di interessi e un efficace impiego nelle sopracitate applicazioni giuridiche. Tali algoritmi si applica anche in materia tributaria ove alcuni di essi sono in grado di individuare le frodi fiscali e risalire al soggetto responsabile della frode medesima.

In particolare, un recente progetto sulla giurisdizione tributaria, finanziata dai fondi del Next Generation EU, è il Prodigit che intende utilizzare un software basato sull'IA per l'analisi delle sentenze con conseguente incremento dell'efficacia del processo[38], permettendo anche una valutazione consapevole per il contribuente sulla presentazione di un ricorso destinato o meno ad un probabile accoglimento. Per la valutazione della corrispondenza tra la massima del giudice in una particolare sentenza, e quella prevista dall'IA, il training del software sarebbe affidato a un gruppo composto principalmente

[35] *infra* § 6

[36] PESCE G., *Sul rapporto tra atto del privato inserito sulla piattaforma tecnologica "sicura ed irretrattabile" (blockchain) e atto pubblico. Riflessi sul procedimento e sul processo* in *Judicium*, 2021, 1

[37] JACOBS P. – PATTERN T., *Natural language processing*, in IEEE Expert, 1994, 9, 1, 35

[38] DE LUCIA A., *Intelligenza artificiale e processo tributario: l'algoritmo "studia" un milione di sentenze*, in *Altalex*, 2022

da giudici tributari. Il successo dell'impiego di questo strumento sarà legato ad una armonica interazione tra la componente umana parte del progetto e quella tecnologica, partendo da algoritmi a bassa polarizzazione e degni, dunque, di fiducia per la loro neutralità e facilmente consultabili.

Avendo citato alcuni degli aspetti problematici e delle applicazioni giuridiche dell'IA, ad avviso di chi scrive è necessaria un'attenta considerazione delle problematiche legate all'IA da parte dei soggetti coinvolti negli ambiti giuridici, al fine di proteggere i diritti e principi della legge stessa, così come sostenuto nella guida della European Lawyers Foundation (ELF) su "l'uso di strumenti basati sull'IA dagli avvocati e dagli studi legali nell'Unione Europea". [39]

Chi scrive ritiene che si tratta di applicazioni che, se da un lato proiettano l'attenzione verso scenari futuribili, dominati dall'automazione, dall'altro sollecitano l'attenzione del giurista rispetto ai rischi per i diritti degli individui. Si potrebbe dire infatti che l'impiego di algoritmi "spersonalizzi" la decisione e l'azione le quali, perdendo connotazione umano, diventano mero output del software, come sostenuto con tenacia da una parte della giurisprudenza.[40]

La questione diviene essenziale a causa della rilevanza delle scelte demandate all'IA, che toccano beni fondamentali della persona, quali la riservatezza, la libertà e persino l'integrità fisica. Diviene dunque impellente la ricerca di un bilanciamento tra i vantaggi dell'IA e il rispetto dei diritti dei singoli.

2.1. *(Segue)*: applicazioni in ulteriori ambiti.

Nel paragrafo precedente si sono illustrati alcuni domini di applicazione della IA in ambiti prettamente giuridici. Si andrà ora a esemplificare ulteriori scenari di impiego della IA che, pur non essendo giuridici in sé, comportano potenziali ricadute legali sia in ambito civilistico che penalistico come illustrato in seguito.[41] Gli ambiti di applicazione sono per lo più connessi alla quotidianità, in termini di individuali e collettivi, in cui la IA ha una permeazione sempre più estesa. Le tecniche utilizzate in tali applicazioni sono il machine learning, il *case-based reasoning*[42][43], il deep learning

[39] European Lawyers Foundation, *Guide on use of Artificial Intelligence-based tools by lawyers and law firms in the EU*, 2022
[40] AMISANO M., *Prevedere -e non predire- attraverso gli algoritmi e le loro insidie* in *Archivio penale*, 2022, 2, 3
[41] *infra* § 4
[42] KOLODNER J. L., *An Introduction to Case-Based Reasoning*, in *Artificial Intelligence Review*, 1992, 4
[43] *case-based reasoning* è un metodo che modella i meccanismi di ragionamento, utilizzando esperienze passate per comprendere e risolvere i nuovi problemi che insorgono

e le reti neurali[44], di cui si tratterà in particolare nell'impiego nella ricognizione facciale.[45]

Infatti, un elemento divenuto parte integrante della vita della maggior parte delle persone è lo strumento tecnologico, quale lo smartphone e il computer, in cui la IA opera in relazione ad alcune funzionalità, queste spaziano, ad esempio, dagli assistenti virtuali, presenti ormai anche nelle abitazioni come oggetti a sé stanti, alla traduzione e sottotitolazione automatica e ai motori di ricerca online, i quali mettono a disposizione i risultati più attinenti alla ricerca medesima. [46] Inoltre, l'operatività su dispositivi personali frequentemente utilizzati consente anche un marketing personalizzato, basandosi sulle capacità predittive dell'IA che analizza il comportamento individuale, con pubblicità in rete che si basano su acquisti e ricerche pregressi, anche grazie all'analisi delle abitudini comportamentali in piattaforme quali Facebook e Instagram.

Un ulteriore elemento tecnologico che beneficia dell'utilizzo della IA è il veicolo a guida autonoma che attraverso *"operazioni intelligenti"* evita ostacoli, rivela i segnali stradali e calcola il percorso più efficiente. I veicoli richiedono quindi *«simultanee soluzioni* in termini di percezione, controllo e pianificazione*»*[47] in base anche ai diversi livelli di autonomia, i quali si diversificano in base alla necessità della presenza del guidatore o meno e per il livello desiderato di automazione. Il veicolo, attraverso l'utilizzo di algoritmi autonomi, e quindi del DL, elabora una vasta quantità di dati e compie contemporaneamente multiple e complesse operazioni. Fra queste rientrano la deduzione e anticipazione delle intenzioni e azioni degli altri veicoli, per mezzo della rappresentazione di input quali le regole del traffico e la geometria stradale.[48]

L'utilizzo dell'IA è implementato anche in ambito sanitario ove viene utilizzato nelle TAC[49] al fine di individuare le infezioni, nell'analisi dei dati medici e nella ricerca di modelli che possano ottimizzare le diagnosi oltre che durante la pandemia da COVID-19 per controllare la temperatura corporea nei luoghi pubblici. Nell'ottica di un futuro impiego, accompagnato da una programmazione specifica, l'utilità della IA potrebbe essere estesa anche nella prevenzione al suicidio, grazie all'utilizzo di modelli di

[44] SARKER I., *AI-Based modelling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems*, in SN Computer Science, 2022
[45] *infra* Capitolo II
[46] SARKER I., *AI Watch. European Landscape on the Use of Artificial Intelligence by the Public Sector,* in *JRC science for policy report science policing report*, EU Commission, 2022, 48
[47] PAREKH D. – PODDAR N. – RAJPURKAR A. – CHAHAL M. – KUMAR N. – JOSHI G.P. - CHO W., *A Review on Autonomous Vehicles: Progress, Methods and Challenges*, in *Electronics*, 2022, 11 (14), 2162
[48] KOLEKAR S. – GITE S. – PRADHAN B., *Behavior Prediction of Traffic Actors for Intelligent Vehicle Using Artificial Intelligence Techniques: A Review*, in *IEEE Access*, 2021, 9
[49] PASCERI G. – BIBBOLINO C. – STASI M. – COPPOLA F. et altr., *Intelligenza artificiale e radiologia*, in *Sirm*, 7

riconoscimento e di risoluzione dei problemi per cui le macchine imparerebbero a riconoscere i modelli comportamentali. [50]

In un'ottica futura, le potenzialità espansive dell'IA promettono di migliorare la sicurezza e la velocità dei trasporti, l'efficienza delle fabbriche e di realizzare un sistema alimentare sostenibile. L'opinione di chi scrive è che l'IA porterà certamente vantaggi in molti ambiti che necessitano di una maggiore autonomia in ragione di una maggiore efficienza, come nel caso del settore sanitario o alimentare. Come espresso in precedenza, bisogna considerare, di pari passo all'evoluzione, la salvaguardia dei diritti degli individui, quali ad esempio la privacy[51], questo perché, come spesso accade, l'evoluzione porta con sé benefici ma anche problemi di rilevante impatto e difficile soluzione. Probabilmente, la via migliore per un bilanciamento tra innovazione e protezione consisterà in un dialogo tra i diversi settori coinvolti, cosicché l'avanzamento sia supportato eticamente, socialmente e giuridicamente.

3. La definizione contenuta nella proposta di Regolamento sull'Intelligenza Artificiale.

Data la crescente e impellente necessità di una definizione della IA[52] nel contesto europeo, al fine di affrontare in maniera adeguata i benefici e rischi connessi all'IA, e date le richieste da parte del Parlamento europeo e del Consiglio europeo, mirate a garantire attraverso un intervento legislativo un mercato interno per i sistemi di IA efficacemente operativo, la Commissione Europea ha presentato una proposta di Regolamento.[53]

A testimonianza di queste esigenze, si riporta quanto sostenuto dal Parlamento Europeo in merito al ruolo dell'IA in quanto «centrale per la trasformazione digitale della società ed è diventata una delle priorità dell'UE. Applicazioni future potrebbero portare grandi cambiamenti, ma non dobbiamo dimenticare che l'intelligenza artificiale è già presente nelle nostre vite».[54] In particolare, l'urgenza di una regolamentazione nell'Unione si è manifestata sin dal 2017, ponendosi la già citata necessità di un armonioso impiego della tecnologia nel rispetto della protezione dell'utente in termine di dati, di diritti e di etica. Successivamente il Consiglio Europeo, anche alla luce della continua evoluzione

[50] FONSEKA, *The utility of artificial intelligence in suicide risk prediction and the management of suicidal behaviours*, cit.
[51] *infra* Capitolo II § 3
[52] *supra* § 1
[53] Commissione Europea - proposta di Regolamento del Parlamento Europeo e del Consiglio, "*che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione"*, 206 final, 2021/0106 (COD)
[54] Parlamento Europeo, *Che cos'è l'intelligenza artificiale e come viene usata*, in *Sito web ufficiale del Parlamento Europeo,* 2020

dei risultati raggiunti dall'IA, ha posto l'accento sulla esigenza di identificarne gli ambiti applicativi potenzialmente ad alto rischio.[55]

La Commissione, pertanto, nel 2021 presenta una proposta che ambisce alla definizione di un contesto economico e giuridico sull'IA che da una parte favorisca lo sviluppo europeo della stessa e delle sue applicazioni e dall'altra garantisca il rispetto dei diritti del cittadino con un adeguato livello di protezione. Affidabilità, sicurezza e conformità alla legge e ai valori dell'Unione delle applicazioni dell'IA risultano, secondo la Commissione, requisiti irrinunciabili per la fioritura di un mercato unico delle stesse, per cui, in tale scenario, la proposta ambisce alla creazione di un ambito normativo che favorisca e attragga investimenti nonché il continuo e armonico progresso dell'IA. Una efficace immissione dei sistemi sopracitati nel mercato potrebbe basarsi su un meccanismo di valutazione del rischio rispettoso dell'ambito normativo e si dovrebbe articolare in un periodo della durata di due anni, il cosiddetto "*grace period*", volto alla predisposizione da parte degli operatori dei necessari adempimenti organizzativi tecnici e commerciali per rendere il sistema di IA conforme alle indicazioni contenuti nella proposta.

L'adozione di tale proposta rappresenterebbe una inversione di tendenza in quanto la materia è stata contraddistinta per la maggior parte dalla gestione attraverso strumenti di *soft law*[56] e, solo in materie specifiche, da norme vincolanti, per cui molti autori evidenziano l'assenza di un quadro legislativo coerente e unico fondato su una condivisa visione etica degli standard di sicurezza dei sistemi di IA.[57] Ambendo a promuovere l'adozione, lo sviluppo e la produzione dell'IA, che dovrebbe divenire uno strumento per perseguire il benessere dei cittadini europei e il beneficio dell'intera società, la proposta di Regolamento definisce l'IA come «una famiglia di tecnologie in rapida evoluzione in grado di apportare una vasta gamma di benefici economici e sociali in tutto lo spettro delle attività industriali e sociali».[58]

Al fine di incoraggiare lo sviluppo della IA, la definizione dei sistemi e l'ambito applicativo dell'intera Proposta si incentrano sulle tecniche e gli approcci[59], ed inoltre, per la stessa finalità, devono essere rispettati dei requisiti obbligatori comuni per la progettazione e lo sviluppo di specifici sistemi di IA prima della loro immissione sul mercato.[60]

---

[55] Consiglio Europeo - Riunione speciale del Consiglio europeo, Conclusioni EUCO 13/20, 2020

[56] *soft law sono* norme prive di efficacia diretta, ad esempio in materia di IA le risoluzioni e i piani di azione approvati dalle istituzioni dell'UE; a livello nazionale il Libro Bianco Agid del 2018

[57] MAGRO M. B., "Robot, cyborg e intelligenze artificiali" in CAPODOPPI A. – CANESTRARI S. et al., *Trattato di diritto penale - Cybercrime*, Milano, 2019, 1207

[58] Commissione Europea, 206 final, 2021/0106 (COD), Relazione, (71)

[59] Commissione EU, 2021/0106 (COD), cit., all. I - *Tecniche e approcci di Intelligenza artificiale di cui all'art. 3, p. 1*

[60] Commissione EU, 2021/0106 (COD), cit., Titolo 1, Capo II

Come evidenzia la relazione di accompagnamento alla proposta, la definizione di *sistema di IA*, che lo indica come «un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono» [61], punta alla neutralità tecnologica così che possa essere adattabile alle future evoluzioni anche di mercato. Infatti, per dotare la definizione della necessaria certezza del diritto, l'allegato I elenca nel dettaglio gli approcci e le tecniche per lo sviluppo della IA. Ai fini della comprensione del centro focale della proposta andremo a considerare il contenuto dell'Allegato I che fornisce un dettagliato elenco delle tecniche e degli approcci di IA. Si ritrova in tale Allegato il già menzionato apprendimento automatico con le sue sottocategorie, quali l'apprendimento supervisionato, non supervisionato e per rinforzo,[62] che prevede per la sua realizzazione l'impiego di diversi metodi, tra cui il deep learning. Oltre all'apprendimento automatico vengono anche riportati gli approcci permeati su logica o conoscenza, deduzione, inferenza[63] e ragionamento simbolico[64] e i sistemi esperti[65], infine quelli statistici, la stima bayesiana[66] e i metodi di ricerca e ottimizzazione. Per mantenere un allineamento col progresso tecnologiche dell'IA e del relativo mercato, la Commissione si riserva la capacità di modificare i contenuti di quanto appena esposto in merito alle tecniche e agli approcci.

Data la complessità della materia è comprensibile come la definizione di IA sia stata esposta a discussioni fra gli esperti del settore, evidenziando come alcuni degli approcci indicati nell'allegato I non siano propriamente inquadrabili quali applicazioni di IA e come manchino alcune tecniche nell'elenco fornito e come la CESE sia arrivata a formulare una diversa definizione di IA e a suggerire l'eliminazione *in toto* dell'allegato I. [67]

Le opinioni che sono state espresse dai giuristi, d'altro canto, in seguito alla presentazione della proposta, evidenziano con positività tale iniziativa, non mancando però di mettere in luce alcune problematicità. Se da un lato la proposta ha il merito di aver fornito una definizione di IA per alcuni autori[68] evidenziano come il focalizzarsi su un approccio che proceda ad elenchi e sui sistemi di IA, data la già evidenziata difficoltà di una definizione condivisibile in modo unico, abbia portato a imprecise

[61] Commissione Europea, 206 final, cit., art. 3
[62] *supra* § 1
[63] inferenza è un ragionamento logico per cui date certe premesse e regole consegue una conclusione che risulta logicamente necessaria
[64] ragionamento simbolico sono le opinioni umane sfruttate matematicamente
[65] sistema esperto è un programma che riproduce la prestazione degli esperti in un determinato campo
[66] ALETTI B., minimizza il valore atteso a posteriori di una funzione di perdita o, equivalentemente, se massimizza il valore atteso a posteriori di una funzione di guadagno, in *Enciclopedia Treccani della Scienza e della Tecnica,* 2008
[67] MULLER C. (relatrice), *Parere del Comitato economico e sociale europeo (CESE) sulla proposta di Regolamento*, 2021, C 517/62
[68] interventi apparsi sulla stampa specializzata, si vedano Chiusi (2021) e Clarke (2021)

definizioni in merito alle caratteristiche dei sistemi di IA, mentre sarebbe stato auspicabile che abbracciasse ogni sistema che possa significativamente impattare le attività umane. Le critiche alla proposta di Regolamento tengono in debito conto la difficoltà sopracitata in un ambito così ampio e differenziato come quello in cui il Regolamento andrebbe ad operare e alla labilità dei confini nella definizione di un sistema di IA e quindi delle relative implicazioni a livello legislativo. [69]

Muovendo l'analisi verso l'ambito penale autori come, ad esempio, Lavorgna e Suffia evidenziano una serie di questione che rimangono ancora sull'impiego dell'IA in tale ambito, considerando la presenza di eccezioni quali le pratiche biometriche e le tecnologie di sorveglianza di massa[70]. Partendo dalla considerazione dell'incidenza dell'ambito penale sui diritti fondamentali degli individui occorrerebbe, dunque, che l'imputazione di responsabilità venisse a determinarsi nel rispetto delle garanzie costituzionali al fine di evitare, come sostengono alcuni autori[71], che si "flessibilizzino" le categorie di reato esistenti, questo perché la proposta anche se non ha una diretta efficacia nel penale definisce quelle che possono essere considerate «aree di "rischio consentito[72]" secondo una logica di precauzione "moderata"».[73]

Proseguendo su questa linea di pensiero ci si preoccupa in merito alla punibilità di un fatto di evitarne una eccessiva anticipazione o la coincidenza con la verificazione dell'evento lesivo, al fine di tutelare l'effettività delle sanzioni. Tali rischi potrebbero essere affrontati considerando l'idoneità dei modelli di responsabilità già esistenti e dunque non limitando la produzione dei sistemi di IA, che potrebbe bloccarne lo slancio innovativo, a meno che il pericolo non superi il beneficio che ci si aspetta, ma tutelare con sanzioni adeguate e che tutelino gli interessi coinvolti una accurata delimitazione delle aree di "rischio consentito".[74] Il problema insorge in quanto nella proposta non viene previsto un obbligo di criminalizzazione, lasciando quindi agli Stati Membri la previsione delle sanzioni adeguate, che potrebbero anche essere amministrative, per potere rispettare gli obblighi derivanti dall'eventuale adozione del Regolamento.

L'opinione di chi scrive è che la presentazione di questa proposta di Regolamento sia un passo positivo nella direzione di un corretto inquadramento giuridico della IA e che le critiche mosse al Regolamento vadano attentamente considerate. Da una parte quelle

---

[69] LAVORGNA A. – SUFFIA G., *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale*, in *Diritto Penale Contemporaneo*, 2021, 94

[70] *infra* Capitolo II § 1

[71] rilevate, a proposito del principio di precauzione, riguardo allo stravolgimento del paradigma colposo da PIERGALLINI C., *Il paradigma della colpa nell'età del rischio: prove di resistenza del tipo*, in *Rivista italiana di diritto e procedura penale*, 2005, 1684

[72] *infra* § 6

[73] MINELLI C., *La responsabilità "penale" tra persona fisica e corporation alla luce della Proposta di Regolamento sull'Intelligenza Artificiale*, in *Diritto Penale Contemporaneo*, 2022, 52

[74] PIVA D., *Machina discere, (deinde) delinquere et puniri potest*, in GIORDANO R. (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Milano, 2022, 683

degli scienziati di IA appaiono fondate, data la conoscenza che essi possiedono in materia, ma al contempo l'approdo a un approccio eliminatorio di una parte della proposta, quale l'allegato I, sia forse estremo.[75] In tal senso anche le criticità mosse dai giuristi in merito alla poca chiarezza della definizione e la presenza di lacune all'interno del Regolamento, che determinerebbero problemi applicativi, oltre al vuoto normativo[76], che precederebbe la conversione della proposta di Regolamento in provvedimento legislativo, evidenziano la necessità di una revisione, in particolar modo per le evidenziate conseguenze a livello sanzionatorio. Proprio in ragione del fatto che questa è la prima definizione riscontrabile a livello europeo, sarebbe auspicabile quindi un ulteriore dialogo e collaborazione tra le parti, al fine di definire ulteriormente i contorni sistemici dell'IA, senza dimenticare che la interdisciplinarità della materia difficilmente consentirà di raggiungere una definizione "perfettamente" condivisa.

3.1. *(Segue):* pratiche di IA vietati e sistemi ad alto rischio.

Dopo aver analizzato la definizione di sistema di IA e le problematicità che questa solleva, ci si focalizza, al fine di comprendere l'approccio basato sul rischio che permea la proposta, sulle pratiche della IA che sono considerate pericolose nel loro impiego e diffusione e che pertanto si ritiene necessario vietare, distinguendo il rischio in inaccettabile, alto, limitato e minimo.[77] Tali pratiche comportano rischi a loro, anche solo potenzialmente, collegati che si ritengono *inaccettabili* in quanto in contrasto con i valori dell'Unione. Fra queste rientrano, ad esempio, le pratiche che sfruttano le vulnerabilità psicofisiche, sociali ed economiche di uno specifico gruppo di individui o che sono potenzialmente in grado di manipolare le persone in modo inconsapevole, con lo scopo di condurre a distorsioni comportamentali che plausibilmente cagionerebbero danni, psicologici o fisici, a tali o ad altri soggetti.[78] Un ulteriore categoria di pratiche vietate rilevanti a livello penale sono quelle impiegate nei sistemi che utilizzando l'identificazione biometrica[79] remota "*in tempo reale*" vengono adottate per una sorveglianza indiscriminata in spazi ai fini di attività di contrasto, la cui utilità in caso di operazioni in situazioni di iper-affollamento è chiara così come o potenziali abusi di un utilizzo sommario.[80]

---

[75] MULLER (relatrice), *Parere del CESE sulla proposta di Regolamento*, cit., C 517/62
[76] LAVORGNA – SUFFIA, *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale*, cit., 97
[77] LIVELLI F.M.R., *La Ue sceglie un approccio basato sul rischio per regolare l'intelligenza artificiale*, in *Network digital 360 – Risk-managment*, 2021
[78] LAVORGNA – SUFFIA, *La nuova proposta europea per regolamentare i Sistemi di* Intelligenza, cit., 92
[79] *infra* Capitolo II § 1
[80] LAVORGNA – SUFFIA, *La nuova proposta europea per regolamentare i Sistemi di* Intelligenza, cit., 93

Vengono però previste delle eccezioni a tali divieti quando tali sistemi siano necessari al fine di localizzare o identificare un potenziale o effettivo autore di un reato particolarmente grave o nella prevenzione di una specifica minaccia terroristica o concernente l'incolumità di persone fisiche o nel caso della ricerca di minori scomparsi oppure potenziali vittime. In questi ambiti l'IA porterebbe un significativo ausilio nel contrastare la criminalità con più semplicità ma, come evidenziato, al fine di garantire una maggiore tutela dei diritti soggettivi e trattandosi di identificazioni, quindi di *riconoscimento facciale*[81], in spazi accessibili al pubblico, è richiesta, con adeguata motivazione, una autorizzazione preventiva dell'autorità amministrativa o giudiziaria dello Stato membro a cui si riferisce l'attività di identificazione, a meno di una situazione di giustificata urgenza.

Come esposto in precedenza, l'utilizzo dell'IA viene considerato con una metodica "*risk based*" per giungere ad una classificazione dei sistemi sulla base del rischio ad essi connesso, che esamina il rischio sulla base delle sue caratteristiche e del contesto a cui si riferisce, al fine di prevenire eventuali danni e, al contempo, di favorire scenari migliorativi in un ambito prospettico.

Seguendo tale metodica il Regolamento identica il livello di rischio che l'utilizzo di un sistema di IA comporta, tale livello può essere inaccettabile, come già discusso, basso oppure alto. In quest'ultimo caso si definisce la categoria "*ad alto rischio*" che la proposta di Regolamento accompagna con delle regole in merito al suo ciclo di vita e utilizzo. La regolamentazione di tali sistemi risulta fondamentale in quanto comportano rischi per i diritti fondamentali degli individui e per la loro sicurezza e salute[82], per cui sono definiti degli obblighi necessari per la loro affidabilità oltre che procedure di verifica della conformità precedenti la loro immissione sul mercato. Si definisce sistema ad alto rischio se soddisfa congiuntamente le condizioni individuate dalla proposta, ossia l'impiego del sistema di IA come componente di sicurezza di un prodotto o quale prodotto a sé stante[83] e la conformità a una valutazione compiuta da terze parti, preventivamente alla messa in opera o all'immissione sul mercato, del prodotto di cui il sistema di IA è componente di sicurezza oppure del sistema considerato come prodotto in sé. La prima condizione rimanda all'elenco della normativa di armonizzazione europea, quali le direttive e i regolamenti, fra cui rientrano, ad esempio, quelli riguardanti i dispositivi medico-diagnostici in vitro (quali i kit di apparecchiature reagenti), l'omologazione dei veicoli a motore e l'interoperabilità del sistema ferroviario dell'Unione.[84]

---

[81] *riconoscimento facciale* è un metodo automatizzato basato sull'IA che identifica o conferma l'identità di una persona, per approfondimenti *infra* Capitolo II § 1

[82] Commissione Europea, 206 final, 2021/0106 (COD), Relazione, cit., 4

[83] Commissione Europea, 206 final, 2021/0106 (COD), cit., art. 6 che rimanda all'all. II per la normativa di armonizzazione del prodotto

[84] Commissione Europea, 206 final, 2021/0106 (COD), cit., all. II

I sistemi così classificati non sono esaustivi dell'intera categoria ad alto rischio che viene ulteriormente dettagliata nell'allegato III che elenca i settori in cui operano i sistemi di IA ad alto rischio i quali spaziano dalla identificazione biometrica, le infrastrutture critiche, l'istruzione e la formazione professionale, l'ambito lavorativo, l'accesso a servizi pubblici e privati, le attività di contrasto, la gestione della migrazione fino alla amministrazione della giustizia. In particolare, in quest'ultimo settore, i sistemi di IA possono fornire un valido supporto nell'espletamento delle attività precipue dell'attività giudiziaria, quali ricerca e interpretazione di fatti e diritto applicabile allo specifico contesto, come già evidenziato in precedenza. Tale elenco è suscettibile di revisione ed aggiornamento, in funzione dello sviluppo e dell'introduzione di nuovi sistemi di IA potenzialmente rischiosi rispetto alle soglie delle linee guida già delineate.

Come per la definizione di IA, anche la classificazione in base al rischio dei sistemi di IA è oggetto di discussione e, ad esempio, alcuni autori sostengono che l'approccio ad elenco utilizzato nel Regolamento potrebbe condurre a legittimare e normalizzare alcune pratiche di IA i cui benefici essi considerano assenti o criticabili.[85] Inoltre, il Regolamento sembrerebbe non trovare applicazione proprio quando il rischio si definisce *minimo*[86], caso in cui incorrono la maggior parte dei sistemi di IA, o *limitato*[87], il che sollecita l'adozione volontaria di codici di condotta in quanto sarebbe assente una regolamentazione[88], mentre, per quanto concerne i rischi alti, i requisiti richiesti non comportano una necessaria diminuzione del rischio di pregiudizio ad essi connessi.[89] Alla luce di queste considerazioni si accompagna quella che considera tale proposta come un buon punto di partenza, come già evidenziato[90], e che il definire requisiti, limiti e l'attribuzione di una responsabilità ai sistemi di IA sia uno slancio verso un futuro espansivo e sostenibile della tecnologia[91], il quale necessita però di una legislazione che colmi il vuoto temporale già citato.[92]

Le opinioni di chi scrive, già espresse in precedenza, rimangono vere anche a proposito di quanto appena trattato in ragione di una visione sistemica del Regolamento, infatti, come sostenuto da una parte della giurisprudenza[93], un confronto multidisciplinare tra

[85] MULLER (relatrice), *Parere del CESE sulla proposta di Regolamento,* cit., C 517/65
[86] *minimo* è il rischio molto ridotto o nullo di lesione di diritti o sicurezza dell'individuo, quali i filtri spam e i videogiochi
[87] *limitato* è il rischio che necessita di precisi obblighi di trasparenza e chiarezza nei confronti dell'utilizzatore, quali le chatbot
[88] MINELLI., *La responsabilità "penale" tra persona fisica e* corporation, cit., 53
[89] MULLER (relatrice), *Parere del CESE sulla proposta di Regolamento,* cit., C 517/62
[90] *supra § 3*
[91] LAVORGNA – SUFFIA, *La nuova proposta europea per regolamentare i Sistemi di* Intelligenza, cit., 98
[92] *supra § 3*
[93] SEVERINO P., *Intelligenza artificiale e diritto penale*, in RUFFOLO (a cura di) *Intelligenza artificiale e responsabilità*, 2017, 531

giuristi evidenzia la disponibilità a un maggiore collaborazione con l'ambito tecnico-scientifico del settore di IA e a una effettiva implementazione di quanto teorizzato.

3.2. *(Segue):* esemplificazioni e sistema di gestione dei sistemi di IA ad alto rischio.

A valle della trattazione delle classi di rischio dei sistemi di IA e in particolare di quelle ad alto rischio, risulta utile un *excursus* che ne descriva alcune esemplificazioni.

In collegamento con quanto detto in tema del settore dell'attività di contrasto in cui i sistemi di IA ad alto rischio possono essere utilmente impiegati, si ricomprendono ambiti quali l'individuazione del rischio di un reato, della sua recidiva e del rischio per le potenziali vittime. Accanto a tale impiego un esempio, con impatto nel *profiling* di un soggetto, è la possibilità di rilevazione dello stato emotivo dell'individuo ed altri esempi rilevanti sono gli elementi di prova la cui affidabilità o meno è oggetto di valutazione durante le indagini o il processo e le ricerche multi-sorgente nell'analisi criminale, atta a identificare modelli o correlazioni di non immediato riscontro tra i dati. Un'ulteriore applicazione rilevante del sistema concerne l'individuazione di informazioni prevalentemente audio-visive che vengono ritenute falsamente vere dagli utenti, il cosiddetto "*deep fake*"[94], per cui tali sistemi devono esplicitare che il contenuto è il risultato di una creazione o rielaborazione artificiale.

È importante sottolineare che l'efficacia della classificazione dei sistemi ad alto rischio è intrinsecamente collegata all'evoluzione sia della tecnologia che degli ambiti applicativi della IA[95] e l'elenco, pertanto, è suscettibile di integrazioni e aggiornamenti nell'eventualità di innovazioni dei sistemi di IA che impattino sui settori d'interesse e quindi sul potenziale rischio ad essi collegato. Detti aggiornamenti garantiscono il mantenimento di un adeguato e necessario livello di attualizzazione dell'allegato e del Regolamento che lo ricomprende.[96] Quando si individua un nuovo sistema di IA, lo si sottoporrebbe a una verifica per decidere se possa essere qualificato ad alto rischio, attraverso l'applicazione dei criteri valutativi individuati dalla proposta di Regolamento[97]. In particolare, sono oggetto di valutazione per la classificazione lo specifico ambito applicativo del sistema di IA, la sua modalità d'impiego anche potenziale e le conseguenze di questo, nonché l'intensità e l'impatto su più individui, anche in relazione alla loro vulnerabilità. Viene, infine, valutata l'impossibilità di

[94] Commissione Europea, 206 final, 2021/0106 (COD), cit., art. 52, *Obblighi di trasparenza per determinati sistemi di IA*, 3

[95] ai sensi dell'art. 7 "Modifiche dell'allegato III", il potere di adozione di atti delegati è conferito alla Commissione. Le condizioni secondo cui possono aggiungersi all'elenco dell'allegato III sistemi di IA è l'appartenenza ai settori elencati e la presenza di un «danno per la salute e la sicurezza, o un rischio di impatto negativo sui diritti fondamentali», il quale sia equivalente o superiore al rischio dei sistemi già citati nell'allegato.

[96] MILANO L., *Il Regolamento europeo sull'intelligenza artificiale*, in *Altalex*, 2022

[97] Commissione Europea, 206 final, 2021/0106 (COD), cit., all. III, art. 7, 2

sottrarsi al risultato prodotto dal sistema, potenzialmente causa di un danno con entità da quantificare e il livello di reversibilità degli stessi effetti dannosi, oltre alla estensione in cui la normativa europea vigente contempli misure di efficace ed efficiente prevenzione o riduzione di tali rischi.

In merito ai sistemi ad alto rischio di cui all'allegato III viene previsto un sistema di conformità e applicazione[98] che regola definizione, organizzazione e documentazione del sistema attraverso un "*sistema di gestione del rischio*"[99], il quale, a sua volta, impiega un "*processo iterativo continuo*" che accompagna la nascita, lo sviluppo e la fine dell'attività di un sistema di IA ad alto rischio e richiede, per essere efficace, un aggiornamento continuo nel tempo e a carattere sistematico. L'amministrazione del sistema di gestione del rischio è realizzabile grazie a detto aggiornamento della tipologia di rischi, che ricomprenda sia quelli potenziali, derivanti da un uso proprio o meno a seconda dell'allineamento o meno con le finalità del sistema, che quelli presumibili e conosciuti. A tali rischi vanno altresì aggiunti quelli nascenti in seguito all'immissione sul mercato del sistema oppure che si palesino nonostante la corretta applicazione delle misure di gestione previste, le quali devono rispondere ad una serie di requisiti. Concorrono al rispetto di tali requisiti una corretta costruzione o progettazione del sistema in grado di alleviare o rimuovere i rischi oppure la definizione di interventi che indeboliscano e controllino quelli ineliminabili, garantendo agli utenti un'adeguata informativa in merito alla preventiva valutazione dei potenziali rischi per l'uso conforme o meno del sistema.

Il sistema di gestione dei rischi è suddiviso in quattro fasi. Nella prima si identificano e analizzano quei rischi intrinsecamente collegabili col sistema di IA e quelli prevedibili. La seconda fase è, invece, volta a stimare e valutare quei rischi che possono insorgere nel momento in cui il sistema di IA ad alto rischio venga impiegato sia in modo conforme al fine per cui è stato progettato sia con uso improprio in linea con una ragionevole previsione. Nella terza fase si valutano ulteriori rischi eventuali che sono il frutto di analisi dei dati raccolti dal sistema di monitoraggio successivamente all'immissione sul mercato. La quarta ed ultima fase mira all'adozione di misure idonee alla gestione dei rischi, tenendo in debita considerazione gli effetti e le possibili interazioni con quanto sancito per i requisiti. Sono considerati accettabili quei rischi residui dello specifico pericolo, comunicati all'utente, o complessivi dell'intero sistema ad alto rischio ove il sistema venga utilizzato in maniera conforme alla propria finalità oppure venga utilizzato in modo improprio ragionevolmente prevedibile.

È necessario garantire per una gestione consona del rischio, una serie di misure quali la soppressione o il contenimento del rischio medesimo con un adeguato sviluppo progettuale e realizzazione, per quanto possibile. Inoltre, è richiesta una adeguata

[98] Commissione Europea, 206 final, 2021/0106 (COD), Relazione, cit., 15
[99] Commissione Europea, 206 final, 2021/0106 (COD), cit., Titolo III, *Sistemi di IA ad alto rischio*, Capo 2, *Requisiti per i sistemi di AI ad alto rischio*, art. 9

attenzione al bagaglio tecnico, esperienziale, di istruzione e formazione riscontrabile dall'utente del sistema e dal contesto in cui lo stesso sistema si troverà ad operare. In particolare, per la tipologia di rischi non eludibili, è importante introdurre misure idonee per ridurre e controllare tali rischi. Il contenimento passa anche attraverso una adeguata campagna informativa i cui contenuti vertano sia sui rischi allineati con le finalità del sistema sia sull'impiego non idoneo del sistema stesso, e, se opportuno, attraverso una formazione specifica dell'utente del sistema medesimo.

Per individuare le opportune misure di gestione del rischio i sistemi di IA ad alto rischio vengono testati e attraverso tali prove si intende assicurare un funzionamento allineato con gli scopi previsti nonché la conformità ai rischi[100]. Il processo attraverso cui vengono testati i sistemi deve essere quello strettamente necessario al conseguimento delle finalità del sistema stesso e le prove effettuate possono avere luogo in qualsivoglia fase dello sviluppo, ma necessariamente a monte della immissione sul mercato o messa in servizio del sistema finale. A seguire, l'articolo 9 introduce una deroga all'articolo 9 Reg. UE 2016/679 GDPR[101], attraverso l'autorizzazione ai fornitori di sistemi di IA al trattamento di dati idonei a identificare informazioni sensibili dell'utente, quali dati genetici e biometrici, razza ed etnia, stato di salute, orientamento politico, religioso, filosofico e sessuale).[102] Il presupposto all'applicazione di tale deroga attiene alla necessità di garantire il corretto funzionamento dei sistemi di IA ad alto rischio attraverso un idoneo monitoraggio, rilevamento ed emendamento di eventuali alterazioni relative al sistema stesso, garantendo le libertà fondamentali e i diritti delle persone fisiche, tra cui il diritto alla riservatezza e sicurezza della privacy.

Il contenuto proposta contiene delle aperture alla futura evoluzione non solo della tecnologia IA ma anche dei sistemi che la utilizzano, in quella che si ritiene essere un elemento positivo in quanto la rende aggiornabile e attualizzabile nel tempo. Naturalmente questo dinamismo dovrebbe altresì ritrovarsi «l'idoneità delle evoluzioni interpretative a dare mediazione giuridica compiuta a fenomeni "nuovi"».[103], in una dialettica che chi scrive ritiene necessaria.

4. Problematiche.

Come evidenziato nei paragrafi precedenti, per quanto l'IA e la tecnologia in generale, siano il motore del progresso, la relativa regolamentazione da una parte rallenta il processo evolutivo, secondo un'ottica tecnica, e dall'altra è necessaria ed essenziale per la tutela dei cittadini, in particolare considerando come l'industria possa avere un

[100] Commissione Europea, 206 final, 2021/0106 (COD), cit., capo II
[101] Regolamento (UE) 2016/679, *General Data Protection Regulation* (GDPR), art. 9, *Trattamento di categorie particolari di dati personali*, *infra* § 4
[102] LIVIO M., *Il Regolamento europeo sulla intelligenza* artificiale, in *Altalex*, 2022
[103] SEVERINO, *Intelligenza artificiale e diritto penale*, cit., 531

metodo non sempre prudente nell'implementazione della tecnologia e quindi, mostrandosi a volte poco incline all'autoregolazione, sarà la regolamentazione pubblica a doversi adoperare per risolvere la dicotomia evidenziata.[104]

I già evidenziati rischi intrinsechi alla tecnologia IA e, in particolare, quelli relativi al pericolo di discriminazione, alla imprevedibilità dell'esito dell'algoritmo verranno di seguito coniugati anche guardando a come essi si riflettano sulla pubblica amministrazione in una società permeata sempre più dalla IA. L'equilibrio di un sistema di IA è incentrato su quello del suo algoritmo e sulla base dati che esso impiega per il suo addestramento e funzionamento[105], così che risulta centrale affrontare il bias o polarizzazione del sistema.

Il *bias*[106] si annida nella modalità con cui si rende operativa l'IA attraverso il training e nella potenziale mancanza di oggettività degli stessi tecnici che codificano gli algoritmi per i quali si presenta, inoltre, l'impossibilità di configurarli qualora si posseggano dati imprecisi e di bassa qualità oppure anch'essi polarizzati. Infatti, un eventuale pregiudizio, consapevole o meno, della componente umana ribalta una polarizzazione sui dati su cui si basano gli algoritmi e sull'applicazione che a sua volta si basa sull'algoritmo. La polarizzazione può, ad esempio, riguardare questioni legate alla etnia oppure alla condizione sociale e, più in generale, qualsiasi elemento in grado di generare una discriminazione[107]. Causa di bias può essere, inoltre, la semplice stima, in eccesso o in difetto, dei fattori che concorrono alla relazione di causa ed effetto in un qualunque fenomeno, situazione o ambito e anche quando tale stima risulti necessaria per analizzare specifiche situazioni ed eventi, ex-post o preventivamente, per cui il bias inciderebbe negativamente sull'efficacia dell'intera analisi.

In merito ai dati, per risolvere il problema della imprecisione e scarsa qualità si potrebbe ricorrere all'ausilio di esperti e alla collaborazione di chi possiede fonti di dati diversificate e accurate, così come per le criticità legate alla conservazione dei dati e alla loro protezione sarebbe risolutiva una fonte affidabile di dati che siano disciplinate, accessibili e sicure. Per utilizzare un database proporzionato alle elevate quantità di dati necessarie alla costruzione di un sistema di IA efficiente ed efficace, risulta problematico raggiungere la potenza di calcolo necessaria. È opportuno evidenziare che quanti più dati vengono generati per raggiungere database di elevato volume e accuratezza, tanti più utenti potrebbero averne accesso. Questo aspetto potrebbe far scaturire un aspetto critico dal momento a che anche coloro che agiscono con finalità

[104] MAURO G., *L'intelligenza artificiale sta per essere regolamentata*, in *Econopoly*, 2021
[105] *supra* § 2
[106] ROBERTS et al., *General Perspectives Toward the Impact of AI on Race and Society* cit., 347-363
[107] approfondimento *infra* § 6.1

illecite tramite il dark web[108] potrebbero accedere a tali dati. Da quanto detto risulta evidente l'importanza della qualità dei dati anche nell'ottica della loro *neutralità*, quindi assenza di bias, che si trasferisce attraverso l'algoritmo all'operato dell'intero sistema di IA, per la quale il dato deve essere *super partes* scaturendo da una selezione e preparazione che contempla, in misura più o meno elevata, il coinvolgimento umano.[109] a seconda che l'algoritmo si basi su apprendimento con o senza supervisione. Quanto osservato necessita di un chiarimento in merito all'auspicata neutralità dei dati in quanto seppur originariamente, non viziati da bias, il risultato potrebbe lo stesso essere discriminatorio e questo dimostra anche la imprevedibilità dell'algoritmo, già insita nel ML, che fa sì che neanche lo sviluppatore riesca sempre a spiegare perché venga prodotto un determinato output. La polarizzazione, dunque, può generare una discriminazione *indiretta*[110], per cui solo al momento di una lamentata discriminazione ci si renderà conto del vizio *ab origine* ed essa può sorgere quando non vengano prese in debita considerazione tutti gli elementi esistenti che concorrono alla situazione di uno specifico soggetto, la quale si distingua da altre simili.

Considerando la imprevedibilità, anche marginale, nel funzionamento di un sistema di IA comprendere i meccanismi algoritmici potrebbe essere di ausilio nella individuazione e auspicabile rimozione degli effetti negativi da essa generati. Affinché ciò avvenga è necessario che l'algoritmo presenti la caratteristica della già citata *trasparenza*[111], quindi dell'assenza di opacità, che rende conoscibili i meccanismi non solo per l'operatore tecnico ma anche per l'utente, che necessita di tale caratteristica per potersi fidare e affidare all'IA. Comprendere e conoscere i meccanismi significa, in pratica, poter ricostruire il percorso logico che lega l'output all'input che lo ha generato ed in tal senso è utile la distinzione fra diverse forme in cui l'opacità può manifestarsi o essere generata. [112]

Come abbiamo evidenziato, gli algoritmi di ML possono già essere viziati intrinsecamente dall'opacità in quanto il loro training e. successiva evoluzione, potrebbe produrre risultati basati su passaggi non pienamente comprensibili, anche se fosse disponibile la versione originale del software[113], giungendo dunque alla cosiddetta opacità *intrinseca*. Inoltre, l'opacità potrebbe essere il risultato intenzionale a protezione del segreto industriale sul codice sorgente e/o sull'algoritmo, nell'ottica

[108] *dark web*: «una parte nascosta del World Wide Web è conosciuta come il Dark Web, con siti web che non possono essere indicizzati dai motori di ricerca tradizionali». Samuel Onyango S. – Steenvoorden E., *Assessing the Health of the Dark Web* in *Elsevier*, 2021
[109] a seconda che l'algoritmo sia stato addestrato con o senza supervisione di un operatore umano *supra* § 1
[110] Corte EDU, sez. I, sent. 24 maggio 2016, *Biao c. Danimarca*, ric. n. 38590/10, 103
[111] *supra* § 2
[112] BURRELL J., *How the machine "thinks": Understanding opacity in machine learning algorithms* in *Big Data & Society*, 2016, 3, 3
[113] cosiddetto "*codice di sorgente*" è la versione originale del software in forma testuale originariamente digitata nella macchina

concorrenziale di compagnie private[114], spesso definita come "*corporate secrecy*". La opacità ha anche una forma collegata alla *alfabetizzazione*[115] tecnologica dei soggetti coinvolti dall'algoritmo, per cui potrebbe essere non comprensibile o di attendibilità non verificabile se non da tecnici del settore o dal progettista del codice sorgente.
In tal senso è utile considerare come la bassa o scarsa conoscenza tecnologica dei cittadini medi e, quindi, la difficoltà di comprensione ed accettazione delle decisioni prese dall'IA sia riconducibile alla percezione della mancanza di trasparenza e la conseguente mancanza di fiducia nella tecnologia e nell'IA. Questo perché la trasparenza dell'algoritmo sarebbe anche foriera di una protezione da illeciti, e dalle possibili conseguenti ingiustizie e discriminazioni. Data la necessità di trasparenza del cittadino in merito alla IA, è evidente che questa sia richiesta anche da chi utilizzi la stessa tecnologia al fine di fornire servizi e prendere decisioni che lo coinvolgono ed in tal senso è inquadrabile la pubblica amministrazione (PA) che si rivolge alla intelligenza artificiale per migliorare efficacia ed efficienza dei suoi servizi al cittadino. La trasparenza, quindi, consentirebbe non solo equità ma anche uno scambio informativo bidirezionale, condizione necessaria per la comprensione da parte dei cittadini delle decisioni della PA.

Il binomio pubblica amministrazione e cittadino, assieme a quello pubblica amministrazione e IA, hanno in sé enormi potenzialità ai fini di una continua integrazione della tecnologia di IA nella società, ma devono tenersi presenti alcuni interventi necessari per tale percorso. Sarebbe necessario, infatti, integrare i sistemi di IA di ultima generazione con quelli già esistenti e sostituire le infrastrutture obsolete accompagnandolo a un adeguato aggiornamento dei soggetti in esse operativamente coinvolti. In questo senso, un aspetto che necessita di soluzioni piuttosto rapide è la creazione di percorsi formativi adeguati alla vastità di impiego che l'IA promette di avere, al fine di poter disporre di un sufficiente numero di specialisti con adeguata esperienza e competenza per far fronte alle sfide intrinseche nella IA.[116] Infatti, una progettazione idonea dell'IA potrà non solo migliorare la qualità della vita del cittadino ma anche il rapporto tra lo stesso e la PA.

In tal senso, la IA consentirà una migliore e più efficace utilizzazione dei servizi pubblici da parte del cittadino garantendo, al contempo, una razionalizzazione dei costi e dei tempi. Questo risultato potrà sortire un duplice vantaggio consistente, per lo Stato e per le istituzioni, una ulteriore ottimizzazione e maggiore efficacia dei procedimenti organizzativi e, per il cittadino utente dei servizi della PA, un miglioramento nella relazione e nella vicinanza allo Stato grazie anche alla sua agilità, capacità di personalizzazione dei servizi e migliorata trasparenza. [117] Il raggiungimento di questi

[114] vedasi casi COIN, supra § 2, COMPAS *infra* § 6.1
[115] *Enciclopedia Treccani*, voce *alfabetizzazione digitale:* «Abilità di individuare, comprendere, utilizzare e creare informazioni utilizzando tecnologie informatiche»
[116] POSPIELOV S., *Top 10 AI Development and Implementation Challenges*, in *Spiceworks*, 2022
[117] AgID, *Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino*, 2018, 8

obiettivi potrà avvenire anche tramite un armonico contributo di specialisti delle tecnologie, di amministrazione e dell'estetica e della comunicazione volta anche a rendere chiaro e fruibile il nuovo contenuto dei servizi basati sull'IA. Un opportuno impiego delle tecnologie di IA avrà anche l'importante merito di incrementare l'intensità e l'efficacia dell'interoperabilità semantica tra le varie amministrazione con ulteriore ricaduta benefica sull'utente finale, cioè il cittadino. Le tecnologie di IA potranno contare su un vastissimo archivio di dati raccolti nel corso del tempo ma si pone il problema della destrutturazione di alcuni dati provenienti da archivi diversi e non colloquianti. Inoltre, il patrimonio di parte di questo sapere non è reperibile in forma scritta all'interno dell'organizzazione ma è racchiuso in coloro che ne hanno memoria.

Un ulteriore ambito in cui l'IA con le evidenziate problematiche, crea questioni da risolvere, è quella della giustizia penale e l'utilizzo della IA nei processi decisionali, che consente l'accesso a informazioni prima di difficile reperimento e una potenziale riduzione dei tempi della giustizia. Vantaggi ma anche dubbi in merito agli strumenti di IA, riguardano il loro impiego nel predictive policing[118], nella profilazione dell'individuo e nella fase di giudizio, in ove si concentrano molti dei dubbi concernenti i bias, la discriminazione e la imprevedibilità, di cui precedentemente trattato.

4.1. *(Segue):* aspetti etici e di privacy.

Un ulteriore aspetto da considerare è quello legato all'impiego della IA e dei suoi algoritmi che investe l'ambito etico e costituisce una vera sfida per raggiungere la piena fiducia e fruibilità della tecnologia IA in una moltitudine di settori e applicazioni. In tal senso la sfida consiste nell'armonizzare due atteggiamenti opposti, in una dicotomia che ricorda quella dello scrittore Umberto Eco [119], da un lato la posizione dei sostenitori dell'innovazione[120] che, fidandosi dello sviluppo tecnologico, sono disponibili a fruirne ed a integrarsi con esso convinti della importanza e ineludibilità del progresso nonché della neutralità della tecnologia e che sia il modo in cui essa viene impiegata a decretarne il beneficio o l'eventuale danno per l'umanità[121]. In senso opposto si pongono i diffidenti nei confronti della innovazione e delle tecnologie, che temono scenari di grave nocumento per il genere umano a causa dell'impiego della tecnologia.[122] Nell'atteggiamento di critica verso una società ritenuta decadente ovvero in quello di fiduciosi consumatori dei media si ravvisa la medesima dicotomia che

[118] *supra* § 2
[119] AgID*, L'Intelligenza artificiale al servizio del cittadino*, cit., 38
[120] cosiddetti "integrati" favorevoli o almeno ben disposti, nei confronti dei media e della società di massa per ECO U.
[121] i cosiddetti "apocalittici" per ECO
[122] ECO U., *Apocalittici e integrati. Comunicazioni di massa e teorie della cultura di massa,* Milano, 1964

l'innovazione tecnologica e, più specificamente, la IA produce sin dai suoi albori nella platea sociale dei potenziali utilizzatori.

La sfida etica[123] che ogni tecnologia, in generale, ma certamente in modo chiaro, forte e diretto la IA, attraverso i suoi algoritmi, è quella di armonizzare con equilibrio, equidistanza e razionalità la posizione di cittadini fiduciosi con quella dei diffidenti. Si tratta, dunque, di coniugare una visione sui positivi effetti che l'innovazione, e in particolare la IA, può arrecare alla società con la prudenza, il rispetto e la protezione di valori oggettivi e fondamentali.[124] Dal momento che gli algoritmi di IA possono trovare ampia applicazione in ambiti delicati, come quello sanitario e giudiziario, la questione etica è di grande rilevanza e deve essere affrontata in modo sistemico, anche in relazione ad aspetti di governance, per non limitare l'impiego della IA e dei suoi algoritmi e necessita di idonee professionalità e risorse per raggiungere l'efficacia desiderata, considerando la natura sensibile dei dati gestiti e sarebbe inoltre auspicabile che lo sviluppo predominante avvenisse nell'ambito della PA, invece che in quello privato.

Con l'accresciuta diffusione dei sistemi basati su IA anche il numero delle sfide tende ad aumentare e, inoltre, col passare del tempo anche il perimetro d'impatto e addirittura la definizione stessa delle sfide può cambiare per tenere il passo con l'evoluzione della IA e quindi delle potenziali problematiche che essa può creare, come già illustrato nel commento all'articolo 9 della Proposta di Regolamento.[125] Un esempio, come su è già in precedenza evidenziato[126], è sfida di protezione della privacy[127], dunque dei dati sensibili degli utenti, particolarmente sfidante per gli algoritmi impiegati dalla PA nella fornitura dei servizi al cittadino. Il miglioramento della tempistica e della qualità del servizio raggiungibile con l'ausilio della IA, infatti, non può e non deve essere vanificato da una ridotta protezione dei dati sensibili degli utenti.[128] Efficacia, efficienza e protezione dei dati sono elementi cardine per la relazione tra PA e cittadino, che l'impiego della IA potrebbe contribuire a rendere sempre migliore. La protezione dei dati sensibili ha implicazioni sia a livello legale che etico e, in particolare, un aspetto con risvolti etici concerne l'eventuale possibile impiego da parte della PA dei dati a sua disposizione in ambiti diversi da quello in cui sono stati acquisiti, anche se per finalità che possono rivelarsi di beneficio per i cittadini. La descrizione sin qui prodotta delle

[123] CEPEJ, 31ª Riunione plenaria, 3-4 dicembre 2018, *Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relative ambienti connessi*, CEPEJ (2018)14, 14
[124] PAGALLO U., *Etica e diritto dell'Intelligenza Artificiale nella governance del digitale: il Middle-out Approach* in RUFFOLO (a cura di) *Intelligenza artificiale e responsabilità*, 2017, 31
[125] *infra*, § 3
[126] *supra*, § 2, 3
[127] di cui si parlerà in modo approfondito in Capitolo II § 3
[128] FINOCCHIARO G., *Riflessione su intelligenza artificiale e protezione dei dati personali* in RUFFOLO (a cura di) *Intelligenza artificiale e responsabilità*, 2017, 237

peculiarità e problematiche insite nella ideazione, progettazione, sviluppo e impiego dei sistemi di IA in vari ambiti applicativi pone in evidenza la complessità di questa tecnologia ma anche le sue interessanti potenzialità.

Ad avviso di chi scrive una visione mediata della IA si colloca a metà tra uno scenario di cooperazione tra gli esseri umani e i robot basati su IA, senza competizione e con armonica integrazione, e quello in cui gli stessi robot diventino pervasivi nella vita dell'uomo e dei suoi processi decisionali. È auspicabile, infatti, una realtà in cui la IA automatizzi in modo intelligente e migliorativo una grande quantità di processi, ripetitivi e/o pericolosi e/o basati su elaborazioni e interpretazioni complesse sempre considerando le sfide insite nella tecnologia IA senza arrivare però a una visione delle responsabilità, che tenda a colpevolizzare l'algoritmo, essendo fondamentale l'individuazione del coinvolgimento dei gestori del sistema e/o degli operatori dei settori applicativi verticali, come si vedrà nel prossimo paragrafo.

5. Sfide presenti e future nell'attribuzione di responsabilità dell'IA.

Dalla precedente trattazione sui sistemi basati di IA, gli elementi che li compongono, le problematiche ad essi connessi e le sfide collegate con la creazione, addestramento e impego degli algoritmi, si deduce che la traduzione di detta complessità in una chiara ripartizione delle responsabilità dei soggetti coinvolti è tutt'altro che lineare. La responsabilità in caso di danni provocati dal sistema di IA, infatti, è stata ed è tuttora, in alcuni casi, oggetto di dibattito.

Un sistema di IA comprende sezioni hardware, algoritmi basati su sviluppi software, dati, da cui gli algoritmi attingono per il loro addestramento e funzionamento e il tutto può avere una natura integrata di prodotto unico ovvero può essere la collezione di sottoprodotti da integrare successivamente. Alla natura plurale della composizione di un sistema di IA, corrisponde una pluralità di soggetto coinvolti e, dunque, appare complessa sia natura del problema che l'individuazione del soggetto responsabile di eventuali danni causati. In alcuni ambiti applicativi, quali ad esempio quello farmaceutico, la vigente normativa italiana non identifica, con conseguente esposizione alla *responsabilità oggettiva*[129], il soggetto "*sorgente*" del prodotto, sia che l'abbia ideato che confezionato, ma solo il mero produttore.[130].

L'algoritmo di un sistema di IA è, come già ampiamente illustrato, elemento chiave del sistema e della sua "*intelligenza*" e, dunque, delle azioni che il sistema stesso suggerisce o intraprende direttamente nell'ambito applicativo di interesse.[131] Una

[129] *responsabilità oggettiva* ai sensi art. 42 c.p. – prescinde dall'elemento soggettivo di dolo o colpa
[130] RUFFOLO U. (a cura di), *Intelligenza artificiale e responsabilità*, Milano, 2017
[131] *supra*, § 4

progettazione dell'algoritmo affetta da *bugs* oppure minata da un certo grado di polarizzazione, impressa al momento della ideazione oppure del training, può avere un impatto diverso da quello che potrebbe palesarsi con semplice difetto di progettazione di un prodotto non basato su IA.

La radice storica di tale questione è rinvenibile nel problema della possibile imputabilità di entità non umane, come le persone giuridiche, considerando che essi non possiedono corpo fisico, mente e spirito, come quelli degli esseri umani, e che invece la responsabilità richiederebbe.[132] Da questo punto di vista, la svolta nell'ordinamento italiano è avvenuta con l'entrata in vigore del d.lgs. 231 del 2001 per cui le persone giuridiche sono divenuti penalmente imputabili con una responsabilità diretta[133], autonoma[134], ed eventualmente con quella dell'autore/i.[135]

La sfida successiva è di ravvisare nell'algoritmo o, forse, per migliorare l'associazione di esso con un oggetto fisico e umanoide, nel robot basato su IA, un bene/una cosa oppure un soggetto anche giuridico, nella catena delle responsabilità, con un contributo specifico ed individuale al danno causato. L'associazione al robot di una identità giuridica, infatti, potrebbe essere ammessa senza per questo riconoscere al robot una natura pseudo-umana o addirittura umana dotata di coscienza, con tutto quello che questa affermazione implica.[136] D'altra parte, si può invece riconoscere una responsabilità al robot, senza per questo attribuirgli una personalità giuridica. Si potrebbe altresì considerare il robot "corpo" senza "cervello", disaccoppiando le due componenti e le loro implicazioni nella catena di responsabilità giuridiche. Tale visione appare potenzialmente distante dalle finalità tecnologiche dell'intero impianto della intelligenza artificiale, che vede nella emulazione del cervello umano, coniugata al superamento delle limitazioni umane dovute all'irrazionalità, il vero punto di forza della cooperazione tra esseri umani e robot basati su IA.

Nella prospettiva della imputabilità di una responsabilità penale dei sistemi di IA, una visione da prendere in considerazione è quella del giurista Gabriel Hallevy il quale introduce tre modelli di responsabilità penale, applicabili separatamente o congiuntamente. Il modello della "*perpetration-by-another*" non ravvede nella IA caratteristiche umane e lo considera una entità innocente. Il sistema di IA, dunque, è semplicemente una macchina e quindi, seppure consapevoli delle prestazioni del sistema, queste non sono sufficienti per considerarlo come autore di un crimine. Invece il modello della "*natural-probable-consequence*" ipotizza un profondo coinvolgimento

---

[132] HALLEVY G., *Liability for Crimes Involving Artificial Intelligence Systems* in *Springer International Publishing AG*, 2014, 41

[133] responsabilità *diretta* è non sussidiaria e alternativa rispetto a quella della persona fisica

[134] responsabilità *autonoma* che non presuppone l'accertamento della responsabilità della persona fisica che ha commesso il reato-presupposto

[135] DE SIMONE G., *La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi) d'imputazione*, in *Diritto Penale Contemporaneo*, 2010, 1,3

[136] RUFFOLO, *Intelligenza artificiale e responsabilità*, cit., 28

del programmatore e/o dell'utente della IA nelle quotidiane attività del sistema di IA, ma essi non pianificano di commettere alcun reato attraverso il sistema di IA. Infine, il "*direct liability model*" si incentra sul sistema di IA in sé, non ipotizzando alcun legame tra essa e un programmatore o utente e consente di determinare con maggiore precisione la responsabilità penale dell'ambiente esterno. La responsabilità penale di un reato è una combinazione di elementi interni ed esterni al reato stesso.[137]

La individuazione della responsabilità si potrà articolare, quindi, considerando i ruoli all'interno della catena del sistema di IA, di cui si tratterà di seguito, anche se questi sono spesso confusi o sovrapposti, sebbene distinguibili in termini di azioni tecniche, data anche la problematicità di determinare singole categorie la cui responsabilità non rientri in due ruoli contemporaneamente ricoperti da un singolo soggetto. Ai fini di questa trattazione, chi scrive ritiene che la distinzione tra tali categorie sia utile per la comprensione tecnica dell'intera filiera di passaggi dall'idea all'utente

Possiamo intanto distinguere in tre fasi, in cui più ruoli rientrano, la prima fase è quella di concezione e realizzazione dell'algoritmo che viene poi scritto e tradotto in software e in questa rientra il progettista o ideatore[138], il programmatore[139] che molto spesso coincide con la prima figura e. La seconda fase consiste nella integrazione del software nell'hardware a cura dell'assemblatore o produttore, figure per lo più coincidenti. La terza è la commercializzazione da parte del venditore. L'acquirente del prodotto è l'utilizzatore. Esiste un'ulteriore figura più flessibile e che può intervenire in vari punti della catena che è quella dell'operatore ossia colui che può fa funzionare l'oggetto integrato, il solo software oppure può occuparsi del training dell'algoritmo, fino a poter eventualmente coincidere con l'utilizzatore del sistema integrato. Tuttavia, ai fini dell'eventuale attribuzione di responsabilità si ritiene più pratico individuare tre ruoli cardine in cui molto spesso gli altri ruoli si vanno a concentrare, come dettagliato di seguito.

5.1. *(Segue):* responsabilità del progettista e del programmatore.

Il *progettista* dell'algoritmo di IA è dunque identificabile come il soggetto autorale (ideatore) e di fornitura della componente immateriale rappresentata dall'algoritmo e, ciò lo espone a responsabilità aquiliane-extracontrattuale "*da algoritmo*" verso i terzi eventualmente lesi dal prodotto difettoso.[140] Un errore di progettazione in un generico prodotto non basato su IA può ravvisarsi con una responsabilità negoziale verso la

[137] HALLEVY G., *The Basic Models of Criminal Liability of AI Systems and Outer Circles*, in *Elsevier* SSRN, 2019, 1, 4, 8

[138] autore di algoritmi che traducono questi ultimi in linguaggio per la macchina e la testano al fine di verificare la presenza di eventuali errori

[139] scrive le linee di codice o il software

[140] RUFFOLO, *Intelligenza artificiale e responsabilità*, cit., 22

controparte contrattuale da parte del soggetto che ha progettato, mentre i soggetti che producono e vendono il prodotto hanno responsabilità verso consumatori e terzi.

Se il sistema di IA, basato su meccanismi avanzati di ML, gode di autonomia e parziale o totale imprevedibilità nell'evoluzione, diviene più articolata l'attribuzione della responsabilità da algoritmo e l'individuazione di un nesso di causa ed effetto. La responsabilità, infatti, potrebbe ancora ricadere sull'autore dell'algoritmo, nell'ipotesi di ritenere il sistema di IA, comunque, uno strumento a controllo umano. Invece, se il sistema di IA è semi-automatico o a controllo di operatore umano si potrebbe individuare una figura di garante nel responsabile del funzionamento del sistema e ricondurre ad un ambito di responsabilità per danno da prodotto la gestione dei problemi causati da un difetto di funzionamento del sistema.

Quindi con riferimento alla sopracitata responsabilità da algoritmo, il soggetto che opera il controllo parziale o totale sul sistema avrebbe sia il compito di evitare danni cagionati dal funzionamento non corretto del sistema che il ruolo di responsabilità in caso di eventi dannosi che non si è riusciti a prevenire. In questo caso, tuttavia, l'evoluzione imprevedibile dell'algoritmo potrebbe interrompere il nesso di causa ed effetto e trasformare la responsabilità dell'autore dell'algoritmo da soggettiva a oggettiva, riconoscendo in qualche modo al sistema di IA e al suo algoritmo una natura di soggetto giuridico, degno di tutela ma anche imputabile di sanzioni.[141] Si pensi, ad esempio, all'algoritmo e al relativo software integrato in un veicolo senza conducente basato su IA e dal cui funzionamento "*appropriato*" dipende l'incolumità dei soggetti a bordo e del veicolo e di quelli che con il veicolo interagiscono durante il suo percorso (altri conducenti o passeggeri di veicoli, pedoni). Un altro esempio di applicazione in cui l'algoritmo può essere causa di danni penalmente rilevanti riguarda la chirurgia permeata o assistita da elementi robotici basati su IA. Un terzo esempio riguarda l'impiego di droni basati su IA per applicazioni sia civili che militari.

Con i sistemi IA basati su autoapprendimento ed evoluzione, in parte o del tutto imprevedibile, diventa complicato prevedere o evitare possibili danni. Partendo, infatti, da due sistemi identici si potrebbe assistere ad evoluzioni anche molto diverse, a meno di non ricorrere a strumenti di inibizione o di controllo di un percorso evolutivo che stia prodromico di possibili danni.

Si tratta quindi di intervenire sui sistemi IA in modo da ricondurli al rispetto di "*principi*" che ricordano in qualche modo le tre famose leggi della robotica di Isaac Asimov, seppure con tutte le differenze che il progresso tecnologico degli ottanta anni intercorsi dalla loro pubblicazione impone di considerare.[142] In accordo alla prima leggi di Asimov, «un robot non deve ferire esseri umani o tramite la sua non azione consentire un danno agli stessi». Per la seconda legge, invece, «un robot deve obbedire

[141] PIERGALLINI C., *Intelligenza Artificiale: da mezzo a autore del reato?*, in *Rivista Italiana di Diritto e Procedura Penale*, 2020, 4
[142] ASIMOV I., *Runaround*, *in Astounding Science Fiction*, 1942

agli ordini degli esseri umani eccetto quando questi siano in contrasto con la prima legge». Infine, la terza legge enuncia che «un robot deve agire per proteggere la sua stessa esistenza fintanto che tali azioni non siano in contrasto con le prime due leggi». Alle tre leggi ne è stata successivamente aggiunta una quarta, per la quale «un robot non deve provocare danno all'umanità sia tramite la sua azione che tramite un comportamento passivo». Le leggi di Asimov hanno anticipato di molti decenni la sfida etica degli algoritmi di IA, già evidenziata, e la necessità di principi da enunciare per tenere in qualche modo sotto controllo i timori di scenari apocalittici nello scontro con l'innovazione tecnologica, in particolare legata alla robotica.[143] L'ambito applicativo dei veicoli a guida autonoma appare un esempio calzante per attualizzare le leggi di Asimov e rileggerle sostituendo alla parola "*robot*" quella di "*veicolo a guida autonoma basato su IA*".

Per il progettista dell'algoritmo di IA la questione della responsabilità parte dalla considerazione che l'algoritmo è, a tutti gli effetti, un componente fondamentale, benché immateriale, per il funzionamento idoneo dell'intero sistema o componente in cui viene integrato. Lo scenario diviene articolato, dal punto di vista della responsabilità penale, se si considera che i possibili danni potrebbero essere causati dal sistema IA che opera sotto il diretto controllo di un operatore umano oppure evolve, a valle del percorso di apprendimento, in maniera, parzialmente o totalmente autonoma, non del tutto prevedibile dagli autori dell'algoritmo.

Nel caso in cui il sistema di IA venga intenzionalmente e consapevolmente programmato al fine di commettere reati, la responsabilità dell'operatore è per dolo. Un'esemplificazione è l'impiego di droni basati su IA per applicazioni militari che vengano impostati con intenzione di uccidere dei civili, per cui la responsabilità di chi imposta il drone o del progettista si basano sull'idea che il drone sia uno strumento agente per volontà umana, determinando una coincidenza tra l'azione intenzionale del drone e la volontà del programmatore o dell'utilizzatore. [144]

Considerando invece la componente di imprevedibilità[145] della IA che evolve grazie all'esperienza, quindi utilizzando l'auto-apprendimento ossia in assenza di operatore, si distinguono due possibili strade per cui in una si ritiene che, data la capacità di indipendenza del sistema di IA, l'operatore non sarebbe mai responsabile per negligenza, mentre nell'altra che la colpa sarebbe di chi immette nell'ambiente ossia il progettista, programmatore o utilizzatore che non abbia previsto la componente di imprevedibilità della macchina. In tal senso si riterrebbe il programmatore responsabile per difetto di programmazione, costruzione, utilizzo, funzionamento o manutenzione[146]

---

[143] *supra*, § 4

[144] MELONI C., *Droni armati in Italia e in Europa: problemi e prospettive*, in *Diritto Penale Contemporaneo*, 2017, 1

[145] *supra*, § 4.1

[146] MAGRO M.B., *A.I.: la responsabilità penale per la progettazione, la costruzione e l'uso dei robot*, in *Altalex*, 2018

quindi avrebbe potuto prevedete l'evento che ha poi assume rilievo penale, quale la morte dei civili causata dal drone o anche da una macchina a guida autonoma. Questo perché è dopo la rilevazione dell'esperienza da parte del sistema di IA, inevitabilmente non omnicomprensivo di qualsiasi situazione, che il programmatore può iniziare a definire delle regole decisionali.

Bisogna inoltre tenere in considerazione che il programmatore, per come la colpa è prevista dal diritto vivente, sarebbe responsabile per la imprevedibilità il cui "logico sviluppo", quali lesioni o morte, era evitabile e quindi per non aver adoperato le cautele necessarie a evitarlo.[147] In particolare, per alcuni autori[148] l'imprevedibilità *"pre-programmata"*[149] non consente l'individuazione della colpa come prevista nei casi di divergenza tra voluto e realizzato, e sulla stessa linea di pensiero ritengono che la cosiddetta "*colpa*[150] *eventuale*[151]" comporterebbe la necessità di accertare la prevedibilità di un tale numero di rischi che da una parte supererebbero la prevedibilità astratta e dall'altra renderebbero "povero" l'accertamento degli elementi soggettivi della colpa.[152]

5.2. *(Segue):* responsabilità di venditore e produttore.

I sistemi di IA, dunque, presentano nuove sfide non solo in termini tecnologici e applicativi, ma anche in quelli di attribuzione delle responsabilità del danno cagionato da cosa in custodia di cui all'art 2051 c.c., che prevede che il custode possa liberarsi della responsabilità provando il caso fortuito, nel caso di mancanza del nesso causale per l'imprevedibilità dell'evoluzione dell'algoritmo di IA, tenendo presente la Direttiva CEE del 1985[153] in materia di responsabilità per danno da prodotti difettosi che disciplina specificatamente la produzione e vendita di beni e servizi di IA, La sfida, dunque, è nel definire il confine tra la capacità di reale controllo sull'algoritmo, che definisce il funzionamento del sistema di IA, da parte del suo ideatore/autore e la indipendenza dell'algoritmo scaturita dalla evoluzione "creativa" del suo

---

[147] MINELLI, *La responsabilità "penale" tra persona fisica e corporation alla luce della Proposta di Regolamento sull'Intelligenza Artificiale*, cit., 51

[148] PIVA, *Machina discere, (deinde) delinquere et puniri potest*, cit., 7

[149] pre-programmata è riferito alla imprevedibilità dell'agente intelligente

[150] colpa è *cosciente*, quando chi agisce non vuole l'evento ma lo ha previsto come possibile conseguenza della sua azione, confidando che non si realizzerà e *incosciente* quando non ha né voluto né previsto l'evento lesivo.

[151] dolo è *eventuale* quando la causazione dell'evento lesivo è il fine del soggetto che accetta inoltre che questo si verifichi

[152] MASSI S., *Affidamento sull'intelligenza artificiale e "disimpegno morale" nella definizione dei presupposti della responsabilità penale* in GIORDANO R. et al. (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Milano, 677

[153] CEE, *Direttiva del Consiglio relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri in materia di responsabilità per danno da prodotti difettosi*, 25 luglio, n. 85/374/CEE, 1985

addestramento. La sua responsabilità è oggettiva verso il soggetto leso e contrattuale nei confronti del produttore del sistema o sua componente integrante l'algoritmo e l'intensità dell'azione del soggetto leso dal sistema nei confronti dell'ideatore dell'algoritmo sarà dunque modulata proprio da tale confine.

Considerando quindi il tema di produzione e distribuzione di prodotti potenzialmente pericolosi molte regole sono state trasferite dall'ambito civile a quello penale e per una parte della dottrina continua però a permanere il problema della definizione di *prodotto*[154] e del soggetto responsabile per i suoi danni e la ripartizione dell'onere probatorio[155], mentre per un'altra parte la definizione di prodotto della Direttiva CEE[156] è estendibile all'algoritmo in quanto componente del prodotto finale. Partendo da queste considerazioni si ritiene necessario esplicare quale sia il comportamento atteso dal produttore, al fine di comprendere se possano essere ricompresi nella definizione di prodotto anche i sistemi di IA.

Il produttore "prudente" deve attentamente verificare il livello di sicurezza attraverso continui test dei prodotti che intende immettere nel mercato, prima di tale immissione, e successivamente monitorare gli effetti del suo prodotto, grazie anche alle opinioni dei consumatori e qualora vi fossero danni o rischi imprevisti dovrà seguire una linea di cautela nonché informare i consumatori e, se richiesto dalla situazione, il ritiro precauzionale del prodotto dal mercato.

In linea di principio, tale approccio potrebbe essere applicato anche ai sistemi di IA [157] che, come visto, presentano molti rischi, cosicché si potrebbero considerare che il produttore e anche il programmatore rivestano una posizione di garanzia del funzionamento del sistema.[158] Quindi, se venisse ad applicarsi tale disciplina, il produttore sarebbe esente da responsabilità qualora provasse il cosiddetto "rischio da sviluppo"[159].

Di tale rischio, tuttavia, si ritiene che il produttore di sistemi di IA non dovrebbe beneficiare nel caso in cui lo sviluppo di condotte non previste al momento della messa in circolazione sia prevedibile o quando abbia avuto la possibilità di controllare il prodotto o i suoi aggiornamenti, anche in modalità da remoto.[160] Infatti, non potrebbe avvalersene quando il prodotto in cui è integrato l'algoritmo presenti un

---

[154] Codice del consumo, d.lgs. 6 settembre 2005, n. 206, art. 115 co. 1 e 2, *prodotto* è ogni bene mobile, anche se incorporato in altro bene mobile o immobile, compresa l'elettricità, mentre per *produttore* s'intende il fabbricante del prodotto finito o di una sua componente,

[155] MINELLI, *La responsabilità "penale" tra persona fisica e corporation alla luce della Proposta di Regolamento sull'Intelligenza Artificiale*, cit., 51

[156] CEE, *Direttiva del Consiglio*, n 85/374, cit.

[157] MAGRO, *Robot, cyborg e intelligenze artificiali*, cit., 1207

[158] MASSI S., *A.I.: la responsabilità penale per la progettazione, la costruzione e l'uso dei robot*, in *Altalex - Ip, It e Data* Protection, 2018

[159] rischio da sviluppo si riferisce al difetto, causa del danno, non prevedibile quando il prodotto è stato immesso sul mercato o sia sorto successivamente a tale momento

[160] High-Level Expert Group on Artificial Intelligence, *Ethic guidelines for trustworthy AI*, 2019

comportamento deviante.[161] [162] Nell'attribuzione della catena di responsabilità si potrebbe poi utilizzare la ridefinizione degli oneri e dei doveri dei produttori che la proposta di Regolamento delinea in merito ai sistemi di IA ad alto rischio[163].

5.3. *(Segue):* responsabilità dell'utilizzatore.

L'utilizzatore di un sistema di IA ha un ruolo che si potrebbe definire di "*catalizzatore di responsabilità*"[164], in quanto disponibile e imputabile immediatamente degli eventi dannosi, e anche di "controllore", che garantisca l'impedimento dei danni evitabili che un malfunzionamento del sistema potrebbe provocare, quando sia titolare di un potere-dovere di intervento di "sovrascrivere" le scelte della macchina. In tal senso, tale obbligo di controllo potrebbe tradursi in un obbligo impeditivo a livello penale.

Una parte della dottrina si domanda se non sia opportuno trarre dall'articolo 590 sexies c.p.[165] una disciplina che escluda la punibilità dell'utilizzatore/controllore quando il perimetro che delinea l'area dei rischi relativi all'impiego della IA sia stato rispettato con l'obbedienza alle regole definite in materia. La stessa corrente di pensiero[166] ritiene che si possa circoscrivere la responsabilità alle ipotesi di colpa *grave*[167], partendo dall'articolo 2236 c.c.[168], tenendo in considerazione che «l'utente che manovri strumenti supportati da meccanismi di intelligenza artificiale, senza cognizione adeguata dei rischi che ciò comporti, versi in una situazione in cui si assume un rischio per lui non controllabile, riproducendo lo schema della cd. "colpa per *assunzione*[169]"».[170] Data la peculiarità del sistema di IA rispetto altre tipologie di prodotti, il suo utilizzatore viene a trovarsi in una situazione in cui è necessaria un'adeguata consapevolezza e in tal senso si pone chi sostiene che la responsabilità non può derivare dal semplice utilizzo del prodotto quando sono state rispettate le istruzioni

---

[161] RUFFOLO U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, 130

[162] BURGIO E. – DE SIMONE L., *Intelligenza Artificiale e responsabilità civile*, in *MediaLaws*, 2021

[163] *supra* § 3

[164] AMOROSO D. – TAMBURRINI G., *I sistemi robotici ad autonomia crescente tra etica e diritto: quale ruolo per il controllore umano*, in *Rivista di BioDiritto*, 2019, 51

[165] Art. 590 sexies c.p., Responsabilità colposa per morte o lesioni personali in ambito sanitario, co 2 «qualora l'evento si sia verificato a causa di imperizia, la punibilità è esclusa quando sono rispettate le raccomandazioni previste dalle linee guida…»

[166] PIVA D., *Spunti per una riscoperta della colpa per assunzione,* in BONDI A. – FIANDACA G. et al. (a cura di), *Studi in onore di Lucio Monaco*, Urbino, 1139

[167] colpa *grave* quando la violazione particolarmente evidente dell'obbligo di diligenza mostri l'allontanamento dalle regole di diligenza, prudenza e perizia richiesti dal caso concreto

[168] art. 2236 c.c., Responsabilità del prestatore d'opera, «se la prestazione implica la soluzione di problemi tecnici di speciale difficoltà, il prestatore d'opera non risponde dei danni, se non in caso di dolo o di colpa grave»

[169] colpa per *assunzione* è esemplificata dallo specializzando responsabile a titolo di colpa quando acconsenta a svolgere una attività per cui è consapevole di non avere la preparazione e la competenza necessarie ad eseguirla assumendosi il rischio di eventuali conseguenze dannose

[170] MASSI, *Affidamento sull'intelligenza artificiale e "disimpegno morale" nella definizione dei presupposti della responsabilità penale*, cit., 678

che il produttore ha fornito.[171] Infatti, ai sensi dell'articolo 13 della proposta di Regolamento[172] gli algoritmi devono essere trasparenti cosicché gli utenti possano interpretare l'output del sistema di IA, che deve essere corredato da istruzioni precise, comprensibili ed esaustive, che devono anche includere le indicazioni utili a garantire il corretto funzionamento del sistema, la manutenzione e gli aggiornamenti del software. Gli utenti devono altresì riceve altre informazioni in merito a caratteristiche, capacità e limiti del sistema e su quanto attiene al controllo umano esercitabile su di esso, ai cambiamenti pre-determinati e ad una stima sulla durata del funzionamento.

Si può sostenere che la responsabilità dell'utilizzatore sorga quando vi sia stata una modifica attiva sul sistema di IA o la custodia su di esso sia mancata o risultata insufficiente[173] e quando, pur avendo controllo sul sistema e potendo intervenire attivamente su di esso, non abbia esercito l'obbligo di controllo o questo sia risultato inadeguato, per cui si potrebbe addebitare una responsabilità per omessa attivazione quando il sistema vada in errore.[174]

Si è fin qui visto il ruolo dell'utilizzatore sotto vari profili in relazione alla IA in quanto prodotto e si può sostenere che l'utente di un sistema di IA, in questo caso anche utilizzatore[175], può essere esente da responsabilità penale quando adotti la diligenza richiesta dalle normative citate e quindi garantendo la sicurezza ai fini della tutela dei diritti fondamentali nel corso dell'intero ciclo di vita del sistema di IA. Un'ulteriore considerazione va fatta in merito alla figura già discussa del programmatore e/o dell'utente, in questo caso utilizzatore, che si dovrebbero ritenere esenti da responsabilità penale quando adottino le cautele previste dalla direttiva CEE[176],dal momento che la responsabilità del "formatore"[177] del sistema di IA è direttamente proporzionale alla capacità di apprendimento, all'autonomia del sistema e alla durata del training.[178] Da quanto detto sembra plausibile che il miglior formatore per l'algoritmo sarebbe chi lo ha concepito, ossia l'ideatore.

5.4. *(Segue):* considerazioni conclusive sulla responsabilità da IA.

L'opportunità di adeguare le normative per chiarire le responsabilità dei vari soggetti che ruotano attorno ad un sistema robotico con capacità autonome, quali il produttore,

---

[171] BERTOLESI R., *Intelligenza artificiale e responsabilità penale per danno da prodotto*, Tesi dottorato Diritto Penale, Milano, 2019, 236

[172] Commissione EU, 2021/0106 (COD), cit., art. 13, *Trasparenza e fornitura di informazioni agli utenti*

[173] nonostante l'atteso obbligo di conservazione della funzionalità del sistema

[174] MINELLI, *La responsabilità "penale" tra persona fisica e corporation alla luce della Proposta di Regolamento sull'Intelligenza Artificiale*, cit., 59

[175] Esenzione che può essere anche valida per il programmatore

[176] CEE, *Direttiva del Consiglio*, n 85/374, cit.

[177] l'*operatore* quando si occupa del training, *supra* § 5

[178] SALVADORI I., *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Rivista italiana di diritto e procedura penale*, 2021, 64, 1, 85

l'operatore e l'utilizzatore, in merito alle azioni e omissioni compiute dal robot che hanno causato danno, è stata evidenziata dal Parlamento Europeo già da alcuni anni.[179] L'autonomia del robot basato su IA si palesa nel processo decisionale autonomo che esso esplica su alcuni temi con conseguenti azioni verso il mondo esterno, il cui grado di penetrazione è legato anche al livello di complessità della progettata interazione robot-ambiente esterno. Maggiore è l'interazione, maggiore la platea di potenziali danni che detta interazione può far scaturire e naturalmente anche la quantità di benefici cresce di pari passo. Appare anche lecita la domanda in merito alla reale necessità di spingere l'autonomia dei robot basati su IA fino al punto da renderne difficile anche un blando controllo. Dal punto di vista del progresso e dei potenziali benefici per il genere umano la risposta affermativa appare scontata, ma dal punto di vista della responsabilità forse non lo è. La già citata risoluzione del Parlamento Europeo per il futuro strumento legislativo si debba valutare se utilizzare l'approccio della responsabilità oggettiva ("*strict liability*") o della gestione dei rischi. Il primo necessita di una semplice prova del danno e la identificazione del nesso causa-effetto tra l'azione del robot e il danno di chi lo ha subito.

La gestione dei rischi si focalizza sul soggetto che è capace di minimizzare i rischi e gestire l'impatto negativo, invece di concentrarsi, come nel caso della responsabilità oggettiva, sul soggetto che ha agito con negligenza. La porzione di responsabilità dei soggetti individuati come responsabili nella catena del danno dovrebbe essere posta in relazione alla quantità di istruzioni impartite al robot e, in tal modo, potrebbe associarsi alla capacità di apprendimento del robot e alla durata del suo apprendimento, quindi a un ammontare significativo di istruzioni in una condizione tecnologica "favorevole". Ciò implica una maggiore responsabilità di colui che effettua il training del sistema di IA[180], e che ha quindi potuto renderlo operativo in un tempo appropriato partendo da un sistema di adeguata qualità. In tale scenario, la responsabilità dovrebbe comunque essere imputata alla componente umana e non a quella robotica, nonostante le capacità di auto-apprendimento del robot medesimo.[181]

Invece di essere utilizzati in alternativa, i due approcci alla responsabilità (oggettiva e gestione dei rischi) potrebbero essere uniti, dove si ipotizza «un regime in cui la natura della responsabilità in questione prescinda dall'esistenza di un elemento doloso o colposo, ricorrendo, dunque, ad uno schema di responsabilità oggettiva, mentre l'applicazione di un cd. "*risk managment approach*" consentirebbe di identificare nella catena produttiva-commerciale soggetti cui tale responsabilità oggettiva potrebbe essere attribuita».[182] Tale approccio integrato alla responsabilità sarebbe compatibile con l'attuale disciplina della responsabilità da prodotto difettoso. I tipici difetti

[179] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, P8 TA(2017)0051, C 252/242, AB
[180] come già visto, può essere a carico del progettista, operatore e perfino dell'utilizzatore
[181] Risoluzione del Parlamento europeo, P8 TA(2017)0051, cit., C 252/249, 53, 54, 56
[182] RUFFOLO, *Intelligenza artificiale e responsabilità*, cit., 87

attribuibili ai sistemi di IA, in generale, e ai robot in particolare possono derivare dalle varie fasi del ciclo di vita: la progettazione oppure la complessa fase di programmazione che supporta l'elemento cardine del sistema, cioè l'algoritmo, il quale, a sua volta, è cruciale per il funzionamento dell'intero sistema. Possono esserci anche difetti di costruzione, dunque relativi alle sezioni hardware e alla loro integrazione e, non ultimo, il difetto può derivare da un errore umano nell'operare il sistema. Nella individuazione delle responsabilità, quella dell'autore dell'algoritmo e quella del produttore del sistema integrato, in particolare il robot, appaiono distinte. Il soggetto che subisce il danno, qualora questo sia cagionato da conseguenze legate a un errato apprendimento da parte del robot/sistema di IA, potrebbe avvalersi di una azione risarcitoria diretta. La attribuzione di responsabilità all'autore dell'algoritmo assurge a elemento di copertura del "vuoto di responsabilità" che la citata Risoluzione del Parlamento Europeo fa risalire alla evoluzione imprevedibile del comportamento del sistema di IA basato su ML e DL a valle della fase di autoapprendimento. Tale vuoto di attribuzione della responsabilità è in qualche modo paragonabile al rischio di sviluppo associabile a prodotti talmente innovativi che lo stato di conoscenza tecnico-scientifico al momento della loro immissione sul mercato con consente di rilevarne in toto la eventuale difettosità e, in questo caso, la normativa europea esenta il produttore dalla responsabilità per i difetti dal prodotto cagionati.[183]

La vigente normativa in materia di responsabilità regola quelle situazioni ove ciò che il robot compie o omette viene attribuito alla componente umana, e dunque ad uno dei soggetti che entrano a diverso titolo nel ciclo di vita del sistema (produttore, operatore, proprietario, utilizzatore), quando il soggetto avrebbe potuto prevedere le azioni del robot ed evitarle. La responsabilità delle azioni o omissioni del robot potrebbero ricadere su detti soggetti (produttore, operatore, proprietario, utilizzatore), non potendo i robot essere considerati responsabili in proprio per atti o omissioni che causano danni a terzi.[184]

Da tale quadro «sono destinati a emergere i limiti di tenuta del tradizionale diritto penale d'evento rispetto a eventuali ascrizioni di responsabilità colposa»[185] cercando di ridurre la "tentazione" a scarica la responsabilità sui soggetti che entrano a diverso titolo nel ciclo di vita del sistema di IA. Ad avviso di chi scrive, ciò che sostiene la giurista Chiara Minelli è la via che il diritto dovrebbe seguire: un diritto penale che sappia essere «proattivo e multilivello» e che sulla scia della proposta di Regolamento[186] possa efficacemente intercettare e gestire i rischi e, pur non essendo la

[183] AMIDEI, *Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo*, in RUFFOLO (a cura di) *Intelligenza artificiale e responsabilità*, 2017, 92
[184] Risoluzione del Parlamento europeo, P8 TA(2017)0051, cit., C 252/242
[185] MINELLI, *La responsabilità "penale" tra persona fisica e corporation alla luce della Proposta di Regolamento sull'Intelligenza Artificiale*, cit., 50
[186] Commissione EU, 2021/0106 (COD), cit.

proposta direttamente applicabile in materia penale, seguire la via di una precauzione "moderata".

Una considerazione più ampia sulla responsabilità si ricollega alle sanzioni applicabili dopo il suo accertamento e ai tipi di pena e alle funzioni che esse svolgerebbero in ambito di IA. Nei confronti della quale sembrano poter essere applicabili ai fini retributivi[187] e special-preventivi[188], come ad esempio lo spegnimento del sistema (arresto oppure ibernazione) e un ricondizionamento attraverso un nuovo training, mentre quella general-preventiva in cui la sola minaccia della pena sia un deterrente[189] non risulta facilmente immaginabile nello scenario presente.

6. Algoritmi predittivi nell'ambito penale.

La complessità che ruota intorno all'intero ciclo di vita di un sistema di IA e al suo centro focale, rappresentato dall'algoritmo, si trasla anche con paragonabile complessità nell'ambito penale. Come già evidenziato, il diritto penale dovrà munirsi di adeguati strumenti per fronteggiare non solo lo scenario presente legato al mondo della IA, ma anche la rapida evoluzione della tecnologica IA che promette numerose questioni con rilevanza penale che si pongono e si porranno con maggiore frequenza. [190] La IA, attraverso i propri algoritmi, può fornire uno strumento di grande utilità che, come già esplicato, pone questioni circa il bilanciamento dei diritti di cui i cittadini sono titolari.

In tal senso, un primo ambito rilevante concerne le attività di "*law enforcement*" dove l'impiego di algoritmi di IA può supportare, incrementandone l'efficacia e la sistematizzazione, tutte quelle attività basate sulla raccolta e l'analisi di dati.[191] In particolare, le attività di "*predicitve policing",* o polizia predittiva, possono trarre indubbio vantaggio grazie all'impiego del machine learning che consentirebbe, con la raccolta di informazioni pertinenti, di identificare quale sia la tendenza a maggior ripetitività nell'ambito degli illeciti e, inoltre, sulla base di queste informazioni sarebbe possibile, ad esempio, organizzare le risorse a disposizione in maniera più congrua, migliorando l'impatto sul contrasto a quegli illeciti che occorrono con maggior frequenza. Nel Report pubblicato in materia di intelligenza artificiale e law

[187] funzione retributiva in cui si punisce il reo come retribuzione del male provocato dal reato
[188] funzione special-preventiva in cui inflizione e esecuzione della pena prevengono che il condannato commetta altri reati in futuro
[189] BASILE, F., *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine* in *Diritto Penale e Uomo*, 2019, 31
[190] BASILE, *Intelligenza artificiale e diritto penale*, cit., 4
[191] BARMANN B., *Intelligenza artificiale e law enforcement*, in *Istituto di Ricerche sulla Pubblica Amministrazione*, 2020

enforcement si segnalano utili esempi applicativi nell'ambito di interesse[192] e alcuni esempi di rilievo sono: i software di computer vision sfruttabili nei casi di reati di furto di autoveicoli; i sistemi di sorveglianza che adoperano droni; varie forme di riconoscimento facciale; gli strumenti predittivi di cui sopra e, unitamente a questi, quelli che identificano e sanzionano autonomamente gli autori di reati di truffa online e quelli che analizzano conversazioni telefoniche basandosi sul ML. Gli strumenti posti a salvaguardia dell'ordinamento necessitano che la cosiddetta "*asimmetria tecnologica*", menzionata nel Report, venga colmata in quanto la conoscenza che è stata acquisita nel tempo da chi commette crimini risulta essere, in alcuni casi, elevata. Si evidenzia come sia fondamentale che le autorità di polizia e di controllo necessitino di una formazione specifica e al passo con l'evoluzione tecnologica, al fine di garantire al meglio il funzionamento degli strumenti di *law enforcement*. L'utilizzo consapevole ed esperto di tali strumenti tecnologici permetterebbe di prevenire e reprimere la criminalità in maniera più efficace e le autorità sarebbero quindi in grado di trarre un ulteriore vantaggio dall'utilizzo degli strumenti tecnologici al fine di prevenire e reprimere la criminalità. Al pari delle problematiche sollevate in precedenza in merito alla IA, si pongono anche in merito a questi strumenti problematiche etiche legate specialmente alla privacy e alla necessità di garantire trasparenza, conoscibilità e comprensibilità delle attività svolte dalle autorità.

Un secondo ambito rilevante riguarda l'utilizzo degli algoritmi a fini decisionali in molteplici ambiti, che comprendono sia quello pubblico che privato, i quali vengono indicati con la denominazione di "*automated decision systems*" e rappresentano metodi alternativi per risolvere controversie. Essi comportano il vantaggio di ridurre i tempi necessari per convergere a una decisione e consentono un risparmio di risorse sia per chi necessita di una decisione che per chi ha la responsabilità di formularla. Un ulteriore vantaggio di tale approccio è che la gestione è spesso avviene completamente in rete. Gli algoritmi possono adoperare per il loro addestramento e la loro operatività ingenti banche dati relative a giurisprudenza, legislazione e precedenti. Proprio tale mole di dati ha consentito di sviluppare e testare dispositivi avanzati che apparentemente operano con ridotta polarizzazione, utilizzando modelli sofisticati quali la teoria dei giochi, l'analisi dei risultati positivi e le strategie di negoziazione al fine della risoluzione delle questioni poste. L'approccio appare anche molto promettente per un futuro sistematico utilizzo nel corso dei procedimenti penali con eventuale, parziale o totale, sostituzione della decisione umana con quella formulata dal sistema di IA.

Una terza tematica utile nel completare il quadro di riflessione sulla responsabilità penale nell'ambito IA riguarda il ruolo che un sistema di IA può avere nell'eventualità di un reato[193] e che, specificamente, può essere di autore, vittima e mezzo

[192] The International Criminal Police Organization (INTERPOL) – United Nations Interregional Crime and Justice Research Institute (UNICRI), *Artificial Intelligence and Robotic for law* enforcement, 2018
[193] UBERTIS*, Intelligenza artificiale, giustizia penale, controllo umano significativo* cit., 80

strumentale.[194] Sulla qualità della IA come autore di un reato l'elemento fondamentale che manca alla IA è la volontarietà perché «il sistema non agisce ma "*è agito*"»[195], visione che contrastare quella di chi sostiene che l'associazione fra intelligenze umana e artificiale ha l'unica differenza nel "contenitore" che le ospita[196], o chi sostiene che l'hardware del sistema di IA ha una "fisicità[197] e quindi potrebbe avere una capacità di azione. Per quanto la IA elabori dati della realtà esterna per auto-apprendere[198], le sue decisioni sono, in realtà, frutto dell'algoritmo, il quale, seguendo tale linea di pensiero, non ha libertà di autodeterminazione. Di conseguenza, le scelte anche autonome dell'algoritmo sarebbero necessariamente il frutto di un funzionamento progettato e forgiato dall'essere umano. In relazione al verificarsi di un fatto di reato per effetto delle scelte autonome dell'algoritmo, va considerato il cosiddetto *rischio consentito* che si riferisce ad attività pericolose che pur avendo una utilità sono potenzialmente pericolose per i soggetti interessati. Se si assimilasse la gestione del corpo umano a quella della gestione non volontaria dell'IA, rimarrebbe il problema della colpevolezza, proprio perché, come già evidenziato, le intelligenze artificiali non possono essere ritenute colpevoli in quanto sprovviste della capacità di scelta.[199] Ricordando quando detto in tema del possibile sistema sanzionatorio applicabile, il giurista Cappellini ritiene che un sistema sanzionatorio rivolto direttamente alla macchina IA possa corrispondere alle esigenze della funzione retributiva e special-preventiva della pena.[200]

La IA potrebbe, inoltre, rivestire il ruolo di vittima di un reato e in questo caso si potrebbero utilizzare gli argomenti a favore del considerare la IA come una "persona"[201], la quale quindi verrebbe a soffrire degli effetti di un reato, non essendo considerato, in tale concezione, solo come oggetto che li subisce materialmente. Anche se, come già visto, questo umanizzerebbe l'IA, concetto che molti criticano ritenendo impossibile che questa abbia sentimenti[202], una possibilità sarebbe quella di modificare le figure di reato esistenti oppure introdurne *ad hoc* cosicché sarebbero punibili specifici attacchi rivolti verso sistemi IA, quali ad esempio i robot utilizzati in *doll* o *pet therapy* di supporto a persone affette da varie patologie e disabilità, le quali potrebbero sviluppare emozioni nei confronti dei robot stessi e subire effetti negativi dal loro danneggiamento.[203] Secondo la linea di pensiero che ricomprende il già citato Hallevy l'IA dovrebbe essere imputabile anche se non è umana (esistono infatti

[194] PIVA, *Machina discere, (deinde) delinquere et puniri potest*, cit., 684
[195] PIERGALLINI, *Intelligenza Artificiale: da mezzo a autore del reato?*, cit., 1767
[196] intelligenza umana ospitata nel cervello, mentre quella artificiale nell'hardware
[197] CAPPELLINI A., *Machina delinquere non potest?*, in *Discrimen*, 2019, 18
[198] *supra* § 1, 2, 5
[199] CAPPELLINI, *Machina delinquere non potest?*, cit., 14
[200] CAPPELLINI, *Machina delinquere non potest?*, cit.,15 e *supra* § 5.4
[201] *supra* § 5
[202] KAPLAN J., *Intelligenza artificiale. Guida al futuro prossimo* in *Luiss University Press*, II, 2018, 126
[203] BASILE, *Intelligenza artificiale e diritto penale*, cit., 32

sanzioni, come quelle dirette alle persone giuridiche, che si sono dimostrate utili in chiave preventiva. [204]

Considerando, infine, la IA come mezzo strumentale, «il presupposto indefettibile per imputare al programmatore, al fornitore e/o all'utente la responsabilità per danni generati dall'IA coincide con il *controllo* che questi sono in grado di esercitare sul software, un controllo che verrebbe meno specialmente a fronte delle più evolute e sofisticate tecnologie»[205].

Si è già evidenziata la possibile catena di responsabilità per i danni causati dall'algoritmo di IA, elemento cruciale del sistema che lo ospita, e vari aspetti sfidanti nel delineare detta responsabilità.[206] Considerando le crescenti capacità di un sistema di IA, appare comprensibile come esso possa addirittura divenire uno strumento attraverso il quale la "*componente umana*" commette un reato. Ambiti assai idonei a questa eventualità riguardano l'informatica, l'ambiente, l'economia, i traffici internazionali di droga e altri prodotti illeciti, la tratta di esseri umani. I sistemi di IA potrebbero anche essere impiegati per le violazioni della privacy[207] e del trattamento dei dati personali, violazioni della proprietà intellettuale e industriale, reati di diffamazione e abuso della ingenuità delle persone attraverso, per esempio, *fakenews* oppure *bot*.[208] [209] Una porzione del traffico dei bot potrebbe produrre effetti negativi su siti e applicazioni. La commissione di reati attraverso sistemi di IA è probabilmente destinata ad aumentare di pari passo con la penetrazione della IA nei settori applicativi e il suo continuo progresso in termini di prestazioni.

Tale tendenza potrebbe trovare terreno favorevole anche a causa della rapida crescita di comportamenti dei singoli che, consapevolmente o no, consentono la raccolta di dati sulle proprie abitudini di vita e comportamenti attraverso l'uso massiccio della rete e della Internet of Things (IoT). Non è da escludersi per il futuro che uno scenario iper-collaborativo tra esseri umani e robot basati su IA porti all'instaurarsi di rapporti di dipendenza e, addirittura, affettivi con il robot, impiegabile in sostituzione di operatori umani (per esempio, badanti o baby-sitter). Gli esseri umani potrebbero trovarsi in situazioni di potenziali vulnerabilità. Da quanto evidenziato, sarà opportuno un rimodellamento se non addirittura la definizione ex novo di fattispecie di reato idonee

[204] *supra*, § 5
[205] BASSINI M. – L. LIGUORI L – O. POLLICINO O., *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in PIZZETTI F.(a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 356
[206] *supra*, § 5
[207] *infra*, Capitolo II § 3
[208] BASILE, *Intelligenza artificiale e diritto penale*, cit., 16
[209] *bot* è un programma, la cui denominazione in ambito informatico deriva dalla parola robot, che opera in rete eseguendo compiti ripetitivi.

a rappresentare i nuovi scenari e le nuove condotte criminose che impiegano la IA per realizzarsi.

Se il sistema IA è dotato di capacità di autoapprendimento con evoluzione autonoma e in parte o del tutto non prevedibile, allora si ritrova la questione sfidante, analizzata a proposito degli aspetti sfidanti nell'attribuzione di responsabilità, di vedere nel sistema di IA, e in particolare nel suo algoritmo, non solo o non più un mero strumento nelle mani di un essere umano, ma un potenziale elemento indipendente capace della realizzazione autonoma del reato.[210] Si apre, in tal caso, la questione sull'intreccio modulabile di responsabilità tra operatore umano e algoritmo e la capacità o meno del sistema di IA di rispondere del reato a livello penale. Questo scenario è riconducibile in qualche modo alla individuazione della responsabilità nei casi in cui il processo decisionale ed esecutivo sia parcellizzato tra una pluralità di soggetti. La novità, nel caso della IA, risiede nel fatto che uno dei soggetti in questione è proprio il sistema di IA. Esiste poi la possibilità di considerare il sistema di IA quale vittima di un reato, nell'ottica sopramenzionata di assimilare il sistema ad una "persona". Tale posizione contrasta, tuttavia, con l'ipotesi che i sistemi basati su IA non hanno e non avranno mai sentimenti; dunque, non raggiungeranno mai un livello di completa umanizzazione.

6.1. *(Segue):* l'*evidence-based sentencing* e le criticità collegate all'impiego dell'IA nelle decisioni giudiziarie.

Nel paragrafo precedente sono stati descritti tre ambiti in cui, a fronte della innovazione tecnologica portata dalla IA, si pongono questioni rilevanti per il diritto penale e, in specie, nel bilanciamento dei diritti di cui i cittadini sono titolari. I tre ambiti sopracitati sono quelli di law enforcementent in particolare il *predictive policing* (PP), automated decisions e il ruolo della IA come strumento, vittima o autore, ai quali si aggiunge il tema qui trattato, quello dell'impiego di algoritmi predittivi per la valutazione della pericolosità di un soggetto in termini di azioni criminali, e dunque la valutazione della probabilità di commissione o reiterazione di un reato, il cd approccio "*evidence-based"*. Tale valutazione parte dalla individuazione di una articolata serie di *predittori* o *fattori di rischio*, correlati con il comportamento criminoso, che hanno sia una natura statica (per esempio: sesso, origine tecnica, precedenti penali) che dinamica (per esempio: età, situazione familiare, situazione lavorativa, ospedalizzazioni, consumo di droghe, psicopatia). Tra i predittori dinamici rientrano anche le variabili del contesto in cui il soggetto si inquadra come, ad esempio, la mancanza di sostegno familiare o sociale, presenza di rei in ambito familiare, la cerchia di persone frequentate.

Per una efficace predizione, l'algoritmo è opportuno che riesca a impiegare la relazione tra fattori di rischio statici e dinamici. Nelle prime applicazioni di valutazione del

[210] *supra*, § 5.1

rischio, che risalgono agli anni Settanta, erano impiegati in maniera preponderante i fattori di rischio *statici* che, per loro natura, non contribuivano alla valutazione dei progressi positivi ottenuti dal soggetto nei percorsi di riabilitazione e, dunque, potevano ingenerare una certa discriminazione nei confronti di un soggetto con rischio di recidiva elevato. I fattori *dinamici* hanno invece rilevanza per identificare il più idoneo trattamento da applicare al soggetto per ridurne il rischio di recidiva.[211]

Gli algoritmi di IA presentano crescenti prestazioni, sia in termini di capacità "*pseudo umane*", amplificate da velocità sorprendenti, che di efficace impiego di enormi volumi di dati, i quali attingono a database sempre migliori per qualità del dato e metodi di accesso. Si sottolinea che la qualità dei dati, inclusa la loro già citata neutralità[212], con cui avviene il training dell'algoritmo risulta particolarmente cruciale al fine della costruzione della funzione predittiva.[213] Il progresso degli algoritmi di IA rende, dunque, disponibili strumenti predittivi di grande raffinatezza tecnica e in continuo miglioramento nella loro facilità di impiego da parte dell'utente (*user-friendly*), capaci di tenere debitamente conto della interazione tra predittori statici e dinamici. Come già evidenziato nell'analisi delle problematiche legate all'impiego della IA nei vari ambiti applicativi, è necessario aspirare a un bilanciamento tra opposti fattori.

Da una parte vi sono i benefici e l'ausilio che un sistema *evidence-based* può portare nella valutazione predittiva della pericolosità di un soggetto, in termini di azioni criminali, e le successive azioni, volte alla riduzione del rischio e la eventuale riabilitazione[214] e dall'altra permangono rischi in cui possono incorrere i diritti fondamentali, le garanzie e i principi in ambito processuale. [215]

Il vantaggio che ne deriverebbe per il giudice sarebbe un più agevole calcolo del rischio di reiterazione del reato quando si tratti di commisurare la pena, applicare le misure alternative o cautelari. [216] Per ciò che concerne la pericolosità sociale, l'algoritmo è in grado di valutare e prevedere la probabilità di una reiterazione a delinquere e dunque esaminare il rischio di recidiva in sede cautelare, quando si applichi la sospensione condizionale o le misure alternative alla detenzione. Inoltre, l'algoritmo può essere lo strumento di ausilio nella individuazione del programma riabilitativo più consono, a seconda del settore di intervento, quale, per esempio, quello delle molestie sessuali. Bisogna però tenere sotto controllo il rischio di esiti discriminatori, in quanto seppure un algoritmo non abbia, in linea di principio, in sé pregiudizi[217] nella valutazione della pericolosità sociale sono possibili effetti discriminatori sui soggetti che provengano da

---

[211] D'AGOSTINO L., *Gli algoritmi predittivi per la commisurazione della pena*, in *Diritto Penale Contemporaneo*, 2019, 2, 359
[212] *supra* § 2, 4
[213] HUQ A.Z., *Racial Equity in Algorithmic Criminal Justice*, in *Duke Law Journal*, 2019, 1076
[214] BASILE, *Intelligenza artificiale e diritto penale*, cit., 17
[215] D'AGOSTINO, *Gli algoritmi predittivi per la commisurazione della pena*, cit., 354, 358
[216] MAUGERI A.M., *L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra evidence based practices e tutela dei diritti fondamentali*, in *Archivio Penale*, 2021, 1
[217] *supra* § 2

classi sociali disagiate[218] in quanto i *database* su cui si basano gli algoritmi possono essere fuorviati basandosi su eccessive generalizzazioni. In tal senso le variabili socioeconomiche possono essere spesso alla base della misurazione del rischio di recidiva e, quindi, si può ritenere che queste determinino un output discriminatorio.

La "Carta etica europea" del 2018 ha specificato che in riferimento ai procedimenti penali che «anche se non sono specificamente progettati per essere discriminatori, l'uso di algoritmi basati sull'IA [...] ha mostrato il rischio di favorire la rinascita di teorie deterministiche a scapito delle teorie dell'individualizzazione della pena»[219], vietando la discriminazione di singoli o di gruppi quando si utilizzino gli algoritmi predittivi in sede giudiziaria.

La individuazione e la scelta di questi ultimi ha come finalità la valutazione del rischio di recidiva. Tale valutazione avviene grazie all'utilizzo di sistemi che impiegano il *Risk-Need-Responsivity* (RNR) come strumento di attuazione degli obiettivi preposti. Il RNR, infatti, è stato utilizzato con successo in Canada e in altri paesi per valutare e riabilitare i criminali e, sulla base di fattori di rischio accertati, sancisce la necessaria proporzionalità tra il trattamento e il rischio di commissione di un nuovo reato. Tale modello è stato formalizzato per la prima volta nel 1990 e negli anni si è dimostrato come uno degli approcci più efficaci per le finalità sopra descritte, essendo elaborato e contestualizzato nell'ambito di una teoria sulla condotta criminale basata sulla personalità dell'individuo e sul contesto sociale.

I principi fondanti del modello vertono, come suggerisce la denominazione, su rischio, necessità e reattività. Un primo principio, relativo al rischio, asserisce la possibilità di prevedere con un alto grado di affidabilità il comportamento criminale e la necessità di focalizzarsi primariamente sugli "*higher risk offenders"*, quindi i soggetti che presentano un maggiore rischio di recidiva.[220] La necessità espressa da un secondo principio è quella di considerare nella predisposizione e attuazione del trattamento i cosiddetti "*criminogenic needs*", i quali sono fattori relativi alla vita del criminale direttamente correlati con la recidività del soggetto. In relazione a questi sono stati individuati i fattori correlati direttamente al crimine: abuso di sostanze, famiglie disfunzionali, valori e/o personalità con un atteggiamento contrario a equilibrio, istituzioni, aspirazioni della società, scarsa capacità di autocontrollo, rapporti con soggetti criminali. Un terzo principio, relativo alla responsività, prevede le modalità di applicazione del trattamento che esalti la capacità del soggetto di imparare dalla

[218] KETH D. – PRISCILLA G. – KESSLER S., *Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing,* in *Responsive Communities Initiative*, *Berkman Klein Center for Internet & Society*, 2017, 16

[219] CEPEJ, 31ª Riunione plenaria, 3-4 dicembre 2018, *Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti connessi*, cit., 48

[220] BONTA J. – ANDREWS D.A., *Risk-Need-Responsivity. Model for Offender Assessment and Rehabilitation*, in *Public Safety Canada*, 2007

riabilitazione grazie a un trattamento basato sul comportamento cognitivo e il monitoraggio dopo il rientro in comunità.

Gli algoritmi predittivi della pericolosità criminale sono, inoltre, impiegati negli Stati Uniti d'America da oltre dieci anni. In particolare, in molti degli Stati è previsto che le decisioni prese dalla Corte possano, oppure addirittura debbano in taluni casi, tenere conto dei risultati forniti dall'algoritmo. Uno strumento predittivo molto diffuso negli Stati Uniti è il software COMPAS (C*orrectional Offender Management Profiling for Alternative Sanctions*), elaborato e commercializzato da una società privata (Northpointe, da gennaio 2017 ridenominata Equivant).[221] Questo algoritmo ha destato pareri discordanti e perplessità sulla sua effettiva accuratezza e imparzialità, attingendo da un ampio database che abbraccia anche periodi storici in cui la tendenza alla discriminazione etnica era particolarmente marcata.[222] Questo strumento, benché fortemente esemplificativo della applicazione da algoritmo, appare limitato anche in termini di trasparenza a causa del segreto industriale, che non permette di assicurare dettagli, a volte necessari, sul suo funzionamento non solo agli imputati ma anche ai giudici.

L'impiego del software COMPAS è al centro del dibattito relativo a una famosa sentenza della Corte Suprema del Wisconsin[223], la quale si pronunciò sull'appello di Eric Loomis condannato a sei anni di reclusione. La pena è stata determinata dai giudici considerando gli output del programma COMPAS, strumento dedicato alla previsione del rischio di recidiva e individuazione delle esigenze specifiche del soggetto, che aveva individuato Loomis come soggetto ad alto rischio di recidiva. La Corte, prima della sentenza sulla determinazione della pena, aveva ordinato un *Presentence Investigation Report* (PSI), ossia una relazione contenente gli esiti delle investigazioni sull'imputato e la sua storia personale, che identificassero le circostanze di applicazione della pena. Proprio a causa del già citato segreto industriale a cui soggiace l'algoritmo di IA, il COMPAS ha sollevato ampie critiche sulla sua trasparenza e reale capacità di predizione. La Corte Suprema ha negato che vi fosse una violazione del principio del giusto processo a causa di questo e che fosse possibile per l'imputato, attraverso il manuale d'uso, mettere in relazione input e output, quindi i risultati finali che calcolano il rischio di recidiva. Il COMPAS è stato quindi ritenuto legittimo, sulla base dei risultati di testi di altri stati americani, come mezzo di calcolo affidabile con la specificazione che i tribunali circondariali hanno il dovere di mettere in relazione i risultati del programma con lo specifico soggetto. In molti Stati la legislazione prevede la considerazione, spesso obbligatoria, di strumenti predittivi da parte delle Corti ed è utile esaminare il *Public Safety Assessment* (PSA) la cui finalità è la garanzia su un funzionamento senza opacità e che capace di cancellare le discriminazioni prodotte dal COMPAS sulla base degli effetti distorcenti causati dai dati concernenti la situazione

[221] BASILE, *Intelligenza artificiale e diritto penale*, cit., 18
[222] D'AGOSTINO, *Gli algoritmi predittivi per la commisurazione della pena*, cit., 365
[223] Corte Suprema del Wisconsin, *State v. Loomis*, 13 luglio, Wisconsin, 2016, § 53-54.

socioeconomia, razziale e di genere.[224] Strumento utilizzato in caso di applicazione di misure cautelari personali o di rilascio su cauzione e di ausilio al giudice nella decisione sulla libertà del soggetto, prima del rinvio a giudizio e nel dibattimento quando si tratti di stabilire la pena a seguito della sentenza di condanna[225].

In relazione al caso Loomis c'è chi pone l'accento su quanto indicato dalla corte suprema del Wiscosin sul fatto che il giudice rimanga sempre un elemento umano necessario proprio per considerare con la sua discrezionalità le peculiarità del soggetto che si trova sotto processo, anche considerando quanto la Corte americana abbia sostenuto sul fatto che lo scopo del COMPAS sia quello di individuare da una parte il rischio di reiterazione e valutarlo e dall'altra i bisogni del soggetto. Tali tipi di pronunce si fondano sul presupposto che un algoritmo, creato in modo appropriato, possa perfezionare le decisioni predittive del giudice uomo che ha una esperienza limitata e questo andrebbe a eliminare le disparità di razza e ridurre la popolazione carceraria. [226] Al contrario alcuni autori sostengono che dato che la desunzione di pericolosità dell'individuo si fonda su quanto deciso nel passato, vi sia un contrasto, per esempio, con quando sancito dalla Costituzione Italiana in riferimento al principio di individualizzazione del trattamento sanzionatorio[227] e che si finisca per rinnegare la funzione rieducativa della pena nel momento in cui l'algoritmo utilizzi informazioni su precedenti penale e condanne.[228]

Il rischio che emerge dal caso Loomis è che i giudici arrivino a fare troppo affidamento sui programmi e potrebbero essi stessi essere soggetti a un bias, il cosiddetto "*automation bias*", per il quale sarebbero influenzati dal risultato del programma nella formazione della loro opinione e che potrebbe condurre alla sostituzione del giudice da parte del sistema predittivo.[229] Inoltre, l'imputato sembra essere minacciato nei suoi diritti e potrebbe, sulla base degli algoritmi predittivi, essere giudicato per quanto potrebbero fare in futuro piuttosto che su quanto hanno commesso, sostenendo che l'uso di programmi predittivi avrebbe un posto legittimo nell'utilizzo in fase di applicazione della sentenza quanto la responsabilità sia già stata accertata[230]

In relazione alla posizione dell'imputato, in tale ottica processuale, vi sono diritti su cui necessario rispetto è di particolare rilevanza, a partire dal diritto di difesa, difficilmente esercitabile se non si può conoscere su quali elementi si basi il risultato fornito dal giudice. Tale diritto è legato a quello di accedere all'algoritmo e, quindi, di

---

[224] GIALUZ M., *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *Diritto Penale Contemporaneo*, 2019, 7
[225] D'AGOSTINO, *Gli algoritmi predittivi per la commisurazione della pena*, cit., 358
[226] KLEIBERG J. – LAKKARAJU H. – LESKOVEC J.et al., *Human Decision and Machine Predictions*, in *The Quarterly Journal of Economics*, 2018, 237
[227] Costituzione – art. 27, co 1,3
[228] MAUGERI*, L'uso di algoritmi predittivi per accertare la pericolosità sociale*, cit., 13-14
[229] FREEMAN K., *Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in State v. Loomis*, in North Carolina Journal Of Law & Technology, 2016, 18, 98
[230] FREEMAN, *Algorithmic Injustice*, cit., 65

conoscere la relativa logica e funzionamento specifico, come se fosse un elemento di prova e di cui dovrebbe essere assicurata l'accessibilità, che anche a livello internazionale viene fissata dal GDPR[231], in accordo al quale sono accessibili anche la qualità dei dati e quanto conti ogni variabile.

L'impiego di algoritmi predittivi, come sin qui illustrato, è di grande interesse anche a livello europeo. In particolare, il Consiglio d'Europa nel 2018 ha pubblicato uno studio denominato "Algoritmi e diritti umani" e la "Carta etica Europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti". Quest'ultima richiede la conformità con il principio del rispetto dei diritti fondamentali quando venga creato e messo in uso uno strumento e un servizio di IA e, in particolar modo, si fa riferimento al soggetto che sviluppa il software, il quale è fondante per il funzionamento dell'algoritmo. Il richiamo a due convenzioni quale quella dei diritti dell'uomo e quella sulla protezione dei dati sensibili da un trattamento automatizzato evidenzia l'interesse che desta l'utilizzo dell'IA nella giurisdizione anche a livello europeo. Per quanto concerne l'ambito di utilizzo degli algoritmi predittivi in merito alla previsione giudiziale nell'ordinamento nazionale un aspetto di controversia riguarda il ruolo della IA come mero strumento di raccolta di documenti, utile per la ricerca della giurisprudenza, o come ausilio attivo nell'individuazione di linee-guida ed elementi di supporto alla previsione del giudizio su un determinato fatto. [232]

Relativamente al processo, una linea di pensiero[233] ravvisa negli algoritmi predittivi una potenziale utilità per la strategia processuale dell'imputato in rapporto ai possibili esiti dibattimentali, ove questo possa scegliere i riti speciali alternativi al rito ordinario, specialmente quelli caratterizzati da attività tipizzate e ripetitive per cui le previsioni algoritmiche fornirebbero elementi di quasi certezza in relazione all'esito del dibattimento. Un esempio potrebbe essere il *decreto penale di condanna*[234] in relazione al quale l'imputato ha la possibilità di accettare o opporsi al decreto o anche nel considerare la convenienza del *patteggiamento*[235] per cui, con l'ausilio dell'algoritmo, potrebbe individuare la probabilità del consenso del pubblico ministero (PM) o che il giudice concordi sulla sanzione discussa nel patteggiamento e la ritenga congrua. Proprio per individuare la statistica decisionale sulle richieste presentate e accolte su reati simili dal giudice, l'algoritmo predittivo rappresenta un utile supporto. L'analisi del giurista Paulesu individua anche quali sono i riti speciali in cui l'algoritmo è

[231] Regolamento (UE) 2016/679, *General Data Protection Regulation* (GDPR), cit., agli art. 13, *Dati personali raccolti presso l'interessato: informazioni da fornire*, art. 15, *Diritto di accesso dell'interessato*

[232] RICCIO G., *Ragionando sulla intelligenza artificiale e il processo penale* in *Archivio Penale*, 2019, 11

[233] PAULESU P.P., *Intelligenza artificiale e giustizia penale. Una lettura attraverso i principi*, in *Archivio Penale*, 2022, 21-22

[234] *decreto penale di condanna* è un procedimento speciale che permette di saltare udienza preliminare e dibattimento che viene disposto su richiesta del PM quando ritiene che possa applicarsi solo la pena pecuniaria, sostituendo quella detentiva, a meno che non si debba applicare una misura di sicurezza

[235] *patteggiamento* o applicazione della pena su richiesta delle parti è un accordo tra PM e imputato sull'applicazione da parte del giudice di una pena di reclusione anche congiuntamente a una pecuniaria

difficile che possa fornire previsioni affidabili, come il *giudizio abbreviato*[236] e il *procedimento con messa alla prova*[237].

Con tale quadro in mente, chi scrive ritiene che l'uso degli algoritmi predittivi possa certamente avere un'utilità in quei casi in cui i dati siano semplici, come sopra citato, ma nel valutare la pericolosità risulta essenziale il coinvolgimento della componente umana e della sua discrezionalità.

Un nodo di difficile scioglimento è quello che concerne l'uso degli algoritmi da parte del giudice in ragione del citato *automation bias* e, forse, una soluzione potrebbe essere che prima il giudice formi la sua decisione e che il risultato dell'algoritmo, qualora sia adeguatamente trasparente, venga presentato e spiegato da un essere umano (anche un esperto o una figura *ad hoc*) o, se dal sistema di IA stesso, successivamente alla decisione non ancora formalizzata del giudice. In questo modo il giudice potrebbe formare una sua opinione prima di considerare il risultato dell'algoritmo attraverso un meccanismo comparativo tra la sua opinione e l'output algoritmico. Tale approccio determinerebbe certamente un "doppio passaggio" nel processo decisionale del giudice, ma potrebbe essere di ausilio alla compensazione dell'*automation bias*,

Infine, ad avviso di chi scrive, come per tutta la IA, la ponderazione e la componente umana sono necessarie per un bilanciamento tra decisioni algoritmiche e umane e l'attenzione rivolta alla discriminazione e alla ricerca di neutralità dell'IA possa essere di ispirazione per porne altrettanta sulla componente umana.

7. Autoria in caso di scelta di computer e software.

Nella declinazione delle problematiche e della individuazione delle responsabilità nel mondo dei sistemi di IA e dei relativi algoritmi si è evidenziata la complessità nella relazione tra i vari soggetti che popolano il ciclo di vita del sistema. La complessità diventa ancora più marcata quando il sistema si basa su machine o deep learning, con evoluzione in parte o del tutto imprevedibile delle azioni, a valle di un ciclo di auto-apprendimento. La natura non umana ma certamente autonoma del sistema rende complessa una sua collocazione in ambito sociale, etico e giuridico. A testimonianza delle prestazioni elevate di questi algoritmi, in particolare in termini di velocità nello svolgimento di azioni comparata con quelle dell'operatore umano, si considera l'acquisto, attraverso i già citati programmi informatici di tipo bot, di biglietti di eventi al fine di creare un mercato parallelo in cui rimetterli in vendita traendone, inoltre, un

[236] *giudizio abbreviato* permette di saltare il dibattimento poiché il giudice dell'udienza preliminare, nel corso della stessa, prenderà la decisione

[237] *procedimento di messa alla prova* è una causa estintiva del reato di possibile attivazione già dalla fase delle indagini preliminari. in presenza di specifici requisiti, se il periodo di "messa alla prova" ha esito positivo

profitto.[238] Se, poi, il contesto operativo ove l'algoritmo intelligente e autonomo opera è quello finanziario, la situazione assurge a livelli di complessità ai limiti della ingestibilità.

In ambito finanziario, infatti, la distinzione tra azioni operate dalla componente umana e quelle eseguite da strumenti e piattaforme informatiche sta diventando sempre più difficile. La componente informatica, infatti, sempre più dotata di intelligenza e autonomia, investe nel mercato in modo indipendente dalle istruzioni di operatori umani per reagire ai mutamenti che investono i contesti in cui operano. Sulla scena dei mercati finanziari, ad oggi, le operazioni vengono condotte da programmi informatici, la cui decisione si fonda su calcoli matematici operante in autonomia. Il soggetto che viene quindi a definirsi è *l'High Frequency Trading* (HFT), che nel compimento di operazioni riporta il rischio di far oscillare in modo rapido e improvviso i prezzi sui mercati finanziari, quali la manipolazione del mercato, con la peculiarità di non determinare alterazioni del valore sostanziale di quanto era oggetto di contrattazione.[239]

Nell'ottica penalistica i "*traders ad alta frequenza*" diventano *decision makers*, il che implica la necessità di rilevare che, rispetto ai soggetti nel cui interesse agiscono quali gli intermediari finanziari, hanno una autonomia operativa.[240] Questi algoritmi sono quindi detentori della capacità di scelta, la quale culmina nella repentina applicazione della strategia di investimento in una operazione effettiva. Ciò significa che vi è stata una selezione tra diverse possibili alternative attraverso l'analisi di variabili sia di carattere matematico che quantitativo. Il cosiddetto "*trader algoritmico*" opera dunque, per così dire, con poca sensibilità economica rispetto a un operatore umano, che considererebbe fattori diversi preventivamente al suo agire sul mercato. L'utilizzo di tale algoritmo e della conseguente automazione delle decisioni su azioni a carattere finanziario, secondo parte della dottrina, determina una difficoltà di attribuzione del dolo del singolo fatto di reato, in virtù del fatto che le scelte sono assunte dal software.

Il *market abuse* provocato da un HFT è un esempio di come si perda la dimensione del dolo, data la «rottura di *autoria* tra transazione finanziaria ed operatore fisico».[241] La turbativa del mercato che si viene a creare è dovuta, per una parte della dottrina, proprio all'affermarsi dell'HFT nella convinzione che questi mini il valore informativo e segnaletico dei prezzi di mercato. La maggior parte degli autori, invece, ritiene che il trader algoritmico non determini alcun pregiudizio ma che, anzi, velocizzi l'incorporazione delle informazioni sui prezzi e ne riduca il grado di volatilità.[242] A prescindere da queste due opposti orientamenti, vi è un sottinteso accordo sulla capacità

[238] BASILE, *Intelligenza artificiale e diritto penale*, cit., 26
[239] BASILE, *Intelligenza artificiale e diritto penale*, cit., 26
[240] CONSULICH, *Il nastro di Mobius*, *Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, 2007, 206
[241] CONSULICH, *Il nastro di Mobius*, cit., 232
[242] CONSULICH, *Il nastro di Mobius*, cit., 203

degli HFT di amplificare il risultato di una manipolazione che altri abbiano commesso in un tempo anteriore.[243]

Il Regolamento Europeo 596/2014, a tal proposito, si poneva il compito di poter efficacemente contrastare queste «nuove forme di negoziazione o nuove strategie potenzialmente abusive» con nuove misure concernenti la manipolazione del mercato. Il reato di manipolazione del mercato prevede la presenza di una condotta vietata che riporti una informazione ingannevole e si sostanzi in una lesione o messa in pericolo delle informazioni a conoscenza degli investitori, ulteriori rispetto a chi commette il reato.[244] A fronte di questo, gli HFT si presentano come una possibilità di manipolazione, sia che gli algoritmi vengano programmati a monte in maniera illecita, sia che l'operazione illecita diventi informazione per gli altri operatori sul mercato. L'effetto è quindi quello di una amplificazione della manipolazione rituale, essendo una delle caratteristiche degli HFT anche la evidente velocità di azione sul mercato. La problematica a livello di attribuzione di responsabilità risulta elevata quando si considera l'eventualità di una persona fisica che non abbia la piena rappresentazione e volizione delle operazioni che vengono attuate effettivamente dall'algoritmo. Si tratta del caso in cui vengano impartite delle istruzioni illecite nella fase di programmazione dal programmatore stesso o dall'intermediario nel momento dell'introduzione sul mercato. Non vi è, infatti, stata alcuna indicazione specifica data all'algoritmo che riguardi titolo, momento o contesto di compimento. Questi elementi non risultano sufficienti all'attribuzione del dolo alla persona fisica, evidenziando una lacuna di tutela a livello penale. Al contrario, questa lacuna viene meno quando avvengano instabilità all'interno del mercato causate da fattori esterni e l'HFT reagisca in maniera distorsiva, non essendo la persona fisica considerabile come responsabile.

Permane la questione dei meccanismi di imputazione, sui quali Consulich si esprime indicando come possibilità l'applicazione del protocollo dell'"*actio libera in causa*" che riguarda «l'imputazione di responsabilità agli attori per azioni non libere in sé stesse, ma libere nelle loro cause».[245] In ottemperanza al quale, per evitare di applicare un principio di presuntiva colpa si mantiene la componente involontaria dell'atto senza attribuirgli connotati intenzionali. Esso opera secondo quello che viene definito il *tracing principle*, secondo la dottrina americana, per cui bisogna ricercare la traccia che determini la responsabilità dell'azione riconducibile alla consapevolezza e alla previa libera scelta, mancando la volontà anti-doverosa.

---

[243] STRAMPELLI G., *L'informazione societaria a quindici anni dal t.u.f: profili evolutivi e problemi,* in *Rivista societaria*, 2014, 1002

[244] *Testo unico delle disposizioni in materia di intermediazione finanziaria* (TUF), d.lgs. 24 febbraio 1998, n. 58, art. 185 «Chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, è punito con la reclusione da uno a sei anni e con la multa da euro ventimila a euro cinque milioni».

[245] DIMOCK S., *Actio libera in causa*, in *Crini. Law and Philos.*, 2013, 7, 550

Da un approfondimento delle attuali strutture regolamentari e tecnologiche dei mercati, emerge come gli HFT sfruttino efficacemente sia gli elementi a carattere informativo che le carenze di efficienza del sistema attraverso una serie di abili strategie. Lo sfruttamento dei vantaggi tecnologici e informativi da parte degli HFT nasce dal pagamento di servizi costosi, quali ad esempio la cosiddetta *colocation*[246] delle infrastrutture dati, che forniscono preziose informazioni ed enormi vantaggi in termini di velocita e che possono essere utilizzati anche per pratiche illegali in relazione alle operazioni degli investitori istituzionali. Pertanto, si è venuto a creare un mercato a "due livelli", proprio a causa del dislivello informativo il cui sfruttamento da parte degli HFT diventa predatorio nei confronti degli investitori istituzionali. [247]

La conoscenza approfondita di tali strategie è cruciale per offrire agli organi regolatori i dati attraverso cui predisporre gli strumenti per minimizzare o annullare conseguenze potenzialmente pericolose e dannose per la qualità del mercato, non impedendo, però, la realizzazione di quelle che costituiscono un vantaggioso contributo per aumentarne liquidità ed efficienza. In alcune di queste analisi si presuppone che gli HFT siano addirittura onniscienti e, dunque, in grado di conoscere le variazioni future dei vari titoli parcellizzate in intervalli di tempo ridottissimi, che solo un approccio HFT riesce a sfruttare appieno in modo vantaggioso.[248] Ricordando che dietro l'approccio HFT c'è l'algoritmica di IA, si comprende appieno la dicotomia più volte evidenziata in questa trattazione che la IA comporta in ogni suo dominio applicativo.

Per affrontare tale fenomeno e inquadrarlo in un ambito di regolamentazione, bisogna innanzitutto tenere conto che le norme che ad oggi tipicamente disciplinano i mercati finanziari sono sagomate sugli investitori "fisici" i quali, essendo umani, sono in questo nuovo contesto degli *slow traders*. Le attuali norme, quindi, non sono in grado di regolamentare gli HFT in ragione della differenza "strutturale" che ormai caratterizza gli operatori finanziari umani e i trader algoritmici che operano sul mercato. La reazione degli ordinamenti di Paesi, quali gli Stati Uniti, che si sono trovati a dover contrastare tale fenomeno non è stata tempestiva come sarebbe stato necessario data la segnalazione di criticità sollevata dalle autorità regolamentari dei mercati.[249] Solo recentemente il Dipartimento di Giustizia statunitense ha dato conferma di una attività investigativa a carattere esplorativo volta a verificazione la effettiva violazione da parte degli HFT della normativa in materia di *insider trading*[250]. I trader, che si sono

[246] *colocation*: nonostante il vasto impiego del cloud per la collocazione dei dati, avere un data center di tipo proprietario rappresenta sempre un elemento strategico e funzionale per molte aziende. Data, tuttavia, la complessità e i costi di gestione dei data center proprietari, sono in espansione i servizi di "co-location" o "housing" della propria infrastruttura dati presso data center esterni.

[247] ADRIAN J., *Informational Inequality: How High Frequency Traders Use Premier Access To Information To Prey On Institutional Investors*, in *Duke Law & Technology Review*, 2016, 14, 256-279

[248] PORRO A., *High Frequency Trading*: *una panoramica*, in *Questioni di Economia e Finanza. Banca d'Italia*, 2013, 34, 38

[249] CONSULICH, *Il nastro di Mobius*, cit., 204

[250] *insider trading* sfrutta la conoscenza di informazioni relative alla quotazione dei titoli non ancora di dominio pubblico, per effettuare operazioni in Borsa

illecitamente avvalsi di algoritmi degli HFT, sono stati soggetti ad un'azione a carattere repressivo, frequentemente correlate da indagini penali per *security fraud*[251] e *market manipulation*[252], da parte della SEC[253] e la Commodity Futures Trading Commission[254].

In ambito europeo il fenomeno è stato inquadrato dalla Direttiva 2014/65/UE[255] in materia ai mercati degli strumenti finanziari e prevede l'obbligo per gli Stati Membri di assicurarsi l'introduzione dei *circuit breakers* provvedimenti automatici che si attivano per bloccare contrattazioni di titoli quando vi sia eccesso di rialzo o di ribasso (del 5% del prezzo) in modo che i sistemi algoritmici, inclusi quelli degli HFT, non pregiudichino il regolare andamento del mercato. Le finalità europee risiedono nell'auspicio di fornire misure sempre più adeguate a relazionarsi con nuove forme di negoziazione e metodologie con potenzialità di abuso.

In conclusione, ad opinione di chi scrive diventa necessaria una definizione precipua della attribuzione di condotta illecita in caso di utilizzo consapevole o meno di algoritmi, quali quelli illustrati in questo capitolo. Infatti, si ritiene che in vista di una sempre maggiore penetrazione della tecnologia e, in particolare, degli algoritmi di IA nella vita quotidiana di cittadini e istituzioni, sia cruciale la diffusione della conoscenza tecnica basilare a tutti i soggetti interessati. Questo perché, in futuro, la permeazione della intelligenza artificiale nella nostra società andrà gradualmente a incrementarsi coinvolgendo sempre più ambiti, richiedendo quindi una tutela efficace e flessibile rispetto all'evoluzione che accompagna da sempre la tecnologia.

[251] *security fraud* avviene sui titoli ed induce gli investitori ad agire sul mercato sulla base di informazioni non veritiere

[252] *market manipulation* corrisponde al tentativo intenzionale di interferire con l'operatività regolare del *free market*, configurandosi come abuso di mercato

[253] (*SEC*) *Securities and Exchange Commission* è l'ente federale statunitense preposto alla vigilanza della borsa valori che regola la sicurezza del mercato».

[254] (*CFTC) Commodity Futures Trading Commission* fornisce regole standardizzate che accrescano l'efficacia e il rilievo della integrità e la resilienza dei mercati dei contratti a termine standardizzati (o futures) che prevedono acquisto di una attività derivata differita e ad un prezzo prestabilito

[255] Direttiva 2014/65/UE, *Market in financial instruments directive* (MiFID II), del 15 maggio 2014, art. 48, *Resilienza dei sistemi, interruttori di circuito e negoziazione elettronica*

CAPITOLO II – IA NELLA PUBBLICA SICUREZZA: FACE RECOGNITION E MASS SURVEILLANCE

SOMMARIO: 1. Introduzione al riconoscimento facciale e alla sorveglianza di massa. – 1.1. *(Segue):* considerazioni critiche. – 2. Diritti fondamentali e pubblica sicurezza. – 3. Data protection e aspettativa di privacy. – 4. Bilanciamento fra diritti e sicurezza. – 4.1. *(Segue):* diritti e sicurezza nel GDPR. – 4.2. *(Segue):* i principi del GDPR. – 4.3. *(Segue):* Gruppo di lavoro "Articolo 29". – 4.4. *(Segue):* bilanciamento e GPDP. – 4.4.1. applicazioni concrete e dottrina sul SARI. – 4.5. *(Segue):* la data retention. – 5. Trattamento dei dati per finalità di contrasto. – 5.1. *(Segue):* diritti nella Direttiva 2016/680 e recepimento. – 6. Considerazioni su ammissibilità, compiutezza e termine di conservazione dei dati. – 6.1. *(Segue):* la visione del CGUE ed elementi di riflessione.

1. Introduzione al riconoscimento facciale e alla sorveglianza di massa.

Come mostrato nel Capitolo I, gli algoritmi di intelligenza artificiale contemplano una vasta gamma di ambiti applicativi che aumentano, con il passare del tempo, sia per gli enormi e continui progressi della tecnologia IA che per la capacità della "componente umana" di concepire, sviluppare e attuare la loro integrazione nelle applicazioni di interesse. Il dominio applicativo della IA su cui si concentra questa trattazione è di particolare criticità, riguardando i metodi che consentono di risalire alla identità di una persona partendo da una serie di grandezze rilevate da vicino oppure a distanza, consapevolmente oppure no da parte del soggetto osservato, e che hanno, come finalità ultima, la cosiddetta *sorveglianza di massa* (*mass surveillance*). Una delle finalità cardine della sorveglianza di massa è la prevenzione dei reati e la garanzia della sicurezza pubblica, anche se durante la pandemia da COVID-19 è stata anche impiegata, attraverso strumenti mirati allo scopo, per il contenimento della sua diffusione.[256] L'identità di una persona può essere determinata, anche in tempo reale, per esempio, attraverso i suoi tratti somatici, impiegando ed elaborando opportunamente foto e video. Questa tecnica è detta di *riconoscimento facciale* o "*face recognition*" in senso stretto e, come già anticipato[257], l'impiego di algoritmi di IA nel contesto del "*predictive policing* trova applicazione, tra l'altro, proprio il *riconoscimento facciale* dei soggetti coinvolti.

Il riconoscimento facciale trae fondamento dalla *disciplina biometrica*, ove lo studio di parametri a carattere biofisico si traduce nella loro misura e nella comprensione delle relative modalità di funzionamento, nonché nella capacità di provocare comportamenti desiderati in sistemi tecnologici di interesse. Il riconoscimento biometrico, sulla base di hardware e software opportunamente progettati, consente l'identificazione di una persona in base a determinate caratteristiche biologiche e comportamentali. Le caratteristiche biologiche generalmente impiegate sono: l'impronta digitale, la retina o

[256] HOSSAIN M.S. – MUHAMMAD G. – GUIZANI N., *Explainable AI and Mass Surveillance System-Based Healthcare Framework to Combat COVID-19 Like Pandemics*, in *IEEE Network*, 2020, 128-129
[257] *supra* Capitolo I § 6

l'iride, la voce e i lineamenti del viso. Tali parametri sono, in linea di principio, unici e non trasferibili da un individuo all'altro. Il riconoscimento può avvenire anche in base ad altre peculiarità della persona, che vanno dal sesso, all'etnia fino all'andatura, il DNA e persino l'emotività, come accennato in precedenza[258]. Inoltre, come anticipato[259], il riconoscimento facciale opera in modo automatico l'identificazione oppure la conferma di identità di una persona sulla base del suo volto, impiegando l'analisi e il confronto di modelli basati sui contorni facciali. I valori misurati rispetto alla variabile associata a determinati punti del volto concorrono così alla identificazione univoca dell'individuo.

Attraverso la creazione di un database di immagini facciali, l'algoritmo di riconoscimento elabora automaticamente le immagini e le confronta per giungere alla identificazione accurata e rapida dell'individuo o degli individui di interesse. In un senso più ampio, il riconoscimento facciale comprende tutti gli strumenti software e algoritmici necessari per ricostruire non solo il volto ma anche la sua posizione, per effettuare l'elaborazione dell'immagine fissa o in movimento e, infine, il riconoscimento.[260]

Gli albori del riconoscimento facciale risalgono agli anni Cinquanta con una evoluzione che ha visto l'impiego sia del machine learning, che delle reti neurali[261] e, oggi, ha nel deep learning lo strumento per il raggiungimento delle prestazioni più avanzate.[262] Secondo l'Istituto Nazionale di Standard e Tecnologie (NIST), l'incidenza dei falsi positivi nei sistemi di riconoscimento facciale è stata dimezzata ogni due anni dal 1993 e, a fine 2011, era solo dello 0,003%. In particolare, per identificare un volto è necessario addestrare le reti neurali in modo che apprendano come riconoscere un essere umano dall'analisi delle immagini.

Le reti neurali possono essere utilizzate per confrontare i milioni di volti memorizzati nel database in tempi rapidissimi e per consentire al sistema di apprendere autonomamente nuove informazioni utili per le successive analisi, portando i sistemi di riconoscimento facciale a un livello sempre più evoluto. La caratteristica della rete neurale, infatti, come già illustrato[263], è quella di apprendere tramite esperienza, similmente a quanto avviene nel cervello umano, e di generalizzare le conoscenze acquisite per poter fare previsioni. Le grandi reti neurali necessitano di una enorme capacità di elaborazione e, in tal senso, Intel ha recentemente annunciato la prima famiglia di processori *Nervana Neural Network Processor* (NNP), nata appositamente

[258] *supra* Capitolo I § 3
[259] *supra* Capitolo I § 3.1
[260] LI X., MU X., LI S., PENG H., *A Review of Face Recognition Technology* in IEEE Access, 8, 2020, 139113.
[261] *supra* Capitolo I § 1
[262] TEOH K.H. – ISMAIL R.C. – NAZIRI S.Z.M. – HUSSIN R. – ISA M.N.M. – BASIR M.S.S, *Face recognition and Identification using Deep Learning Approach* in *Journal of Physics: Conference Series*, 2021, 4
[263] *supra* Capitolo I § 1

per l'Intelligenza Artificiale.[264] Il DL[265], poi, grazie ai suoi meccanismi avanzati e autonomi di emulazione del cervello umano, è in grado di sviluppare meccanismi automatici di apprendimento da cui il riconoscimento facciale può e potrà sempre più in futuro trarre enormi benefici di efficacia ed efficienza.[266] Fino ad oggi, il riconoscimento facciale è stato utilizzato prevalentemente in ambito sicurezza, ma gli ambiti applicativi stanno rapidamente evolvendo, proprio grazie alla integrazione degli algoritmi di intelligenza artificiale. L'impiego di questa tecnica di riconoscimento avrà un enorme impatto nell'accesso a smartphone, pagamenti digitali, app e non solo. La velocità di elaborazione degli algoritmi IA è, come in altri scenari applicativi riportati nel Capitolo I, il vero elemento di svolta rispetto a operazioni umane o semi-automatiche.

Il sistema di riconoscimento facciale basato su IA presenta una serie di vantaggi ma suscita anche varie perplessità, con potenziali ricadute in ambito etico e legale. Il principale vantaggio è, come anticipato, la mancanza di contatto fisico tra il soggetto da riconoscere e il sistema di riconoscimento, ma è anche uno degli elementi di potenziale perplessità. Le immagini facciali vengono, infatti, catturate a distanza e la loro elaborazione può avvenire senza alcuna consapevolezza da parte del soggetto osservato. Il sistema opera, dunque, in modo quantomai efficace per le finalità di sicurezza, ad esempio relative alla partecipazione del soggetto a un evento specifico per data e luogo. Al contempo, l'algoritmo è generalmente poco o per nulla trasparente e potrebbe incorrere in errori di non facile individuazione, che potrebbero a loro volta causare effetti discriminatori o violazione dei diritti dell'individuo. Come già evidenziato per altri ambiti applicativi[267], anche nel riconoscimento facciale è necessario che l'algoritmo sia progettato in modo da massimizzarne correttezza, trasparenza e assenza di polarizzazione. Si affronteranno tali aspetti in dettaglio nell'ambito del bilanciamento tra i diritti dell'individuo e la pubblica sicurezza, anche alla luce delle normative poste a tutela di tali diritti, quali il GDPR[268].

Il riconoscimento facciale può operare con diversi livelli di complessità, a partire dalla tecnica più di base impiegata, ad esempio, in applicazioni "social", quali Instagram e Snapchat, dove la fotocamera dello smartphone impiega un algoritmo per la ricerca di volti, quindi un prodromo della vera e propria *face recognition*. Quest'ultima è, invece, alla base dello sblocco con il volto di dispositivi personali, per esempio uno smartphone, che scatta una foto del viso e ne misura la distanza tra i tratti, in modo tale che ogni volta che si vuole accedere esegue una procedura di controllo e conferma della identità del soggetto. Se l'identificazione di un soggetto è, invece, necessaria per

[264] MARIA M., *Riconoscimento facciale: che cos'è e perché rivoluzionerà gli smartphone*, in Network Digital 360, 2022
[265] *supra* Capitolo I § 1
[266] TEOH et al., *Face recognition and Identification using Deep Learning Approach*, cit., 3
[267] *supra* Capitolo I
[268] *infra* § 4

finalità legate a sicurezza, polizia ma anche pubblicità gli algoritmi impiegano un database di volti ampio, associando in varie iterazioni un insieme di profili a quello in esame, fino a convergere su quello/quelli che hanno la maggior probabilità di corretta identificazione. Nella maggior parte dei casi il riconoscimento facciale si basa su immagini "piatte" o bidimensionali (2D) che, seppure efficaci per rilevare, per esempio, la distanza inter-pupillare, non possono rilevare la dimensione della profondità, ad esempio utile per determinare la lunghezza del naso. Le immagini facciale 2D, inoltre, si basano sulla luminosità e, dunque, non sono fruibili con illuminazione ridotta, ove aumenta il tasso di errore nell'identificazione. Per migliorare il riconoscimento è possibile ricorrere a una termocamera, che supera il problema del 2D con poca luce, oppure a una tecnologia volumetrica (3D), con aumento della complessità e dei costi.[269] L'uso combinato di rilevamento 2D e 3D aumenta in modo significativo la precisione dell'algoritmo. Come accennato, le potenzialità di un errato riconoscimento saranno trattate in relazione alle normative vigenti[270], evidenziando come esse siano al centro di grandi perplessità relative all'utilizzo non discriminatorio della tecnologia di IA.

I progressi sulle prestazioni degli algoritmi di identificazione basati su parametri biometrici sempre più sfidanti, in particolare quelli di riconoscimento basato sul volto e la relativa applicazione per la sorveglianza di massa procedono celermente, come tutto ciò che attiene al comparto tecnologico della IA e dei suoi domini verticali. Il miglioramento delle prestazioni della IA nei vari ambiti applicativi comporta, in genere, una crescente fiducia da parte di operatori e utenti "fiduciosi"[271] nei benefici della IA, ma questa equazione non è sempre appropriata. Infatti, l'ambito applicativo della sorveglianza di massa attraverso il riconoscimento dei volti ha molti aspetti delicati e la potenzialità di violare consistentemente i diritti delle persone.

1.1. *(Segue):* considerazioni critiche.

L'impiego degli strumenti di *mass surveillance* basati su parametri biometrici è uno degli aspetti trattati nella proposta di Regolamento[272]. In particolare, è di rilevanza per l'ambito della giustizia penale il divieto di identificazione biometrica da remoto in spazi pubblici per funzioni di polizia, se a fini di sorveglianza indiscriminata.[273] Questi sistemi, infatti, ripropongono in modo eclatante la necessità, già rilevata e descritta nella trattazione in relazione a vari domini applicativi della IA, di un bilanciamento tra

[269] ABATE A.F. – NAPPI M. – RICCIO D. – SABATINO G., *2D and 3D face recognition: A survey*, in *Elsevier Pattern Recognition Letters*, 28, 2007, 1885–1906
[270] *infra* § 4
[271] *supra* Capitolo I § 4.1
[272] *supra* Capitolo I § 3, 3.1, 3.2
[273] LAVORGNA – SUFFIA, *La nuova proposta europea per regolamentare i Sistemi di* Intelligenza, cit., 99

i benefici della algoritmica intelligente e la garanzia dei diritti e della imparzialità dei singoli. La sorveglianza di massa, infatti, da un lato è un valido ausilio all'operatività delle forze dell'ordine in casi di vaste e potenzialmente caotiche aggregazioni di folle ma, dall'altro, in presenza di un suo impiego indiscriminato e/o di possibili errori dell'algoritmo di IA, apre a possibili abusi. Su una base di valutazione specifica sui singoli casi in termini della situazione e conseguenze, la proposta sembrerebbe ammettere eccezioni. Anche il riconoscimento facciale rientra in alcuni casi nella catalogazione di sistemi di IA a rischio inaccettabile, in particolare quando l'impiego sia da parte di una autorità pubblica.

La proposta di Regolamento sembra recepire una serie di perplessità e critiche a questo dominio applicativo della IA diffuse a livello Europeo, con richieste di sospensione dell'uso del riconoscimento facciale nei paesi della UE, vista la fallibilità dimostrata in vari casi da questo meccanismo di identificazione e l'invasione nella sfera privata delle persone.[274] [275] Un gruppo di 51 organizzazioni dedicate ai diritti umani ha perfino invitato la Commissione europea a bandire completamente l'impiego della tecnica del riconoscimento facciale per la sorveglianza di massa, senza alcuna eccezione.[276] Inoltre, i Membri del Parlamento Europeo con una Risoluzione[277] si sono opposti all'utilizzo dell'IA da parte della polizia, al fine di combattere il rischio di pregiudizi degli algoritmi e ponendo l'accento sulla necessità di una supervisione umana a cui rimanga il potere decisionale finale, con il supporto di "forti" leggi applicabili in materia di IA.

Alcuni detrattori delle tecniche di mass surveillance sostengono che l'impiego in ambito europeo mostra che l'applicazione si è spostata da misura di contrasto per il terrorismo a controllo indiscriminato dei cittadini, creando dunque una dicotomia tra diritti e sicurezza che, a sua volta, potrebbe essere foriera di conseguenze potenzialmente ampie a livello sociale[278]. D'altra parte, la tecnica verrebbe invece ammessa in alcuni casi speciali, quali, ad esempio, la ricerca di bambini scomparsi o la gestione di minacce e attacchi di natura terroristica, oppure per lo svolgimento di attività legate a indagini su individui sospetti di reati che comportino almeno tre anni di reclusione.[279]

---

[274] JAKUBOWSKA E., *Ban Biometric Mass Surveillance A set of fundamental rights demands for the European Commission and EU Member States*" in *European Digital Rights (EDRI)*, 2020, 10

[275] MONTAG L. et al, The rise and rise of biometric mass surveillance in the EU - Legal analysis of biometric mass surveillance practices in Germany, the Netherlands, and Poland in European Digital Rights (EDRI), 2021, 10

[276] LEPRINCE-RINGUET D., *Facial recognition tech is supporting mass surveillance. It's time for a ban, say privacy campaigners*, in *ZDNET*, 2021, 2

[277] Parlamento Europeo, Risoluzione del 3 maggio 2022, *Intelligenza artificiale nell'era digitale*, 2020/2266 (INI)

[278] MARAS M. H., *The social consequences of a mass surveillance measure: What happens when we become the 'others'?*, in *Elsevier International Journal of Law, Crime and Justice*, 40, 2012, 66

[279] LAVORGNA – SUFFIA, *La nuova proposta europea per regolamentare i Sistemi di* Intelligenza, cit., 99

Va comunque tenuto presente che il concetto stesso di sorveglianza di massa, anche se non basata su IA, ingeneri impatto in ambiti etici, psicologici e perfino commerciali[280] ed è, quindi, immaginabile che il suo impiego attraverso una tecnologia molto pervasiva come la IA possa condurre a conseguenze difficili da prevedere. D'altra parte, sono stati anche riportati risultati confortanti sui benefici della sorveglianza di massa basata su IA in specifici contesti applicativi [281]. L'opinione di chi scrive ricalca quanto espresso dai membri del Parlamento Europeo nella Risoluzione sopracitata sulla necessità di una forte base normativa sulla quale innestare una figura di un operatore umano che supervisioni non solo il funzionamento del sistema di IA di sorveglianza ma anche la sua decisione finale.

2. Diritti fondamentali e pubblica sicurezza.

Per poter comprendere come la sorveglianza di massa incida sulle libertà degli individui è utile esplicitare il concetto di diritti fondamentali ed esaminare quali siano le fonti che le tutelano. Sono considerati *fondamentali* i diritti e le libertà che appartengono a tutti gli individui, prescindendo da origine sociale, ideologia e stile di vita. In particolare, guardando all'Unione Europea questi diritti applicano principi quali dignità, equità, rispetto e uguaglianza. I diritti fondamentali sono al centro del progetto europeo e sono stati sanciti nella Carta dei diritti fondamentali, la cui tutela e promozione è affidata alla *European Union Agency for Fundamental Rights* (FRA).

La tutela dei diritti fondamentali dell'uomo si sviluppa su tre dimensioni: a livello nazionale, con la Costituzione, e a livello europeo, attraverso la CEDU e il diritto dell'Unione, oltre alla applicabilità di strumenti internazionali. L'ampliamento della tutela è avvenuto col riconoscimento alla Carta dei diritti fondamentali, da qui in poi "Carta", dello stesso valore giuridico dei trattati e ai diritti garantiti dalla CEDU del valore di principi generali dell'Unione[282]. Sull'adesione dell'Unione alla CEDU sono in corso negoziati formali, anche se i paesi parte dell'UE sono già parte della CEDU,

[280] PANCHANKIS Y, *Mass Surveillance, Behavioral Control, and Psychological Coercion The Moral Ethical Risks in Commercial Devices*, in *AIRCC Publishing Corporation*, 2022, 151

[281] RAJENDRAN L., SHANKARAN R. S., *Bigdata Enabled Realtime Crowd Surveillance Using Artificial Intelligence and Deep Learning*, in *IEEE International Conference on Big Data and Smart Computing (BigComp)*, 2021

[282] Trattato di Lisbona, *Modifiche del trattato sull'Unione Europea e del Trattato che istituisce la Comunità Europea*, 2007/C 306/01, introduzione modifiche all'art. 6 del Trattato sull'Unione Europea (TUE) «L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea […]. L'Unione aderisce alla [CEDU] […] i diritti fondamentali garantiti dalla [CEDU] e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali.»

che se andassero a buon fine determinerebbero la possibilità per i privati di presentare reclami avverso l'Unione davanti alla Corte EDU di Strasburgo.

In tal modo, l'Unione dovrebbe rimediare alle violazioni contestate in virtù della CEDU e ciò permetterebbe di porre le medesime basi sui diritti umani su tutto il continente e garantire la coerenza tra le decisioni della Corte EDU e la Corte di giustizia dell'Unione (CGUE)[283]. Tale considerazione è stata espressa dal Consiglio d'Europa nel 2023 in merito alla complessa vicenda relativa all'adesione dell'Unione Europea alla Convenzione Europea sui diritti dell'uomo e sulle libertà fondamentali.[284]

Sui diritti sanciti dalla Carta vige l'obbligo[285] di interpretazione della loro portata e del loro significato allo stesso modo dei diritti della CEDU, tranne se la Carta prevede una protezione più ampia e, da quanto descritto, emerge come siano fonti distinte ma coordinate. Nello specifico, la carta dei diritti fondamentali è suddivisa in Capi concernenti dignità, libertà, uguaglianza, solidarietà, cittadinanza e giustizia. Il tema del riconoscimento facciale e della sorveglianza di massa sono strettamente interallacciati con i diritti concernenti la libertà dell'individuo, in particolar modo questa trattazione si focalizzerà sulla violazione di tale diritto, in particolare concernente il "rispetto della vita privata e della vita familiare" e la "protezione dei dati di carattere personale, rispettivamente all'articolo 7 e 8 della Carta.

Partendo dalla considerazione che se i diritti fondamentali fossero esercitabili senza alcun limite, quindi al di fuori delle leggi, la garanzia dei diritti dell'uomo diventerebbe probabilmente illusoria, emerge che la loro salvaguardia necessiti di essere in armonia con quanto sancito dall'ordinamento ai fini di una pacifica convivenza. In tal senso il rispetto dell'ordine pubblico[286] assicura a tutti l'effettivo godimento dei propri diritti. L'ordine è mantenuto dall'autorità di pubblica sicurezza[287] la quale, nell'esercizio delle sue funzioni, quando il mezzo per garantire la sicurezza sia un sistema di sorveglianza di massa basato su IA incorre in un rischio potenziale di collisione con i diritti fondamentali.

---

[283] *Corte di giustizia dell'Unione europea* (CGUE), «interpreta il diritto dell'UE per garantire che sia applicato allo stesso modo in tutti gli Stati membri e dirime le controversie giuridiche tra governi nazionali e istituzioni dell'UE», in Sito ufficiale Unione Europea, 2023

[284] Consiglio d'Europa*, Adesione dell'Unione europea alla Convenzione europea dei diritti dell'uomo – Domande e risposte*, in *sito Consiglio d'Europa*, 2023

[285] Carta dei diritti fondamentali dell'Unione europea (CDFUE o Carta di Nizza), 2000/C 364/01, art. 52, par 2

[286] *Brocardi*, voce *Ordine pubblico*, il complesso delle condizioni che assicurano la tranquillità e la sicurezza materiale di tutti i cittadini,

[287] Regio Decreto, 18 giugno 1931, n. 773, *Approvazione del testo unico delle leggi sulla pubblica* sicurezza, (TULPS), art. 1, «l'autorità di pubblica sicurezza veglia al mantenimento dell'ordine pubblico, alla sicurezza dei cittadini, alla loro incolumità e alla tutela della proprietà; cura l'osservanza delle leggi e dei regolamenti generali e speciali dello Stato, delle province e dei comuni, nonché delle ordinanze delle autorità»

Un esempio eclatante di tale labile equilibrio e delle problematiche concernenti la sorveglianza di massa è quello del "Big Brother Watch c. Regno Unito"[288] concernente la conformità delle pratiche adottate dai paesi membri del Consiglio d'Europa[289] alla CEDU. L'inizio di tale caso si ricollega alle dichiarazioni o *rivelazioni* dell'informatico e attivista statunitense, Edward Snowden[290] rilasciate circa dieci anni prima della sentenza, momento in cui sono incominciate le inchieste. Tali rivelazioni concernevano documenti secretati della *National Security Agency* (NSA) e palesarono l'esistenza di programmi di sorveglianza di massa intergovernativi. Sembrerebbe quindi che la raccolta massiva di dati e dei contenuti di comunicazioni, conservati per un periodo di tempo esteso, fossero stati utilizzati per fornire un'analisi di altri Paesi in termini politico-economici. I ricorsi presentati alla Corte EDU da svariate organizzazioni per la difesa dei diritti individuali avviarono nel 2013 il caso che si concluse con decisione della Corte in merito alla violazione dell'articolo 8 della CEDU da parte del *Government Communication Headquarters* (GCHQ)[291] per lo spionaggio di massa dei dati concernenti le comunicazioni.

La violazione del diritto alla vita privata e familiare era avvenuta attraverso il programma *Tempora*, volto ad intercettare i flussi di dati, incluse e-mail, telefonate, e molto altro, in transito nei cavi a fibra ottica, anche se sottomarini[292]. Tali dati venivano poi comunicati all' NSA statunitense, il quale supervisionava il programma *PRISM*[293] e *Upstream*[294]. Tutto questo si verificava rispettando quanto sancito dal *Regulation of Investigatory Powers Act* (RIPA)[295] in merito alla possibilità del Segretario di Stato di autorizzazione intercettazioni come quella in discussione se necessaria a garantire la sicurezza nazionale inglese anche in chiave preventiva. Tale "rete" di intercettazione venne denunciata dall'associazione *Big Brother Watch*[296].

In merito alla intercettazione *preventiva* basata su un "ragionevole sospetto", argomento sul quale i ricorrenti basavano la dimostrazione di legittimità dell'utilizzo della sorveglianza di massa, la Corte sostenne che tale sospetto non permetterebbe un

---

[288] Corte EDU, Grande Sez., sent. 25 maggio 2021, *Big Brother Watch and others c. The United Kingdom,* ric. n. 58170/13, 62322/14, 24960/15

[289] *Consiglio d'Europa*, «sostiene la libertà di espressione e dei media, la libertà di riunione, l'uguaglianza e la protezione delle minoranze. [… e] promuove i diritti umani attraverso convenzioni internazionali» in sito ufficiale *Council of Europe*, 2023

[290] Snowden ha lavorato nella *Central Intelligence Agency* (CIA) in merito a temi di sicurezza informatica dopo un periodo in cui aveva lavorato nello stesso ambito nella *National Security Agency* (NSA). Nel 2013, quando lavorava per una azienda informatica, ha rilasciato dichiarazioni sconcertanti.

[291] *GCHQ* è l'agenzia governativa britannica a capo della sicurezza e dello spionaggio delle comunicazioni

[292] Amnesty International, *Why we're taking the UK government to court over mass spying*, in *Amnesty International UK/Mass surveillance*, 2020

[293] *PRISM* è un programma di sorveglianza elettronica di massima segretezza che gestisce informazioni da varie fonti, tra cui internet

[294] *UPSTREAM* è un programma di intercettazione di traffico telefonico e dati su internet attraverso l'infrastruttura internet domestico e internazionale

[295] *RIPA* disciplina l'uso della sorveglianza segreta da parte degli enti pubblici in Inghilterra

[296] *Big Brother Watch* è un'associazione inglese per la protezione delle libertà civili

funzionamento efficace della sorveglianza. In ragione di ciò, le autorità generalmente non possono conoscere preventivamente quali comunicazioni potranno essere di ausilio nella protezione della sicurezza nazionale, altrimenti la misura di sorveglianza risulterebbe priva di ogni interesse operativo.[297] La Corte espone approfonditamente come il Governo inglese abbia violato l'articolo 8 della CEDU concernente il diritto al rispetto della vita privata e familiare e l''articolo 10 della CEDU sul diritto alla libertà d'espressione, in quanto la sorveglianza dovrebbe essere «accessibile alla persona interessata» e «prevedibile nei suoi effetti».[298]

Inoltre, sarebbe stato di valido ausilio un organismo autonomo che decidesse preventivamente gli ambiti di indagine, quali operazioni dell'intelligence fossero legittime, supervisionandole, nell'ottica di evitare la degenerazione in un controllo governativo senza limiti, indiscriminato e su ampia scala.

In conclusione, la Corte ha evidenziato come la sorveglianza di massa possa essere un mezzo valido[299] per la individuazione di eventuali nuovi pericoli al fine di garantire la sicurezza nazionale e che ogni Stato abbia la possibilità di decidere e agire. Tale margine di apprezzamento può operare solo nel rispetto della necessità e proporzionalità della sorveglianza di massa, aderendo alle salvaguardie indicate dalla stessa Corte a tutela dei diritti fondamentali dell'individuo. Si richiede, a titolo esemplificativo, che si tratti di un reato per cui è prevista la possibilità di intercettazione e i cui soggetti ad essa sottoponibili siano inquadrati in una categoria previamente definita. È necessaria anche la definizione della durata e con quale procedura i dati ottenuti dall'intercettazione verrebbero analizzati, utilizzati e conservati oltre ai casi in cui verrebbero rimossi o eliminati. [300] Se anche una o alcune delle salvaguardie non venissero rispettate è possibile di appurare se la legislazione oggetto della contestazione sia generalmente allineata con le garanzie della CEDU. [301] Da questa vicenda emerge che, per quanto l'interesse pubblico consenta una deroga ai diritti fondamentali dell'individuo, è necessario sancire un limite invalicabile per evitare di sfociar in un abuso da parte dei poteri pubblici. Questo è un caso esemplificativo delle criticità correlate al complesso rapporto tra diritti fondamentali e riconoscimento facciale quale strumento di ausilio alle autorità preposte alla sicurezza pubblica, nonché, della necessità di una *intermediazione umana* nelle pratiche della *face recognition* e delle insorgenti preoccupazioni ad essa collegate.

---

[297] Corte EDU, Grande Sez., sent. 25 maggio 2021, *Big Brother Watch and others c. The United Kingdom,* cit., 301, 92

[298] D'AGOSTINO L., *Sorveglianza di massa, algoritmi e intelligenza artificiale: lo stato dell'arte al livello nazionale ed europeo*, in *Relazione al Seminario "Stati Generali del Diritto di Internet"*, 2021, 3

[299] Corte EDU, Grande Sez., sent. 25 maggio 2021, *Big Brother Watch and others c. The United Kingdom,* cit., 323, 98

[300] D'AGOSTINO, *Sorveglianza di massa, algoritmi e intelligenza artificiale*, cit., 3

[301] ZANIRATO S.*, La Vittoria di Pirro del diritto alla privacy*, in *Strategic Litigation (STRALI)*, 2021

Ad avviso di scrive, l'importanza della componente umana nella intermediazione tra algoritmo e impiego del suo output e, nella fattispecie tra tecnica di riconoscimento biometrico/facciale e sorveglianza di massa e la relativa traduzione nel trattamento dei dati, costituisce un necessario ausilio nel bilanciamento tra diritti e pubblica sicurezza. Si è usato il condizionale perché la reale efficacia della intermediazione umana deve rispondere ad un principio di neutralità ed equità, per evitare la creazione di una bias direttamente collegata allo stesso, sebbene tale requisito non sembri essere facilmente reperibile nell'essere umano.

3. Data protection e aspettativa di privacy.

Come appena descritto la sorveglianza di massa e la sua realizzazione attraverso il riconoscimento facciale pur avendo utili potenzialità di sicurezza pubblica presentano altresì aspetti controversi e potenzialmente lesivi dei diritti degli individui, in particolar modo della privacy. È opportuno evidenziare che la *privacy* è un concetto interconnesso alla *data protection* o protezione dei dati dal quale si distingue in quanto concernente il diritto alla riservatezza di dati a carattere personale che ci si aspetta non vengano divulgati senza il proprio consenso e dai quali vengono esclusi i terzi.[302]

Il trattamento dei dati che consente la identificazione di un soggetto direttamente o indirettamente, o *data protection,* è un diritto fondamentale ai sensi della Carta dei diritti fondamentali[303] per la quale il trattamento dati in linea con le sue finalità richiede il consenso dell'interessato oppure di basi stabilite dalla legge. L'importanza del consenso[304] è evidente anche nel GDPR[305], anche ai fini della dimostrazione da parte del titolare del trattamento della prestazione di tale consenso dell'interessato. Tale prova dell'avvenuto consenso in una dichiarazione scritta deve essere presentata in modo che sia comprensibile e di facile accesso, ma non è vincolante se viola una qualsiasi parte del GDPR stesso. A tutela dell'interessato questi ha la possibilità di revocarlo, sebbene ciò non pregiudichi la liceità del trattamento[306] e di questo sia data conoscenza all'interessato. Come si vedrà il consenso deve essere prestato liberamente ed è richiesta chiarezza.

---

[302] Carta dei diritti fondamentali dell'Unione europea, 18 dicembre 2000, C 364/10, art. 7, «Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni»

[303] Carta dei diritti fondamentali dell'Unione europea, cit., art. 8

[304] Regolamento (UE) 2016/679, GDPR, cit., art. 8, *Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione*, indica la liceità del trattamento dei dati del minore qualora abbia almeno 16 anni, anche se gli Stati membri possono stabilire una soglia di età più bassa ma non inferiore ai 13 anni.

[305] Regolamento (UE) 2016/679, GDPR, cit., art. 7, *Condizioni per il consenso*

[306] *infra* § 4.3

Inoltre, il titolare dei dati ha diritto di accesso e di rettifica sugli stessi e a garanzia del rispetto di tali regole viene preposta un'autorità indipendente. La rivelazione di come, ad insaputa dei cittadini, la privacy sia stata in modo eclatante e ripetutamente violata mette in luce come la strada per un'effettiva e affidabile protezione dei dati personali sia piena di intricati interrogativi. L'importanza del consenso del titolare dei dati, necessaria alla liceità del loro trattamento, è alla base del rapporto con il titolare del trattamento da cui ci si aspetta che i dati forniti vengano impiegati secondo le finalità dichiarate e non in maniera difforme. Considerando tale dinamica, definibile come *aspettativa di privacy*, ben si comprende come il soggetto titolare dei dati oggetto di trattamento nutra delle ragionevoli aspettative in merito a questo sulla base del rapporto che intercorre con il titolare del trattamento. Questi, infatti, nel bilanciare i propri interessi legittimi deve tener conto di tali aspettative dell'interessato, anche quando si tratti, ad esempio, di compiere un ulteriore trattamento che soccomberebbe agli interessi e ai diritti fondamentali dell'interessato, qualora questi non possa ragionevolmente aspettarselo.

Quando si tratti di autorità pubbliche nell'esecuzione dei propri compiti, la cui base giuridica è definita dal legislatore, non è valida la medesima base giuridica per un legittimo interesse del titolare del trattamento e qualora si tratti di un'ulteriore elaborazione, il diritto nazionale o europeo definisce i confini della liceità e compatibilità con il trattamento necessario per compiti di interesse pubblico o per l'esercizio di pubblici poteri del titolare del trattamento. Questo ulteriore trattamento potrà avvenire solo nel rispetto del GDPR e con la doverosa informativa all'interessato delle ulteriori finalità, dei suoi diritti e del suo eventuale diritto di opposizione. [307]

Muovendo da questa considerazione è di ausilio ad una migliore comprensione di tale aspettativa l'articolo 2 ter del Codice Privacy[308] con le ultime modifiche apportate nel 2021 al Capo II. Tale articolo è denominato "Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri" ed individua, al comma 1-bis[309], i soggetti che possono eseguire il trattamento dei dati personali[310]. In particolare, si definisce trattamento dei dati personali quella operazione o insieme di operazioni, effettuate eventualmente, ma non necessariamente, attraverso meccanismi automatizzati, definizione che verrà approfondita nel trattare il GDPR.[311]

---

[307] Regolamento (UE) 2016/679, GDPR, cit., considerando 47, 50

[308] Codice della Privacy, *Codice in materia di protezione dei dati personali,* d.lgs. 30 giugno 2003 n. 196, con modifiche apportate da d.l. 8 ottobre 2021, n. 139 convertito da l. 205/2021 e da d.l. 30 settembre 2021, n. 132 convertito da l. 178/2021

[309] introdotto da d.l. 8 ottobre 2021 n.139, convertito da l. 23 novembre 2021 n. 178

[310] Codice della Privacy, cit., art. 2-ter, co 1

[311] Regolamento (UE) 2016/679, GDPR, cit., art. 6, lett. e) «Il trattamento è lecito solo se e nella misura in cui […] il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento», *infra* § 4

Coloro ai quali è consentito tale trattamento possono esercitarlo anche quando risulti necessario all'adempimento di un «compito svolto nel pubblico interesse» o all'esercizio dei poteri pubblici di cui sono detentori cosicché la tutela di diritti e libertà dei soggetti i cui dati vengono trattati non subisca un «pregiudizio effettivo e concreto». I principi sanciti dal comma 1-bis devono essere esercitati in accordo a quanto sancito in materia di liceità del trattamento all'articolo 6 del GDPR[312]. I soggetti abilitati al trattamento dei dati personali sono l'amministrazione pubblica[313], incluse le autorità indipendenti[314] e le amministrazioni riconosciute con provvedimento annuale dall'ISTAT[315] e, inoltre, le società a controllo pubblico statale, escludendo i trattamenti relativi ad attività nel libero mercato, oppure a controllo pubblico locale, limitatamente ai solo gestori di servizi pubblici.

La comunicazione tra questi soggetti del trattamento dei dati personali, per l'esecuzione di un "compito svolto nell'*interesse pubblico* o connesso all'*esercizio di pubblici poteri*", non può ricomprendere dati relativi a condanne penali e reati[316] e quelli che rivelino, ad esempio, origine razziale o etnica, dati biometrici che identifichino in modo univoco un soggetto, opinioni politiche ed orientamento sessuale.[317] Se non si tratta di questi dati, la comunicazione è invece ammessa. In particolare, il trattamento dei dati personali relativi a condanne penali, reati, misure di sicurezza connesse, sulla base dell'articolo 6, paragrafo 1, può avere luogo unicamente sotto controllo dell'autorità pubblica o se tale trattamento è autorizzato da Unione o Stati membri con appropriate garanzie per gli interessati.

La diffusione e comunicazione dei dati, trattati per finalità di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti con altre finalità di trattamento è ammessa solo se la base giuridica sia una norma di legge, un regolamento oppure si tratti di atti amministrativi generali[318] o quando necessario ai fini del comma 1-bis. Per diffusione si intende il portare i dati personali a conoscenza di soggetti non determinati sia mettendoli a loro disposizione che attraverso la consultazione. La distinzione con la comunicazione risiede nel fatto che quest'ultima riguardi i dati personali di cui si dà

---

[312] *infra* § 4

[313] *autorità pubbliche* per cui si intendono tutte le amministrazioni dello Stato di cui all'art. 1, co 2 del d.lgs. del 30 marzo 2001 n. 165

[314] *autorità indipendenti* possiedono un discreto grado di indipendenza dal potere politico e con una elevata competenza tecnica di cui alla l. 31 dicembre 2009 n. 196, fra cui il Garante per la protezione dei dati personali

[315] ISTAT è l'Istituto nazionale di statistica è un ente di ricerca pubblico

[316] Regolamento (UE) 2016/679, GDPR, cit., art. 10, *Trattamento dei dati personali a condanne penali e reati*

[317] Regolamento (UE) 2016/679, GDPR, cit., art. 9, co 1

[318] D.lgs. 14 marzo 2013, n. 33, *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*, art. 12, co 1 «direttive, circolari, programmi, istruzioni e ogni atto che dispone in generale sulla organizzazione, sulle funzioni, sugli obiettivi, sui procedimenti, ovvero nei quali si determina l'interpretazione di norme giuridiche che riguardano o dettano disposizioni per l'applicazione di esse»

conoscenza a soggetti determinati[319] e di cui è possibile la conoscenza anche in forma di interconnessione, quale il collegamento fra reti di telecomunicazione.

Secondo una linea di pensiero, il periodo del nuovo comma 1-bis[320] che si riferisce al "*pubblico interesse*" e ai "*pubblici poteri*", inserito in fase di conversione del decreto, ridimensiona la portata potenzialmente incisiva della previsione e non amplia le possibilità di trattamenti privacy da parte dei soggetti pubblici, conducendo, con l'inserimento del riferimento all'articolo 6 del GDPR, a una "neutralizzazione" in quanto non è presente una nuova norma sul piano sostanziale. In linea con tale visione, altri sostengono che il rischio di tali innovazioni potrebbero perfino portare allo svuotamento di significato dell'applicazione del GDPR alla pubblica amministrazione. Un'altra linea di pensiero, pur evidenziando la suddetta neutralizzazione, pone l'accento sull'utilità dell'introduzione di rinvii a fonti nazionali ed europee in materia di privacy in quanto essa fisserebbe i parametri di riferimento necessari per l'interpretazione e l'applicazione della norma.

Al fine di garantire il rispetto della privacy è stata istituita dalla legge sulla privacy[321] un'autorità amministrativa indipendente, il Garante per la Protezione dei Dati Personali (GPDP) che viene disciplinata dal Codice Privacy[322] e definita dal GDPR[323] come l'autorità di controllo designata anche ai fini dell'attuazione dello stesso. Il Garante ha diversi compiti di controllo della conformità al GDPR e normative nazionali dei trattamenti dei dati personali. È altresì cruciale che il Garante mantenga la collaborazione con altre autorità di controllo unitamente a segnalazioni proattive verso il Parlamento e altri organismi, solleciti la consapevolezza del pubblico e dei titolari del trattamento. Oltre a ciò, ha il compito di indicare le misure idonee allo svolgimento corretto del trattamento, di gestire ammonimenti e reclami oltre quello di formulare pareri e la informazione del suo operato con una relazione annuale.

Un'ulteriore competenza concerne la diretta elaborazione e la promozione dell'adozione di regole deontologiche[324], che fissano le condizioni di liceità dei trattamenti dei dati alle quali si riferiscono e il cui rispetto rappresenta un requisito irrinunciabile affinché il trattamento dei dati sia lecito e regolare. Se sono elaborate per dei trattamenti in determinate circostante[325], il Garante verificherà, grazie anche alle

[319] Codice della Privacy, cit., art. 2-ter, co 3, soggetti a cui è data conoscenza che non siano l'interessato, il rappresentante del titolare nel territorio dell'UE, il responsabile o il suo rappresentante nel territorio dell'UE, le persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile

[320] novelle introdotte dal d.l. 8 ottobre 2021, n. 139, art. 9

[321] l. 31 dicembre 1996, n. 675. *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*

[322] Codice della Privacy, cit.

[323] Regolamento (UE) 2016/679, GDPR, cit., art. 51

[324] Codice della Privacy, cit., art. 2-quater

[325] Regolamento (UE) 2016/679, GDPR, cit., Capo IX, fra cui obblighi di segretezza e trattamento e libertà d'espressione e di informazione

opinioni dei soggetti interessati, la loro conformità alle disposizioni in vigore oltre ad adoperarsi affinché le regole vengano conosciute e rispettate. L'esistenza del Garante della privacy dovrebbe costituire di per sé un elemento di tranquillità nella aspettativa di privacy del cittadino i cui dati vengono continuamente trattati per varie finalità. Tuttavia, ad avviso di chi scrive, se venisse rispettata pedissequamente l'aspettativa di privacy creando fiducia nel titolare dei dati in una *data protectio*n adeguata, sarebbe anche più facile adattarsi a una penetrazione della IA, in particolare l'impiego di dati biometrici nella sorveglianza di massa. Diventa pertanto cruciale, per poter garantire con queste tecniche di sorveglianza una più sicura società, che i dati non diventino "merce di scambio"[326] scavalcando il consenso e la conoscenza di tale trattamento da parte dei titolari dei dati.

4. Bilanciamento fra diritti e sicurezza.

Il bilanciamento tra i diritti fondamentali e la necessità di garanzia della sicurezza da parte delle pubbliche autorità è un ambito di complessa realizzazione. Una corretta armonia tra la protezione dei diritti e un corretto trattamento dei dati in uno scenario tecnologico avanzato, ha una centralità negli obiettivi nazionali e sovranazionali. Nell'Unione Europa la protezione dei dati personali, in particolare quelli ottenuti attraverso rilevamenti a carattere biometrico e, dunque, per mezzo del riconoscimento facciale, sono regolati attraverso tre strumenti. Il primo è il *General Data Protection Regulation* **(**GDPR**)**[327], che si pone l'obiettivo di garanzia della certezza giuridica, l'armonizzazione delle fonti e la semplificazione delle norme di trasferimento dei dati personali dall'ambito europeo verso il resto del mondo.

Il secondo strumento, di cui si tratterà in seguito, è la Direttiva UE 2016/680[328], finalizzata invece alla protezione delle persone fisiche in relazione all'uso dei dati personali da parte delle autorità per attività di prevenzione, indagine, accertamento e perseguimento dei reati o esecuzione di sanzioni penali, e alla libera circolazione di tali dati. Tale direttiva ha abrogato la decisione quadro 2008/977/GAI relativa alla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di

[326] Sent., *Big Brother c. UK*, *supra* § 3

[327] Regolamento (UE) 2016/679, GDPR, cit., con rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione Europea del 23 maggio 2018, n.127

[328] Parlamento Europeo e Consiglio, Direttiva del 27 aprile 2016 n. 680, *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*, *infra* § 5

polizia in materia penale. Esiste, infine, la Direttiva (UE) 2016/681[329] del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa all'uso dei dati del codice di prenotazione (PNR) a fine di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e i reati gravi. I dati PNR sono informazioni personali fornite dai passeggeri che vengono raccolte e conservate dai vettori aerei. Comprendono informazioni quali il nome del passeggero, la data di viaggio, l'itinerario, il posto assegnato, il bagaglio, i dati di contatto e le modalità di pagamento. Di seguito verrà esposto il GDPR e la sua relazione con le tecniche di IA che utilizzano i dati biometrici degli individui, quali la sorveglianza di massa, e il recepimento da parte della giurisprudenza e dei cittadini europei.

Il Regolamento 2016/679 introduce regole più chiare rispetto alla precedente normativa su informativa e consenso ed introduce limiti al trattamento automatizzato dei dati personali. Il trasferimento dei dati al di fuori dalla UE viene regolato da criteri rigorosi, la cui violazione, il cosiddetto *data breach*, è punita da norme altrettanto rigorose. Il GDPR si applica ai trattamenti effettuati da un titolare o responsabile del trattamento nell'Unione, prescindendo dal luogo in cui il trattamento venga effettuato, potendo essere anche fuori dall'Unione. Quando il titolare o responsabile non è stabilito nell'Unione e le attività di trattamento non concernono l'offerta di beni o prestazioni di servizi a interessati che si trovano nell'Unione oppure il monitoraggio del loro comportamento quando questo abbia luogo nell'Unione. In tal caso si applica il Regolamento anche quando il titolare del trattamento sia stabilito in uno Stato membro in virtù del diritto internazionale pubblico.[330]

Un aspetto importante del Regolamento è la sua apertura verso nuovi diritti dei cittadini europei legati ai loro dati. Viene anche creato il ruolo del *titolare del trattamento* dei dati, il cui compito è la determinazione dei rischi e delle misure a livello tecnico e organizzativo atte a mantenere la gestione dei dati a un consono livello di sicurezza. In particolare, da parte del titolare del trattamento è richiesta chiarezza, intellegibilità e accessibilità degli scambi informativi con il titolare dei dati. Quest'ultimo deve essere agevolato nell'esercizio dei suoi diritti e adeguatamente informato delle azioni intraprese con i suoi dati, con scambi tempestivi e, se ha trasmesso i dati in modalità elettronica, deve ricevere informazioni possibilmente con lo stesso mezzo. Le richieste dell'interessato devono, tuttavia, essere fondate e non esuberanti per non incorrere in spese o rifiuto di soddisfarle da parte del titolare del trattamento.[331] Se il fine del trattamento non richiede, da principio o in seguito, l'identificazione dell'interessato

[329] Parlamento Europeo e Consiglio, Direttiva del 27 aprile 2016, n. 681, *sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi*

[330] Regolamento (UE) 2016/679, GDPR, cit., art. 3

[331] Regolamento (UE) 2016/679, GDPR, cit., Capo III, *Diritti dell'interessato,* Sezione I, *Trasparenza e modalità*, articolo 12, *Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato*

attraverso i dati personali, il titolare del trattamento non ha l'obbligo di conservare, acquisire o trattare ulteriori dati per l'identificazione e qualora, in tali casi, possa dimostrare di non poter identificare l'interessato, se possibile lo informa.[332]

L'articolo 9[333] del Regolamento permette di definire norme più stringenti agli Stati membri della UE in merito al *trattamento dei dati biometrici* [334] e di quelli genetici relativi alla salute. A livello nazionale, l'Italia ha recepito la possibilità consentita dall'articolo 9 attraverso l'articolo 2-septies introdotto nel d.lgs. 196/2003 che prevede per il GPDP la possibilità di definire misure specifiche in merito al trattamento dei dati biometrici e, dunque, anche per quelli trattati nell'ambito del riconoscimento facciale. L'articolo 9 vieta esplicitamente il trattamento di dati personali che evidenzino elementi che potrebbero indurre discriminazione, quali razza, etnia, opinioni politiche, religione, credo filosofici, appartenenza sindacale.

Vieta, altresì, il trattamento di dati genetici, biometrici, di specifica rilevanza per il tema di interesse della trattazione, volti all'univoca identificazione dell'individuo, oltre a dati sulla salute e la sfera sessuale (comportamenti, orientamento). Nel paragrafo 2, elenca poi tutti i casi in cui il paragrafo 1 non è applicabile. Tra questi, in potenziale relazione con le applicazioni di sorveglianza di massa, sono di rilievo i casi relativi a motivi di "interesse pubblico", sia in generale che specificamente nel settore della sanità pubblica e per finalità legate alla ricerca scientifica. Gli Stati membri possono, come già specificato relativamente ad altri articoli, mantenere oppure estendere a ulteriori condizioni oppure introdurre limitazioni, con specifico riferimento ai dati genetici, di salute e *biometrici*. La conseguenza è che recepimento e armonizzazione delle tecniche biometriche, in particolare del riconoscimento facciale, e del loro impiego nella sorveglianza di massa acquista anche un carattere specifico di implementazione a livello di ciascuno Stato membro dell'Unione.

Nelle questioni relative alle attività di sicurezza nazionale il GDPR esclude la sua applicabilità, in particolare, attraverso gli articoli 16, 19 e 20. Nello specifico, l'articolo 16 sancisce proprio che il Regolamento non è applicabile alla garanzia di diritti e libertà fondamentali o alla libera circolazione di dati personali quando esse siano riferite ad attività non contemplate nella applicazione del diritto dell'Unione, tra cui rientrano, come anticipato, tutte quelle relative alla sicurezza nazionale. La non applicabilità riguarda anche il trattamento dei dati personali da parte degli Stati membri per attività collegate alla politica estera e di sicurezza comune dell'Unione. Il Regolamento non dovrebbe altresì applicarsi per i trattamenti dei dati personali effettuati per le finalità dettagliate nell'articolo 19, in particolare la protezione delle persone fisiche da parte delle autorità per obiettivi di prevenzione, indagine, accertamento e perseguimento di

[332] Regolamento (UE) 2016/679, GDPR, cit., art. 11, *Trattamento che non richiede l'identificazione*
[333] Regolamento (UE) 2016/679, GDPR, cit., art. 9, *Trattamento di categorie particolari di dati personali*, par. 4
[334] *supra* § 1

reati o esecuzione di sanzioni penali, «incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica, e la libera circolazione di tali dati sono oggetto di uno specifico atto dell'Unione».

Quando utilizzati per dette finalità, i dati personali trattati dalle autorità pubbliche sono, invece, regolamentati dalla già menzionata Direttiva 2016/680[335], «nella misura in cui [il trattamento] ricada nell'ambito di applicazione del diritto dell'Unione». Ai sensi della stessa, per il trattamento di dati personali per tali altre finalità, gli Stati membri possono attribuire alle autorità altri compiti che non rientrano necessariamente in quelli già citati che mirano alla prevenzione, indagine, accertamento, perseguimento e applicazione di sanzioni penali. Infine, l'articolo 20 specifica che il diritto dell'Unione o degli Stati membri potrebbe specificare le operazioni e le procedure per il trattamento dei dati personali effettuato da autorità giurisdizionali e da altre autorità giudiziarie, anche se alle attività delle stesse si applichi il GDPR. Tali trattamenti dovrebbero essere controllati da specifici organismi appartenenti al sistema giudiziario dello Stato membro, col compito di garantire il rispetto del GDPR e diffonderne la conoscenza relativa in particolare agli obblighi della magistratura, nonché di ricezione ed esamina di reclami relativi a tali trattamenti.

4.1. *(Segue):* diritti e sicurezza nel GDPR.

Guardando all'oggetto del Regolamento 2016/679[336] esso mira a stabilire norme che proteggano gli individui in merito al trattamento dei dati personali e che regolino la libera circolazione degli stessi, alla quale non ci sono limiti opponibili se il trattamento avviene secondo le norme del medesimo Regolamento. La protezione dei diritti e delle libertà fondamentali delle persone fisiche e, nello specifico il diritto alla protezione dei dati personali, è il fulcro del Regolamento.

Per comprendere il rapporto con la sicurezza risulta di particolare rilevanza l'ambito di applicazione materiale del Regolamento[337] che comprende il trattamento, del tutto o in parte automatizzato, dei dati personali da archiviare o archiviati. Se il trattamento viene effettuato da organi, uffici e agenzie dell'Unione, si applica il Regolamento 2018/1725[338] che, allo stesso modo del GDPR, definisce i concetti di titolare responsabile e contitolare del trattamento. Inoltre, ne chiarisce la responsabilità, fornendo quindi delle linee guida utili per le istituzioni e gli organi dell'Unione anche per l'applicazione pratica dei concetti definiti nel GDPR. Il Regolamento 2018/1725 ha come obiettivo quello di uniformare il più possibile le norme concernenti la

[335] *infra* § 5
[336] Regolamento (UE) 2016/679, GDPR, cit., Capo I, *Disposizioni generali*, art. 1, *Oggetto e finalità*
[337] Regolamento (UE) 2016/679, GDPR, cit., art. 2, *Ambito di applicazione materiale*
[338] Regolamento (UE) del 23 ottobre 2018, n.1725, sulla *tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati,* che ha abrogato Regolamento (CE) n. 45/2001

protezione dei dati per istituzioni, organi e organismi dell'Unione e le norme dell'ordinamento interno degli Stati membri nel settore pubblico.

Per quanto concerne, invece, i prestatori intermediari di servizi, la loro responsabilità è sancita, con riferimento al "*mere conduit*" o semplice trasporto, nella Direttiva 2000/31/CE, la cui applicazione non viene pregiudicata dal GDPR. In tale caso, si considera non responsabile il prestatore di un servizio della società dell'informazione per conto della quale fornisce accesso alla rete oppure trasmette le informazioni, originate da un destinatario del servizio, su una rete di comunicazione. Tali attività prestate comprendono la memorizzazione automatica, intermedia e transitoria delle informazioni trasferite, solo se risulti necessario per trasmetterle sulla rete e rientrando in un lasso ragionevole di tempo per tale finalità. La non responsabilità non implica, però, l'impossibilità di impedimento o cessazione da parte di un organo giurisdizionale o autorità amministrativa, in caso di violazione dell'ordinamento dello Stato membro in cui tali attività si svolgono.

In tale articolo emergono importanti informazioni relative alla protezione del diritto dell'individuo al trattamento dei dati personali, sia per quanto concerne l'eventualità di una violazione delle norme del proprio ordinamento che per il lasso temporale in cui sono "trattenibili" i propri dati in transito. Tale Direttiva ha formulato una disciplina unitaria concernente i *provider*[339]*,* tutelandoli dagli illeciti commessi dai terzi che fruiscono dei servizi forniti, a condizione che i provider stessi agiscano tecnicamente e in modo automatico all'unico fine di rendere più efficiente la trasmissione dei terzi, in termini di *caching* o memorizzazione temporanea.[340] Qualora, però, il provider, dopo aver analizzato i dati, rivisiti i contenuti di cui è intermediario, partecipi alla loro redazione oppure migliori la funzionalità della sua piattaforma, si considera *attivo*. Non essendo più ritenuto neutro nello scambio di dati, il provider è soggetto a responsabilità oggettiva, per cui ha l'obbligo di rimozione di informazioni illecite o di blocco del loro accesso. [341]

Come alcuni[342] sostengono, in materia di mercato digitale si percepiva come gli strumenti forniti dal GDPR non fossero adeguati a regolarne il funzionamento. La necessità di nuove regole, pertanto, è collegata al rapido e diffuso sviluppo dei servizi digitali e alla garanzia che «la legislazione europea evolva con loro»[343]. In tal senso, la

[339] *provider* fornisce a pagamento servizi telematici, come collegamenti di posta elettronica e di accesso a Internet, e non da origine alla trasmissione né seleziona il destinatario della trasmissione non modifica, né seleziona i dati trasmessi

[340] Parlamento Europeo e Consiglio, Direttiva CE, 8 giugno 2000, n. 31, *relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno*, «Direttiva sul commercio elettronico»

[341] SPANO L., *Il ruolo e la responsabilità delle piattaforme di E-commerce*, in *Amministrazione in Cammino*, 2022, 7

[342] SIBILLA F. – GUERRESCHI E., *UE – DSA e DMA, strumenti chiave per correggere i limiti del GDPR*, in *Diritto di Internet*, 2022

[343] Commissione Europea, *Il pacchetto Digital Services Act*, in *Sito Ufficiale dell'Unione Europea,* 2023

Commissione nel 2020 ha presentato delle proposte, sulle quali è stato raggiunto un accordo politico nel 2022, in materia di legge sui mercati digitali (DMA)[344] e sui servizi digitali (DSA)[345], la cui applicazione è *in fieri*. Gli obiettivi perseguiti sono quello di creare uno spazio digitale che garantisca una maggiore tutela dei diritti fondamentali degli utenti dei servizi digitali, oltre a creare un mercato equo in cui sia possibile promuovere l'innovazione e favorire la competitività, a livello sia europeo che mondiale. Nello specifico, le norme del DSA riguardano gli intermediari e le piattaforme online, mentre quelle del DMA concernono le piattaforme digitali che hanno un ruolo sistemico nel mercato interno quali punto di accesso o "*bottleneck*" tra utenti commerciali e consumatori.

Si presenta, in un'ottica futuribile, una protezione dei dati personali più estesa e "aggiornata" ai continui sviluppi del mercato, per cui dalla tutela fornita dal GDPR si passerà a quella fornita dalle due leggi sopracitate che, partendo dai principi già sanciti, potenzieranno l'effetto benefico sulla protezione dei dati personali. Questo approccio è un esempio di un'auspicabile evoluzione normativa della tutela dei dati, anche se tale evoluzione diviene più complessa quando si tratta di ambiti che si sviluppano "al di fuori" delle garanzie fornite dal GDPR.

In particolare, vengono in rilievo quegli ambiti in cui il Regolamento 2016/679 non si applica e fra i quali emerge quello relativo alla trattazione dei dati personali effettuata da autorità competenti per prevenire, indagare, accertare o perseguire reati o eseguire sanzioni penali, includendo l'ambito che pone dubbi in materia di bilanciamento tra diritti e sicurezza. Tale ambito riguarda la «salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse»[346], che corrisponde all'oggetto e agli obiettivi della Direttiva 2016/680.[347] Le misure normative, concernenti la trattazione effettuata dalle autorità competenti ai fini sopraindicati e anche ai fini della sicurezza nazionale e pubblica prevenzione[348], devono contenere disposizioni specifiche riguardo alle finalità o alle categorie del trattamento e alle categorie di dati personali oggetto del trattamento stesso.

Tali misure concernono le limitazioni, nella misura in cui rientrino nella cornice definita dai medesimi articoli sugli obblighi e i diritti[349], a cui possono essere sottoposti gli obblighi, i diritti e i principi sanciti dal GDPR. È necessario, inoltre, che vengano rispettati i diritti e le libertà fondamentali e che la misura legislativa sia «necessaria e proporzionata in una società democratica» per le finalità sopra specificate, che non esauriscono l'insieme completo di quelle salvaguardate. Infatti, le limitazioni introdotte

[344] Digital Markets Act (DMA), proposto dalla Commissione nel dicembre 2020, accordo politico il 25 marzo 2022
[345] Digital Services Act (DSA), proposto dalla Commissione nel dicembre 2020, accordo politico il 23 aprile 2022
[346] Regolamento (UE) 2016/679, GDPR, cit., art. 2
[347] Direttiva (UE) 2016/680, cit., art.1, co 1, *Oggetto e obiettivi*
[348] Regolamento (UE) 2016/679, GDPR, cit., art. 23, *Limitazioni*
[349] Regolamento (UE) 2016/679, GDPR, cit., art. 12-22

devono essere definite nella loro portata insieme ai rischi che comportano per i diritti e le libertà dei soggetti interessati. Tuttavia, tali limitazioni possono non essere esplicitate qualora la loro comunicazione possa minare la finalità della limitazione stessa. Ai fini di una precipua informazione ai soggetti di quanto accade ai propri dati, sono necessarie disposizioni che definiscano le garanzie capaci di prevenire abusi, accesso o trasferimento dei dati illeciti. Inoltre, sono essenziali garanzie pertinenti alla natura, applicabilità e fine dello specifico trattamento o delle categorie di dati a cui sarà applicato. Entrambe le garanzie concorrono alla realizzazione del bilanciamento con la tutela dei diritti degli interessati. Infine, deve essere precisato il titolare del trattamento e il periodo di tempo in cui i dati saranno oggetto di trattazione da parte dello stesso.

4.2. *(Segue):* i principi del GDPR.

In virtù di quanto descritto nel precedente paragrafo, per addentrarsi più profondamente nel centro focale del Regolamento 2016/679, è opportuno individuare i principi fondanti del GDPR e come essi si pongano in relazione con le tecniche di sorveglianza di massa che utilizzano i dati biometrici dei cittadini europei. Per tale finalità, è di ausilio un'analisi critica di alcune delle definizioni, utili ai fini della presente trattazione, contenute nell'articolo 4 del GDPR stesso.[350] In particolare, le definizioni di dato personale, trattamento, profilazione e consenso dell'interessato presentano elementi intrinseci di riflessione sugli aspetti evidenziati in merito alla rilevazione facciale e alla sorveglianza di massa, pur senza contenere nessun elemento specifico a riguardo. Sarà poi successivamente esplicitata dal medesimo articolo la definizione di dati biometrici.

Per dato personale si intende «qualsiasi informazione riguardante una persona fisica identificata o identificabile», definito anche come interessato, identificabile in modo diretto o indiretto. L'individuazione di una persona può avvenire attraverso vari parametri, dal nome, un identificativo numerico o online, ai dati concernenti la posizione, unitamente agli elementi legati alle caratteristiche fisiche, genetiche, psichiche, socioculturali ed economiche. Si comprende, dunque, come molti dei parametri della rilevazione biometrica già descritti[351] possano essere direttamente o indirettamente interpretati e ricadere proprio in tale definizione di dato personale. Il trattamento al quale viene sottoposto il *dato personale* è una qualsiasi operazione, anche plurima, non necessariamente condotta in modo automatizzato, ad esempio, con o senza l'ausilio di un sistema come quello di IA, che ricomprende tutte le fasi

[350] Regolamento (UE) 2016/679, GDPR, cit., art. 4, *Definizioni*, che definisce dato personale, trattamento (e sua limitazione), profilazione, pseudonimizzazione, archivio, titolare e responsabile del trattamento, destinatario, terzo, consenso dell'interessato, violazione dei dati personali, dati generici, dati biometrici, dati relativi alla salute, stabilimento principale, rappresentante, impresa, gruppo imprenditoriale, norme vincolanti d'impresa, autorità di controllo, autorità di controllo interessata, trattamento transfrontaliero, obiezione pertinente e motivata, servizio della società dell'informazione, organizzazione internazionale.
[351] *infra* § 1

necessarie. Tali fasi vanno dalla collezione del dato fino al suo impiego, in modalità diretta o per consultazione attraverso la conservazione del dato. Le fasi necessarie per la disponibilità del dato comprendono la sua registrazione, organizzazione e strutturazione, come può essere, ad esempio, la rappresentazione del dato attraverso una forma tabulare o in codici numerici, anche binari. Il dato può anche essere modificato o adattato alle esigenze della specifica tipologia di trattamento e persino cancellato o completamente eliminato, ed è inoltre suscettibile di essere messo a disposizione e/o comunicato con possibilità di confronto o connessione. In merito a quanto descritto, si potrebbe ritrovare in tale definizione anche la raccolta, diretta o meno, dei dati personali derivati dall'utilizzo di tecniche biometriche e *trattati* attraverso la sorveglianza, come ad esempio l'impronta digitale fornita con consenso o l'individuazione inconsapevole del viso da parte di una telecamera, oltre naturalmente alla conservazione di tali rilevazioni.

Anche la definizione di *profilazione* offre spunti interessanti rispetto a questa riflessione, essendo intesa come qualsiasi forma di trattamento automatizzato dei dati personali che li utilizzi nell'analisi di aspetti personali di un individuo. Il fine può essere quello di stimarne o prevederne il comportamento, elemento utilizzato (ad esempio, dai sistemi di IA che valutano il rischio di recidiva con l'approccio *evidence-based* [352]), l'affidabilità, la posizione e gli spostamenti (utilizzabili, ad esempio, per rintracciare una persona scomparsa o un fuggitivo), oltre alla condizione economica, di salute, professionale e le preferenze personali. In particolar modo, gli elementi legati alla ubicazione e lo spostamento potrebbero essere considerati come uno specifico risultato della sorveglianza di massa, a valle del riconoscimento attraverso i dati del volto. In relazione ai processi decisionali automatizzati, l'interessato ha diritto a non essere sottoposto a una decisione basata unicamente su questi, inclusa la profilazione, in ragione della possibilità di produzione di effetti giuridici che lo riguardino.

Se poi si analizza la definizione di *consenso* dell'interessato, questo può essere manifestato esplicitamente con una dichiarazione o, in sua assenza, con un agire che inequivocabilmente si consideri come manifestazione di volontà al trattamento. Essa deve essere fornita in modo libero e relativamente allo specifico trattamento di cui i dati sono oggetto. Diviene lampante quanto evidenziato nel paragrafo 1 in merito alla sorveglianza di massa attraverso, in particolare, il riconoscimento facciale, in quanto l'interessato potrebbe non averne consapevolezza oppure, qualora l'avesse, non avrebbe modo di rilasciare alcun consenso.

Si arriva, poi, nell'articolo 4 alla definizione di *dati biometrici*, con la conoscenza dell'inquadramento degli stessi e della metodologia della sorveglianza di massa in relazione al Regolamento. Rimane, comunque, un aspetto di rilievo che esista in tale articolo una definizione dedicata al dato biometrico, inteso come «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche,

[352] *supra* Capitolo I, § 6.1

fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici». Esso, infatti, rappresenta una presa d'atto sulla esistenza, impiego ed evoluzione prospettica di queste tecnologie, che stimolano la necessità di comprenderne appieno la portata in termini sia di benefici ma anche di potenziali aspetti negativi. A valle degli elementi scaturiti dalle definizioni riportate si possono correlare più efficacemente i principi, di cui si andrà a parlare, con gli aspetti legati al tema della trattazione.

Infatti, all'articolo 5 vengono individuati i principi applicabili al trattamento dei dati personali, il quale specifica una serie di elementi che rendono il trattamento dei dati chiaro e ben codificato. Liceità, correttezza e trasparenza del trattamento dell'interessato mirano ad evitare quanto evidenziato come problematico in materia di sorveglianza. La raccolta dei dati avviene per una specifica *limitata* finalità, esplicita e legittima, che deve essere rispettata per la durata del trattamento, ad eccezione di un'archiviazione che avvenga nel pubblico interesse, scientifico, storico o statistico. In relazione a detta finalità i dati sono limitati a quanto necessario e, quindi, *minimizzati*, oltre ad essere per essa pertinenti e adeguati. Essi devono essere inoltre *esatti* e, quando necessario, essere aggiornati ed eliminati o rettificati qualora inesatti rispetto la finalità del loro trattamento.

Per quanto concerne la loro conservazione, essa è *limitata* al tempo necessario per il conseguimento del fine del trattamento, non può, quindi, essere conservato per più tempo, ad eccezione, come prima, di un'archiviazione per pubblico interesse, e deve essere conservata in una forma che consenta l'identificazione degli interessati. Il periodo di tempo di conservazione del dato personale può essere definito con il termine *data retention*. L'eccezione per la quale può essere allungato il tempo di trattamento non è senza limiti e, infatti, sono riscontrabili le tutele dei diritti e delle libertà sancite dal GDPR medesimo nell'attuazione delle misure tecniche e organizzative, oltre alla *responsabilizzazione* del titolare del trattamento. Inoltre, la necessità di garantire l'*integrità* e la *riservatezza* dei dati rientra nell'aspettativa di privacy dell'interessato, che, come già visto[353], a seconda della sua implementazione nel trattamento, alimenta o meno la fiducia in esso. Nel GDPR la protezione è estesa anche ai trattamenti non autorizzati o illeciti e alla perdita, distruzione o danno accidentale dei dati. Gli elementi analizzati sono quelli che, se rispettati, farebbero crescere il sostegno alle tecnologie di IA e plausibilmente aumenterebbe, in tal modo, anche il livello di sicurezza che esse potrebbero assicurare. In particolare, il riferimento nell'articolo 5 al trattamento *trasparente* ed al dato *esatto* sono ulteriori stimoli per la riflessione sulla raccolta dei dati con i metodi descritti nel paragrafo 1, dal momento che la sorveglianza di massa potrebbe trovarsi a violare uno o più principi.

[353] *supra* § 1

In particolare, il GDPR specifica una serie di condizioni che devono essere verificate perché il trattamento dei dati sia lecito[354]. All'articolo 6 vengono definite le condizioni di cui almeno una deve essere soddisfatta e attribuisce agli Stati membri la possibilità di mantenere o introdurre disposizioni più specifiche. È necessario che le ulteriori condizioni siano in accordo a situazioni di trattamento specificate nel Capo IX[355], al paragrafo 1-c), sulla liceità del trattamento adempiente ad un obbligo legale, e 1-e), nell'adempimento di un compito di pubblico interesse o collegato comunque ai pubblici poteri del titolare. Il trattamento dei dati in questi ultimi due casi si può basare sul diritto dell'Unione oppure su quello dello Stato membro del titolare del trattamento.

Tra le condizioni di liceità del trattamento rientrano il già citato consenso dell'interessato, il trattamento che risulti necessario per salvaguardare interessi vitali dell'interessato o altra persona fisica o legittimi del titolare o di terzi, a meno che non ci siano prevalenti diritti e libertà fondamentali dell'interessato per cui sia richiesta la protezione dei dati. Tali circostanze non sono applicabili al trattamento dati da parte di pubbliche autorità nell'esercizio delle loro funzioni.

Un caso sopracitato è il trattamento effettuato per una finalità diversa da quella che ha motivato la raccolta dei dati, non basato sul consenso dell'interessato o sulle leggi dell'Unione o degli Stati membri. Tale trattamento deve costituire una «*misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23 paragrafo 1*[356]», quindi, nei casi di non applicabilità del GDPR. In tal caso, il titolare del trattamento nella verifica sulla compatibilità della diversa finalità tiene conto di una serie di fattori quali il nesso tra le finalità, il contesto della raccolta, la natura dei dati personali, le possibili conseguenze di un ulteriore trattamento.

Inoltre, il titolare valuta la presenza di garanzie adeguate ricomprendenti la cifratura[357] e la pseudonimizzazione[358]. Queste due modalità di garanzia della salvaguardia dell'interessato prevedono che, nel primo caso, il dato venga reso non comprensibile, così da garantire la protezione dell'informazione grazie all'impiego di un algoritmo di cifratura, del crittogramma e di un valore segreto che funziona da chiave per l'accesso a tale informazione. Nel secondo caso, i dati personali non possono più condurre a uno specifico individuo interessato, se non utilizzati con altre informazioni, che devono essere conservate in un luogo separato e assoggettate a misure che garantiscano la non riconducibilità a un soggetto identificato o identificabile.

---

[354] Regolamento (UE) 2016/679, GDPR, cit., art. 6, *Liceità del trattamento, supra* § 3

[355] Regolamento (UE) 2016/679, GDPR, cit., Capo IX, *Disposizioni relative a specifiche situazioni di trattamento*

[356] *supra* § 4.1

[357] AMBESI A. – CICCARELLI M., *GDPR e cifratura: concetti base e approcci pratici*, in *ICT Security Magazine*, 2019

[358] Regolamento (UE) 2016/679, GDPR, cit., art. 4

4.3. *(Segue):* Gruppo di lavoro "Articolo 29".

Gli effetti dell'entrata in vigore del GDPR si sono palesati anche in relazione all'attività di un gruppo di lavoro preesistente, che operava a livello europeo proprio nell'ambito del trattamento dei dati personali. Delineare le attività del gruppo e come queste siano state trasformate dall'operatività del GDPR rende evidente la centralità di questo Regolamento in materia di trattamento dei dati.

Il suddetto Gruppo di lavoro era denominato "Articolo 29" o Article 29 Working Group (WG)[359] e all'entrata in vigore del GDPR è stato sostituito dal Comitato europeo per la protezione dei dati, di cui si parlerà a breve. Analizzare la composizione, i compiti e le attività del WG è utile per comprendere al meglio il mutamento di cui è stata oggetto la protezione dei dati personali e di come sia attualmente tutelata attraverso il nuovo Comitato. Il WG era quindi il gruppo di lavoro europeo consultivo e indipendente istituito dall'articolo 29 della Direttiva 95/46/CE del Parlamento europeo e del Consiglio, relativa alla protezione delle persone fisiche con riferimento al trattamento dei dati personali e alla libera circolazione dei dati stesso. Detto articolo dal titolo "Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali" stabiliva proprio la creazione di un gruppo mirato alla tutela delle persone in termini di trattamento dei dati personali, definendone composizione, modalità di funzionamento e adozione delle decisioni. La composizione del gruppo comprendeva un rappresentante dell'autorità di protezione dei dati personali designate da ogni Stato membro, dal Garante europeo della protezione dati (GEPD) e da un rappresentante della Commissione. Le attività del gruppo vertevano, quindi, principalmente sui compiti affidati ai membri dei garanti nazionali e, in particolare, sulla verifica dell'applicazione delle norme nazionali di esecuzione della Direttiva.

Inoltre, il WG forniva pareri sul livello di tutela nella CE e in paesi terzi e sui codici di condotta comunitari, nonché consigliava la CE in merito ai progetti di modifica della Direttiva o relativi a misure comunitarie con impatto su diritti e libertà degli individui. Formulava altresì raccomandazioni su ogni questione inerente alla protezione dei dati personali all'interno della Unione e sviluppava linee guida e documenti di indirizzo in merito alle varie tematiche collegate alla protezione dei dati, agli sviluppi tecnologici e ai necessari adattamenti. Definiva, inoltre, criteri di adeguatezza per i paesi terzi. Il WG aveva, inoltre, competenza per la gestione sia dei reclami che di eventuali violazioni delle norme europee allora vigenti e nazionali dei singoli Stati membri relative alla protezione dei dati. In presenza di divergenze tra le legislazioni degli Stati membri potenzialmente in grado di pregiudicare l'equivalenza della tutela delle persone, il WG interveniva, informandone la Commissione. Attraverso la menzionata formulazione proattiva di raccomandazioni in materia di trattamento di tutela dei dati

[359] Parlamento Europeo e Consiglio, Direttiva del 24 ottobre 1995, 95/46/CE, relativa alla *tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, n. l. 281 (attualmente non in vigore), art. 29

personali, trasmetteva dette raccomandazioni alla Commissione, la quale era poi tenuta ad informare il WG del seguito ottenuto dai suoi pareri e raccomandazioni.

La Direttiva 95/46CE è stata abrogata a decorrere dal 25 maggio 2018, data di entrata in vigore del GDPR che l'ha sostituita. Una volta entrato in vigore il GDPR, anche il gruppo di lavoro, come anticipato, è stato sostituito dall'*European Data Protection Board* (EDPB), previsto dall'articolo 68 del GDPR e che ha l'obiettivo di garantire una coerente applicazione del GDPR stesso e di promuovere la cooperazione tra le diverse autorità di protezione dei dati in ambito UE. L'EDPB, con sede a Bruxelles, è composto dai rappresentanti delle autorità nazionali per la protezione dei dati e dal GEPD, nonché dalle autorità di controllo degli Stati EFTA/SEE[360], in relazione al GDPR e alle questioni ad esso collegate, che non hanno diritto di voto o di essere eletti alla guida del Comitato o alla sua vicedirezione. La Commissione Europea e, per ciò che concerne il Regolamento generale sulla protezione dei dati, l'Autorità di vigilanza EFTA hanno titolo a partecipare alle attività e alle riunioni del comitato senza diritto di voto.

È opportuno sottolineare che il Comitato ha anche come obiettivo la garanzia di applicazione della Direttiva 2016/680[361]. Ha potere di adottare orientamenti generali con la finalità di chiarire le disposizioni europee sulla protezione dei dati, in modo da provvedere per tutti i destinatari ad una uniforme interpretazioni dei loro doveri e diritti in materia. Il Comitato, inoltre, può adottare decisioni vincolanti ai sensi del GDPR verso le autorità nazionali di controllo, a garanzia di una coerente applicazione delle norme. Il Comitato può, quindi, generare linee guida, raccomandazioni e prassi ottimali, dunque orientamenti a carattere generale, ma anche esercitare una attività consultiva verso la Commissione europea su ogni tema inerente alla protezione dei dati personali e a proposte normative in UE. Può, altresì, adottare strumenti di coerenza in materia di protezione dei dati in casi transfrontalieri e promuovere la cooperazione e l'efficace scambio di informazioni e prassi ottimali tra autorità di controllo nazionali. La relazione annuale del Comitato viene, tra l'altro, inviata al Parlamento europeo, al Consiglio e alla Commissione.

Il Comitato opera nell'alveo di principi ispiratori che vedono le linee guida per il miglior operato possibile nella indipendenza e imparzialità, come anche nella capacità di gestire e amministrare con integrità nella cooperazione, trasparenza, efficienza e modernizzazione, proattività e collegialità. Alla luce di tali principi, il Comitato ha un ruolo importante per rendere il bilanciamento tra sviluppo tecnologico, sicurezza e rispetto dei diritti dei cittadini un obiettivo possibile, anche in settori delicati quali

[360] La *European Free Trade Association* (EFTA) o *Associazione Europea di Libero Scambio* è un'organizzazione intergovernativa che promuove la libera circolazione di beni, servizi, persone e capitali, nonché le politiche correlate (concorrenza, trasporti, energia, cooperazione economica e monetaria) e l'integrazione economica fra i suoi membri, in Europa e a livello globale. L'accordo sullo Spazio Economico Europeo (SEE) riunisce l'Islanda, il Liechtenstein e la Norvegia (paesi SEE-EFTA) nel mercato interno dell'UE

[361] *infra* § 5

quelli legati all'impiego di tecniche biometriche e sorveglianza. In particolare, l'EDRI[362] riporta la definizione del Comitato delle *tecniche biometriche*, descritte come elaborazione automatica di immagini digitali che contengono i volti degli individui ai fini di identificazione, autenticazione/verifica o categorizzazione degli stessi, a prescindere dal loro consenso o consapevolezza circa l'impiego di tali dati [363]. Il richiamo a tale definizione, a parere di chi scrive, sembra essere utilizzato come elemento rafforzante delle perplessità espresse in merito alla raccolta dei dati biometrici e al loro impiego nella sorveglianza di massa.

Un elemento importante nel bilanciamento tra tecnologia, diritti e sicurezza concerne la decisione basata unicamente sul *trattamento automatizzato*[364], di cui all'articolo 22 del GDPR. In tal caso, il Comitato specifica che si sottintende l'assenza di una componente umana che, in forza della propria autorità o competenza, in linea di principio potrebbe condizionare o, addirittura, modificare il risultato della decisione. Inoltre, specifica che, nel prendere decisioni automatizzate, si potrebbe utilizzare o meno la profilazione. A seconda, quindi, della modalità di utilizzo dei dati si potrebbe così partire da un processo decisionale di tipo automatizzato e giungere ad uno basato sulla profilazione.[365] Il Comitato, al fine di prevenire che il divieto sancito dal GDPR venga eluso, ha fornito un'interpretazione estensiva[366] della nozione di *trattamento automatizzato*, determinando la possibilità di inclusione dell'intervento dell'essere umano nel processo decisionale. In tal modo si ricomprende il caso in cui la componente umana si trovi a non concordare con la soluzione prospettata dal processo automatizzato.

Ad opinione di chi scrive, questo approccio ribadisce l'importanza della presenza della componente umana in quanto elemento di "valutazione" nella catena decisionale automatizzata, in particolar modo con riferimento a quei fattori di cui l'algoritmo non potrebbe tenere conto in maniera completa ed efficace. Naturalmente, ciò si riferisce allo stato attuale delle prestazioni algoritmiche e quanto potrebbe accadere in uno scenario prospettico sarà oggetto di trattazione nel Capitolo III.[367] Secondo la linea interpretativa della Commissione sopradescritta, il divieto di adozione di una decisione automatizzata si applicherebbe anche in presenza di un intervento umano, sebbene

[362] European Digital Rights, *supra* § 1.1
[363] JAKUBOWSKA, *Ban Biometric Mass Surveillance*, cit., 10
[364] *supra* § 4.2
[365] l'esempio riportato dalla Commissione concerne la richiesta di un prestito online sul quale un essere umano deciderebbe basandosi su un profilo creato in modo automatizzato, mentre un algoritmo deciderebbe e poi vi sarebbe l'automatica trasmissione all'interessato
[366] Gruppo di lavoro "Articolo 29" per la protezione dei dati, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, in *European Commission Guidelines*, 2018, 8
[367] *infra* § 5.2

questo non sia effettivo, al fine di evitare, come già detto, che tale divieto venga aggirato.[368]

4.4. *(Segue):* bilanciamento e GPDP.

Come si è visto, una componente del Comitato, prima parte del WG, e figura fondamentale nella garanzia del rispetto dei principi del GDPR, è il Garante della privacy.[369] La dicotomia evidenziata tra sicurezza e sorveglianza di massa, di assai difficile bilanciamento, è uno degli aspetti cruciali su cui il Garante si focalizza, tenendo conto dell'importanza strategica dell'intelligenza artificiale nell'ambito del diritto dell'Unione. Tale tema appartiene ad un settore in "inarrestabile" espansione, tanto che il Garante nel 2021 ha istituito un dipartimento denominato Intelligenza Artificiale, come unità organizzativa di primo grado[370], i cui ambiti di intervento sono molteplici[371]. In particolare, monitora, con riguardo agli aspetti giuridici, le basi e i metodi progettuali oltre alla realizzazione e all'utilizzo di sistemi informatici basati su IA e apprendimento automatico, o ML. Partecipa, inoltre, a iniziative nazionali, europee ed internazionali in merito a quelle aree in cui IA, diritto e protezione dei dati si interallacciano. Ha anche un ruolo di supporto all'attività istruttoria in materia di ispezioni e affari, la cui competenza sia di altre Unità organizzative, oltre a collaborare all'esamina di atti normative o proposte di legge con natura regolamentativa della materia.

All'interno dello stesso Garante molte sono le questioni a cui è difficile dare una soluzione univoca e nelle quali si rimanda spesso al GDPR come sistema di riferimento centrale sul trattamento dei dati e base per ulteriori possibili sviluppi in materia. È lo stesso Garante a mettere in discussione i sistemi di videosorveglianza odierni, come è accaduto in relazione all'utilizzo di un particolare sistema automatico di riconoscimento facciale, denominato Sistema Automatico di Riconoscimento Immagini (S.A.R.I.) da parte del Ministero dell'Interno. È certamente consentita la raccolta di dati personali ai fini della sicurezza, ma il Garante evidenzia come sia necessario evitare un sistema di sorveglianza di massa che consentirebbe l'ottenimento di ulteriori informazioni. Ad esempio, conoscere la partecipazione di un individuo a una messa può portare a individuarne l'orientamento religioso, così come la partecipazione a un comizio politico o una manifestazione lgbt possono rendere individuabile l'orientamento politico o sessuale.[372] La contrarietà all'impiego del

[368] ZIROLDI A., *Intelligenza artificiale e processo penale tra norme, prassi e prospettive*, in *Questione di Giustizia*, 2019
[369] *supra* § 3
[370] GPDP, *Regolamento 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali*, 2000, Art. 8, *Organizzazione generale dell'ufficio*, commi 2 e 3, «le unità organizzative di primo livello sono i dipartimenti e i servizi nonché, laddove costituite, le unità temporanee»
[371] Garante per la protezione dei dati personali, *Organigramma*, in *GPDP*, 2021
[372] GHIGLIA A., componente del Garante per la protezione dei dati personali, in *Invervista di Coccorese P., È sottile il confine tra la sicurezza e la sorveglianza di massa*, in *GPDP*, 2021

sistema SARI in tempo reale è motivata dal Garante in ragione della impossibilità di trovare una «giustificata base normativa». Prima di poter utilizzare telecamere e algoritmi è fondamentale comprendere che «deve esserci un interesse proporzionato per permettere una ricerca di questo tipo», come potrebbe essere l'interesse a identificare un omicida, ma prevedendo la minimizzazione del dato.

È importante ricordare che le pubbliche amministrazioni devono fornire una valutazione d'impatto della protezione dei dati, indicata come *Data Protection Impact Assessment* (DPIA), nella quale viene valutato l'impatto del rischio elevato che corrono i diritti e le libertà degli interessati, prima del trattamento dei loro dati. Tale attività prevede, qualora il titolare non ritenga le misure tecniche e organizzative adeguate a ridurre l'impatto del rischio, la consultazione dell'autorità di controllo. In tal modo si assicurarebbe un bilanciamento tra diritti e sicurezza. In particolare, per quanto concerne il SARI, esso è un sistema che consente l'analisi in tempo reale dei volti delle persone che si trovano in una specifica area di interesse, attraverso le telecamere installatevi. Utilizzando una banca dati predefinita, la cosidetta *watch-list*, che può arrivare a una ragguardevole capienza, i volti rilevati dalle telecamere vengono confrontati con tali dati. L'algoritmo di riconoscimento facciale, a questo punto, se trova corrispondenza tra i volti catturati e quelli nella *watch-list*, può generare un segnale che allerta (*alert*) le forze di polizia.

Dalla descrizione si comprende come SARI sia un sistema sofisticato che ha generato grandi perplessità, tanto che al momento il suo utilizzo non è consentito, così come ne creano anche sistemi di sorveglianza più semplici. Ad esempio, uno dei componenti del Garante, Ghiglia, ha palesato la propria contrarietà a un sistema del Comune, dal momento che non è titolare di compiti di ordine pubblico e, dunque, non risulta proporzionato il motivo di condivisione delle informazioni di telecamere che riprendono in video i cittadini, in ragione delle degenerazioni a cui potrebbe condurre. Un conto è quindi che venga effettuata una ripresa per la tutela in caso di attacco o violenza, anche ad insaputa del soggetto, ma per ogni altra situazione è opportuno ricorrere direttamente alle forze di polizia.

Come già detto, il Garante ha ritenuto mancante una base giuridica nella documentazione fornita dal Ministero dell'interno, legittimante i dati biometrici trattati in modo automatizzato, in quanto il rischio sarebbe quello di giungere ad una forma di sorveglianza di massa indiscriminata. I requisiti per un'adeguata base giuridica sono rinvenibili nell'attenta considerazione dei diritti e delle libertà degli individui e nella specificazione dei casi in cui utilizzare il sistema di riconoscimento. La maggior precisione possibile nell'elencare i casi ammessi comporterebbe alla eliminazione teorica della discrezionalità da parte di chi utilizza il sistema. Rimane poi aperto il problema dei cosiddetti *falsi positivi*, frutto di un riconoscimento non corretto causato da errori nell'algoritmo o da rilevazioni di scarsa qualità, quali scarsa luminosità o definizione. Anche in questo caso viene in rilievo la potenziale discriminazione di

carattere etnico, per cui è difficile che un sistema di riconoscimento facciale sia adeguato.

In tal senso, approfondire il funzionamento del sistema SARI può consentire una migliore comprensione dei timori espressi. Il SARI nasce come soluzione di tipo mobile, quindi collocabile nel luogo in cui vi sia l'esigenza di effettuare il riconoscimento facciale, al fine di supportare le forze di polizia in relazione a determinate esigenze di Polizia Giudiziaria o alla gestione dell'ordine e sicurezza pubblica. La criticità del sistema concerne la registrazione delle immagini catturate dalle telecamere, il che fa emergere tre tipi di problemi: la durata della conservazione dei dati, o *data retention*[373], l'assenza del consenso di chi viene ripreso e la ripresa anche di individui estranei alla finalità di rilevamento da parte delle forze di polizia. Nonostante il Ministero abbia specificato che le immagini raccolte verrebbero immediatamente cancellate, tali immagini, parte della watch-list, sono allo stesso tempo la base dell'evoluzione del sistema di sorveglianza. Il pericolo è che si passi da una sorveglianza mirata ad una potenzialmente indiscriminata, in ragione della necessità per un tale sistema di IA di volumi di dati sempre più ampi per il suo addestramento.

Il Garante ritiene, inoltre, che rivesta estrema criticità l'impiego delle tecniche di riconoscimento facciale in un approccio preventivo e repressivo dei reati. La forte interferenza nella vita privata degli individui conduce a prudenza nell'impiego dei sistemi di riconoscimento e sorveglianza. Per questo motivo esiste un'estrema cautela in materia di privacy relativamente al trattamento dei dati biometrici e di specifiche categorie di dati, atti a palesare il credo politico, religioso, sindacale e l'orientamento sessuale. Tali dati, e quelli biometrici in particolare, per la loro natura estremamente delicata devono trovare inquadramento in una adeguata base normativa.

Si è visto[374] che uno dei compiti del Garante per la Protezione dei Dati Personali è di sollecitare la consapevolezza in merito al trattamento dei dati del pubblico. La maggior consapevolezza, infatti, innesta un ciclo virtuoso in cui la collaborazione tra cittadini e istituzioni potrebbe agevolare il raggiungimento dell'agognato bilanciamento tra diritti e sicurezza. Tra le iniziative condotte da Garante per tale opera di sensibilizzazione si inquadrano, ad esempio, la sessione del Convegno[375] dedicato a *"la protezione dei dati: da 25 anni la bussola del futuro"* nel 2022, in cui quattro componenti del GPDP sono stati intervistati su temi cruciali, anche per questa trattazione, cioè IA, sanità digitale e sorveglianza di massa. Dalle interviste sono emerse alcune delle perplessità più volte evidenziate nella trattazione, sia nei confronti della intelligenza artificiale che della sorveglianza di massa. In particolare, l'impatto della IA dovrebbe essere condotto

[373] *supra* § 4.3
[374] *supra* § 3
[375] GDPD, *Convegno "la protezione dei dati: da 25 anni la bussola del futuro". I quattro componenti dell'Autorità intervistati su AI, sanità digitale, sorveglianza di massa,* in *Metaverso,* 2022

mantenendo comunque la centralità dell'essere umano nell'intero processo evolutivo e individuando i limiti da non travalicare per evitare una sostituzione della componente umana da parte della IA. Tale obiettivo, che vede dunque il permanere di un sistema antropocentrico anche in uno scenario di veloce progresso tecnologico, è realizzabile garantendo decisioni che non siano solo automatizzate, in linea con quanto sta accadendo nella normativa europea, il GDPR e l'Artificial Intelligence Act, che mirano a sistemi di IA sicuri, trasparenti, etici, imparziali e, appunto, sotto il controllo umano.

Anche sulla sorveglianza di massa sono state evidenziate le menzionate perplessità in merito al riconoscimento facciale massivo senza le dovute garanzie verso gli individui. Proprio il GDPR rappresenta, allora, un bilanciamento tra libertà e sicurezza, grazie alle garanzie introdotte. Il tema della sanità digitale è comunque anch'esso collegato ai dati sensibili, alla loro protezione e al monitoraggio che può essere effettuato come strumento di "controllo" a carattere sanitario. Infatti, l'enorme diffusione di tecniche di monitoraggio da remoto, cosiddette *Remote Patient Monitoring* (RPM) basate su IA, di pazienti oncologici, con problemi cardio-vascolari, o del sistema circolatorio e respiratorio, farà crescere sempre di più il numero di coloro che ricevono a domicilio assistenza e cura sanitaria e si stima che nel 2027 l'1,4% della popolazione mondiale sarà curata con soluzioni IA-RPM[376].

Un'ulteriore iniziativa del Garante, nell'ottica di una maggior consapevolezza sul tema del trattamento, è rappresentata da una serie di video, intitolata "*Le parole dell'AI*", che raccontano le tematiche principali legate alla IA e alla loro relazione con il tema cruciale della protezione dei dati. A opinione di chi scrive, questi strumenti sono molti utili per raggiungere i cittadini e aprire non solo riflessioni con inviti alla cautela nei confronti delle applicazioni delle tecnologie basate su IA, ma anche accrescere la consapevolezza sullo stato dell'arte del progresso e innescare riflessioni su come si possa massimizzarne il beneficio.

4.4.1. *(Segue):* applicazioni concrete e dottrina sul SARI.

Come appena descritto il SARI è un sistema esemplificativo della criticità tra applicazione e bilanciamento dei diritti nell'ambito del riconoscimento facciale applicato alla sorveglianza di massa particolarmente contrastata dal GPDP in molte occasioni. Alcune prospettive evidenziano che un sistema come SARI possa essere di grande ausilio, per la sua velocità ed efficienza, alle attività investigative, nonostante non vengano dimenticate le probabilità di risultati inaffidabili, discriminatori o controllati. Come altri sottolineano, maggiore è la *zona d'ombra* delineata sull'utilizzo dei sistemi di rilevazione dei dati biometrici e più ci si allontana dalla «piena

[376] FABBRI F., *"IA, quest'anno nel mondo saranno monitorati da remoto 75 milioni di pazienti"*, in *Key4biz*, 2023

compatibilità con le garanzie processuali costituzionali accordate all'indagato»[377], per cui è molto stretta la relazione fra trasparenza e comprensibilità degli algoritmi evidenziata precedentemente.[378]

Considerare la prospettiva processuale in cui verrebbero a inquadrarsi tali "indagini atipiche"[379] permette di comprendere il problema che si crea quando l'azione investigativa, che mira a fornire prove, abbia confini indefiniti in quanto apre la strada a possibili abusi. La questione, quindi, riguarda in quale ambito processuale si possa inquadrare il riconoscimento facciale che, per parte della dottrina, rientra nell'ambito del riconoscimento fotografico effettuato dalla polizia giudiziaria, con la differenza che al posto della polizia giudiziaria opererebbe l'algoritmo. Il possibile punto di approdo di tale approccio sarebbe il superamento dell'affidabilità umana, sempre nel rispetto dei requisiti di trasparenza e chiarezza dell'algoritmo.[380] Il SARI non sembra rientrare in tali requisiti, e il suo inserimento all'interno del processo andrebbe a contrastare la necessità di chiarezza da parte del giudice del funzionamento dell'algoritmo e del software che lo implementa e non sarebbe configurabile il contraddittorio, data la difficoltà di ripetizione del riconoscimento facciale effettuato dal sistema.

Il controverso impiego del SARI è anche al centro di una vicenda penale per violenza di gruppo avvenuta nel 2022 a Milano. Gli indagati sono stati presi in tempi ridotti, proprio perché il SARI ha fornito un ausilio al riconoscimento, attraverso la rilevazione dei volti e il successivo riconoscimento da parte delle vittime degli individui "scelti" dal software[381]. Tre dei presunti aggressori sono stati processati con rito abbreviato su decisione del GIP. Il riconoscimento degli indagati è avvenuto attraverso l'impiego di SARI e di una ricerca automatica nel database di fotosegnalamenti a disposizione delle forze dell'ordine, denominato Automated Fingerprint Identification System (AFIS). Per l'identificazione è, come già menzionato, importante che il dato da mettere a confronto abbia una buona nitidezza e qualità, per poter convergere rapidamente all'identificazione, mentre in caso contrario è necessario l'intervento dell'operatore per effettuare la scelta ottimale tra l'insieme dei possibili incroci forniti dal sistema.

Con tale procedura, l'errore si potrebbe annidare nell'operare integrato della componente umana e del sistema automatico, con responsabilità finale dell'operatore

---

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

[378] *supra* Capitolo I § 2

[379] art. 189 c.p.p., «quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova», l'utilizzabilità di tale nozione non è condivisa da tutti in materia di riconoscimento facciale, dati i suoi confini non particolarmente definiti e la vastità di attività in essa ricomprendibile

[380] SACCHETTO E., *face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *Giustizia penale e nuove tecnologie*, 2020

[381] GAROFALO L., *Riconoscimento facciale. Il branco di Milano identificato con il software 'Sari'*, in *key4biz*, 2022

che effettua la scelta finale. Il funzionamento di SARI è basato, come evidenziato nel paragrafo precedente, sia su un riconoscimento di volti contenuti in immagini (modalità Enterprise) oppure di video (modalità Real Time), ed è proprio la modalità real-time che ha ricevuto il parere negativo del Garante[382].

Quanto affrontato in tema di bilanciamento tra diritti e sicurezza pone in luce, ad avviso di chi scrive, come il GPDP e il GDPR siano la necessaria base di partenza per un'espansione giuridica in termini processuali dell'utilizzo di sistemi di videosorveglianza. Come detto anche nelle precedenti considerazioni, l'uomo è certamente la componente introduttrice di bias, ma può anche essere la soluzione affinché strumenti, che possono fare la differenza all'interno del processo penale e garantire una maggiore giustizia, possano essere applicati.

4.5. (Segue): la data retention.

Col termine *data retention* si fa riferimento alla conservazione dei dati personali che, come anticipato, devono essere conservati per il tempo richiesto dalla specifica finalità del trattamento in corso secondo quanto previsto dal GDPR, il quale prevede inoltre delle eccezioni. Il tema è al centro di un vasto dibattitto a livello europeo ed è oggetto di decisioni della Corte di Giustizia dell'Unione Europea (CGUE), le quali contribuiscono ad una più ampia riflessione sul bilanciamento tra diritti e sicurezza, che si manifesta anche attraverso l'appropriata conservazione dei dati degli individui interessati dal trattamento.

Il tema della *data retention* è stato oggetto della sentenza *Digital Rights Ireland* [383] del 2014, in cui già veniva ribadito dalla CGEU il divieto di conservazione generalizzata, dichiarando invalida la direttiva che determinava un'ingerenza nei diritti fondamentali dei cittadini, in particolare della privacy e della vita privata. Successivamente, nel 2020 la Corte ha dichiarato l'invalidità della Decisione della Commissione Europea 2010/87 in merito all'adeguatezza della protezione fornita dal *"EU-US privacy shield"* in rapporto al GDPR. Nella sentenza Schrem II[384] la Corte ritiene infatti che non sia rispettato il limite dello *strettamente necessario* stabilito nel diritto europeo, in relazione all'accesso da parte dei programmi di sorveglianza basati sulla normativa americana. Il mancato rispetto del limite concerneva i dati di provenienza europea di cui le normative USA stabilivano accesso e utilizzo da parte delle autorità americane. Si stabilisce, infine, che il meccanismo di mediazione non offra un mezzo di ricorso che abbia le medesime garanzie di quello europeo, sia perché carente dal punto di vista

[382] *supra* § 4.4

[383] CGUE, Grande Sez., sent. 8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, The Attorney General*, causa (C-293/12)

[384] CGUE, Grande Sez., sent. 16 luglio 2020, *Data Protection Commissioner c. Facebook Ireland Ltd, Maximillian Schrems,*, causa C-311/18

dell'indipendenza che per la vincolatività delle decisioni dell'autorità mediatrice rispetto all'intelligence americana. La successiva sentenza *H.K.*[385] pronunciata dalla Corte ribadisce l'importante differenza che sussiste tra dati concernenti il traffico e l'ubicazione e quelli identificativi degli utenti e dunque relativi alla loro identità civile. Quest'ultimi possono essere conservati e utilizzati come utile strumento nel contrasto alla criminalità generale.

Al contrario, la conservazione indiscriminata dei dati relativi al traffico e all'ubicazione, in merito ai quali sono posti limiti più stringenti dalla Corte, è consentita solo in caso di prevenzione di minacce rilevanti alla sicurezza pubblica o lotta alla criminalità grave. In quest'ultimo caso è possibile accedere ai dati qualora l'accesso sia limitato nel volume o nel tempo. Vengono pertanto posti limiti sull'accesso ai dati per fini di contrasto, confermando quanto definito nelle precedenti decisioni della Corte proprio in relazione all'«accesso illecito a dati conservati da parte delle autorità nazionali».[386] Si pone l'accento sul fatto che l'ordinamento del singolo Stato membro deve definire le normative sull'ammissibilità delle prove nei procedimenti penali e garantire un processo equo. Tale principio pone, quindi, il divieto di ammissibilità nel processo di prove derivanti dalla conservazione dei dati relativi a ubicazione e traffico indiscriminata e generale, essendo contraria al diritto dell'Unione.

In tal senso, molte sono state le segnalazioni al Parlamento italiano fatte dal GPDP in riferimento alla conservazione dei dati per sei anni imposta dalla legge italiana agli operatori telefonici e telematici, violando quanto sancito nella sentenza del 2020[387] che si oppone a una normativa nazionale di tale tipo. La Corte di Cassazione riafferma che la disciplina italiana è rispettosa delle direttive in materia di privacy secondo l'interpretazione della CGUE, ribadendo che rientra nei limiti temporali stabiliti. La Cassazione afferma come sia il legislatore a dover intervenire in materia, in quanto la CGUE interpreta in maniera generica i casi concernenti i dati di traffico telematico o telefonico, ribadendo che è il legislatore nazionale che deve «trasfondere i principi interpretativi» che la CGUE delinea in una legge.

In seguito, è intervenuto il legislatore italiano nel 2021[388], modificando l'articolo 132 del Codice Privacy[389], e stabilendo che quando minaccia, molestia e disturbo siano gravi e i dati del traffico telefonico siano rilevanti per accertare i fatti, si possano acquisire gli stessi dati a due condizioni. Innanzitutto, devono sussistere indizi di reati di minaccia, molestia o disturbo a mezzo telefonico e di reati per cui è stabilita la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni. Inoltre,

[385] CGUE, Grande Sez., sent. 2 marzo 2021, *H.K. c. Prokuratuur*, causa C-746/18
[386] MARTORANA M. – PINELLI L., *Data retention, impatto critico sui procedimenti già aperti*, in *Altalex,* 2021
[387] CGUE, Grande Sez., sent. 6 ottobre 2020, *État luxembourgeois c. B*, causa C-254/19
[388] d.l. del 30 settembre 2021 n. 132, convertito in l. 23 novembre 2021, n. 178, *misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP*
[389] Codice Privacy, cit., art. 132, *Conservazione di dati di traffico per altre finalità*¸

l'acquisizione dei dati risulta possibile solo con autorizzazione del giudice, con decreto motivato, o dietro richiesta del pubblico ministero o su istanza delle parti. Qualora, poi, vi sia fondato motivo di ritenere che il ritardo potrebbe provocare grave pregiudizio alle indagini e ricorrano ragioni di urgenza, il pubblico ministero dispone l'immediata acquisizione dei dati con decreto motivato.

Come si vedrà, il tema della data retention è centrale nel bilanciamento tra diritti e sicurezza e, ad avviso di chi scrive, un concetto fertile per potenziali proposte volte a migliorare il connubio tra attività di pubblica sicurezza e processo penale in relazione all'uso dell'algoritmica di IA.

5. Trattamento dati per finalità di contrasto.

Come anticipato nel paragrafo 4, accanto al GDPR si colloca un ulteriore strumento normativo europeo, la Direttiva 2016/680[390] che si occupa del trattamento dei dati personali in un ambito importante e, per sua natura, complesso. La Direttiva 680 viene detta anche "Direttiva di Polizia" e nota come LED ovvero *Law Enforcement Directive*, la quale, insieme al GDPR, costituisce il cosiddetto "pacchetto privacy". Rispetto al GDPR, la Direttiva 680 si pone in maniera speculare con la specificità del soggetto titolare del trattamento dei dati personali e dell'ambito di applicazione.

In tal senso, infatti, il soggetto centrale della Direttiva 2016/680 è solo l'autorità competente, per cui l'uso dei dati da parte delle autorità di pubblica sicurezza è focalizzato al perseguimento dei reati, alle necessarie fasi di indagine e accertamento, e di esecuzione delle sanzioni penali. La Direttiva concerne altresì gli aspetti relativi alla circolazione dei dati raccolti per tali finalità.[391] Fra le autorità competenti sono ricomprese quelle pubbliche (autorità giudiziarie e polizia), le altre incaricate di applicare la legge e qualsiasi entità o organismo incaricati dal diritto nazionale di esercitare autorità e poteri pubblici per le finalità sopraindicate. Qualora le finalità siano diverse da quelle menzionate si applicherà, invece, il GDPR.[392] La sentenza della Corte di Giustizia Europea[393] sancisce che la trasmissione dei dati personali effettuata dall'Interpol non rientri nell'ambito applicativo della Direttiva 2016/680, considerando l'articolo 54 della Convenzione di applicazione dell'Accordo di Schengen (CAAS) e l'articolo 50 della Carta dei diritti fondamentali. In tal senso, l'interpretazione indicata dalla Corte ritiene che tali norme consentano il trattamento dei dati personali inclusi in un avviso rosso emesso dall'Interpol[394], fino a che non sia accertato che sui fatti alla

[390] Direttiva del 27 aprile 2016 n. 680, cit., *supra* § 4
[391] Direttiva del 27 aprile 2016 n. 680, cit., Capo I, *Disposizioni Generali*, in cui abroga la decisione quadro 2008/977/GAI del Consiglio
[392] GALGANI B., *Giudizio penale, habeas data e garanzie fondamentali*, in *Archivio Penale,* 2019, 3
[393] CGUE, Grande Sez., sent. 12 maggio 2021, *Bundesamt für Fremdenwesen und Asyl*, C-505/19
[394] *Interpol* è un'organizzazione internazionale della polizia criminale dedita alla cooperazione della polizia e al contrasto del crimine internazionale

base dell'avviso si applichi il principio del *ne bis in idem*[395]. Il trattamento è consentito, naturalmente, solo se rispettoso delle condizioni della Direttiva 680 e sia quindi necessario per l'esecuzione di un compito di una autorità competente.

Una importante precisazione riportata nell'articolo 1[396] sottolinea che l'ambito di azione della Direttiva include la protezione e la prevenzione di minacce alla pubblica sicurezza. Come già evidenziato in questa trattazione, la specificità dell'ambito applicativo in cui il bene di "molti" è in pericolo, rende il diritto del singolo, sempre in termini di dati personali e loro trattamento, meritevole di una normativa dedicata. Naturalmente, il bilanciamento tra diritti e sicurezza non può essere derogato neanche in queste circostanze, ma il confine tra di essi si sposta ed è compito della normativa proteggere le persone e le autorità con un quadro appropriato, giusto e considerevole delle finalità particolari in cui si opera. Si comprende, dunque, il motivo della Direttiva 2016/680, ma anche della 2016/681[397] evidenziata nel paragrafo 4 e relativa ad un ambito ancora più specifico e ristretto. Il fine è fornire alle autorità competenti gli strumenti per agire sempre nel rispetto del valore che i dati personali rivestono e che, grazie in particolare al GDPR, hanno conquistato la centralità che meritano. Infatti, i dati personali hanno uno stretto legame con i diritti e la dignità degli esseri umani. Il fine di prevenzione e salvaguardia contro le minacce alla pubblica sicurezza dovrebbe ricomprendere la protezione degli interessi vitali dell'individuo, per cui il consenso, centrale nel GDPR, in questo caso, non è la base giuridica per il trattamento dei dati. Infatti, la manifestazione di volontà dell'interessato non si può considerare *libera* quando deve adempiere ad un obbligo legale, anche se ci sono casi in cui gli Stati membri possono prevedere il consenso dell'interessato, come nel caso del test del DNA durante le indagini.[398]

Nell'articolo 1, relativo all'ambito di applicazione, oltre al trattamento dei dati da parte delle autorità competenti, se ne indica anche il tipo, ricomprendendo diverse opzioni tecniche. In particolare, quindi, si fa riferimento alla gestione automatizzata e non dei dati e all'accesso ad archivi (cartacei) e, dunque, non automatizzato. A tal proposito, è importante sottolineare che il trattamento di tipo "automatizzato" evoca il possibile impiego di tecniche basate su algoritmi di IA e tutti i possibili benefici e punti di criticità già emersi nella trattazione. Un aspetto importante del trattamento nello scenario normato dalla Direttiva 680 è contenuto nell'articolo 6, in merito alla distinzione tra diverse categorie di interessati[399]. Infatti, in base a quanto disposto dagli Stati membri, il titolare del trattamento dei dati, in base alla opportunità e possibilità,

[395] *ne bis in idem*, principio desunto dall'articolo 649 c.p.p. che definisce il divieto di sottoposizione dell'imputato a un nuovo giudizio sul medesimo fatto per cui sia stato assolto o condannato in via definitiva
[396] Direttiva del 27 aprile 2016 n. 680, cit., art. 1, *Oggetto e obiettivi*
[397] Direttiva del 27 aprile 2016, n. 681, cit., *supra* § 4
[398] Direttiva del 27 aprile 2016 n. 680, cit., C35
[399] Direttiva del 27 aprile 2016 n. 680, cit., art. 6

distingue tra i dati personali relativi a individui che, sulla base di fondati motivi, il titolare possa ritenere abbiano commesso un reato, stiano per commetterlo o siano condannati per un reato.

La categorizzazione dovrebbe poi in modo puntuale identificare e differenziare i dati delle reali o potenziali vittime di un reato e quelli delle altre parti rispetto ad esso. Tra queste si ricomprendono i possibili testimoni nel corso delle indagini o dei conseguenti procedimenti penali, coloro che sono in grado di fornire informazioni sul reato oppure persone solo collegate ai sospetti o autori del reato. Come ausilio agli aspetti preventivi del reato e di sue eventuali recidive, ad avviso di chi scrive, potrebbero essere di ausilio le tecniche basate su IA di tipo *evidence-based* [400], naturalmente con il relativo bagaglio di aspetti positivi e potenziali criticità operative evidenziate in precedenza.

5.1. *(Segue):* diritti nella Direttiva 2016/680 e recepimento.

Un corredo cruciale per la natura del trattamento dati oggetto della Direttiva è quello relativo alla liceità del trattamento[401], in quanto gli Stati membri ammettono il trattamento solo in presenza della necessità d'intervento di un'autorità competente per le medesime finalità indicate nel GDPR[402] e si basa sul diritto dell'Unione o dello Stato membro interessato. Il diritto del singolo Stato, che inquadra il trattamento nell'ambito applicativo della 680, deve indicare almeno le finalità del trattamento e il tipo di dati che si possono trattare. Come disposto dall'articolo 9[403], i dati personali raccolti dalle autorità competenti per le finalità esposte non possono essere impiegati per obiettivi diversi, salvo una autorizzazione specifica proveniente dal diritto dell'Unione oppure dello Stato membro interessato. Se trattati per finalità diverse, per i dati si applica quanto sancito dal GDPR, salvo che il trattamento sia relativo ad una attività non rientrante nella applicabilità del diritto dell'Unione.

Oltre alle condizioni specifiche di cui all'articolo 9, si deve anche tenere conto di quanto indicato nell'articolo 10[404] che menziona i dati a carattere biometrico, ricollegabili alle sue implicazioni applicative nel riconoscimento facciale e nella sorveglianza di massa. L'articolo dispone che il trattamento di dati particolarmente critici, perché rivelatori di elementi potenzialmente causa di discriminazioni, quali razza o etnia, credo politico, religioso o filosofico, appartenenze sindacali, nonché i dati genetici, biometrici e relativi alla sfera della salute, vita od orientamento sessuale, possa essere effettuato solo se strettamente necessario. L'impiego di tali dati deve comunque essere effettuato mantenendo le garanzie necessarie per la salvaguardia dei

[400] *supra* Capitolo I § 6.1
[401] Direttiva del 27 aprile 2016 n. 680, cit., art. 8
[402] Regolamento (UE) 2016/679, GDPR, cit., art. 2, co 2, lett. d)
[403] Direttiva del 27 aprile 2016 n. 680, cit., art. 9, *Condizioni di trattamento specifiche*
[404] Direttiva del 27 aprile 2016 n. 680, cit., art. 10, *Trattamento di categorie particolari di dati personali*

diritti e le libertà degli individui. Inoltre, detto trattamento necessita di un'autorizzazione da parte dell'Unione o dello Stato membro interessato, deve essere relativo a dati comunque resi pubblici da parte dell'interessato oppure deve essere inteso alla salvaguardia di un suo interesse vitale o di altro soggetto.

Nell'ottica di tutela dell'interessato è richiesta l'informazione da parte dell'autorità competente, senza ingiustificato ritardo, nel caso in cui la violazione dei dati presenti un potenziale e cospicuo rischio per i diritti e le libertà del soggetto, che potrebbe così prendere opportune precauzioni.[405] Per questo motivo tale informazione deve esplicare la natura della violazione e segnalare le modalità di attenuazione delle possibili conseguenze sfavorevoli. Inoltre, la comunicazione deve essere effettuata in collaborazione con l'autorità di controllo, nel rispetto di quanto essa o altre autorità competenti abbiano impartito. Tuttavia, la comunicazione potrebbe essere omessa in casi eccezionali qualora, per esempio, non sia possibile evitare di compromettere la prevenzione, indagine, accertamento o perseguimento dei reati col ritardo o la limitazione della comunicazione della violazione. In tal senso l'articolo 13[406], oltre a ribadire i principi fondamentali dei diritti delle persone interessate al trattamento, indica comunque che, per motivi di sicurezza pubblica nazionale, è lasciata agli Stati membri la gestione dei dati alla luce di interessi che, in dette circostanze, diventano superiori rispetto ai diritti dell'interessato. Gli Stati membri possono adottare misure legislative volte a ritardare, limitare o perfino escludere la comunicazione all'interessato, ai sensi del comma 2, nella misura e per il tempo in cui ciò sia richiesto e in linea con una società a carattere democratico, tenendo comunque in debito conto i diritti fondamentali e gli interessi legittimi delle persone oggetto del trattamento. Tali finalità riguardano il rischio di compromissione di indagini, inchieste o procedimenti ufficiali e giudiziari oppure di attività di prevenzione, indagine, e perseguimento del reato o di esecuzione di sanzioni penali. Le finalità ricomprendono altresì la già citata protezione della sicurezza pubblica, nazionale o delle libertà e diritti altrui.

Il soggetto interessato al trattamento conserva il diritto alla rettifica o cancellazione dei dati, come disposto nell'articolo 16, pur permanendo la possibilità per gli Stati membri di non accogliere tali richieste. I rifiuti di rettifica o la cancellazione dei dati personali o la limitazione del trattamento devono essere oggetto di comunicazioni scritte a carico del titolare del trattamento verso l'interessato, fornendo opportuna motivazione dei rifiuti, in accordo a quanto disposto dagli Stati membri. Gli stessi possono altresì adottare misure legislative mirate alla limitazione totale o parziale dell'obbligo di fornire tali informazioni, se tale misura sia, come già indicato precedentemente, necessaria e in linea con una società a carattere democratico, tenendo comunque in debito conto i diritti fondamentali e gli interessi legittimi delle persone oggetto del

[405] Direttiva del 27 aprile 2016 n. 680, cit., C62
[406] Direttiva del 27 aprile 2016 n. 680, cit., art. 13, *Informazioni da rendere disponibili o da fornire all'interessato*

trattamento, per le stesse finalità sopra evidenziate in merito all'esclusione della comunicazione con l'interessato. Gli Stati membri dispongono, comunque, che il titolare del trattamento informi l'interessato della possibilità di opporre un reclamo presso l'autorità di controllo o di proporre un ricorso giurisdizionale.

Inoltre, sempre seguendo il principio di interessi superiori, gli Stati membri possono trasferire i dati dell'interessato a paesi terzi o organizzazioni internazionali come regolato nell'articolo 35[407], che specifica come gli Stati membri debbano disporre che qualsiasi trasferimento effettuato dalle autorità competenti in merito a dati personali oggetto di un trattamento o che lo diventeranno dopo il trasferimento verso un paese terzo o verso una organizzazione internazionale (sia destinatario finale che intermedio), avvenga solo se tale trasferimento è necessario per gli obiettivi di cui all'articolo 1 comma 1 oppure che i dati siano trasferiti al titolare del trattamento in un paese terzo/organizzazione internazionale che sia autorità competente, in accordo al medesimo comma, oppure se i dati sono trasmessi o messi a disposizione da un altro Stato membro e questo abbia autorizzato preliminarmente il trasferimento, in armonia con le proprie normative nazionali. Naturalmente, per tutti i casi, «deve essere fatta salva la conformità adottata a norma delle disposizioni della presente direttiva».

Da quanto delineato emerge un quadro della normativa ritenuto da parte della giurisprudenza[408] di bilanciamento "apprezzabile" tra la protezione dei dati personali e le esigenze investigative come mostrato dalla necessità di conformarsi ai principi di correttezza, liceità, funzionalità e legalità del trattamento e all'esattezza e qualità dei dati. La limitazione dei diritti dell'interessato può avvenire solo in linea con le specifiche esigenze di sicurezza e investigative e purché «costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi» dell'interessato. Nel rispetto del principio di proporzionalità il diritto alla tutela dei dati personali deve essere rapportato al suo ruolo a livello sociale e armonizzato con altri diritti fondamentali.[409]

Per quanto concerne l'ordinamento italiano, la Direttiva è stata recepita e trasposta col d.lgs. 51 del 2018 e in cui i soggetti che rivestono il ruolo di autorità competenti vengono vincolati quali titolari del trattamento eseguito per le finalità ivi indicate, tra cui le forze di polizia e gli altri organismi o entità che possano esercitare le funzioni previste dalla Direttiva sulla base dell'ordinamento italiano. L'autorità competente deve adottare politiche interne e considerare i risultati di eventuali valutazioni

[407] Direttiva del 27 aprile 2016 n. 680, cit., art. 35, *Principi generali per il trasferimento di dati personali*
[408] RESTA F., *La Direttiva sulla protezione dei dati personali in ambito giudiziario penale e di polizia e la tutela dei terzi* in CIRIELLO A. – GRASSO G. (a cura di), *Il trattamento dei dati personali in ambito giudiziario,* 2021, 41
[409] PIZZETTI F. (a cura di), *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in PIZZETTI F. (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, 39

d'impatto sulla protezione dei dati nello sviluppare le procedure. Dette procedure dovranno essere, quindi, attuate in linea con il principio della protezione dei dati durante l'intero trattamento, così come avviene nel GDPR. [410]

In tal senso, l'autorità deve effettuare una valutazione d'impatto sulla protezione dei dati personali, la già citata DPIA[411], prima dell'attuazione di un trattamento che genererebbe un elevato rischio per libertà e diritti dei soggetti interessati. Il rischio viene valutato in ragione della natura, applicazione e utilizzo di tecnologie innovative del trattamento.[412] Diversamente dal GDPR, quando i trattamenti vengono eseguiti nell'esercizio delle funzioni giudiziarie del pubblico ministero e giurisdizionali da parte dell'autorità giudiziaria, il Garante, o autorità di controllo, non deve verificare che le norme del decreto siano rispettate.[413] Per tale motivo le autorità competenti devono fare riferimento alle norme sancite nel codice di procedura penale e non più al d.lgs. attuativo della Direttiva 680.

Nella relazione di accompagnamento al d.lgs. 51/2018 si sottolineava come la proposta avesse l'obiettivo di «adottare un testo unitario, dedicato alla complessiva disciplina del trattamento di dati personali in ambito penale, con l'obiettivo di creare un vero e proprio statuto, contenente principi generali di regolamentazione della materia, rivolti anche al legislatore futuro, e disposizioni di dettaglio, nei vari settori in cui si può articolare il trattamento dei dati personali»[414]. Non vi è dubbio che tale obiettivo racchiudesse una sintesi sistemica e prospettica di grande rilievo per l'implementazione della Direttiva europea sia nel momento della ricezione e trasposizione nell'ordinamento italiano e sia nel futuro. Tuttavia, secondo alcuni[415] il decreto ha solo incorporato in modo fedele quanto riportato nella 680, senza dunque realizzare l'ambizioso obiettivo enunciato nella relazione. In tal modo alcuni elementi sono rimasti connotati, come nel testo della 680, in modo qualitativo ma non quantitativo, come sarebbe invece auspicabile per una migliore applicazione delle norme. Un esempio in tal senso è rappresentato dal periodo di conservazione dei dati, la già descritta data retention[416], la cui durata dipende dalla necessità dell'obiettivo del

[410] ALVERONE G., *La DPIA sui trattamenti per finalità di polizia e di giustizia penale*, in *Diritto.it*, 2022
[411] *supra* § 4.4
[412] D.lgs. 51/2018, 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*, art. 23, *Valutazione d'impatto sulla protezione dei dati*
[413] D.lgs. 51/2018, cit., art. 37, *Autorità di controllo*, co 6
[414] Ministero della Giustizia*, XVIII LEG – Schema di D.Lgs. – Attuazione della direttiva (UE) 2016/680/UE protezione delle persone fisiche con riguardo al trattamento dei dati personali,* Relazione di accompagnamento, 23
[415] GALGANI B., *Giudizio penale, habeas data e garanzie fondamentali*, in *Archivio Penale,* 2019, 9
[416] *supra* § 4.5

trattamento e la non inadeguatezza della cancellazione, descrizione certamente non adatta a definire valori numerici definiti in termini temporali.

L'approccio della Direttiva 2016/680 e, dunque, la sua traduzione nel decreto, tuttavia, è giudicato "più maturo"[417] in termini del binomio tra privacy e sicurezza, che, come si è visto nella trattazione, è di complessa realizzazione per i molti fattori in gioco e il loro delicato equilibrio[418.] La Direttiva, infatti, cerca di indirizzare verso un modello basato sul principio di proporzionalità nel trattamento dei dati, che devono essere *pertinenti* e *non eccedenti* in relazione alle finalità perseguite per poter essere trattati, ma proprio per questo principio la protezione dei dati personali è un diritto ma deve essere anche considerato in relazione alla sua funzione sociale e armonizzato con altri diritti fondamentali.

La proporzionalità, essendo un bilanciamento tra fattori diversi, crea comunque un terreno potenzialmente favorevole alla realizzazione dell'equilibrio fra potere giudiziario e di polizia e diritti e libertà degli individui. La suddetta potenzialità non sempre è realizzabile, per la natura discrezionale del bilanciamento, ma anche per la velocità del progresso tecnologico, già menzionato, che produce nuove sfide e criticità affrontabili con il ricorso all'«adozione di clausole aperte o comunque a formulazione indeterminata» che, dunque, porta ad una traduzione in termini normativi «non del tutto soddisfacente»[419]. Comunque, il margine di manovra che la Direttiva lascia agli Stati membri è ampio e, di conseguenza, l'obiettivo della armonizzazione tra i vari ordinamenti non è semplice da raggiungere.

Ad avviso di chi scrive, la Direttiva introduce elementi rilevanti per una gestione sistemica del trattamento dati ai fini della pubblica sicurezza. Il principio di proporzionalità potrebbe rappresentare l'elemento chiave per giungere ad una quantificazione condivisa dei parametri coinvolti e, dunque, ad una migliore applicazione operativa della normativa. Partendo da questa considerazione nel Capitolo III si tornerà su un possibile ruolo del principio di proporzionalità nel miglioramento della relazione dell'ambito penale con l'algoritmica di IA.

6. Considerazioni su ammissibilità, compiutezza e termine di conservazione dei dati.

La trattazione ha esplorato sin qui il complesso scenario in cui, partendo dall'intelligenza artificiale, si ritrovano sue applicazioni attuali e futuribili in cui alcune decisioni che sono o potrebbero essere demandate alla componente algoritmica, in toto o in parte. L'innesto, in tale dinamica realtà, di un quadro normativo europeo, che ha

[417] GALGANI, *Giudizio penale, habeas data e garanzie fondamentali*, 7
[418] *supra* § 3, 4
[419] GALGANI, *Giudizio penale, habeas data e garanzie fondamentali*, 8

nel GDPR il suo fulcro e che attraverso proprio il GDPR e le Direttive correlate (2016/680 e 681), rinvigorisce i quadri normativi degli Stati membri e li stimola a evoluzioni giuridiche che tengano il passo con il progresso delle applicazioni IA. In tal modo, accresce la sensibilità sul tema nelle istituzioni, come nei comuni cittadini, e acuisce le criticità di alcuni domini in cui la IA sta divenendo pervasiva e che necessitano di adeguamenti se non addirittura di innovazioni normative.

L'ambito applicativo delle rilevazioni biometriche, in particolare di quella del riconoscimento dei volti e la sua applicazione a tecniche di sorveglianza di massa, è il contesto ideale per comprendere quali siano i valori irrinunciabili in presenza di un rilevante progresso tecnologico, gli strumenti normativi a disposizione, quelli ancora da definire e il ruolo della componente umana in questo complicato quadro sistemico. Nel Capitolo III si affronterà proprio il bisogno prospettico a livello giuridico per mantenere i benefici della tecnologia e non essere, dunque, responsabili per un rallentamento delle conoscenze e del progresso del genere umano, senza ledere diritti che, proprio attraverso il GDPR, sono diventati evidenti a tutti coloro che hanno analizzato il Regolamento non solo a livello normativo ma anche nelle pieghe della consapevolezza che ognuno deve possedere per essere un "integrato" *protetto* nei diritti e non un "apocalittico"[420].

Ci sono molti aspetti chiave che a questo punto della trattazione si potrebbero evidenziare, ma tra essi emergono con forza dallo scenario descritto due binomi o se, non si risolveranno in modo efficace, dicotomie: dato-diritti e dato-qualità. Si è diffusamente sviluppato il tema del bilanciamento tra protezione dei dati e aspettativa di privacy, come anche di diritti e sicurezza. Per poter impiegare i dati oggetto del trattamento devono essere verificate tutte le condizioni dettagliate nei paragrafi precedenti del corrente Capitolo, seguendo l'inquadramento normativo del GDPR e le sue relative implicazioni nazionali attraverso i Garanti degli Stati membri e della 2016/680 (e anche 681). In pratica un *buon* dato, da punto di vista del suo impiego, non deve ledere i diritti dell'interessato e deve essere il frutto di una motivazione adeguata e prevista da Regolamento e Direttiva europee. Tra questi diritti va menzionata anche la durata della conservazione del dato[421]. Inoltre, la bontà del dato è anche relativa al suo effettivo contenuto informativo, cioè il dato deve contenere elementi utili, chiari e precisi affinché il suo impiego non sia di danno né per il titolare dei dati, né per il titolare del trattamento e né per autorità interessate al dato stesso. Un dato impreciso induce errori e gli errori sono sia forieri di possibili discriminazioni, o comunque violazioni dei diritti, ma anche di un rallentamento dell'opera delle autorità preposte alla protezione dei cittadini attraverso le loro attività investigative e di tutte le fasi successive necessarie per perseguire un reato.

[420] ECO, *Apocalittici e integrati*, cit.
[421] *supra* § 4.5

Emergono, dunque, tre aspetti nell'uso del dato personale che riassumono quanto detto: l'*ammissibilità*, la *compiutezza* e la *conservazione*. Se queste caratteristiche rispettano l'ambito normativo, il dato sarà utile e impiegato in modo legittimo. In termini di *ammissibilità* dei dati, la criticità del tema era già evidente prima della emanazione ed entrata in vigore del GDPR e della Direttiva 2016/680 sul trattamento dei dati personali. In particolare, creava perplessità il rapido progresso tecnologico in grado di fornire agli inquirenti variegati strumenti di sorveglianza corredati e relative elaborazioni dei dati rilevati. Tra questi strumenti di rilevazione dei soggetti interessati non si annoverano solo le telecamere per la videosorveglianza, precursori "meno intelligenti" del sistema SARI[422], ma anche la localizzazione in tempo reale a mezzo di sistemi quali il Global Positioning System (GPS)[423] e le attività finalizzate alla rilevazione di «flussi unidirezionali di dati non comunicativi (c.d. perquisizioni online)»[424], che possono avvenire anche semplicemente attraverso quanto pubblicato dal soggetto sui suoi profili social (per esempio, Facebook). Tali rilevazioni, i limiti relativi alla loro ammissibilità, il loro bilanciamento con la sfera privata dell'individuo nonché l'impatto di tale tutela sul diritto processuale penale rappresentano un delicato equilibrio, che oggi può avvalersi anche del quadro normativo europeo offerto dalla 680. Come anzidetto, un dato "informativo" è un dato di buona qualità, completo, corretto e che, dunque, riduce il margine di errore e di opinabilità sia nella sua elaborazione automatica che nella sua interpretazione umana, algoritmica o integrata. L'efficacia del dato ai fini del suo impiego, ma nel rispetto dei diritti degli interessati, rappresenta un delicato equilibrio anche in termini di *quantità*, non solo di qualità. Il dato, dunque, oltre a dover essere di qualità ai fini delle attività di trattamento per cui è destinato, deve anche non eccedere la quantità necessaria ai fini del trattamento stesso.

Ad opinione di chi scrive, l'esuberanza quantitativa del dato, infatti, oltre ad aumentare la mole delle informazioni personali del titolare che escono dall'alveo della sua sfera personale, può non essere di aiuto neanche per i destinatari del trattamento, esigendo maggior risorse di tempo nell'esaminarlo e di capacità di memoria dei dispositivi di archiviazione elettronica atti alla conservazione. Il difficile compromesso, dunque, per un dato per essere considerato di appropriata *compiutezza* è ovviamente la pertinenza con le finalità del trattamento, la completezza, sia in termini di contenuti che di qualità, e la non eccedenza e quindi la quantità necessaria e non eccedente le finalità per cui è richiesto. Gli elementi descrittivi della compiutezza di un dato personale si possono

[422] *supra* § 4.4

[423] *GPS* è un sistema per la determinazione delle tre coordinate geocentriche relative alla posizione di ogni punto posto sulla superficie terrestre o al di sopra di essa.

[424] ANDOLINA E., *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della privacy e onde eversive*, in *Archivio Penale*, 2015, 3, 916

considerare intrinseci alla natura del dato e, infatti, i principi enunciati sono già evidenti nella disseminazione[425] del Garante precedente all'entrata in vigore del GDPR[426].

Per quanto concerne la data retention, appare complessa la gestione del tempo di conservazione dei dati, perché esso è collegato al tipo di informazione contenuta nel dato stesso, la cui importanza nel lasso temporale può essere non omogenea all'interno dato complessivo. Il dato, infatti, quando presenta informazioni articolate e diverse tra di loro, e dunque non è omogeneo, ha una parte del contenuto che perde d'importanza più rapidamente nel tempo e un'altra più resiliente alla durata dell'intervallo temporale. A parere di chi scrive, l'omogeneità nel dato in termini di rilevanza nell'intervallo temporale sarebbe di ausilio ad una più efficace data retention. Tale approccio comporta che il dato da richiedere all'individuo per un determinato trattamento deve essere ben "progettato" preventivamente, anche alla luce delle criticità legate alla sua *conservazione*, in modo che contenga un elevato livello di omogeneità dal punto di vista della sua durata, cioè dell'intervallo in cui è utile conservarlo.

La conservazione, tra l'altro, ha, come sopra evidenziato, non solo una dimensione temporale legata alla durata, ma anche una di spazio di archiviazione richiesta alle memorie elettroniche e, conseguentemente, di velocità di accesso alle memorie stesse per il recupero del dato al bisogno. L'analisi già effettuata sulla data retention[427] rende anche evidente come la durata della conservazione sia difficile da uniformare non solo nei vari Stati membri ma anche in relazione ai diversi domini applicativi nei quali il trattamento è richiesto. Il caso del trattamento dei dati dei gestori telefonici con le conseguenti deliberazioni della Corte di Giustizia europea[428] offrono uno scenario esemplificativo della doppia dimensione geografica e applicativa che la conservazione dei dati personali possiede intrinsecamente.

6.1. *(Segue):* la visione della CGUE ed elementi di riflessione.

Per comprendere la visione della CGUE risulta utile considerare il percorso definito dalle sue sentenze, dalle quali emergono elementi utili per riflessioni e proposte in merito al futuro del trattamento dei dati, sia in termini di conservazione che di tipologia. Per quanto concerne l'ambito delle comunicazioni elettroniche, dove, come già evidenziato, la data retention è un elemento di centrale rilevanza e che dunque fornisce utili spunti per comprendere come tale aspetto debba essere trattato nei vari ambiti applicativi.

---

[425] *disseminare* per stimolare la consapevolezza e conoscenza sulla materia dei trattamenti dei dati personali e della privacy, *supra* § 4.4
[426] PECORA L. – STAGLIANÒ G., (curatore LEANTE M.), *Massimario 1997-2001. I principi affermati dal Garante nei primi cinque anni di attività*, 2004, 23
[427] *supra* § 4.5
[428] *supra* § 4.5

In particolare, nella sentenza G.D. del 2022[429], alcuni autori[430] evidenziano l'intento della CGUE di ridisegnare l'assetto della data retention sulla base del già citato principio di proporzionalità, sostenendo una conservazione dei dati limitata a luoghi, zone, tempi e soggetti specifici, quindi a «bassa intensità». In tale sentenza viene richiamato quanto stabilito nella previa sentenza Tele2 Sverige[431] e, come già evidenziato nella trattazione[432], in merito all'illegittimità di una conservazione indifferenziata e generalizzata dei dati di traffico e ubicazione degli utenti iscritti sui mezzi di comunicazione elettronica «per finalità di contrasto alle forme di criminalità grave». Tale conservazione, infatti, viene ritenuta dalla Corte come gravemente invasiva dei già richiamati diritti alla privacy e alla protezione dei dati personali e, tuttavia, non vengono apposti i limiti presenti nella sentenza G.D. del 2022, relativamente a soggetti che potrebbero essere coinvolti nella commissione di un reato grave. Inoltre, nella sentenza Tele2 Sverige non vengono incluse limitazioni, diversificazioni o eccezioni a seconda della finalità perseguita e non si richiede alcun tipo di relazione tra i «dati oggetto di trattamento e conservazione e una minaccia per la sicurezza pubblica».[433]

In merito alla sentenza La Quadrature du Net[434] del 2020, viene ribadita l'interpretazione della direttiva 2002/58/CE[435], considerata sulla base della Carta dei diritti fondamentali[436] e del TUE[437], che si oppone a una normativa nazionale che detenga in modo preventivo, generalizzato e indifferenziato i dati relativi a traffico e ubicazione degli utenti di servizi di comunicazione elettronica accessibili al pubblico, per fini che non collegati alla salvaguardia della sicurezza nazionale e a correlate minacce reali o prevedibili. Inoltre, tale interpretazione è avversa alla subordinazione, dell'accesso ai dati conservati da parte delle autorità competenti, a un controllo

[429] CGUE, Grande Sez., sent. 5 aprile 2022, *G.D. c The Commissioner of the Garda Síochána e a.*, C-140/20
[430] CISTERNA A., *Data retention: la lotta ai crimini gravi non giustifica la conservazione generalizzata dei dati* in *Guida al diritto*, 15/2022, 16-23
[431] CGUE, Grande sez., sent. 21 dicembre 2016, *Tele2 Sverige AB c. Post-och telestyrelsen*, causa C-203/15
[432] *supra* § 4.5
[433] NINO M., *La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE* in *Il diritto dell'unione europea*, 2021, 1, 93-124
[434] CGUE, Grande sez., sent. 6 ottobre 2020, *La Quadrature du Net c. Premier ministre e a.*, causa C-511/18 e C-512/18
[435] Parlamento europeo e Consiglio, Direttiva del 12 luglio 2002, n. 58, *relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)*
[436] Carta dei Diritti Fondamentali, cit., art. 7 *Rispetto della vita privata e della vita familiare*, art. 8 *Protezione dei dati di carattere personale*, art. 11 *Libertà di espressione e d'informazione*, art. 52, *Portata dei diritti garantiti*
[437] Trattato sull'Unione Europea, C 326, 2007, art. 4 co 2, «L'Unione rispetta l'uguaglianza degli Stati membri davanti ai trattati e la loro identità nazionale insita nella loro struttura fondamentale, politica e costituzionale»

preventivo di un giudice o organo amministrativo indipendente. Un ulteriore e importante aspetto legato alla tipologia di dati personali è l'inclusione attuata dalla medesima sentenza degli indirizzi IP[438] e dei dati relativi all'identità civile. In merito agli indirizzi IP essi vengono ritenuti strumentali per l'individuazione del soggetto che possiede, ad esempio, il computer che dà origine alla comunicazione. La raccolta delle informazioni relative ai terzi destinatari della comunicazione viene esclusa e, pertanto, l'indirizzo IP detiene contenuti ad inferiore grado di sensibilità rispetto ad altri dati personali. Per la Corte la conservazione generalizzata e indifferenziata degli stessi risulta giustificata, considerando che gli indiritti IP possono essere uno strumento di ausilio per il contrasto alla criminalità e la prevenzione di minacce alla sicurezza pubblica e nazionale, entrambe a carattere di alta gravità. L'indirizzo IP consente, infatti, di poter risalire alla navigazione online e quindi permette l'individuazione del soggetto, ma tale conservazione necessita di condizioni, qui non ben definite, sostanziali e procedurali.[439]

Quanto esposto riflette la richiesta del Consiglio dell'Unione alla Commissione in merito ad un'unitaria ed omogenea rielaborazione della normativa europea sul tema cruciale della data retention.[440] La base di tale rielaborazione è l'esigenza che le svariate categorie di dati siano accessibili alle autorità nazionali giudiziarie e di polizia, che consentano un efficace lotta alle forme gravi di criminalità e terrorismo e la considerazione della necessità di cooperazione e scambio di informazioni tra le autorità competenti nei casi transfrontalieri. Tale necessità sarebbe negativamente influenzata dalle differenti norme giuridiche tra gli Stati membri in merito al trattamento dei dati personali.

Ulteriori elementi di riflessione concernono l'interpretazione fornita dalla CGUE dell'articolo 55, comma 3 del GDPR[441], in merito al quale ritiene che sia ammissibile la messa a disposizione temporanea dei documenti di un procedimento giurisdizionale, che ricomprendano dati personali, da parte dell'organo giurisdizionale. La destinazione di tali documenti sono i giornalisti cosicché possano riferire in merito allo svolgimento dello specifico procedimento con maggiore accuratezza e completezza. Tale tipo di apertura rientra, secondo tale interpretazione, nelle funzioni giurisdizionali dell'organo stesso[442] e consentendo allo stesso tempo la diffusione di informazioni che non ledano i diritti dei soggetti interessati oltre i limiti stabiliti dalle normative europee.

---

[438] *Internet Protocol Address* o indirizzo IP è un codice numerico usato da tutti i dispositivi, quali i computer o server web, per navigare in Internet e per comunicare in una rete locale.
[439] NINO, *La disciplina internazionale ed europea della data retention*, cit., 93-124
[440] Consiglio dell'Unione europea, *Conclusioni del Consiglio dell'Unione europea sulla conservazione dei dati per finalità di lotta contro la criminalità*, 27 maggio 2019, 9663/19
[441] Regolamento (UE) 2016/679, GDPR, cit., art. 55, 3 «Le autorità di controllo non sono competenti per il controllo dei trattamenti effettuati dalle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali»
[442] CGUE, Sez. I, sent. 24 marzo 2022, *X, Z c Autoriteit persoonsgegevens*, Paesi Bassi, C-245/20

Nell'opinione di chi scrive, quanto sancito dalla sentenza La Quadrature du Net in merito alle prove ammissibili nei tribunali penali nazionali, offre uno spunto di riflessione sulla sorveglianza di massa. In tal senso, una prova che viene assunta in modo illegittimo, in violazione della Direttiva n. 2002/58, può considerarsi ammissibile qualora sia contestabile, per cui tale meccanismo si potrebbe ritenere trasferibile alla contestazione della prova assunta con sistemi di sorveglianza di massa. Per esempio, nel caso di una ripresa, effettuata nello stesso istante di quella di un sistema di sorveglianza, da parte di soggetti vicini all'interessato, essa potrebbe, come prova, fornire ulteriori elementi integrativi. Plausibilmente, potrebbe riprende gli eventi che avvengono nell'eventuale "punto cieco" delle telecamere utilizzate dal sistema di sorveglianza. In tal senso, così come indicato nella sentenza sopracitata, quando è possibile per il soggetto interessato contestare la legittimità di una prova che lo riguarda, il diritto di difesa e al giusto processo si può ritenere rispettato, se non garantito.

CAPITOLO III – ASPETTI COMPARATIVI, PROPOSTE E PROSPETTIVE DEL RICONOSCIMENTO FACCIALE E DELLA SORVEGLIANZA DI MASSA

SOMMARIO: 1. Confronto tra scenari normativi extra-UE. – 2. Face recognition e discriminazione: gli Stati Uniti. – 2.1. *(Segue):* regolamentazione e criticità. – 3. Riconoscimento facciale e impiego nel Regno Unito e in Australia. – 4. Riconoscimento facciale in altre parti del mondo. – 4.1. *(Segue):* ulteriori criticità e discriminazioni. – 5. Riconoscimento facciale nel "modello" cinese. – 5.1. *(Segue):* ipotesi sul modello cinese. – 5.2. *(Segue):* il PIPL. – 5.3. *(Segue):* opposizione tra benefici e rischi. – 6. Ambiti di azione e relative proposte. – 6.1. *(Segue):* ruolo dell'operatore e algoritmi. – 6.2. *(Segue):* progettualità di algoritmi autovalutativi. – 6.3. *(Segue):* progettualità del dato personale per il principio di proporzionalità. – 6.4. *(Segue):* progettualità del dato per la conservazione ottimale. – 6.5. *(Segue):* progettualità del rischio per la data protection by design. – 7. Prospettive penali sull'inquadramento della IA nel processo. – 8. Conclusioni.

1. Confronto tra scenari normativi extra-UE.

Come già ampiamente dibattuto nei Capitoli precedenti, l'algoritmica di IA e, nella fattispecie le tecniche di riconoscimento facciale, possono essere affette da polarizzazione e sortire effetti discriminatori su razza, etnia e genere. Tale aspetto, peggiora il rapporto non solo tra IA e cittadini ma anche tra IA ed autorità preposte al controllo, poiché espone le autorità stesse in tal senso. Il mondo scientifico, anch'esso diviso su benefici e rischi dell'algoritmica, ma certamente allineato con i progressi tecnologici in modo estremamente prospettico, continua a adoperarsi per correggere e migliorare limitazioni prestazionali e bias presenti negli algoritmi. Ad esempio, è stata proposta una possibile tecnica per valutare la quantità di polarizzazione presente negli algoritmi di facial recognition e la relativa base dati di appoggio in relazione ai sottogruppi fenotipici.

Il fenotipo, essendo un insieme di caratteristiche morfologico-funzionali ed ambientali di un individuo, di fatto è distintivo di alcune caratteristiche soggette a potenziale discriminazione, quale ad esempio la razza[443]. La tecnica proposta è stata applicata ad un insieme di dati e il risultato è davvero interessante per comprendere la portata dei potenziali errori algoritmici di riconoscimento in termini di discriminazione[444]. Infatti, si è rilevato che i maggiori errori di classificazione si hanno nel riconoscimento di donne di colore, per le quali la rilevazione è errata nel 34.7% dei casi, mentre la categoria di uomini dalla pelle chiara viene erroneamente riconosciuta solo nello 0.8% dei casi.[445] I risultati, pertanto, sanciscono una netta disparità nella accuratezza del riconoscimento proprio in relazione a due fattori universalmente riconosciuti come discriminatori, non solo dagli algoritmi ma, e soprattutto, dal genere umano, cioè razza

[443] BUOLAMWINI J, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in *Proceedings of Machine Learning Research,* 81 (Conference on Fairness, Accountability, and Transparency), 2018, 1

[444] NAJIBI A., *Racial Discrimination in Face Recognition Technology*, in *Harward University- SITN*, 2020

[445] BUOLAMWINI J, *Gender Shades*, cit., 6

e genere.[446] Questi risultati sono importanti, ad avviso di chi scrive, per comprendere dove migliorare gli algoritmi di IA, in modo che i punti deboli del riconoscimento facciale, poiché discriminatori, possano essere emendati in modo che tali algoritmi costituiscano un efficace ausilio per le autorità preposte alla pubblica sicurezza.

Come anticipato nell'introdurre nel dettaglio le tecniche di facial recognition e la sorveglianza di massa[447], l'accettazione del rilevamento biometrico e il suo impiego varia passando da un contenente all'altro e, nell'ambito di uno stesso continente, da uno Stato all'altro. L'Unione europea, come si è visto nel corso della trattazione, ha una collocazione definita sul trattamento dei dati personali e, in particolare, su quello dei dati biometrici che, partendo dalla GDPR e dalla Direttiva 2016/680, si specializza con normative nazionali nei vari Stati dell'Unione. Un rischio collegato alla traduzione nazionale della normativa europea è, come già evidenziato, con una potenziale disomogeneità causata dalla genericità di alcuni passaggi nella normativa europea che, dunque, lascia ampia libertà di interpretazione e implementazione a livello del singolo Stato.[448] Per inquadrare ancora meglio lo scenario europeo e nazionale e individuare gli elementi propositivi in chiave prospettica che saranno oggetto dei due paragrafi conclusivi del presente Capitolo, si intende nei prossimi paragrafi analizzare alcuni scenari extra-UE in merito all'impiego del riconoscimento facciale e alla sorveglianza di massa.

2. Face recognition e discriminazione: gli Stati Uniti.

Come già descritto[449], migliorare le prestazioni degli algoritmi di IA a supporto dei rilevamenti biometrici e, in particolare, il riconoscimento facciale, è particolarmente auspicabile per non acuire il quadro particolarmente delicato negli USA della relazione tra forze dell'ordine e popolazione di colore[450], in particolare dopo la recente morte del medesimo G. P. Floyd[451], avvenuta a Minneapolis nel 2020 e la cui responsabilità è stata attribuita ad un agente di polizia e, per mancato intervento, a tre suoi colleghi.[452] La correzione degli aspetti discriminatori dell'algoritmica di riconoscimento che, applicata alla sorveglianza di massa potrebbe ingenerare criticità anche per le autorità

[446] GROTHER P. – NGAN M., – HANAOKA K., *Face Recognition Vendor Test (FVRT). Part 3: Demographic Effects*, NISTIR 8280, 2019
[447] *supra* Capitolo II § 1
[448] *supra* Capitolo II § 5.1
[449] *supra* § 1
[450] United States District Court, *Floyd v. City of New York*, 959 F. Supp. 2d 540, 2013, class action che pone l'accento sulla mancanza di qualsiasi ragionevole sospetto di effettuare fermi e perquisizioni nel caso specifico, in violazione del Quarto Emendamento e sulle evidenti disparità razziali di chi viene fermato e perquisito dal New York Police Department (NYPD).
[451] United States District Court, *State of Minnesota v. Chauvin*, Court File n. 27-CR-20-12646, 2021
[452] GRANDE E., *La condanna di Derek Chauvin per la morte di George Floyd: giustizia è fatta*, in *Questione Giustizia*, 2021

preposte alla pubblica sicurezza, è di interesse anche per i produttori dei sistemi di riconoscimento facciale e del software ivi ricompreso, che devono focalizzare gli sforzi per giungere a prestazioni migliori non solo in termini di velocità, ma soprattutto di imparzialità e trasparenza con un approccio responsabile. Dunque, il miglioramento è interesse di tutte le parti coinvolte: individui oggetto del rilevamento, autorità e venditori di algoritmi, software e sistemi integrati di riconoscimento facciale americani. In questo quadro si innesta la restrizione autonomamente decisa da parte di colossi del software per il riconoscimento facciali, quali IBM, Google, Amazon[453] e Microsoft, e la loro richiesta di normative federali sulla materia. Per esempio, IBM ha indirizzato una lettera al Congresso degli Stati Uniti ponendo l'accento sulla scarsa trasparenza su cui i rapporti negoziali tra agenzie di controllo e imprese impiegate si fondano e sollecitava una disciplina di tale materia. Inoltre, si evidenziavano nella lettera i rischi riconducibili alla sorveglianza di massa, la profilazione di tipo razziale e la violazione dei diritti umani e delle libertà fondamentali. [454] La necessità di normative a riguardo è motivata anche dall'elemento critico rappresentato del profitto che le grandi aziende possono trarre dai sistemi di sorveglianza in dotazione alla polizia e dalla mancanza di una regolazione dell'impiego da parte delle autorità preposte alla pubblica sicurezza.[455]

La scarsa accuratezza e attendibilità dei software di riconoscimento aveva già sollevato molte proteste, considerando la potenziale pericolosità se la metodologia di identificazione non produce risultati corretti. Ad opinione di chi scrive, il rischio collegato alla possibile violazione dei diritti basata sulla non accuratezza e sugli errori degli algoritmi è uno dei parametri cruciali su cui intervenire per rendere la IA un alleato e non una fonte di problemi nelle attività di pubblica sicurezza. Su questo aspetto si tornerà nel paragrafo 3 di questo Capitolo, per collegarlo anche a possibili proposte migliorative per l'uso della face recognition nella pubblica sicurezza nel bilanciamento necessario tra diritti e sicurezza.

Tra le aziende americane produttrici di sistemi e software per il riconoscimento facciale, dopo la citata uccisione di Floyd, si sono avute diverse reazioni. Esse vanno dal divieto temporaneo di impiego del proprio software da parte della polizia, come ad esempio per il pacchetto Rekognition prodotto da Amazon o Azure Viso o Video Indexer di Microsoft[456] o il software di IBM, alla sospensione generalizzata dell'impiego del face recognition e della commercializzazione dei software biometrici, come per Google, fino alla interruzione dello sviluppo di tale tecnologia, come per IBM, motivata dalla limitata affidabilità che si scontra con i profili etici nella sua applicazione. Va sottolineato la decisione più radicale adottata da IBM nel dichiarare

[453] LECHER C., *Shareholders are pushing Amazon to stop selling its facial recognition tool*, in *theverge*, 2019
[454] COLACURCI M., *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema Penale*, 14
[455] FEINER L. – PALMER A., *Rules around facial recognition and policing remain blurry*, in *CNBC*, 2021
[456] LEVY A., *Microsoft says it won't sell facial recognition software to police until there's a national law 'grounded in human rights'*, in *CNBC,* 2020

la cessazione di ogni sviluppo, ricerca e vendita delle tecnologie di riconoscimento facciale utilizzate a scopi di law enforcement.[457] In alcuni casi, taluni dei software sono stati mantenuti per l'impiego in specifiche applicazioni di particolare gravità, come ad esempio la ricerca di bambini scomparsi o la tratta dei minori.

È utile collegare quanto descritto in merito allo scenario americano, di applicazione delle tecniche di face recognition per applicazioni di pubblica sicurezza, con i pericoli sulla sorveglianza evidenziati dal Prof. Richards nel 2013[458], anno lontano sia dalla presa di posizione europea sulla privacy con il GDPR e la Direttiva 2016/680 che dagli eventi del Texas relativi alla morte di Floyd. L'aspetto interessante è che nello scritto si menziona genericamente il progresso tecnologico, pur senza uno specifico riferimento all'intelligenza artificiale, alle rilevazioni biometriche in generale e al riconoscimento facciale in particolare, ma si conclude che la sorveglianza deve essere gestita attraverso regolazioni normative e sociali, riconoscendone l'utilità in talune circostanze, ma anche la pericolosità in caso di abuso[459]. Se incardiniamo queste considerazioni in una realtà come quella americana, dove la discriminazione razziale è storicamente un tema dai connotati estremamente complessi, e le correliamo con i potenziali errori degli algoritmi di IA, il quadro può davvero assumere connotati delicati.

2.1. *(Segue):* regolamentazione e criticità.

Il quadro normativo americano che emerge, e che si vedrà anche in relazione agli altri Stati, appare caratterizzato da un vuoto normativo in cui l'utilizzo di strumenti di facial recognition sono lasciati alla scelta dei singoli uffici che collaborano direttamente con le imprese che vendono tali strumenti. Emerge quindi un quadro impregnato da interessi commerciali e di gestione dell'ordine pubblico.[460]
Secondo questa linea di pensiero la pressione esercitata dalle aziende per avere regolamenti biometrici miti sia la causa della mancanza degli stessi regolamenti, ritenendo che sarebbero di ostacolo all'innovazione disegni di legge più generali.

Vi è chi riporta[461] che la polizia newyorkese abbia speso dal 2007 circa 159 milioni di dollari in un "Fondo per Spese Speciali", poco noto, che non richiedeva un'approvazione da parte del consiglio cittadino o altri ufficiali municipali. Tali informazioni e documentazione vennero rese pubblico da due organizzazioni per i diritti civili, la Legal Aid Society e la Surveillance Technology Oversight Project (STOP), il cui direttore esecutivo Albert Fox Cahn sta lottando per l'accesso a tali documenti governativi che il New York Police Department (NYPD) si rifiuta di fornire.

[457] COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali*, cit., 14
[458] RICHARDS N. M., *The Dangers of Surveillance*, in *Harward Law Review*, 2013, 1937
[459] RICHARDS, *The Dangers of Surveillance*, cit., 1964
[460] COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali*, cit., 13
[461] FUSSELL S., *The NYPD Had a Secret Fund for Surveillance Tools*, in *Wired,* 2021

I documenti contrattuali rilasciati sono stati censurati in tale modo che risulta difficoltoso comprenderne il contenuto e, in particolare, il rapporto tra l'NYPD, fornitori e la popolazione. Un evento rilevante in termini di possibili peggioramenti dello stato è stata la protesta da parte del movimento Millions March, affiliato a quello del Black Lives Matter, per l'uccisione di Eric Garner, avvenuta nel 2014 da parte di un poliziotto. La peculiarità che si è verificata è consistita nei problemi dei dispositivi elettronici dei manifestanti che si sospetta sia stata causata da un segnale interferente intenzionale ad opera della polizia stessa.

A parere di chi scrive, considerando l'importanza del tema dei dati personali di questa trattazione, relativamente ai quali si è parlato di *raccolta* dei dati, emerge qui una deprivazione del diritto alla manifestazione pacifica, sancito nel Primo Emendamento della Costituzione americana, e alla privacy delle comunicazioni personali, soprattutto in assenza di alcuna richiesta di consenso. Tale ingerenza nella sfera personale dei manifestanti ha portato il New York City Liberties Union (NYCLU)[462] a fare causa all'NYPD per ottenere maggiori informazioni sull'utilizzo degli strumenti *stingray* presumibilmente utilizzati per interferire con i telefoni dei manifestanti. Gli strumenti stingray, di cui sono stati rilasciati i documenti di acquisto da parte della polizia, sono falsi ripetitori di telecomunicazioni che innestandosi al posto di una stazione base nella comunicazione coi i dispositivi cellulari, possono di fatto anche rilevarne i contenuti, in particolare della messagistica oltre a poter risalire alla posizione degli individui. Gli individui oggetto di questa intercettazione non risultavano essere accusati di alcun crimine, evidenziando ancor di più la violazione delle libertà che era stata perpetrata, nella pacifica manifestazione tutelata dalla Costituzione americana. La ripetuta dichiarazione da parte della polizia di non poter né confermare né negare il possesso di tali strumenti condusse alla causa Millions March NYC v. NYPD[463] che costituisce un precedente in merito alla risposta *non-Glomar*, ovvero un rifiuto vago e continuo alla richiesta di documenti pubblici, di solito utilizzata solo quando si tratta di questioni altamente sensibili di sicurezza nazionale. Tale precedente relativo a una maggiore trasparenza sulla intercettazione telefonica, in termini di sorveglianza, assume rilevanza in quanto potenzialmente in grado di prevenire che le forze di polizia usino tali sistemi in modo indiscriminato e di nascosto.

Il quadro che si viene a delineare in merito alla sorveglianza telefonica mostra come essa sia uno strumento vastamente utilizzato in America, sebbene a volte vi siano concessioni da parte dello Stato o di agenzie federali per il loro utilizzo, come nel caso del procuratore distrettuale californiano e dei suoi accordi di condivisione degli strumenti stingray con i dipartimenti di polizia di Oakland e di Fremont. Inoltre, il

[462] *NYCLU* è una organizzazione no-profit americana e uno dei principali difensori delle libertà e dei diritti civili

[463] Supreme Court of the State of New York, *Judgment Millions March NYC v. NYPD*, January 14, 2019, NYSCEF, doc. n. 21, index 100690/2017

dipartimento di sicurezza nazionale, Homeland Security, ha finanziato l'acquisto di tali strumenti per le forze d'ordine sia locali che statali. [464]

A livello federale, il Commercial Facial Recognition Privacy Act (CFRPA)[465] è l'atto di regolamentazione più recente in materia di privacy, relativamente al riconoscimento facciale, che risale al 2019 ed è stato introdotto al Senato. Il CFRPA mira alla espansione della conoscenza dell'utilizzo commerciale del riconoscimento facciale in un'ottica di trasparenza. Inoltre, sancisce per le entità di natura privata il divieto alla raccolta e diffusione dei dati dei propri clienti in mancanza di consenso e di utilizzo della tecnologia a fini discriminatori. In aggiunta, impone che i dati non siano condivisi con terze parti e richiede il necessario consenso affermativo degli utenti a cui i dati appartengono.

È utile, per avere un quadro complessivo del contesto statunitense, descrive qualche elemento dell'attuale regolamentazione degli stati americani. Infatti, benché esista una situazione non completamente definita della regolamentazione a livello federale che, come è stato illustrato, sta causando criticità e rallentando sia l'accettazione da parte della popolazione che una adeguata traduzione normativa, i vari Stati stanno gestendo in maniera disomogenea la materia del riconoscimento facciale. Tale considerazione suggerisce un confronto con la situazione europea in cui esiste un contesto normativo sovranazionale a cui adeguarsi da parte degli Stati membri, pur essendoci sia nel Regolamento 2016/679[466] che nella Direttiva 2016/680[467], un certo grado di libertà su alcuni aspetti che può tradursi in un divario nel recepimento e attuazione.

La situazione che si delinea negli Stati americani è diversificata non solo in ragione della diversa regolamentazione ma anche della mancanza di questa nella maggior parte degli Stati, come Colorado e Montana, che hanno fallito nei tentativi di emanare una legislazione sul riconoscimento facciale. Perciò, almeno allo stato attuale, la maggior parte degli Stati non ha emanato una regolamentazione per impedire alle aziende private di utilizzare la tecnologia di riconoscimento facciale, mentre sembra esserci una nuova tendenza nei diritti alla privacy tra gli Stati, quali Illinois, Texas e California, che hanno introdotto normative che limitano l'uso dei dati biometrici, in assenza di preventivo consenso, da parte delle aziende private. In California dal 2018 si regola la legge sulla privacy dei consumatori rivolta a entità a scopo di lucro che acquistino, ricevano, vendano o condividano dati personali di un elevato numero di utenti, dispositivi o nuclei familiari e da cui traggano più della metà del loro profitto annuale.

[464] KNOX L., *NYPD, told it can't use "Glomar" denial, now claims it has no records on Millions March cell phone surveillance* in *Muckrock,* 2019
[465] 116th Congress (2019-2020): *Commercial Facial Recognition Privacy Act,* 14 marzo 2019, S.847, Congress.gov, Library of Congress,
[466] ROSSI DAL POZZO, *Alcune riflessioni a margine della nuova disciplina in materia di protezione dei dati personali di cui al Regolamento (UE) 2016/679/UE*, cit., 19
[467] GALGANI, *Giudizio penale, habeas data e garanzie fondamentali*, cit., 9

La peculiarità di tale legge risiede nella copertura offerta al riconoscimento facciale, includendo tra i dati personali anche le informazioni biometriche e i dati di riconoscimento facciale, oltre a richiedere il consenso dei consumatori previo all'utilizzo.

Il consenso risulta centrale anche in una legge dell'Illinois del 2008, tuttora vigente, nella raccolta, inclusiva dei dati biometrici, delle informazioni personali e la cui particolarità risiede nella possibilità di fare causa a un'azienda che abbia raccolto dati senza consenso e senza avere l'onere di dimostrare il danno. La menzionata legge dell'Illinois va sotto il nome di Biometric Information Privacy Act (BIPA)[468] e consente, infatti, un diritto di azione privato, che qualora mancasse determinerebbe la necessità della decisione del soggetto da citare in giudizio da parte dei procuratori generali. Data la potenziale nascita di azioni collettive, che estenderebbero la durata della causa, oltre a culminare in sentenze di grande rilievo, le aziende si oppongono alla possibilità dei soggetti di un'azione privata. In relazione a quest'ultima, nel 2018 con una sentenza[469], la Corte Suprema dell'Illinois ha precisato che sia necessaria la verifica di una violazione e non necessariamente la dimostrazione di avvenuti danni. I limiti posti alle aziende in materia di dati biometrici sono stati regolamentati nel Texas dallo Statuto, approvato nel 2009, The Capture or Use of Biometric Identifiers Act (CUBI) conosciuto anche come Texas Business and Commerce Code che richiede la preventiva informazione e consenso dell'interessato in funzione dell'acquisto e/o vendita dei dati biometrici oltre alla subitanea distruzione delle stesse.[470] Nello Stato di Washington l'acquisizione o possesso dei dati biometrici non è regolamentata, ma è prevista la registrazione degli stessi secondo un modello per cui i dati non sono direttamente riconducibili all'immagine di un soggetto, anche se nei database essi vengono abbinati alle informazioni identificative. [471] Si può ritenere che in tale modello vi sia un certa protezione del soggetto in quanto l'informazione viene, in pratica, criptata e quindi solo attraverso di una chiave di criptazione si può accedere al dato "in chiaro". Ad opinione di chi scrive, anche se i dati fossero criptati, la protezione verso il titolare sarebbe relativa poiché i dati sono in possesso di chi li ha acquisiti, senza che sia stato richiesto alcun consenso.

Per quanto concerne i tentativi espletati nel limitare l'uso del riconoscimento facciale da parte delle forze dell'ordine, confrontandolo con la situazione newyorkese in merito al tema, alcuni Stati si stanno muovendo nella protezione dei dati biometrici dei

[468] Illinois, *Biometric Information Privacy Act (BIPA)*, 740 ILCS 14/1 et seq. (West 2016), 2008
[469] Illinois Supreme Court, *Judgment Rosenbach v. Six Flags Entertainment Corp*., 2018, docket n. 123186
[470] Texas Statute, *The Capture or Use of Biometric Identifiers Act* (CUBI) or *Business and Commerce Code*, title 11, *personal identity information,* subtitle a., *identifying information,* chapter 503, *biometric identifiers,* 2007 modificato da Acts 2017, 85th Leg., R.S., Ch. 913 (S.B. 1343), Sec. 1, eff. September 1, 2017
[471] Washington, House Bill 1493, 2021, app.leg.wa.gov

cittadini. In tale direzione si è mosso lo Stato del Vermont che nel 2020 ha vietato l'utilizzo del face recognition da parte delle forze dell'ordine a valle della approvazione di una moratoria proprio relativa a questa tecnologia[472]. Tra l'altro è interessante l'ampliamento che il Vermont ha implementato della definizione di face recognition, riconoscendo anche quell'aspetto della captazione biometrica che riguarda i frangenti emotivi, già menzionati nel Capitolo II[473].[474]

Uno degli storici Stati del Sud, la Virginia, ha vietato l'acquisizione o distribuzione del sistema per il riconoscimento facciale alle forze dell'ordine locale e alla polizia del campus universitario. Tuttavia, le forze dell'ordine locali possono utilizzare il riconoscimento distribuito da altri e quelle dello Stato non sono state limitate nell'uso di questa tecnologia.[475]

Al contrario, il Massachusetts ha approvato una legge, la Facial and Other Remote Biometric Recognition[476], che stabilisce il necessario l'ordine del tribunale o un'emergenza immediata perché le forze dell'ordine statali possano utilizzare la tecnologia di face recognition.[477] Nello Stato del Maine, similmente, esiste una legge che vieta l'uso della sorveglianza facciale da parte di specifici dipendenti e funzionari governativi. Tale legislazione si differenzia dalla precedente in quanto si applica a tutti i dipendenti governativi, a meno che non stiano conducendo un'indagine relativa ad un crimine considerato grave e via sia ragionevole motivo di ritenere che chi ha commesso il crimine sia il soggetto non identificato in una immagine.[478] In tale caso si differenzia nuovamente dal Massachusetts che richiede un ordine del tribunale che autorizzi l'utilizzo del riconoscimento facciale e che venga emesso un mandato penale da un tribunale che ne ha la competenza. La legge dello Utah è molto simile a quella del Maine, introducendo anch'essa l'eccezione di utilizzo in presenza di indagini in cui emerga una "buona" probabilità che il soggetto sia autore o connesso in qualche modo al crimine in esame.

È utile per completare questo *excursus* in alcuni degli Stati americani, menzionare, anche alla luce degli avvenimenti di New York e delle conseguenti proteste sopra menzionate, che la California abbia legiferato in merito al divieto di impiego del

[472] Vermont Statute S.124 Acts and Resolves No. 166. Sec. 14, *Moratorium On Facial Recognition Technology*, 2020
[473] *supra* Capitolo II § 1
[474] ACLU of Vermont, *enactment of s.124, the nation's strongest statewide ban on law enforcement use of facial recognition technology*, in *ACLU of Vermont*, 2020
[475] Virginia, HB 2031, *Facial recognition technology; authorization of use by local law-enforcement agencies and public institutions of higher education*, in *LIS Virginia's legislative information system,* 2021
[476] Massachusetts, *Facial and Other Remote Biometric Recognition*, 2021
[477] PEASLEE E., *Massachusetts Pioneers Rules For Police Use Of Facial Recognition Tech*, in *NPR*, 2021
[478] Maine House and Senate, *An Act to Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials*, 2021

riconoscimento facciale delle telecamere corporee da parte delle forze dell'ordine, non menzionando però le altre telecamere in dotazione alla polizia.[479]

2.1.1. *(Segue):* prospettive.

Dal quadro delineato emerge come alcuni Stati abbiano percepito la urgenza di limitare l'utilizzo indiscriminato e non regolamentato dei software di riconoscimento facciale e biometrico da parte delle forze dell'ordine. È parso che la implementazione di un diritto di azione privata, come in Illinois, sia stato un buon deterrente per iniziare a garantire che le aziende rispettino i diritti di privacy dei propri consumatori. Nonostante questi segnali potenzialmente positivi l'assenza di leggi federali concernenti l'utilizzo di strumenti di sorveglianza, gli eventi che continuano a verificarsi nello scenario americano indicano, oltre a un clima di tensione anche la violazione dei diritti dei cittadini americani, mettono in evidenza l'assenza di leggi federali.

Ciononostante, è stato di recente compiuto un passo avanti nella consapevolezza e definizione del bilanciamento tra diritti e sicurezza, anche in relazione alla sorveglianza di massa. Infatti, nel 2022 in materia di privacy il Congresso ha introdotto il *Data Privacy and Protection Act*[480] atto a creare forti meccanismi di supervisione e stabilire un'applicazione significativa dei diritti fondamentali sulla privacy dei dati. Nello stesso anno, l'Ufficio della Casa Bianca sulle Politiche Scientifiche e Tecnologiche ha pubblicato il *Blueprint* per una *Bill of Rights* in materia di IA[481], un modello di supporto allo sviluppo di politiche e pratiche di protezione dei diritti civili e di promozione di valori democratici nel costruire, distribuire e amministrazione dei sistemi automatizzati. Tale documento è un libro bianco non vincolante e non è parte della politica governativa degli Stati Uniti che si pone nella direzione di una tutela di contrasto alla discriminazione algoritmica. Il quadro delineato dal libro bianco è applicabile ai sistemi automatizzati che possono impattare in modo significativo i diritti dei cittadini o l'accesso a risorse o servizi essenziali.

Ad opinione di chi scrive sono riscontrabili similitudini nelle dichiarazioni programmatiche del Blue Print con il GDPR[482], nello specifico per quando concerne il consenso dell'interessato. Il Blue Print ritiene che progettisti, sviluppatori e distributori di sistemi automatizzati dovrebbero chiedere il consenso e rispettare le scelte del soggetto il più possibile. Al contempo, si richiede comprensibilità e chiarezza della richiesta del consenso, come nel GDPR, e del funzionamento del sistema.

---

[479] California State, *The California Privacy Rights Act (CPRA)*, 2020, formerly the California Consumer Privacy Act (CCPA), which takes effect January 1, 2023

[480] 117th Congress, *American Data Privacy and Protection Act*, H.R.8152, 2022

[481] White House Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*, 2022, 5-6

[482] *supra* Capitolo II § 4.1

Si aggiunge inoltre che non dovrebbero essere utilizzata una sorveglianza perpetua in ambiti in cui potrebbe provocare la limitazione dei diritti, le opportunità o l'accesso dei titolari dei dati.

Come sostenuto in precedenza da chi scrive, il Blue Print pone l'accento sulle tutele da prendere per contrastare la discriminazione algoritmica così da utilizzare e progettare sistemi in modo equo e includendo nella fase di progettazione del sistema valutazioni proattive dell'equità, oltre a una valutazione d'impatto algoritmica indipendente che ricomprenda i risultati dei test effettuati dal sistema. Un'interessante aggiunta nel documento americano è la possibilità di scegliere l'alternativa umana al posto del sistema automatizzato, qualora, dato il contesto e le aspettative di protezione ad esso collegato, sia necessario proteggere gli individui da impatti particolarmente dannosi.

Una prospettiva che, ad opinione di chi scrive potrebbe essere utilmente impiegata, è la maggiore attenzione rivolta a sistemi automatizzati che, in ragione dell'ambito di applicazione sensibile e del loro impatto su diritti e libertà, quale giustizia penale, salute, istruzione e occupazione, dovrebbero essere progettati *ad hoc*, con un ulteriore sviluppo mirato proprio per la finalità a cui sono destinati. Ulteriormente, tali sistemi dovrebbero essere facilmente ispezionabili, consentendo l'accesso per tal fine, e dovrebbero prevedere uno specifico addestramento per qualsiasi soggetto che si trovi ad interagire con il sistema stesso[483]. Inoltre, è necessario includere il punto di vista della componente umana in merito a decisioni negative o ad alto rischio. Con particolare riferimento ai processi di *governance umana* e le valutazioni in merito a tempestività, accessibilità, risultati ed efficacia si suggerisce una relazione sulle attività, che dovrebbe essere resa pubblica ogniqualvolta possibile.[484] Secondo chi scrive, il documento americano fornisce ottimi spunti di implementazione pratica, ma non nell'ambito prettamente giuridico quanto piuttosto nell'organizzazione delle attività relative al sistema di IA e di una maggiore trasparenza sui meccanismi che operano nel sistema medesimo, al fine di prevenire le eventuali conseguenze legali già evidenziate.

In attesa che i principi enunciati nelle varie iniziative in corso per bilanciare diritti e sicurezza in un quadro normativo che ricomprenda la sorveglianza di massa e il riconoscimento facciale, continuano le attività di sensibilizzazione verso i diritti dei cittadini da parte di movimenti e organizzazioni mirate allo scopo. Infatti, per contrastare il fenomeno "intrusivo" nelle vite dei cittadini sono nate iniziative e campagne mirate a vietare l'uso dei sistemi di riconoscimento facciale e a ottenere l'accesso ai documenti della polizia americana proprio in merito ai contratti di acquisizione delle tecnologie. La campagna *Ban The Scan*, lanciata da Amnesty

[483] *supra* Capitolo II § 2, 4.3
[484] White House Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights*, cit., 7

International[485] nel 2021, la quale sostiene la necessità di vietare l'uso dei sistemi di riconoscimento facciale sostenendo che questa tecnologia minaccia i diritti fondamentali sia quando lavora correttamente che quando commette degli errori. Tale iniziativa ribadisce le ricadute discriminatorie sulle comunità di minoranze etniche e di colore sia in ragione della sua poca accuratezza che del suo funzionamento. Quanto illustrato si ricollega con la nascita del movimento dei già citati Black Lives Matter che, essendo stato preso di mira con il riconoscimento facciale, ha intentato causa alla polizia di New York per ottenere i documenti di quella sorveglianza.[486]

3. Riconoscimento facciale e impiego nel Regno Unito e in Australia.

Dopo aver approfondito gli aspetti legati al riconoscimento facciale, normativi e di criticità, e la sorveglianza di massa nella democrazia liberale degli Stati Uniti, si intende rivolgere l'attenzione verso altre realtà e per prima si intende focalizzarsi sul Regno Unito, considerando che da poco tempo non è più parte dell'Unione Europea e pertanto, rappresenta un significativo punto di partenza per la esplorazione delle regolamentazioni al di fuori dell'UE.

In Inghilterra la pronuncia del 2019 fornisce una base di legittimità all'utilizzo da parte delle forze dell'ordine della tecnologia di riconoscimento facciale, osservando inoltre come le normative in materia riescano a garantire un uso corretto della stessa in linea con quanto regolamentato per i diritti umani. Tale osservazione si basa anche sulla presenza del Commissario per la conservazione e l'uso dei dati biometrici, istituito nel 2012 successivamente al caso davanti alla Corte EDU[487] che condannava l'Inghilterra in ragione della violazione dell'art. 8 della CEDU data la conservazione delle impronte digitali dei richiedenti, dei dati legati al DNA e dei campioni cellulari, per trattare questioni relative al consenso, la conservazione e l'utilizzo di informazioni biometriche.

Il gruppo per le libertà civili Big Brother Watch[488], già citato a proposito della sentenza Big Brother Watch[489], nel luglio del 2022 ha denunciato all'Ufficio del Commissario per l'informazione del Regno Unito la cooperativa regionale di consumatori Southern Co-op e la compagnia Facewatch. Quanto è stato denunciato concerne l'utilizzo del face recognition in tempo reale, utilizzato per creare un profilo biometrico di ogni persona che entri in un negozio che utilizza i sistemi forniti da Facewatch. Viene

[485] *Amnesty International* è un'organizzazione non governativa internazionale impegnata nella difesa dei diritti umani
[486] UCCI M., «Il Grande Fratello vi guarda», in *Zeta LUISS*, 2022
[487] Corte EDU, Grande sez., sent. 4 dicembre 2008, S. and Marper v. United Kingdom, ric. n. 30562/04 and 30566/04)
[488] Big Brother Watch Team, *Big Brother Watch Files Legal Complaint Against Co-Op's "Orwellian" Facial Recognition,* in *Big Brother Watch*, 2022
[489] *supra* Capitolo II § 2

denunciata la violazione dei diritti sui dati e sulla privacy in quanto il negoziante se nutre il ragionevole sospetto, senza peraltro che la Facewatch fornisca linee guida precise a riguardo e, quindi, lasciando margini interpretativi all'operatore, che un cliente stia commettendo un reato. Il negoziante può quindi aggiungere il soggetto alla lista di "soggetti di interesse" e la polizia ha il potere di aggiungere foto e informazioni di corredo alla descrizione del reato che si ritiene essere stato commesso, che sia rubare o una condotta molesta.[490] Non solo vengono raccolti dati senza consenso ma vengono anche trasferiti ai clienti della Facewatch che possono negare l'ingresso al soggetto "schedato" oltre ad essere pubblicati sul sito della polizia e sul sito dell'ente di beneficenza per la prevenzione del crimine Crimestoppers. Inoltre, in materia di data retention, i dati vengono conservati fino a due anni, a meno che la polizia non ne richieda la proroga, mentre per gli altri soggetti la conservazione è limitata a tre giorni. Una "politica" nata per contrastare l'aumento del taccheggio con l'avvento del COVID-19, è diventato ora un sistema di sorveglianza esteso e di chiara violazione, ad opinione di chi scrive, della privacy dei cittadini oltre a non essere regolamentato. In tal senso si coglie la differenza rispetto agli orientamenti europei in materia di riconoscimento facciale in tempo reale rispetto al governo del Regno Unito. Va però riconosciuto che il Regno Unito abbia, secondo alcuni per prima, affrontato il problema di compatibilità dell'uso da parte della polizia di sistemi di riconoscimento facciale con la tutela dei dati personali e dei diritti fondamentali.[491]

Su tale problematica l'esempio dell'Australia mostra un interessante approccio organizzativo e promettente, in senso prospettico, sul piano normativo e come un orientamento lontano geograficamente possa, invece, essere vicina concettualmente a quello che ha implementato e la plausibile direzione futura dell'Unione Europea. Per inquadrare la relazione con il riconoscimento facciale del Continente Australiano è emblematico quanto accaduto nel 2020 in ragione della distribuzione delle tecnologie di rilevamento biometrico facciale e delle prove effettuate dalla Polizia Federale Australiana dei software dell'azienda statunitense Clearview AI. La controversia che nacque è derivata dalla incompatibilità con le norme sulla privacy e in tal senso si possono cogliere le divergenze di approccio sulla materia con gli Stati Uniti.

Nel 2022, i ricercatori della University of Technology di Sydney hanno completato il Facial Recognition Model Law Project, un progetto che risponde alle richieste di riforma in ragione delle innovazioni tecnologiche e propone un modello di legge che regolamenti nel Paese il riconoscimento facciale. Tale modello di tecnologia del riconoscimento facciale, redatto in collaborazione da un ex commissario dei diritti umani ed esperti di intelligenza artificiale,[492] parte dalla considerazione che le

[490] VETCH F., *UK supermarket uses facial recognition tech to track shoppers*, in *Coda*, 2023
[491] High Court of Justice, Queen's Bench Division, Divisional Court, September 4, 2019, Judgment R (Bridges) v. CCSWP e SSHD, Case n. CO/4085/2018
[492] DAVIS N., PERRY L., SANTOW E., *Facial recognition technology: Towards a model law*, in *Human Technology Institute, The University of Technology Sydney*, 2022

tecnologie biometriche possono essere usate sia per fare del bene che del male, in un'ottica che ricalca l'opinione di scrive sulla neutralità della tecnologia[493]. In tal senso, il modello non vieta né liberalizza tali tecnologie ma riconosce che in presenza del vuoto normativo siano a rischio i diritti dei cittadini.

È possibile impiegare in modo coerente con la legge internazionale sui diritti umani il riconoscimento facciale anche nel raggiungimento di benefici a livello collettivo ma tenendo presente che, in ragione della sua natura, il riconoscimento può limitare alcuni diritti umani. Perciò la legge modello si occupa della definizione dei singoli domini applicativi nel loro funzionamento, distribuzione e pubblicità nonché delle decisioni prese sulla base di tali tecnologie. Assume rilievo centrale il consenso dei soggetti interessati ai fini di decisioni libere e informate in materia dei loro dati biometrici.

Il documento si rivolge affinché implementi tali cambiamenti al Procuratore Generale Federale Australiano, indicando gli step di azione, fra cui rileva la responsabilità da attribuire, ad esempio, al Commissario Australiano per l'Informatore la creazione di standard tecnici in materia di riconoscimento facciale e l'indirizzamento degli sviluppatori con approfondimenti e risorse. Il processo di integrazione partirebbe dall'ambito territoriale per armonizzare la legge nelle giurisdizioni australiane arrivando, quindi, a coinvolgere altri ministri federali per instituire una *taskforce* governativa. Le finalità della stessa sono, ad opinione di chi scrive, da prendere a modello anche in altri contesti geografici, in quanto prevedono da una parte lo sviluppo delle tecniche biometriche in armonia con gli standard etici e legali e dall'altra condurre il paese a un coinvolgimento in ambito internazionale sulla medesima tecnologia, dimostrando come l'Australia possa protegge con la legge e incentivare l'innovazione simultaneamente.[494]

Come visto a proposito delle normative dei singoli Stati americani, si prospettano obblighi che influenzeranno le organizzazioni coinvolte nello sviluppo dei sistemi di riconoscimento facciale a livello privato. La differenza che si sottolinea concerne la previsione di obblighi anche per le organizzazioni governative a più ampio spettro.[495]

Il progetto australiano sin qui descritto è, secondo l'opinione di chi scrive, un buon modello sulla materia del riconoscimento facciale e nelle intenzioni del bilanciamento così complesso tra diritti e sicurezza. Se tutti i contenuti trovassero idonea implementazione a livello normativo ci si potrebbe raffrontare anche con un ottimo esempio di regolamentazione sulla materia e, in tal senso, si potrebbe trovare un terreno comune per potenziali collaborazione con l'Unione Europea. In quest'ottica giova ricordare che l'Australia nel suo progetto di legge e l'Europa nella Proposta di

[493] *supra* Capitolo I § 4.1

[494] MASCELLINO A., *Researchers pitch model law for facial recognition to Australian government*, in *Biometric*, 2022

[495] CATANIA P. – ALLEN C., *Facial recognition technology: a model law*, in *Corrs Chambers Westgarth*, 2022

Regolamento[496], utilizzano un approccio *risk based*[497], differenziando i diversi livelli di rischio. Nel progetto australiano sono base, elevato e alto e una simile categorizzazione è presente nella proposta europea in cui i livelli sono minimo, limitato, alto.[498] Inoltre, nel progetto australiano è prevista una valutazione d'impatto, Facial Recognition Impact Assessment, che terrebbe conto dei fattori di utilizzo del riconoscimento facciale, quali funzioni, prestazione, il contesto spaziale e se è stato prestato il consenso libero e informato. Oltre a tali fattori, lo sviluppatore o installatore della tecnologia dovrebbe considerare anche se i possibili risultati della stessa possano condurre a conseguenze legali o comunque significative. Guardando a tali fattori emerge la similitudine con la Proposta di Regolamento europea e la prospettiva di una integrazione del modello di tali proposte porta ad auspicare che sia una delle possibili strade nella garanzia del tanto ricercato equilibrio tra innovazione e protezione.

4. Riconoscimento facciale in altre parti del mondo.

Per continuare l'analisi dell'impiego e dell'eventuale scenario normativo in cui si inserisce la tecnologia di IA in tema di sorveglianza e riconoscimento, verranno illustrate alcune realtà ritenute significative per giungere a un quadro sistemico. Partendo dall'India, la Internet Freedom Foundation (IFF)[499] ha segnalato come la tecnologia di riconoscimento facciale sia stata utilizzata contro le comunità delle minoranze musulmane a Nuova Delhi, in particolare, a proposito di alcuni fornitori di software "opachi" alla polizia. Amnesty international ha lanciato la campagna Ban the Scan, già in corso contro il sistema di riconoscimento usato a New York[500], anche nei confronti del governo indiano in ragione della minaccia ai diritti delle comunità minoritarie e delle persone con la pelle più scura particolarmente a rischio di falsa identificazione e arresti. Nonostante ciò, si evidenzia come il governo abbia speso miliardi di rupie per una tecnologia di riconoscimento facciale, che vi sia o meno il consenso degli interessati, che utilizza le immagini dai social media, dai database e dalla polizia e dai giornali.

La segnalazione che il sistema utilizzato a Dehli sia accurato nel 2% dei casi[501], effettuata nel 2018, è certamente motivo di preoccupazione. Inoltre, Nel 2022, è stata

[496] Commissione Europea - proposta di Regolamento del Parlamento Europeo e del Consiglio, "*che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione"*, 206 final, 2021/0106, cit.
[497] *supra* Capitolo I § 3.1
[498] *supra* Capitolo I § 3.1
[499] *Internet Freedom Foundation* (IFF) è un'organizzazione indiana per le libertà digitali che cerca di garantire che la tecnologia rispetti i diritti fondamentali e il cui obiettivo è garantire che i cittadini indiani possano utilizzare Internet con le libertà garantite dalla Costituzione.
[500] *supra* § 2
[501] Press Trust of India, *Delhi police facial recognition software has only 2 per cent accuracy: HC told*, in *Business Standard*, 2018

segnalata la costruzione di centro di comando e controllo, Command and Control Center (CCC), in Hyderabad, capoluogo dello stato di Telangana nell'India Meridionale. Questa città è stata segnalata come una delle città più sorvegliate nel mondo[502] il cui CCC si connette all'infrastruttura a circuito chiuso di videocamere, *CCTV*[503], e costituisce il supporto al trattamento di dati provenienti da circa 600,000 videocamere, le quali possono anche essere usato con gli strumenti di riconoscimento facciale forniti alla polizia di Hyderabad.[504] Queste informazioni sono il frutto di ricerche condotte da Amnesty International con la collaborazione di volontari a Telagana che hanno inoltre identificato l'area in cui questo circuito di sorveglianza si dirama.

Ciò che è ancora più problematico è l'assenza di legislazioni sia a livello federale che locale in materia di privacy, diritti e sistemi di IA.

Un caso esemplificativo è l'utilizzo di strumenti di riconoscimento facciale già in uso in India, quali l'imposizione di misure di blocco, l'identificazione degli elettori e l'uso da parte della polizia e le testimonianze video di utilizzo da parte della polizia di Hyderabad di tablet per fotografe civili per strada. Tali episodi si sono susseguiti nel periodo dell'emergenza COVID-19, dalla fine del 2019 a luglio 2021, ed il tutto senza dare spiegazioni del perché della costrizione di abbassare la mascherina per essere fotografati. Tale episodio si pone in violazione con l'Identification of Prisoners Act[505] del 1920, per il quale la polizia non è autorizzata a scattare fotografie di individui che non siano stati arrestati o condannato per un reato, né a condividere le foto con altre forze dell'ordine. L'IFF ha affermato, infatti, la violazione dell'articolo 28 del IPA.

Il crescente utilizzo da parte delle forze dell'ordine non è certamente il solo punto critico della situazione. Attualmente non esiste alcuna legislazione che tuteli la privacy dei cittadini e, per quanto concerne la sorveglianza remota essa non è ricompresa nell'atto che regolamenta le comunicazioni elettroniche, l'Information Technology Act[506]. Il fatto che non vi siano deterrenti implica un plausibile aumento dell'utilizzo della tecnologia in modo indiscriminato, come dimostra l'aumento dei crimini informatici.[507] Nel 2019 è stata introdotta la legge sulla protezione dei dati che include il riconoscimento facciale e i dati biometrici[508] e nel quale il Chapter III è dedicato alle

[502] SUR A., *Hyderabad second most surveilled city in world, beats New York, London*, in *New Indian Express*, 2021
[503] *Closed-Circuit Television (CCTV)* in *Cambridge dictionary*, un sistema che invia segnali televisivi a un numero limitato di schermi, spesso utilizzato nei negozi e nei luoghi pubblici per prevenire la criminalità
[504] BANSAL V., *The Hyderabad model of CCTV surveillance*, in *Livemint*, 2020
[505] Law Commission of India, *The Identification of Prisoners Act*, 9 settembre 1920, act n. 33, in *Indian Kanoon*
[506] Ministry Of Law, Justice and Company Affairs (Legislative Department), *Information Technology Act*, n. 2, n. DL-33004/2000
[507] National Crime Records Bureau (NCRB), in *ncrb.gov*, 2020
[508] The Personal Data Protection Bill, n. 373, 2019

basi per trattare dati personali senza il consenso, come nel caso di un'epidemia o di disordini pubblici, quando debba essere fornita assistenza o garantita la sicurezza.

Inoltre, in tale disegno di legge alla clausola 36 è prevista l'esenzione dal trattamento dei dati personali nell'interesse della prevenzione, dell'accertamento, dell'indagine e del perseguimento di un reato o altra infrazione della legge in vigore. È prevista l'istituzione di un'Autorità per la protezione dei dati (DPA) per proteggere i dati sensibili e riservati da qualsiasi tipo di violazione e garantire anche un'attuazione efficiente del disegno di legge.

Nel caso di rapporti fiduciari[509], i dati che vengono trasferiti al fiduciario del diritto possono essere utilizzati come dati biometrici sono con l'autorizzazione del governo centrale, come previsto alla clausola 92. Il più recente disegno di legge, The Digital Personal Data Protection Bill[510], pubblicato, dopo mesi di consultazioni, dal governo federale indiano al fine di recepire le opinioni pubbliche in materia di dati personali. Alcuni sostengono che se venisse applicato permarrebbe il consenso "presunto", sulla b del quale la polizia avrebbe la facoltà di agire.

Dal quadro delineato in merito alla normativa, o forse alla sua assenza, emergono tutte le problematiche già evidenziate in merito all'impiego del riconoscimento facciale. Il collegamento tra riconoscimento facciale e dati personali ed è quindi importante fare riferimento alla Costituzione Indiana[511]. L'articolo 21 riconosce il diritto alla privacy il quale, successivamente a una sentenza della Corte Suprema Indiana[512], è stato riconosciuto come libertà fondamentale esercitabile nei limiti di conformità con la legge. Il rischio che mette in risalto la dicotomia della tecnologia con il diritto alla privacy è che in assenza di garanzie legali, è probabile che l'esecutivo agisca in maniera arbitraria con gli strumenti di riconoscimento facciale, come nei casi sopracitati, molto spesso inesatti e questo mette a rischio anche il diritto a un equo processo nelle indagini penali.

Per quanto riguarda i settori privati, la mancanza di limiti legali nell'utilizzo dei dati biometrici ha dato vita a scenari di ampio impiego della tecnologia di riconoscimento facciale, alimentando le preoccupazioni di chi ritiene che ci si stia avvicinando a una preoccupante e indiscriminata sorveglianza di massa. In particolare, in Nuova Delhi il governo indiano ha permesso che le banche[513] utilizzino il riconoscimento facciale per verificare le singole transazioni, che superino un certo limite annuale, oltre allo scan biometrico dell'iride, in alcuni casi, nel tentativo di ridurre le frodi e l'evasione

[509] *negozio fiduciario* è un negozio giuridico in cui il fiduciante trasferisce ad un altro soggetto, fiduciario, un diritto, che dev'essere esercitato in un modo determinato e con uno scopo ben definito
[510] Ministry of electronics and information technology, *The Digital Personal Data Protection Bill*, 2022
[511] *Constitution of India*, 1949
[512] Supreme Court of India, *Justice K. S. Puttaswamy (Retd.) vs. Union of India*, Writ Petition (Civil), n. 494 of 2012, (2017) 10 SCC 1
[513] THORAT S.B. – NAYAK S. K. – DANDALE J. P., *Facial Recognition Technology: An analysis with scope in India*, in *International Journal of Computer Science and Information Security (IJCSIS)*, 8, 1, 2010

fiscale.[514] Alcune banche di grandi dimensioni hanno cominciato a usare tale opzione e, in linea con il quadro generale sin qui delineato, l'interessato non ha coscienza di quanto accade poiché la verifica non è segnalata in alcun modo né è di dominio pubblico.

Un altro interessante contesto applicativo del riconoscimento facciale è quello del sistema DigiYatra disponibile per i voli domestici attualmente in New Dehli, che Ministro dell'aviazione civile ha anticipato che verrà rilasciato in altri aeroporti, quali Hyderabad, Pune, Vijayawada e Calcutta, e la futura implementazione di questo sistema in ogni aeroporto.[515] Tale sistema è progettato per agire *contactless* per favorire un processo più scorrevole delle partenze aereoportuali. La garanzia per i passeggeri risiederebbe nel conservare i dati in formato criptato e decentralizzato sui loro dispositivi, che possono essere condivise con l'aeroporto di partenza fino a un giorno prima della partenza.

Tale decisione di decentralizzazione deriva dalla considerazione delle problematiche che insorgerebbero in un sistema centralizzato riguardo alla privacy e al rischio di furto di dati. Il sistema DigiYatra consente ai viaggiatori di passare attraverso i punti di controllo dell'aeroporto senza alcuna interazione con lo strumento del controllo in quanto con il rilevamento dei dati biometrici del volto[516] si associa l'identità del passeggero poi collegata con la carta d'imbarco. Il presupposto del funzionamento di questo sistema prevede che l'individuo scarichi la DigiYatra app sul proprio dispositivo, collegare i propri dati, fare una foto del proprio viso e, quindi, aggiornare la carta d'imbarco. Ad avviso di chi scrive, la data retention in questo caso sembra essere decentralizzata e a carico del passeggero, escludendo la responsabilità in materia dell'aeroporto. Rimane la domanda di quale sia la politica dell'aeroporto stesso in merito alla conservazione dei dati che i viaggiatori forniscono.

Un aspetto che richiede, per sua natura, un approfondimento è l'individuazione dei fornitori delle tecnologie di riconoscimento facciale. Ad esempio, la società che fornisce le tecnologie di face recognition impiegate presso gli aeroporti è Vision-Box. Un altro esempio è l'azienda che ha fornito alla polizia indiana in alcuni paesi i prodotti di riconoscimento e che recentemente si è aggiudicata il contratto di fornitura per gli aeroporti, con la capacità di identificazione anche con la mascherina. Queste e altre società rimangono silenziose in merito a come si svolgano le attività di riconoscimento e quali siano le politiche di protezione dei diritti umani o sostengono di non averne ma di seguire le leggi e linee guida indiane.[517] A proposito di linee guida, i principi delle

[514] OHRI N., *India lets banks use face recognition, iris scan for some transactions - sources*, in *Reuters,* 2023

[515] PTI News Agency, *Facial recognition technology introduced at 3 airports in India under Digi Yatra initiative*, in *The Indian Express*, 2022

[516] *supra* Capitolo I § 1

[517] Amnesty International, *Ban The Scan Hyderabad*, in *Ban The Scan*, 2022

Nazioni Unite su Imprese e Diritti Umani[518] determinano la responsabilità per le aziende di rispettare i diritti umani e quindi di disporre di una politica in materia. Tale responsabilità si estende anche al dovere di adottare misure che identifichino, prevengano, riducano i rischi che le loro attività possono comportare per i diritti umani.

Per concludere le considerazioni sull'India è opportuno menzionare l'Automated Facial Recognition System[519], proposto dal Ministero dell'Interno, che consentirebbe di identificare, tracciare e catturare criminali ed è presentato dal National Crime Record Bureau come un tentativo di modernizzare la polizia. Quello che giova sottolineare è che si prevede un database centralizzato a livello nazionale che consenta alle autorità statali di utilizzare il riconoscimento facciale pur permanendo la mancanza di una effettiva protezione, anche basilare, della privacy, dei diritti e della sicurezza dei cittadini.

4.1. *(Segue):* ulteriori criticità e discriminazioni.

Ulteriori perplessità e criticità per i diritti degli individui risultano dall'impiego del riconoscimento facciale e della sorveglianza di massa nella Corea del Sud, in merito alla quale si teme per la possibile violazione dei diritti per la raccolta indiscriminata dei dati facciali dei cittadini da parte del governo e il loro successivo impiego. La Commissione indipendente per i Diritti Umani (NHRCK)[520], organo consultivo indipendente del governo, che protegge, sostiene e promuove i diritti umani in Corea, ha evidenziato tali timori. Essi, in particolare, concernono la minaccia alla libertà di riunione e associazione a cui si accompagna la raccomandazione al Primo Ministro di stabilire una moratoria, in attesa che venga adeguata la legislazione a protezione dei diritti fondamentali della persona, al fine di impedire al governo l'introduzione e l'impiego del riconoscimento di massa in tempo reale negli spazi pubblici. Tale approccio è simile, come si vedrà, a quello attuato dalla infrastruttura di sorveglianza in Cina.[521]

La Corea del Sud, infatti, ha attivato nel 2021 un'intensa sorveglianza dei luoghi pubblici per mezzo di algoritmi di intelligenza artificiale per il riconoscimento biometrico, in particolare del volto, a partire dalla città di Bucheon, per tracciare i movimenti delle persone contagiate da COVID-19 e gli eventuali contagi.[522] Tale iniziativa allinea la Corea del Sud con le scelte di altre nazioni, quali la Cina, di cui si parlerà nel prossimo paragrafo, Russia, India, Polonia e Giappone, le quali hanno

[518] The Human Rights Council, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, HR/PUB/11/04, 2011
[519] National Crime Records Bureau*, Request For Proposal To procure Automated Facial Recognition System*, 02/001, 2018
[520] National Human Rights Commission of Korea (NHRCK)
[521] *infra* § 5
[522] CARBONI K., *In Corea del Sud parte un progetto di sorveglianza biometrica di massa contro COVID-19*, in Wired, 2021

sperimentato i sistemi di riconoscimento facciale su larga scala per tracciare i contagiati dal COVID, sfruttando i poteri straordinari conferiti nella situazione di emergenza per combattere la pandemia.

Il sistema di sorveglianza dispiegato dalla Corea del Sud incrocia dati variegati derivanti dalle transazioni delle carte di credito, dalla localizzazione dei dispositivi mobili, dai filmati delle telecamere e da ulteriori fonti. Il governo sudcoreano ha già attuato violazioni dei diritti fondamentali, fornendo foto dei volti di cittadini sudcoreani e stranieri a società private, con la presunta finalità di sviluppare l'intelligenza artificiale, anche se forse è stato in realtà effettuato un vero e proprio censimento sull'immigrazione. Lo NHRCK ha raccomandato che il riconoscimento facciale in tempo reale sia vietato per legge, poiché tale tecnologia dovrebbe essere destinata solo a circostanze davvero eccezionali, in nome del pubblico interesse e con motivazioni chiare, come ad esempio la ricerca di bambini scomparsi.

Per quanto concerne altri scenari paesi, è interessante l'impiego della tecnologia di sorveglianza della società AnyVision, con quartiere generale in Israele. Il governo Israeliano ha un contratto con AnyVision per la sorveglianza, utilizzata in un contesto dove esiste una discriminazione istituzionalizzata contro i Palestinesi.[523] La medesima tecnologia AnyVision si rinviene anche in Cisgiordania, dove le telecamere alimentate da tale tecnologia sostengono la continua occupazione e l'oppressione dei palestinesi. Inoltre, sono stati siglati contratti per lo sviluppo di *smart city* con migliaia di telecamere di sorveglianza per il riconoscimento facciale, finanziate dalla Cina[524], per l'installazione nella città mongola di Ulaanbaatar.

A questo punto, risulta interessante l'approfondimento proprio sulla Cina e su quello che, chi scrive, ha definito il "modello" cinese relativo alla sorveglianza di masse e al riconoscimento facciale.

5. Riconoscimento facciale nel "modello" cinese.

La Cina usa diffusamente la sorveglianza di massa e i rilevamenti biometrici, tanto da apparire come un sistema in cui i diritti della popolazione siano "affievoliti"[525], in quanto, proprio la Carta costituzionale[526] sancisce che «i cittadini nell'esercizio dei loro diritti e libertà, non possano violare gli interessi dello Stato, della società o della collettività». In un ambito, dunque, dove il Partito è «l'interprete unico dell'uniformità di intenti che deve contraddistinguere l'azione statale a tutti i livelli» i sistemi che realizzano la sorveglianza della popolazione trovano enorme e variegata applicazione.

[523] CARBONI K., *Israele sta usando in maniera indiscriminata il controllo biometrico sui Palestinesi*, in *Wired*, 2021
[524] *infra* § 5
[525] CALDERINI B., *Sorveglianza di massa, la Cina è un sistema a "diritti affievoliti": perché lo tolleriamo e cosa rischiamo*, in *Agenda Digitale*, 2022
[526] People's Republic of China, Constitution, December 4, 1982, artt. 51, 53, 54

Le città cinesi sono, infatti, le più monitorate al mondo, come testimoniato dai numerosi sistemi e progetti di reti estese di sorveglianza, quali Golden Shield, Skynet, Safe Cites, Police Clouds, solo per citarne alcuni. Infatti, è il più grande campo di sperimentazione delle *smart city*[527] finanziati da investimenti pubblici e privati, volti anche a favorire lo sviluppo tecnologico in settori quali la mobilità, sanità, sicurezza e accesso ai servizi pubblici. In tali contesti, distrettuali o cittadini, si attuano le sperimentazioni delle tecnologie di sorveglianza come "campo di prova" per la successiva estensione ad aree sempre più vaste.

Data la presenza di circa 800 di tali progetti diversificati e la partecipazione di differenti amministrazioni è complessa la diffusione a livello nazionale dei risultati e dei dati e, comunque, rimane minimo il coinvolgimento dei cittadini nei processi decisionali, nonostante il progresso tecnologico che concerne il rapporto pubblica amministrazione-cittadini.

La mole di dati prodotta e raccolta ogni giorno è enorme, visto che quasi tutti i cittadini sono sottoposti al riconoscimento biometrico. In tal senso, viene rilevato a livello internazionale[528], come la Cina abbia sviluppato la infrastruttura di sorveglianza più estesa al mondo tramite un impressionante numero di telecamere a circuito chiuso vicino plausibilmente ai 600 milioni di unità[529], che rappresentano circa la metà di tutte le telecamere del mondo e 2,6 milioni delle quali sono nella stessa città, Chongqing, grande agglomerato urbano situato nel sud-ovest del paese.

Tali telecamere interagiscono con software di face recognition, localizzazione e scansione corporea, consentendo una rapida identificazione di soggetti e veicoli. I dati così raccolti convergono in una base dati molto sofisticata che incrocia con gli identificativi delle persone (documenti, gruppo sanguigno, campioni di DNA), le rilevazioni biometriche (facciali, dell'iride, impronte) e le attività dei soggetti (tracciamento dei telefoni, monitoraggio degli acquisti online, decrittazione dei messaggi), unitamente a tutte le informazioni sono sottoposte al controllo da parte del governo. Il programma di sorveglianza di massa, "Xue Liang", ovvero "Occhio di falco", si basa su una integrazione di vari tipi di tecnologie, vecchie e nuove, come gli *spyware*[530] nei telefoni cellulari, i dispositivi d'intercettazione del traffico dati (sniffer Wi-Fi) e le telecamere per il riconoscimento facciale, e ambisce al controllo 1,4 mld di abitanti in Cina.

---

[527] ANDORNINO B. G. (a cura di), *La Cina: sviluppi interni, proiezione esterna*, in *Torino World Affairs Institute*, 2020, 67, un documento realizzato dall'*Osservatorio di Politica Internazionale* (progetto realizzato congiuntamente con Senato della Repubblica, Camera dei Deputati, Ministero degli Affari Esteri e della Cooperazione Internazionale)

[528] ANDORNINO (a cura di), *La Cina: sviluppi interni, proiezione esterna*, cit., 69

[529] HERSEY F., *China to have 626 million surveillance cameras within 3 years*, in *TechNode*, 2017

[530] *spyware* è un software malevolo, cosiddetto "malware", che si nasconde sui dispositivi, monitora le attività dell'utente e sottrae informazioni sensibili

Il modo con cui i dati rilevati convergono del citato database è stato anche descritto da due giornalisti del New York Times, Paul Mozur e Aaron Krolik, che con dovizia di particolari e riscontri video hanno riportato come le autorità di polizia di ogni livello impieghino le tecniche di rilevazione e come i dati raccolti possano essere resi accessibili a numerose terze parti sia pubbliche, per molte finalità, tra cui intelligence e sicurezza pubblica, che private, per scopi commerciali e di marketing. La raccolta di tutti questo dati personali avviene, tra l'altro, nel quadro di prestazioni degli algoritmi ancora significativamente fallaci.[531] In questo quadro, risultano piuttosto sorprendenti i risultati di uno studio proprio relativo al riconoscimento facciale[532] in cui gli autori sottolineano che gli aspetti di privacy legati al riconoscimento facciale sono una delle maggiori preoccupazioni a livello sociale, proprio in un'epoca caratterizzata da un impressionante scambio di informazioni.

Tuttavia, nello studio condotto sul tema attraverso interviste, i risultati hanno mostrato una sostanziale fiducia degli intervistati sulla tecnologia e sulle piattaforme che utilizzano face recognition, pur percependo i rischi per la privacy. Inoltre, gli intervistati, nonostante la percezione del potenziale rischio, tendono comunque a fornire dati personali negli scambi informativi per i servizi e le applicazioni di cui hanno bisogno, anche se per fare questo si deve accedere ad una piattaforma che impiega il riconoscimento facciale, ad esempio per confermare l'identità del soggetto. Gli intervistati sembrano inclini a superare, dunque, le perplessità sulla privacy, percependo l'utilità del riconoscimento facciale. Gli autori dello studio sottolineano che i rischi della face recognition, dunque, sono soprattutto "fattori esterni" al suo impiego, legati alle prestazioni della tecnologia in termini di accuratezza e maturità[533], pur ammettendo che il campione degli intervistati è soprattutto composta da giovani, dunque con una grande confidenza e familiarità nei confronti della tecnologia. Al di là dei risultati molto rosei riportanti nel suddetto studio, da cui di fatto risulta fiducia nel riconoscimento facciale, nonostante la consapevolezza sia del rischio per la privacy che di una maturità prestazionale ancora parziale di questa tecnologia, è proprio il punto sulla attuale limitazione nelle prestazioni di accuratezza che torna come elemento comune alle perplessità da varie parti del mondo, anche caratterizzate da tradizioni, ordinamenti e stili di vita completamente diversi.

Oltre alla sorveglianza effettuata "sulla massa", i cittadini cinesi sono sorvegliati nelle proprie attività online attraverso software di monitoraggio e censura sempre aggiornato. Tale ulteriore tipo di sorveglianza è resa possibile dall'accentramento delle funzioni di governance concernenti il cyberspazio, le cui politiche mirano

[531] CALDERINI, *Sorveglianza di massa, la Cina è un sistema a "diritti affievoliti*, cit.
[532] LIU T. – YANG B. – GENG Y. – DU S., *Research on Face Recognition and Privacy in China—Based on Social Cognition and Cultural Psychology*, in *Frontiers in Psychology*, 12, 2021, 1
[533] LIU, *Research on Face Recognition and Privacy in China*, cit., 3, 5, 10

all'attestazione del suo controllo rigoroso a livello nazionale e dei flussi di dati scambiati. [534]

Per implementare tali politiche e proteggere i propri confini cibernetici, espletando anche attività oltre confine, il governo cinese ha iniziato con lo strutturare un sistema "reticolare", il cosiddetto "Great Firewall", riaffermando tali principi con la Cybersecurity Law[535] nel 2017 e portando, a fronte di grandi investimenti, al controllo capillare, la censura e la profilazione dei cittadini.[536] Tale sistema potenzialmente in grado di controllare in modo molto pervasivo i contenuti delle comunicazioni online, costituisce, dunque, un'alternativa all'attuale rete globale decentrata.

L'obiettivo permane quello del raggiungimento di una sovranità digitale e un affrancamento dalle influenze estere in cui lo strumento prescelto per conseguirlo sembra essere proprio la sorveglianza di massa. In questo scenario si inserisce anche il cosiddetto "Project Sharp Eyes"[537], risalente al 2015, in cui le tecniche videosorveglianza andranno a coprire tutti gli spazi pubblici significativi, che vanno dall'ingresso nei ristoranti, centri commerciali, stazioni degli autobus, scuole, ospedali, cinema, palestre e luoghi di intrattenimento, attraverso una rilevamento tridimensionale dei volti. Si prevede l'installazione di telecamere e i sopracitati dispositivi d'intercettazione del traffico dati (scanner e sniffer Wi-Fi) compatibili con il software del riconoscimento facciale, con l'obiettivo dichiarato di protezione dei cittadini da rapine, atti di violenza e in generale dai pericoli del quotidiano, quindi per supportare il benessere della collettività. Sempre nell'ottica di protezione dei cittadini, la polizia può scansionare i codici QR, cioè i codici a barre a risposta rapida Quick Response Code, disponibili sulla porta delle case e collegati alle informazioni sugli abitanti che vi risiedono.

Ad opinione di chi scrive, il "modello" adottato da parte del governo cinese per l'impiego dei rilevamenti biometrici, in particolare, del riconoscimento facciale, e dell'impiego delle informazioni così rilevate ai fini della sorveglianza di massa mostra da una parte una ricerca spasmodica di controllo dei propri cittadini e, dall'altra, che questo controllo è basato su una delle seguenti ipotesi.

La prima è che il governo nutra una *fiducia totale* nelle tecnologie impiegate, ma non sempre del tutto motivata o supportata da dati scientifici, oppure l'attribuzione di una *scarsa rilevanza* all'effettivo al grado di accuratezza e affidabilità dei rilevamenti raccolti ai fini del controllo. È opportuno soffermarsi su entrambe le ipotesi, per valutarne l'impatto anche nei termini del tema, importante per questa trattazione, del bilanciamento tra diritti e sicurezza.

---

[534] ANDORNINO (a cura di), *La Cina: sviluppi interni, proiezione esterna*, cit., 72

[535] People's Republic of China, Cybsersecurity Law, November 7, 2016

[536] ALÙ A., *Sorveglianza di massa: così la Cina attua il suo modello "orwelliano"*, in *Agenda Digitale*, 2022

[537] ALÙ, *Sorveglianza di massa: così la Cina attua il suo modello "orwelliano*, cit.

5.1. *(Segue):* ipotesi sul modello cinese.

Nella prima ipotesi, se si suppone che il governo cinese nutra una fiducia molto elevata nelle tecniche di sorveglianza impiegate, si potrebbe anche ipotizzare che, essendo una parte rilevante dei sistemi prodotti localmente, si abbia una cieca fiducia in quanto le aziende cinesi producono. L'alternativa è che comunque si voglia dare verso il mondo esterno un'immagine granitica dello Stato e delle sue capacità tecnologiche, con l'implementazione diretta sulla propria popolazione. I risultati in termini di esportazione delle tecnologie di sorveglianza basate su IA sembrerebbero sugellare tale ipotesi, dal momento che la tecnologia prodotta in questo contesto da alcune grandi aziende cinesi, quali Huawei, Hikvision, ZTE e Dahua, viene esportata in 63 Paesi.[538] La tecnologia di sorveglianza basata su IA non è tuttavia alimentata solo dalle suddette aziende cinesi, in quanto altre importanti aziende, quali NEC e IBM, ferme restando le azioni intraprese dopo accadimenti statunitensi a Minneapolis[539], hanno esportato o esportano in oltre dieci Paesi e altre aziende, geograficamente collocate in democrazie liberali quali Francia, Germania e Israele, contribuiscono con le loro attività allo sviluppo e applicazione delle tecniche di riconoscimento facciale. È anche interessante notare che più della metà dei Paesi in cui la Cina esporta le proprie tecnologie di riconoscimento sono parte della cosiddetta "Belt and Road Initiative" (BRI)[540], una iniziativa del governo cinese per lo sviluppo attraverso l'investimento in un numero considerevole di Paesi e di organizzazioni internazionali, che tra l'altro mette la Cina in una posizione centrale nel panorama mondiale dal punto di vista dell'innovazione.

In materia di innovazione, il Partito Comunista Cinese ha delineato delle espressioni che illustrano i principi alla base del National Innovation System (NIS)[541], il quale, specifico per ogni Stato, si definisce come la rete costituita da istituzioni pubbliche e private e che ha come obiettivo l'ideazione, implementazione, diffusione di tecnologie innovative. Tali espressioni "slogan" vengono ripetute in svariati contesti come in occasione degli eventi pubblici e politici nonché citate in leggi e regolamenti. La ripetizione di tali slogan persegue l'effetto di suggellare gli obiettivi a medio-lungo termine e uniformare in una direzione comune tutti i livelli governativi, economici e sociali.[542] Un settore di interesse strategico attenzionato dal NIS è lo sviluppo tecnologico ad impiego duale o *dual use* che condivide una stessa tecnologia per applicazioni sia in ambito civile che militare e riguarda vari settori, fra cui quello di interesse dell'intelligenza artificiale[543], che dunque possiede anche una dimensione anche a carattere strategico. A questo quadro si aggiunge, inoltre, la supposizione che

---

[538] CALDERINI B., *Sorveglianza di massa, la Cina è un sistema a "diritti affievoliti"*, cit.
[539] *supra* § 2
[540] Belt and Road Forum for International Cooperation, Beijing, May 14 -15, 2017
[541] Organisation for Economic Co-Operation and Development, *National Innovation Systems*, ai sensi Convention of Paris against Discrimination in Education, December 14, 1960
[542] ANDORNINO (a cura di), *La Cina: sviluppi interni, proiezione esterna*, cit., 59
[543] ANDORNINO (a cura di), *La Cina: sviluppi interni, proiezione esterna*, cit., 60

il progresso tecnologico cinese si ritagli un "margine" sulla condivisione delle effettive prestazioni dei sistemi di riconoscimento e sorveglianza e delle inerenti informazioni.

La seconda ipotesi su cui si innesta il controllo estensivo del governo cinese sui propri cittadini attraverso le tecnologie di riconoscimento e sorveglianza che sarebbe peggiore di quella della smisurata fiducia nella tecnologia o nelle proprie aziende. Infatti, l'alternativa è che il governo attribuisca una importanza *relativa* al fatto che le rilevazioni facciali, o biometriche in genere, abbiano un livello di sicurezza adeguato a minimizzare i rischi collegati a un errato riconoscimento. Un tale errore, infatti, unito alle evidenti violazioni della privacy e del consenso, almeno nel senso attribuitogli dalla Unione Europea e non solo[544], potrebbe degenerare in una persecuzione ingiustificata dei cittadini identificati.

Si è già diffusamente discusso nella trattazione sui rischi collegati a mancanza di affidabilità e accuratezza nei sistemi di IA, che generano potenzialità di errori anche gravi negli output algoritmici. Tale rischio è proprio alla base della prudenza sull'impiego dei sistemi di riconoscimento anche in ambito Europeo. Una sottovalutazione o una non attribuzione di importanza da parte del governo cinese sui possibili danni creati da errori algoritmici, se questa l'ipotesi di cui si sta discutendo fosse esatta, potrebbe essere un elemento di preoccupazione ulteriore sul "modello" cinese della sorveglianza basata su IA.

5.2. *(Segue):* il PIPL.

Esiste comunque un quadro normativo in Cina relativo alla protezione dei dati personali, che consta tre leggi focalizzate, rispettivamente, sugli aspetti di cybersecurity, attraverso la, già citata, Cybersecurity Law, in vigore dal 1° giugno 2017, sulla sicurezza dei dati, attraverso la Data Security Law[545], in vigore dal primo settembre 2021 e sulla protezione della privacy, la Personal Information Protection Law[546], avente efficacia dal 1° novembre 2021[547]. In particolare, la Personal Information Protection Law (PIPL) è intesa a regolamentare la protezione dei dati e, ad esempio, indica regole precise sul loro trasferimento con un impatto sulle aziende internazionali che operano in Cina o che desiderano mantenere relazioni a carattere commerciale con la Cina. La legge, che dovrebbe in linea di principio rappresentare un passo avanti, si inserisce tuttavia in un sistema regolatorio che evolve continuamente e, quindi, con condizioni di imprevedibilità di impatto sia nazionale che internazionale. Tale imprevedibilità, in particolare inerente alle misure per lo sviluppo di tecnologie di riconoscimento facciale e di intelligenza artificiale, hanno scoraggiato alcune aziende con attività in territorio

[544] *supra* § 3
[545] People's Republic of China, Data Security Law of the, June 10, 2021
[546] People's Republic of China, Personal Information Protection Law, August 20, 2021
[547] BONOMI S., *Personal Information Protection Law (PIPL): la Cina approva la prima legge in materia di data protection*", in *CyberLaws*, 2021

cinese, che hanno deciso di ritirarsi. Il PIPL appare simile al GDPR, dal punto di vista del modello di impostazione, ma gli oneri sono in numero maggiore e alcuni molto stringenti. È interessante analizzare alcuni aspetti del PIPL, partendo dall'articolo 3 relativo all'ambito territoriale di applicazione della legge e che ne estende l'applicazione al trattamento di dati personali al di fuori della Cina. I casi in cui il PIPL si applica sono quelli in cui il trattamento dei dati personali avviene o *nel* territorio cinese, posto in essere da aziende cinesi o affiliate locali di multinazionali con sede in Cina, oppure al di *fuori* dei confini cinesi, se il trattamento è finalizzato alla fornitura di prodotti/servizi a persone situate nel territorio o allo svolgimento di analisi e valutazione del comportamento delle stesse. Una terza applicazione concerne le cosiddette *altre* circostanze previste da leggi e regolamenti amministrativi, che tuttavia non vengono specificati nel PIPL, fra cui si annovera il caso delle imprese con sede al di fuori del territorio cinese ma obbligate a nominare un rappresentante o a stabilire un ente in Cina.

Il trattamento dei dati personali deve poi sottostare ai principi contenuti nel Capitolo I della legge, che assomiglia all'articolo 5 del GDPR, indicando trasparenza, liceità, buona fede, necessità e minimizzazione come necessari per il trattamento. A differenza del GDPR, però, la necessità si applica, come nel GDPR, a tutte le attività di trattamento, mentre la minimizzazione si riferisce solo alla raccolta dei dati personali. Inoltre, è contemplato nell'articolo il principio, fondamentale nel diritto cinese, della "buona fede", che a chi scrive appare come un fin troppo grande elemento di flessibilità.

In nome della trasparenza, esiste l'obbligo di informare l'interessato sulle modalità di espletamento del trattamento in modo conciso, accessibile, comprensibile, chiaro e semplice. In tale ottica, è necessario che l'informativa sulla privacy sia disponibile, anch'essa chiara e leggibile, sul proprio sito web o app. È anche necessario che le informazioni personali siano trattate in modo lecito e, dunque, si richiede che il trattamento soddisfi le condizioni di legge. La normativa, prima della PIPL, associava la liceità in modo preponderante al consenso, che era, a meno di diverse disposizioni da parte di leggi e regolamenti amministrativi, l'elemento principale su cui si basava il trattamento. In modo simile ad GDPR, invece, il PIPL contempla una serie di basi giuridiche su cui innestare il trattamento che, oltre naturalmente al consenso, prevedono la conclusione o esecuzione di un contratto con gli interessati oppure la gestione delle risorse umane conformemente ai regolamenti sul lavoro e ai contratti collettivi. Rientra nel novero delle basi giuridiche di cui tenere conto anche il generale adempimento agli obblighi stabiliti dalla legge, nonché la risposta ad una emergenza sanitaria o la protezione, in caso di emergenza, della vita, della salute (come è stato il COVID-19), o della proprietà di una persona. Sono anche contemplati i trattamenti di informazioni rese pubbliche dagli stessi interessati e altre circostanze previste da leggi e regolamenti ma, a differenza del GDPR, come base giuridica del trattamento non è previsto il legittimo interesse. Da quanto si evince, ad avviso di chi scrive, in merito al

trattamento dei dati esiste un quadro che presenta qualche similitudine con il GDPR, ma che, d'altra parte, è strutturalmente in linea con l'inquadrato "modello" cinese. Le aziende che hanno deciso di lasciare il territorio cinese, dopo l'entrata in vigore del PIPL, non hanno probabilmente ravvisato l'opportuna base giuridica per legittimare i trattamenti e gli specifici adempimenti tra le menzionate opzioni stabilite dal PIPL.

Un ulteriore aspetto che è interessante esaminare, anche alla luce di quanto si è detto nella trattazione a proposito della qualità dei dati e delle conseguenze in mancanza di qualità, sono le disposizioni del PIPL sulla qualità delle informazioni. Il PIPL si preoccupa di precisare che occorre predisporre adeguate misure atte a garantire *accuratezza, completezza* e *aggiornamento* dei dati personali. La qualità del dato, proprio quella che nella "schedatura" di massa si è rilevato che potesse non essere così prioritaria[548], diventa invece una preoccupazione nel PIPL. Per chi scrive, tale discrasia suggerisce una contraddizione tra normativa e operato oppure il possesso. da parte dei sistemi di riconoscimento cinesi, di algoritmi molto più accurati di quanto sia noto. Entrambe le ipotesi aprono scenari potenzialmente critici, ad avviso di chi scrive. Il contenuto del PIPL su questo aspetto è assolutamente condivisibile ed in linea con quanto già evidenziato nella trattazione[549] e nella proposizione progettuale del trattamento dei dati personali per rispettare il principio di proporzionalità[550].

Inoltre, in accordo all'articolo 9 del PIPL, i Personal Information Processor (PIP)[551], che corrispondono ai responsabili del trattamento di dati personali del GDPR, sono tenuti ad adottare le misure necessarie per garantire la sicurezza, cosa che ha impatto sulle aziende internazionali che operino in territorio cinese. Per sicurezza dei dati, si intende la quantità di informazioni, le metodiche. la frequenza del trattamento e l'eventuale coinvolgimento di porzioni sensibili nelle informazioni. L'articolo implica che debba essere dimostrabile al governo cinese anche l'adozione delle misure di sicurezza e la conformità alla normativa. Tale dimostrazione comporta, tra l'altro, una formalizzazione delle procedure e dei metodi di conservazione delle informazioni, realizzando, altresì, delle attività di formazione dei titolari del trattamento. Il PIPL prevede altresì la nomina di un Personal Information Officer, simile al Data Protection Officer del GDPR, ma senza dettagliare le caratteristiche e competenze necessarie per ricoprire tale ruolo.

Un aspetto particolarmente rilevante per le aziende europee riguarda le regole, sancite nell'articolo 38 del PIPL, per il trasferimento dei dati personali al di fuori del territorio cinese che, come per il GDPR, non può avvenire liberamente ma deve rispettare una serie di condizioni. Esse comprendono l'ottenimento del consenso informato dell'interessato, che come si è visto e solo una delle basi giuridiche del trattamento.

[548] *supra* § 5
[549] *supra* Capitolo I § 6.1
[550] *supra* § 6.3
[551] BOCACCINI P. – PRELATI S.*, Trasferimenti internazionali di dati: le nuove disposizioni cinesi sulle clausole contrattuali standard*, in *Cybersecurity 360*, 2022

L'opinione di chi scrive è che in tal modo il consenso finisca per perdere, o comunque vedere ridimensionato, il suo valore che, invece, è il centro della normativa europea. Infatti, in Europa, è stata necessaria l'emanazione una Direttiva, la 2016/680, che accompagna del GDPR, per garantire che il consenso prestato dall'interessato non perda di valore rispetto alle necessità della pubblica sicurezza, ma debba essere con esse bilanciato.

Un'ulteriore condizione riguarda l'effettuazione di una valutazione di impatto e il soddisfacimento di una di quattro condizioni "*speciali*". La prima condizione speciale consiste nel superamento di un "security assessment", effettuato dal Cyberspace Administration of China (CAC)[552]. Il PIPL, infatti, estende quanto previsto nella sopracitata Cybersecurity Law, in merito alla localizzazione e al security assessment. Prevede, quindi, che gli operatori di infrastrutture informatiche critiche, ossia strategiche e d'impatto sulla sicurezza nazionale, e i titolari il cui trattamento raggiunge un elevato volume di dati gestiti, debbano conservare in Cina le informazioni personali raccolte e generate all'interno del territorio cinese. La seconda condizione speciale per un lecito trasferimento dei dati consiste nel conseguimento di una certificazione di protezione delle informazioni personali, anche se il PIPL non specifica come ottenerla. La terza concerne la conclusione di un contratto con il destinatario conforme al contratto standard formulato dal sopracitato CAC, standard non incluso nel PIPL ma oggetto di disposizioni successive (Draft Standard Contract Provisions on the Export of Personal Information)[553]. Infine, la quarta delle condizioni speciali include altre possibilità prescritte da leggi, regolamenti amministrativi o dal CAC.

Ulteriormente, in accordo al PIPL, i dati personali conservati in Cina non possono essere forniti a autorità giudiziarie o di polizia al di fuori della Cina, a meno di previa autorizzazione dalla competente autorità cinese competente.[554]

Il quadro normativo cinese è comunque in evoluzione, anche se emergono già dal PIPL le difficoltà per quelle realtà internazionali che intendano iniziare o continuare ad operare sul territorio cinese. In conseguenza dell'entrata in vigore del PIPL, vari colossi del web hanno abbandonato la Cina, tra cui Linkedin e Yahoo, proprio a causa di un ambiente legale e commerciale in graduale inasprimento per le aziende internazionali, anche se Yahoo non ha mai associato formalmente il suo ritiro al PIPL. Tenendo conto del ritiro dal mercato cinese di Google nel 2010 e il precedente blocco da parte della Cina di Facebook e Twitter nel 2009, la sospensione dei servizi di queste società ai cittadini cinesi rappresenta un ulteriore elemento di controllo *indiretto* sulla popolazione da parte del governo centrale. L'entrata in vigore del PIPL è parte del

[552] *Cyberspace Administration of China* (CAC) è l'agenzia centrale di regolamentazione, censura, supervisione e controllo di Internet per la Repubblica popolare cinese

[553] BOCACCINI P. – PRELATI S., *Trasferimenti internazionali di dati*, cit.

[554] BELFI M., *PIPL, cosa dice la Legge privacy i Cina: ecco le regole per adeguarsi*, in *Cybersecurity 360*, 2021

quadro normativo finalizzato alla regolamentazione dell'ambito tecnologico in merito alle pratiche anticoncorrenziali e la sicurezza dei dati personali, nonché a linee guida per il contrasto dei monopoli, con pesanti impatti su grandi aziende di commercio elettronico, quali Alibaba e Tencent.

5.3. *(Segue):* opposizione tra benefici e rischi.

Dall'analisi effettuata emerge che in Cina è più percepibile il contrasto tra gli aspetti positivi e negativi nell'impiego di algoritmica di intelligenza artificiale che, in alcune circostanze, appaiono portate agli estremi. In quanto segue si vuole entrare in specifiche circostanze che rientrano in questo quadro di continuo contrasto tra benefici e rischi, sviluppati nel corso della trattazione, caratterizzanti la IA.

Un benefico impiego dell'IA nell'ordinamento cinese riguarda, in particolare, la velocizzazione e lo sfoltimento dei procedimenti di giustizia ordinaria, un beneficio che alcuni autori auspicano si verifichi nell'ordinamento italiano. L'automatizzazione concerne le "procedure di cancelleria", quali l'organizzazione di prove o la trascrizione di note effettuata da algoritmi di riconoscimento vocale. In tal senso, ad opinione di chi scrive, se si mantiene la presenza dell'operatore umano, l'ausilio della IA può risultare davvero di beneficio alla crescita dell'efficienza del sistema giudiziario. Un altro beneficio concerne alcuni procedimenti legali in corso di svolgimento in Cina dove vengono utilizzati messaggi per inviare le sentenze oppure l'archiviazione automatica degli atti o sistemi di videochiamata in luogo della effettiva presenza del soggetto coinvolto[555]. Quest'ultimo strumento è regolamentato in Italia[556] in materia di partecipazione a distanza con collegamenti audiovisivi nel dibattimento, previsto originariamente solo per i collaboratori di giustizia[557]. Inoltre, per supportare i processi decisionali nell'ordinamento cinese del giudice "umano" vengono utilizzati algoritmi di analisi dei casi ed esiste la possibilità di presentare richieste e appelli tramite app (China Mobile WeCourt) all'interno della piattaforma WeChat. Per la maggior parte dei casi «l'utilizzo dei sistemi AI favorisce un'interpretazione giurisprudenziale uniforme a livello nazionale rilevando deviazioni rispetto alla norma».[558]

Questi ed ulteriori benefici devono essere confrontati, ad opinione di chi scrive, con la dura realtà dei fatti relativi alla degenerazione a cui può giungere l'utilizzo di un sistema di IA, pur partendo da intenzioni "nobili" quali la tutela della pubblica sicurezza nell'utilizzo del riconoscimento facciale nel più ampio ambito della sorveglianza di massa.

---

[555] ANDORNINO (a cura di), *La Cina: sviluppi interni, proiezione esterna*, cit., 79

[556] art. 146-*bis* norme att. c.p.p., *Partecipazione al dibattimento a distanza*, come modificato da l. del 23 giugno 2017, n. 103

[557] art. 147-*bis* norme att. c.p.p., *Esame degli operatori sotto copertura, delle persone che collaborano con la giustizia e degli imputati di reato connesso*, come modificato da l. del 11 gennaio 2018, n. 6

[558] Chinese Courts and Internet Judiciary, *Chinese Courts and the Internet Judiciary*, December 2019

Un esempio dell'impiego distorto della sorveglianza basata sul riconoscimento facciale riguarda una vera e propria incarcerazione di massa «a cielo aperto»[559] contro la minoranza etnica musulmana degli Uiguri[560], la quale vive prevalentemente nel nord-est della Cina nella regione dello Xinjiang chiamata Xinjiang Uyghur Autonomous Region (XUAR). Il Parlamento europeo nel 2019 è intervenuto con una Risoluzione[561] chiedendo un dialogo con la Cina, ricordando che essa «ha aderito al quadro internazionale sui diritti umani firmando una molteplicità di trattati internazionali in materia». Inoltre, ha invitato il Consiglio ad adottare, se ritenuto necessario e di ausilio effettivo, misure contro i funzionari responsabili di aver elaborato e attuato tale politica di detenzione di massa. Politica di detenzione che, come riportato da Amnesty International[562] nasce nel 2014 e che si unisce a molteplici violazioni dei diritti umani e dell'abuso del potere politico in Cina.

Tutt'oggi rimane una priorità a livello internazionale e mondiale, come testimoniato dalle petizioni di Amnesty International e dal World Report 2023, sugli eventi del 2022, dello Human Rights Watch[563]. Già nel 2017, l'HRW ha riportato l'esistenza di un documento ufficiale del 2017[564], che fornisce la descrizione di un database governativo, contenente dati rilevati con tecniche biometriche e mirato, in particolare, al controllo proprio degli Uiguri. Tali rilevamento venivano inseriti in un quadro di politiche per sedicenti finalità di lotta al terrorismo, ma in cui invece le Nazioni Unite hanno ravvisato l'idoneità a costituire crimini contro l'umanità. Nel dicembre 2021 gli Stati Uniti hanno adottato, con un forte supporto bilaterale, lo Uyghur Forced Labor Prevention Act (UFLPA) che è divenuto legge nel dicembre dello stesso anno[565] ed è solo l'ultima di una serie di iniziative per affrontare la drammatica situazione degli Uiguri e di altre minoranze perseguitate nella sopracitata regione cinese dello XUAR. La legge crea la presunzione confutabile che non può entrare negli Stati Uniti tutta la merce prodotta, completamente ma anche parzialmente, nella regione dello XUAR, in quanto frutto del "lavori forzati" delle minoranze ivi confinate. Nell'opinione di chi scrive, tali "misure" potrebbero non essere la risposta adeguata alla efferata repressione della libertà religiosa, di movimento e di altri diritti fondamentali degli Uiguri.

---

[559] HASSAN T., *A New Model for Global Leadership on Human Rights*, in *Human Right Watch World Report*, 2023, 6, «Xi Jinping's open-air prison for the Uyghurs in China»

[560] HASSAN, *A New Model for Global Leadership on Human Rights*, cit., 6, 9, 71, 80

[561] Parlamento europeo, Risoluzione del 19 dicembre 2019 sulla *situazione degli uiguri in Cina («China Cables»)*, (2019/2945(RSP)), C 255

[562] Amnesty International, *Rapporto annuale del 2021 - 2022 sulla Cina*, 2022

[563] *Human Rights Watch (HRW)* è un'organizzazione non governativa internazionale che si occupa della difesa dei diritti umani, con sede principale a New York

[564] CALDERINI, *Sorveglianza di massa, la Cina è un sistema a "diritti affievoliti"*, cit., The [Xinjiang Uyghur Autonomous] Region Working Guidelines on the Accurate Registration and Verification of Population

[565] FLACKS M. – SONGY M., *The Uyghur Forced Labor Prevention Act Goes into Effect*, in *Center for International Foreign Studies*, 2022

Le tecniche biometriche legate alla vicenda degli Uiguri tornano, purtroppo, in questo caso a mostrare una loro criticità, già evidenziata nella trattazione, ma anche a confermare come sia la "componente umana" a decretare un uso negativo della tecnologia del riconoscimento biometrico e non la tecnologia di per sé. Tra l'altro, come già descritto[566], uno dei rilevamenti biometrici possibili riguarda la cattura delle emozioni e, presumibilmente, dei sentimenti dell'individuo, attraverso il rilevamento dei movimenti muscolari del viso ed espressioni facciali collegate a tristezza, felicità, noia o rabbia, dunque impiegando un riconoscimento facciale con algoritmica estesa a tale finalità. Il rilevamento delle emozioni può anche essere effettuato in base al tono della voce e i movimenti del corpo. La raccolta di dati rilevatori di emozioni può essere utile per prevenire comportamenti violenti e crimini, ma anche per incrementare gli elementi per la profilazione e il monitoraggio dei cittadini cinesi, che sono già molto controllati e sempre più lo saranno in prospettiva. Gli algoritmi di riconoscimento emotivo utilizzano archivi di dati con espressioni create da attori o attrici, ma le espressioni del viso sono variegate passando da una cultura all'altra e, dunque, intrinsecamente forieri di imprecisioni e bias a carattere etnico. I sistemi di riconoscimento di una azienda cinese, la *Taigusys,* includono perfino un identificatore specifico per gli Uiguri[567], a conferma di un uso distorto da parte delle autorità cinesi sia del riconoscimento facciale base che di quello che include l'analisi delle emozioni,

Le implicazioni sociali e legali del riconoscimento facciale spinto su un terreno molto delicato, quale quello della "selezione" su base etnica è molto critico e rischia di acuire la diffidenza che ha portato agli avvenimenti descritti in merito agli Stati Uniti[568]. Gli aspetti critici del "modello cinese" si ritrovano anche nelle applicazioni di monitoraggio sviluppate ed applicate durante la pandemia da COVID-19, di cui il cosiddetto "Health Code", che è stato utilizzato nella città di Hangzhou, ne è un esempio. Il sospetto è che il monitoraggio da sanitario si trasformi in qualcosa di più, passando di fatto dal "codice sanitario" a veri e propri passaporti digitali che vanno ad alimentare, dunque, database per finalità diverse e non dichiarate da quelle del contenimento pandemico.

Un elemento che apre qualche spiraglio sui diritti dei cittadini cinesi, in materia di riconoscimento facciale, è rappresentato dall'esito di una sentenza che ha riconosciuto, per la prima volta, il diritto di un individuo di chiedere la cancellazione dei dati personali raccolti da un privato attraverso rilevamenti biometrici[569]. Certamente questo non riduce le perplessità sul descritto controllo dei cittadini da parte del governo ma rappresenta un comunque un elemento positivo. In particolare, una corte cinese ha emesso una sentenza

[566] *supra* Capitolo II § 1
[567] CARBONI K., *La nuova frontiera del controllo in Cina è il riconoscimento delle emozioni*, in *Security*, 2021
[568] *supra* § 2
[569] CARBONI K., *Come è andata a finire la prima causa sul riconoscimento facciale in Cina*, in *Wired*, 2021

nel 2020 a favore di Guo Bing[570], che aveva denunciato lo zoo di Hangzhou per aver utilizzato impropriamente il riconoscimento facciale, senza che lui avesse potuto esprimere il consenso. Aveva, infatti acconsentito al rilevamento dell'impronta digitale prevista per l'abbonamento annuale di accesso allo zoo, ma nel corso dell'anno la struttura aveva cambiato il tipo di riconoscimento che era divenuto di tipo facciale e aveva comunicato ai clienti che per accedere allo zoo avrebbero dovuto necessariamente usare il nuovo sistema. Guo, che non intendeva sottoporsi al riconoscimento facciale, giudicandolo troppo invasivo, e non potendo usare il suo abbonamento precedente, ha chiesto alla struttura, oltre al rimborso, la cancellazione dei i propri dati personali, ma lo zoo ha rifiutato. Guo, ha pertanto, denunciato lo zoo per violazione dei termini contrattuali. La Corte ha ordinato allo zoo di rimborsare Guo e cancellare i suoi dati biometrici, sentenza ribadita anche in appello. La sentenza assume un grande rilievo nel quadro dell'ordinamento cinese perché ha stabilito i cittadini hanno il diritto di richiedere la cancellazione dei propri dati e ha aperto la strada all'emanazione nel 2021 del PIPL.

Dopo l'approfondimento sull'impiego, l'abuso e la regolamentazione del riconoscimento facciale, il quadro che si delinea è molto critico. Probabilmente non sono del tutto noti tutti gli abusi e le discriminazioni che alcuni governi stanno portando avanti ai danni della popolazione, impiegando il riconoscimento facciale e la sorveglianza di massa. L'associazione tra queste tecnologie e la violazione dei diritti umani, che sta accadendo in molteplici contesti non deve fare dimenticare, però, che la responsabilità di violazioni, abusi e discriminazioni non è della neutrale tecnologia, ma degli esseri umani. Nei prossimi paragrafi si addiviene ad alcune proposte anche operative per contribuire al bilanciamento tra diritti e sicurezza anche utilizzando sistemi di IA per il riconoscimento facciale.

6. Ambiti di azione e relative proposte.

La trattazione ha mostrato luci e ombre degli effetti che il progresso tecnologico della intelligenza artificiale sta producendo nel suo innesto nella vita quotidiana dei cittadini e delle istituzioni. La rapidità con cui la IA è divenuta pervasiva sia in termini di prestazioni algoritmiche e velocità di addestramento ma anche, e questa dimensione è tutt'altro che secondaria, nel numero di domini applicativi in cui può essere applicata. Tale numero cresce ancora più rapidamente delle prestazioni ed è proprio in uno dei settori in cui questo sta avvenendo con maggior lentezza e riluttanza da parte dei soggetti e delle istituzioni coinvolte che la trattazione ha trovato fertile terreno per innestarsi con analisi di criticità, esperienze e risultanze e che intende, in questo paragrafo, condurre a riflessioni e proposte. L'ambito applicativo è quello della

[570] Hangzhou Fuyang District Court, *Bing Guo v Hangzhou Safari Park*, Zhejiang 0111, Civil No. 6971, 20 November 2020

pubblica sicurezza dove, anche senza parlare di IA, si entra in una dimensione in cui il confine tra protezione nel pubblico interesse e diritti dell'interessato percorrono strade complesse e intrinsecamente piene di ostacoli, rischiando di non incontrarsi facilmente.

Se, poi, si pensa alla IA come un ausilio per le autorità preposte alla pubblica sicurezza, l'equilibrio tra i molti fattori diviene ancora più complicato da raggiungere. Se, poi, la IA è intesa come algoritmo di rilevazione della "identità biometrica" degli individui, in particolare del volto, e atto a sorvegliare le persone e, attraverso questo tipo di rilevazioni, si intende fornire un ausilio alla pubblica sicurezza, allora il bilanciamento tra sicurezza e diritti degli individui diviene ancora più frastagliato e difficile da raggiungere. Ci si interroga su quali siano gli elementi più critici in questo scenario e quali le opportunità per migliorare il bilanciamento. Per poter poi entrare in concreto in proposte di possibili azioni e sviluppi da perseguire, è utile riassumere alcuni elementi cardine individuati ed elaborati nella trattazione e creare con essi un quadro d'insieme.

Esistono tre realtà coinvolte nel problema descritto, due sono umane e una no. Le due realtà umane sono gli individui e le autorità preposte alla pubblica sicurezza, mentre la componente non umana è chiaramente l'algoritmo di IA. Le tre realtà condividono un elemento che considerano importante: i dati. I *dati personali* sono patrimonio dell'individuo, fonte di conoscenza per le attività investigative e processuali delle autorità preposte alla pubblica sicurezza. I dati sono anche la base dell'addestramento di un algoritmo e, in particolare, i dati personali degli individui formano quella "esperienza" dell'algoritmo che gli permette di poter essere d'ausilio per le attività di pubblica sicurezza. Senza i dati personali, dunque, l'incontro tra pubblica sicurezza, individui e IA non sarebbe realizzabile. Un altro elemento accomuna individui, autorità preposte alla pubblica sicurezza e algoritmi di IA: la possibilità di commettere *errori*. Se ognuna delle tre realtà fosse infallibile, l'incontro tra di esse non avrebbe luogo, perché gli individui non commetterebbero reati e le autorità preposte alla pubblica sicurezza avrebbero poco da fare e l'algoritmo non avrebbe motivo di essere di ausilio.

In questo quadro si innesta il principio di autodeterminazione informativa dell'individuo il quale, dunque, dovrebbe poter decidere autonomamente in che misura condividere fatti personali e, in particolare, dati personali. Il dato personale è al centro del contesto di salvaguardia ordito dal GDPR, che protegge proprio il sopracitato principio, a meno che il trattamento non sia finalizzato ad attività da parte delle autorità per prevenire e perseguire reati o eseguire sanzioni penali, quando diventa la Direttiva 2016/680 il terreno su cui cercare il bilanciamento tra diritti dell'individuo e sicurezza. Inoltre, è anche l'ambito in cui innestare l'eventuale ausilio algoritmico della IA e, in particolare, del rilevamento biometrico e della collegata identificazione con i sistemi di sorveglianza. Come evidenziato nella trattazione[571] il Regolamento e la Direttiva europei hanno molti aspetti apprezzabili anche se lasciano alcune aree non

[571] *supra* Capitolo II § 4, 5

completamente definite e bisognose di completamenti sia a livello nazionale da parte degli Stati membri che europeo.[572]

Per poter definire gli ambiti di intervento in cui una proposizione è possibile un possibile criterio è quello di identificare i parametri che possono essere progettabili nel trattamento dei dati per finalità di pubblica sicurezza coadiuvate da algoritmi di IA e, in particolare di riconoscimento facciale. In tal senso, un aspetto interessante in termini prospettici è contenuto nell'art. 25 del GDPR, che è dedicato alla "Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita", la cosiddetta "*data protection by default and by design*".[573] L'articolo offre, già dal titolo, un aspetto *progettabile* ai fini della protezione dei dati personali dell'individuo. Infatti, i paragrafi 1 e 2 indicano alcune attività, a carico del titolare del trattamento, che riguardano la realizzazione di misure "tecniche e organizzative adeguate" definite tenendo conto di una serie di fattori legati a costi, ambito applicativo, contesto, obiettivo del trattamento e rischi (in termini di probabilità e gravità) per diritti e libertà delle persone del trattamento stesso.

Ad opinione di chi scrive, tali fattori costituiscono, di fatto, un insieme di "specifiche" su cui impostare il "progetto" delle suddette misure a carattere tecnico-organizzativo, e dove il rischio del trattamento potrebbe essere considerato un elemento dalla cui valutazione scaturisca la "bontà" del progetto oppure la necessità di ulteriori iterazioni progettuali per giungere a una adeguata riduzione del rischio stesso. La procedura descritta potrebbe anche essere "compresa" e realizzata da un algoritmo di IA, dopo un opportuno addestramento su un insieme di dati rappresentativo di una ampia casistica dei parametri in gioco. L'art. 25 esemplifica due tecniche applicabili per abbassare il rischio del trattamento per i titolari dei dati, cioè la pseudonimizzazione[574] e la minimizzazione del contenuto allo strettamente necessario ai fini del trattamento stesso. La "progettazione" delle misure tecnico-organizzative comprende anche portata, periodo di conservazione e accessibilità dei dati personali oggetto del trattamento, e dunque che tali dati siano opportunamente protetti nelle varie dimensioni di possibile esposizione (intervallo di tempo, quantità di persone che possono accedervi). Anche tali elementi potrebbero essere efficacemente gestiti con l'ausilio di un algoritmo basato su IA.

Un ulteriore aspetto interessante dal punto di vista progettuale è contenuto nel paragrafo 3 dell'articolo, dove si delinea la possibilità di verificare la conformità ai paragrafi 1 e 2 dell'articolo 25 stesso attraverso un meccanismo di certificazione, approvato ai sensi dell'art. 42 del Regolamento. La certificazione sugella l'aderenza di un progetto ad uno *standard* effettivo o de facto e, dunque, garantisce la "bontà" del

[572] ROSSI DAL POZZO, *Alcune riflessioni a margine della nuova disciplina in materia di protezione dei dati personali di cui al Regolamento (UE) 2016/679/UE*, cit., 17, 19
[573] DEL PIZZO A., *Privacy by design: il ponte tra diritto e tecnica nella tutela dei dati personali*, in *Cammino Diritto*, 7, 2020, 18
[574] *supra* Capitolo II § 4.2

prodotto e, quindi, delle misure tecnico-organizzative per la protezione dei dati personali. L'art. 42 stabilisce proprio che l'istituzione di procedure di certificazione sia incoraggiata da parte di tutti, quindi a livello europeo e nazionale dei singoli Stati membri, dalla Commissione allo EDPB[575] e alle autorità di controllo. La certificazione implica anche la definizione di marchi e sigilli di protezione dei dati, a testimonianza della conformità al Regolamento e, dunque, alle indicazioni su tutte le fasi di gestione del dato e la loro aderenza ai diritti del titolare dei dati stessi. Come ogni elemento del complesso quadro del trattamento, anche la certificazione deve bilanciare i diversi soggetti coinvolti e, dal momento che essa può costituire un onere maggiore per le imprese di dimensioni limitate, il Regolamento tiene conto delle specifiche esigenze delle micro, piccole e medie imprese nella gestione del trattamento, comunque proteggendo i diritti e le libertà degli individui oggetto del trattamento.

La certificazione ha anche il vantaggio di rendere più evidenti le violazioni e, dunque, di contribuire al maggior rispetto dei principi e le metodiche indicate nel Regolamento. Un ulteriore vantaggio, a opinione di chi scrive, è che la certificazione può anche evolvere, in modo sistemico ma sempre oggettivo, nel tempo per raccordarsi con le evoluzioni del quadro tecnologico ma anche sociale e geopolitico, rappresentando dunque uno strumento anche di interazione con paesi terzi. e organizzazioni internazionali, come già indicato nel paragrafo 2 del presente articolo. L'articolo mette in risalto nel paragrafo 3 la natura «volontaria e accessibile tramite una procedura trasparente» della certificazione. Nel complesso quadro del trattamento dati, ogni qual volta si introduce un elemento progettabile e gestibile attraverso un meccanismo *trasparente* si sortisce un doppio effetto, secondo l'opinione di chi scrive. La progettualità conferisce flessibilità nel tempo e nel contesto e la trasparenza induce chiarezza in chi opera e in chi è coinvolto a vario titolo. La certificazione, dunque, in base all'articolo 41, rientra perfettamente in questa descrizione. Tra l'altro, essa non riduce la responsabilità da parte titolare del trattamento di agire in modo conforme al Regolamento, come specificato nel paragrafo 2, ed è rilasciata dagli organismi di certificazione dall' autorità di controllo competente oppure dallo EDPB in accordo, rispettivamente agli articoli 43, 58 e 63 del Regolamento. Si può allora dire che la certificazione, che viene rilasciata al titolare del trattamento per un periodo di tre anni, rinnovabili se persistono le condizioni favorevoli alla certificazione stessa, esalta l'applicazione del Regolamento, conferendo una dimensione di progettualità aggiuntiva. Se le condizioni che hanno condotto al rilascio della certificazione non sono più verificate, essa viene revocata.

Da quanto evidenziato sin qui, si individua un ruolo importante della *progettualità*, nel quadro normativo creato dal GDPR e dalla Direttiva 2016/680. La progettualità, infatti, può aiutare la trasformazione delle indicazioni *qualitative*, su alcuni elementi chiave che concorrono al trattamento dei dati personali rispettoso dei diritti degli individui e

[575] European Data Protection Board, *supra* § 4.3

bilanciato nel garantire alle autorità preposte alla sicurezza pubblica di operare, in *quantitative*. Tale trasformazione è alla base di una possibile evoluzione del quadro normativo sia nazionale che europeo, per raccogliere le crescenti sfide sul trattamento dei dati personali che la pervasività della IA e, in particolare, delle tecniche di identificazione biometrica basate sul riconoscimento facciale, pongono in un numero crescente di settori applicativi. Anche se si decidesse a priori di rinunciare all'impiego del riconoscimento facciale in ausilio alle autorità preposte alla pubblica sicurezza, questo non fermerebbe in alcun modo il progresso della tecnologia di IA. Garantire la pubblica sicurezza in un mondo ad alta pervasività della IA può trovare proprio nella sua adozione come "aiutante" una serie di benefici, che naturalmente possono essere ridotti se non addirittura vanificati da algoritmi ad alto tasso di errore o da una non adeguata interazione tra operatori umani e algoritmi. Nei prossimi paragrafi verranno delineate possibili proposte che vanno nella direzione di una progettualità del trattamento dei dati personali compatibile con l'impiego della IA, e in particolare del face recognition, in un quadro di bilanciamento tra diritti e sicurezza.[576]

6.1. (*Segue*): ruolo dell'operatore e algoritmi.

Nella trattazione si è più volte sottolineata l'importanza della componente umana nella catena operativa e decisionale che contempla l'impiego di algoritmi di IA. In particolare, se ne è sottolineata l'importanza, a parere di chi scrive, descrivendo l'impiego degli algoritmi predittivi nell'approccio evidence-based e la ricerca di un bilanciamento basato sull'assenza di pregiudizi e polarizzazione sia algoritmica che umana nelle decisioni.[577] Si è poi ribadita la necessità dell'operatore umano per l'impiego dei sistemi di sorveglianza di massa basati sul riconoscimento biometrico del volto, con compiti di supervisione e con la responsabilità della decisione finale.[578] La presenza della componente umana nella catena decisionale automatizzata è stata anche ribadita nella descrizione della posizione dello EDPB in materia di trattamenti completamente automatizzati[579] poiché, ad opinione di chi scrive, l'algoritmo potrebbe non tenere in debito conto alcuni fattori, almeno allo stato attuale delle prestazioni algoritmiche della IA e, in particolare, del riconoscimento facciale.

Ad avviso di chi scrive, dunque, la presenza umana nella catena operativa e decisionale, anche in presenza di una elevata automatizzazione e di algoritmi molto "indipendenti", perché basati su tecniche di auto apprendimento e comportamento predittivo di deep learning, non è eliminabile. Tale conclusione riguarda sia le applicazioni di ausilio alle autorità di pubblica sicurezza che le fasi cruciali del processo penale, in cui la versione algoritmica del giudice non appare praticabile[580] neanche in prospettiva, visto il

[576] *supra* Capitolo II § 4
[577] *supra* Capitolo I § 6.1
[578] *supra* Capitolo II § 1
[579] *supra* Capitolo II § 4.3
[580] GALGANI, *Giudizio penale, habeas data e garanzie fondamentali*, cit., 23

delicato equilibrio necessario per giungere alle decisioni e l'impatto delle stesse sul futuro degli imputati, anche in termini di possibile privazione del diritto alla libertà che la reclusione implica.

Se l'operatore umano si ritiene, come chi scrive sostiene, ineliminabile, ci sono una serie di conseguenze da mettere in luce. La prima riguarda l'*algoritmo* che, evidentemente, si ritiene meno affidabile dell'operatore cosa che, per gli algoritmi di face recognition, è stato illustrato con particolare riferimento alle vicende statunitensi degli ultimi due anni.[581] La fallibilità degli algoritmi si è particolarmente rilevata in merito ai volti di categorie potenziali oggetto di discriminazioni da parte degli esseri umani, prima ancora che dall'algoritmo. Bisogna precisare, infatti, che l'algoritmo non possiede una coscienza e una attitudine intrinseca a commettere ingiustizie, ma è il rilevamento "tecnico" che si è trovato essere più erroneo se il viso è di una donna ed è di colore. Si ritiene, tuttavia, che le suddette limitazioni dell'algoritmo di riconoscimento potranno essere sanate sia con il progresso della tecnologia che con l'addestramento su basi di dati di buona qualità e mirate a risolvere la specifica fallacità.

La seconda conseguenza del ritenere non eliminabile la presenza dell'operatore è che si debba supporre, anche in presenza di un algoritmo che nel tempo avrà prestazioni di affidabilità crescenti, che la *componente umana* sia comunque meno fallace e meno polarizzata dell'algoritmo, soprattutto nel prendere la decisione finale sulla identificazione del volto e l'associazione ad uno specifico individuo. Se all'algoritmo si chiede di migliorare le prestazioni, anche all'operatore si deve evidentemente chiedere di migliorare nel tempo le sue, sia in termini tecnici che concettuali. La parte tecnica concerne la necessità di addestramenti mirati sulla IA e sull'impiego degli algoritmi di riconoscimento per essere in grado di governare l'algoritmo ed interagire con esso in modo dinamico. In particolare, si potrebbe immaginare in termini prospettici che l'algoritmo sia in grado di valutare il proprio margine di errore in una decisione, basandosi su una previsione simile a quella che, dal punto di vista meteorologico, annuncia pioggia in una certa località e in una determinata fascia oraria. In presenza di un algoritmo che fornisce la sua probabilità di errore, all'operatore verrebbe richiesto di "assisterlo" con dati di input "migliori", cosa che implica per l'operatore un addestramento ancora più complesso. Oltre alla prestazione tecnica, l'operatore umano deve garantire l'assenza di pregiudizio e la capacità di decisioni eque. Su questo aspetto, che in linea di principio dovrebbe essere intrinseco nell'operatore, si può comunque ipotizzare un addestramento mirato in tal senso.

6.2. (*Segue*): progettualità di algoritmi autovalutativi.

Si è descritto[582] uno scenario per l'impiego di algoritmi di IA per il riconoscimento facciale a supporto della pubblica sicurezza in cui la presenza dell'operatore umano si

[581] *supra* § 1
[582] *supra* § 6.1

propone essere inalienabile ma "addestrata" sia tecnicamente che eticamente. Si è anche evidenziato che un algoritmo con prestazioni tali da poter valutare, per esempio in termini percentuali, la sua probabilità di errore è tutt'altro che impossibile, visto il rapido progresso del deep learning e di tecniche di intelligenza artificiale cosiddette *empatiche* (*Empathic AI*, EA). Tali evoluzioni della IA partono dalla finalità di migliorare la collaborazione tra componente umana e artificiale diminuendo quella distanza che nasce dalla diversità nell'approccio logico, ferreo per la IA e "inquinato" dalla emotività degli esseri umani. Un algoritmo di IA empatica sarà sempre più capace di rispondere a emozioni umane in modo empatico. La componente artificiale, dunque, sarà in grado di "comprendere" le emozioni dell'interlocutore umano e rispondere in modo adeguato ad esse, come dovrebbe in linea di principio accadere nel colloquio tra esseri umani. Tale evoluzione nell'algoritmica IA potrebbe essere l'elemento cruciale per rendere l'ausilio della IA più efficace nell'ambito della pubblica sicurezza e del processo penale.[583]

Secondo alcuni esistono vari collegamenti tra empatia e responsabilità, in accordo a risultati prodotti in varie discipline, quali la psicologia, le scienze sociale e organizzative, poiché l'empatia è di ausilio alle sfide tecnico-sociali collegate con la responsabilità.[584] Le prestazioni di una IA empatica vanno dunque nella direzione di una *umanizzazione* della relazione da parte della componente artificiale in cui è inquadrabile anche una certa "coscienza" della IA sui suoi limiti davanti ad un dato problema e un dato insieme di dati di addestramento. La capacità dell'algoritmo, opinione condivisa non solo nel mondo scientifico ma anche in quello della informazione, di imparare da solo[585] è foriera di un processo di miglioramento autonomo della IA che, se indirizzato sull'obiettivo di ridurre gli errori, potrebbe condurre a risultati sorprendenti in un prossimo futuro. Inoltre, un algoritmo consapevole dei propri limiti, traducibili in una percentuale di errore da fornire all'operatore addestrato tecnicamente ed eticamente, è un buon punto di partenza anche per migliorare la fiducia in esso da parte della componente umana. Un algoritmo "sincero" sui suoi limiti e capace di migliorare attraverso i suoi sbagli, cosa che si traduce in un aggiornamento periodico del suo addestramento in cui, tra i dati forniti si includono quelli dei casi in cui si è palesato l'errore, rischia di diventare un ottimo compagno di lavoro, in talune circostanze preferibile alla componente umana. Si ritiene che tale dimensione evolutiva degli algoritmi di IA sia quella più consona ad una loro adozione efficace nel mondo della pubblica sicurezza e del processo penale, sempre mantenendo, come già ribadito[586], la centralità dell'operatore umano nella catena decisionale.

---

[583] GALGANI, *Giudizio penale, habeas data e garanzie fondamentali*, cit., 23

[584] SRINIVASAN R. – SAN MIGUEL GONZÁLEZ B., *The role of empathy for artificial intelligence accountability*, in *Elsevier - Journal of Responsible Technology*, 6, 2022, 3

[585] GARITO E., *Dall'algoritmo egoista all'algoritmo responsabile (e forse anche generoso)*, in *Economopoly*, 2022, 2

[586] *supra* § 6.1

Un ulteriore aspetto dello scenario prospettato concerne il caso in cui sia l'operatore umano a commettere un errore che l'algoritmo non commetterebbe, quindi per enunciarlo in termini probabilistici, un errore che l'algoritmo commette nello 0% dei casi. Al momento, l'algoritmo non ha modo di essere di ausilio in queste situazioni, ma dal punto di vista delle sue capacità prestazionali questa attività è già alla sua portata. Si potrebbe ipotizzare un contributo dell'algoritmo alla rilevazione di errori dell'operatore con cui "collabora", che segnala con una messaggistica di *alert* o un *warning* la presenza di un errore, corredata della spiegazione su come risolverlo, in modo da non ridurre l'efficienza nella attività in cui si è palesato l'errore. Si considera, infatti, che le attività legate alla pubblica sicurezza siano molto spesso a carattere di urgenza e un ritardo nella esecuzione potrebbe comportare un danno significativo alla «prevenzione, indagine, accertamento e perseguimento dei reati o esecuzione di sanzioni penali»[587].

Un ulteriore situazione che potrebbe verificarsi, auspicabilmente in un numero ridotto di casi, è un abuso da parte dell'operatore della sua autorità e per comprendere il quale l'algoritmo, in linea di principio, potrebbe non essere programmato e addestrato. Se, però, si intende conferire all'algoritmo la capacità di rilevare abusi, già con le attuali prestazioni della IA lo si può programmare e addestrarlo *ad hoc* per rilevare l'abuso e agire secondo una codificata lista di azioni che faranno parte del suo corredo esperienziale, tra cui un *alert/warning* che dovrebbe essere non solo rilevabile dall'operatore, che potrebbe aver sbagliato in buona fede, ma anche a specifiche autorità. In una successiva evoluzione dell'algoritmo rilevatore di abusi, si potrebbe prevedere una correzione in tempo reale degli effetti dell'abuso, per quanto possibile, dall'algoritmo, anche attraverso le indicazioni della autorità informata in parallelo dell'abuso stesso.

Quanto detto in merito allo scenario evolutivo di una algoritmica che anche nel riconoscimento facciale divenga un efficace ausilio alle autorità preposte alla pubblica sicurezza, rimane la criticità, più volte evidenziata nella trattazione, sulla neutralità e non opacità dell'algoritmo che, in fin dei conti, è sempre progettato e addestrato da esseri umani. È vero che l'autoapprendimento nel deep learning può portare ad una evoluzione autonoma dell'algoritmo che si discosta quindi dallo stadio iniziale programmato da esseri umani, ma l'esperienza dell'algoritmo e il suo addestramento partono da logiche e dati "umane". Quindi, il punto cruciale rimane la necessità di una garanzia formale che l'algoritmo agisca seguendo un approccio etico, non discriminatorio e trasparente. Inoltre, se i suoi compiti dovessero comprendere le sopracitate rilevazioni di errore o abuso da parte della componente umana, è davvero importante essere certi di avere a che fare con un prodotto "garantito".

[587] Direttiva del 27 aprile 2016 n. 680, cit., art. 1, *Oggetto e obiettivi*

Torna, dunque, preponderante il tema di una certificazione o un sigillo o una forma di garanzia a carico di una autorità neutrale preposta per tale finalità. Tale autorità potrebbe essere europea oppure nazionale e potrebbe coincidere, ad esempio, con i Garanti istituiti negli Stati membri e coordinati attraverso lo EDPB oppure con altra autorità istituita a tale scopo. Un importante elemento per giungere alla certificazione o garanzia sulla "bontà" dell'algoritmo è la natura intrinsecamente interdisciplinare della materia, che contempla, oltre agli aspetti a carattere giuridico-penale, quelli squisitamente tecnici e tecnologici, sociologici, psicologici, etico-filosofici. Inoltre, per essere certi che qualsiasi fattore di polarizzazione e discriminazione non rientri nella logica di programmazione e di addestramento dell'algoritmo, il processo di certificazione o di garanzia dovrebbe prevedere il passaggio attraverso un possibile comitato la cui composizione sia di per sé garanzia di neutralità rispetto alle numerose forme di discriminazione che hanno già reso il percorso di accettazione degli algoritmi di face recognition molto accidentato.[588]

6.3. (*Segue*): progettualità del dato personale per il principio di proporzionalità.

Dopo aver proposto alcuni scenari di collaborazione tra autorità di controllo alla pubblica sicurezza e algoritmi di IA per il riconoscimento facciale, si intende approfondire i profili di progettualità insiti in alcuni dei parametri ed elementi che attraverso il GDPR e la Direttiva 2016/680 definiscono il quadro della protezione in merito al trattamento dei dati personali, nel riconoscimento facciale e in generale nella rilevazione biometrica.

Un primo elemento progettabile è nel trattamento dei dati personali è costituito dal principio di proporzionalità, concetto già anticipato in merito all'analisi della Direttiva 2016/680[589] e delle considerazioni sulla compiutezza dei dati stessi[590]. Per ricondurre il principio di proporzionalità a una dimensione progettuale bisogna provare a rappresentarlo in termini potenzialmente quantitativi, per quanto sia non immediato immaginare un numero associato ad un principio.

Il principio chiede, in sostanza, ai dati personali oggetto del trattamento di avere compiutezza, la quale si può raggiungere attraverso un bilanciamento tra i vari fattori che vi concorrono e che sono sintetizzabili in tre parametri principali: *pertinenza*, *completezza* e *non eccedenza*. Se tali parametri sono ben dosati in assoluto e relativamente tra loro, si raggiungerà un livello di compiutezza tale da rispettare la proporzionalità auspicata dal principio. Supponendo di riuscire a quantificare il livello giusto di *compiutezza*, che potrebbe essere definito in un intervallo di valori anche molto semplice, come ad esempio tra 0 e 1, significando che se la compiutezza si attesta sul valore 0 il principio di proporzionalità è completamente disatteso, mentre se vale 1

[588] *supra* § 1
[589] *supra* Capitolo II § 5.1
[590] *supra* Capitolo II § 6

il principio è onorato in pieno, si è realizzato il primo passo per una progettualità del principio stesso. Infatti, il valore di compiutezza dei dati desiderato diventa una specifica a cui il risultato della progettazione deve obbedire per poter dire di aver progettato bene. I valori progettabili di compiutezza si attesteranno tra i due valori sopracitati 0 e 1, perché se è pur vero che si vorrebbe la massima compiutezza in ogni circostanza, dunque pari a 1, è anche vero che essendo il bilanciamento di tre parametri, ciascuno a sua volta da progettare, è verosimile che ci si accontenterà di valori minori di 1, ma lontani da 0 come, a mero titolo di esempio, 0.95.

A questo punto, la progettazione consiste in quella dei tre parametri che concorrono alla compiutezza, cioè pertinenza, completezza e non eccedenza dei dati del trattamento e del loro bilanciamento. Per quanto riguarda la pertinenza, essa misura l'aderenza alle finalità di uno specifico trattamento dei dati e, per quanto siano immaginabili un numero molto variegato di tali finalità, esse sono comunque un elenco che, per quanto lungo, ha un inizio e una fine. Anche la pertinenza si può ricondurre ad una quantificazione e, sempre per motivi di semplicità nella illustrazione del concetto, la si potrebbe immaginare collocata in un intervallo tra 0 e 1, come si è supposto per la compiutezza, quindi pari a 1 in caso di piena pertinenza con il trattamento dati e 0 in caso di non pertinenza. Il valore della pertinenza ha attinenza con *quale* tipo di dato viene chiesto all'interessato per le finalità del trattamento, cioè la tipologia del dato. Per ogni finalità di trattamento e possibile redigere la lista dei dati ad esso più o meno pertinenti e a ciascuna tipologia può essere assegnato un peso specifico in modo che alla fine sia possibile quantificare la pertinenza risultante dalla scelta dei dati che si ritiene di dover usare. Se la pertinenza risultante risulta troppo bassa, è evidente che bisogna ritornare su qualcuna delle scelte fatte e aggiornare i dati da richiedere per il trattamento.

Il secondo parametro da progettare per il principio di proporzionalità è la *completezza* del dato oggetto di trattamento che, come descritto in precedenza[591], ricomprende sia la bontà dei contenuti che la qualità del dato stesso. I contenuti devono essere completi, cioè inclusivi di tutte le informazioni necessarie per l'andata a buon fine del trattamento in cui sono richiesti. Inoltre, il dato deve essere di qualità consona alle finalità del trattamento, poiché una qualità scarsa può inficiare i risultati del trattamento. Anche la completezza si può ricondurre ad una quantificazione e, per semplicità nella illustrazione del concetto, la si potrebbe immaginare collocata in un intervallo tra 0 e 1, come si è supposto per la compiutezza e la pertinenza, quindi pari a 1 in caso di completezza dei dati e 0 in caso di non completezza assoluta. Volendo poi articolare il modello, si potrebbe quantificare sia la bontà del contenuto che la qualità con un indicatore numerico, e quindi progettare la completezza attraverso il progetto separato di contenuto e qualità.

[591] *supra* Capitolo II § 6

Il terzo parametro progettabile, che concorre al principio di proporzionalità, è la *non eccedenza*, quindi la quantità "giusta" di dati, cioè di *quanti* dati si ha davvero necessità per effettuare il trattamento. L'esubero, come già evidenziato[592] comporta effetti negativi sulle risorse necessarie (memorie, tempo di accesso) e complica inutilmente le fasi di trattamento. Anche la non eccedenza si può ricondurre ad una quantificazione e, sempre per motivi di semplicità nell'illustrare il concetto, la si potrebbe immaginare collocata in un intervallo tra 0 e 1, come si è supposto per gli altri parametri, quindi pari a 1 in caso eccedenza nulla dei dati, dunque di non eccedenza perfetta e 0 in caso contrario. La quantificazione dei parametri progettabili appena descritta è compatibile con l'approccio logico di un algoritmo di intelligenza artificiale che, dunque, potrebbe essere un ausilio nella progettazione del principio di proporzionalità.

Nel caso del riconoscimento facciale, il tipo di dati oggetto del trattamento sono i volti rilevati ai fini della identificazione. La pertinenza con la finalità del trattamento è evidente, in quanto si rilevano volti per identificare volti. La compiutezza, invece, potrebbe essere non sempre adeguata, dal momento che il rilevamento potrebbe coinvolgere anche volti di persone diverse da quella oggetto del trattamento e la qualità dell'immagine (fissa o in movimento) rilevata potrebbe non essere alta. Si comprende come una bassa completezza sia alla base di potenziali errori di riconoscimento. Per quanto riguarda la non eccedenza, per mantenerla a valori ottimali è necessario rilevare solo le immagini strettamente necessarie.

6.4. *(Segue):* progettualità del dato per la conservazione ottimale.

Un ulteriore elemento di progettualità che contribuisce all'efficacia del trattamento e alla conservazione del dato è la composizione del dato in termini di caducità temporale. Se tutte le componenti del dato hanno la stessa "decadenza" in termini informativi al passare del tempo, la conservazione del dato può avere un'unica data di scadenza, altrimenti generalmente la retention del dato è guidata da quella parte che dura di più nel tempo, il che porta a conservare il dato anche se solo una parte di esso sarà necessaria in futuro. La conseguenza è una inefficienza sia nel trattamento che nella archiviazione che, come già evidenziato[593] impegna risorse di spazio di memoria e di tempo di accesso nella ricerca del dato, allontanando la possibilità di effettuare una conservazione a bassa intensità. Inoltre, la gestione di un dato di questo tipo è anche poco sostenibile e la sostenibilità è un tema che non può più essere tenuto in disparte in nessuna attività umana.Lo sforzo a livello europeo in tale direzione è rimarchevole ed è vicino il momento in cui vivere in un ambiente sostenibile verrà annoverato tra i diritti fondamentali, esattamente come lo è diventato l'accesso alla connessione Internet.

[592] *supra* Capitolo II § 6
[593] *supra* Capitolo II § 6

Il bilanciamento, quindi, tra diritti e sicurezza presto dovrà anche considerare il tema sostenibilità, come, a titolo esemplificativo, il consumo energetico necessario per mantenere attivi i server in cui i dati sono conservati. In tale ottica, se si adotta l'approccio progettuale al trattamento dati, la sostenibilità dovrebbe già rientrare tra i requisiti di progetto.

La progettazione del dato per la omogenea caducità è anche in linea con i già discussi aspetti della pertinenza e della non eccedenza. Se è forse più pratico raccogliere in una sola volta dati, in linea di principio, pertinenti con la finalità della raccolta ma differibili nel loro impiego nel tempo, dal punto di vista della bontà del dato come omogenea caducità tale approccio non è efficace. Se la raccolta è automatizzata ma basata su una attenta progettazione, coadiuvata da elementi normativi che supportano la quantificazione dei parametri, effettuare due raccolte potrebbe essere preferibile ad effettuarne una sola. Per quanto riguarda la caducità temporale, essa è legata al dominio applicativo per il quale è richiesto il trattamento. In linea di principio, è possibile codificare la relazione tra dominio applicativo, composizione ottimale del dato richiesto, massima necessità di conservazione del dato. Una tale categorizzazione è, come si intuisce, un input compatibile con un algoritmo di IA, che potrebbe divenire di ausilio anche in questo tipo di progettazione.

Nella raccolta di immagini da un sistema di riconoscimento facciale il differimento temporale della raccolta è un elemento della progettazione in termini di caducità, come anche l'aggiunta di altri elementi all'immagine di disomogeneo comportamento nel tempo. Tali elementi aggiuntivi potrebbe avere una maggiore o minore caducità temporale rispetto a quella delle immagini che si raccolgono con la rilevazione facciale. Di conseguenza, la caducità del dato complessivo, immagini più i dati integrati successivamente, verrà conservato in base alla "scadenza" dell'elemento che più dura nel tempo, ad esempio i dati anagrafici rispetto all'immagine in un dato momento temporale. Quindi, se l'immagine di un soggetto in un particolare anno ha una utilità ridotta nel tempo per la sua identificazione, dati perduranti come quelli anagrafici "costringeranno" a conservare comunque entrambi gli elementi, fotografici e anagrafici.

Naturalmente, però, l'incrocio dell'immagine o delle immagini fisse o in movimento, "catturate" dal sistema di riconoscimento, con altri dati presumibilmente pertinenti con il soggetto di interesse può essere utile in alcune circostanze connotate da particolare rilevanza penale. Un esempio di tale circostanza può essere l'utilizzo di un sistema di riconoscimento facciale al fine di catturare un reo o un fuggitivo, per cui l'incrocio dei dati può essere fondamentale a tale fine. Tuttavia, la creazione di un "dato integrato", che dunque sarà intrinsecamente non omogeneo in termini di caducità temporale, dovrebbe avere due tipi di garanzie. Tali garanzie sarebbero volte alla *efficacia* dell'azione conseguente alla cattura del dato integrato, da parte delle autorità competenti per la pubblica sicurezza, e al *rispetto* dei diritti dell'interessato che il

medesimo dato integrato, proprio per la sua natura multidimensionale, potrebbe violare più facilmente. La prima delle garanzie che si dovrebbero osservare per la creazione del dato integrato riguarda la attendibilità della rilevazione facciale in termini di accuratezza, ovvero di una bassa probabilità di essere errata. Abbinare con altri dati relativi all'individuo in oggetto un elemento potenzialmente errato abbassa la affidabilità dell'intero dato integrato e riduce l'efficacia dell'azione correlata al dato stesso.

La seconda garanzia è legata al rispetto dei diritti del soggetto che l'incrocio di dati non omogenei potrebbe mettere a rischio. Come si è visto[594], infatti, la disponibilità di dati integrati può degenerare in una "schedatura" di massa, come sta avvenendo in Cina con i sistemi di sorveglianza già in uso e la rete avanzata in progettazione. Se, comunque, le finalità della creazione del dato integrato possono essere giustificate, potrebbe divenire utile l'algoritmo di IA, descritto in precedenza[595], capace di valutare autonomamente la sua capacità di errore, per ovviare alle criticità enunciate. Infatti, in presenza di una autovalutazione dell'algoritmo sulla probabilità di errore, si potrebbe stabilire di procedere alla creazione del dato integrato se tale probabilità si mantiene al di sotto di una certa soglia. Tale soglia, come tutti gli altri elementi progettabili presentati sin qui[596], potrebbe essere oggetto di regolamentazione, o almeno di linee guida formali per le attività di pubblica sicurezza che impieghino la IA e il rilevamento biometrico in forma estensiva.

6.5. *(Segue):* progettualità del rischio per la data protection by design.

Come descritto in precedenza[597], la progettualità del trattamento dei dati è insita nei regolamenti europei e, nella ricerca del delicato bilanciamento tra diritti e pubblica sicurezza c'è spazio per la progettazione anche del *fattore di rischio*, sia in termini di probabilità che di gravità, associato al trattamento dei dati personali. Il rischio è relativo alla possibilità di ledere diritti e libertà della o delle persone coinvolte nel trattamento ed è oggetto di una valutazione solo qualitativa, che vede nella necessità del trattamento il fattore principale con cui effettuare il bilanciamento. L'ampio margine soggettivo nella valutazione della necessità rende il consolidamento del rischio non univoco e complesso da raggiungere. Tuttavia, anche se la materia appare difficile da riportare in termini squisitamente quantitativi, si ritiene che uno sforzo in questa direzione renderebbe più efficace la gestione e più ripetibili le scelte da effettuare in uno specifico insieme di circostanze, con conseguente semplificazione anche dal punto di vista della responsabilità in caso di violazioni.

[594] *supra* § 5
[595] *supra* § 6.2
[596] *supra* § 6.1, 6.2, 6.3
[597] *supra* § 6

Per quantificare il rischio è necessario definire in modo preciso i fattori che concorrono ad esso e attribuire un fattore di ponderazione alle necessità dei trattamenti, in modo che la scelta porti a una valutazione inequivocabile del rischio associato. Il rischio, a sua volta, oltre a rappresentare la probabilità di violazione dei diritti del soggetto, deve essere collegato alla quantificazione della gravità, intesa come la combinazione di conseguenze prevedibili e la porzione di imprevedibilità che ricade sui soggetti coinvolti, direttamente oppure indirettamente, a causa del trattamento. Per quanto appaia complicato il dedalo di possibilità da identificare in tal senso, è comunque possibili stendere una lista sufficientemente esaustiva e codificare la "gravità" della conseguenza in termini quantitativi.

Un approccio così parcellizzato al problema del rischio è, di nuovo, compatibile con un ausilio algoritmico basato su IA, che possa prospettare all'operatore responsabile della decisione e del trattamento utili elementi quantitativi per formulare una scelta. Tra l'altro, se la decisione non richiede un'azione tempestiva o in tempo reale, si potrebbe predisporre un software di simulazione per valutare gli effetti a breve, medio e lungo termine del trattamento sui soggetti interessati.

Un approccio basato sulla quantificazione del rischio consente, inoltre, un potenziale miglioramento del rischio stesso, introducendo correttivi nell'azione o elementi aggiuntivi che integrino quelli a disposizione. Disponendo di un software di simulazione, è quindi possibile rivalutare il rischio e constatarne la effettiva diminuzione, a livello simulativo. In questo modo il trattamento e la modalità di implementazione dello stesso possono divenire oggetto di un ciclo virtuoso di progettazione che abbia come obiettivo la riduzione del rischio e della gravità associata alo stesso. Gli elementi aggiuntivi da associare al trattamento hanno un ruolo delicato perché si vuole abbassare il rischio senza creare inutili dati integrati[598] e "schedature" non supportate da elementi oggettivi. In questo senso, il supporto algoritmico potrebbe essere molto efficace, per gestire al meglio le risorse informative a disposizione e il loro impiego per ridurre il rischio.

La valutazione del rischio può condurre a due scenari diversi. Nel primo, viene creato un vincolo normativo per il quale al di sopra di un certo rischio il trattamento non può avvenire, a meno di eventuali deroghe in casi particolari. In un secondo approccio, è l'operatore responsabile del trattamento e prendersi la responsabilità di agire, anche in presenza di rischio alto, con le conseguenze del caso. Se la decisione è fortemente basata sull'output dell'algoritmo, si ricade negli scenari descritti in precedenza[599] per errori dell'algoritmo o dell'operatore o di entrambi.

[598] *supra* § 6.4
[599] *supra* § 6.1, 6.2

7. Prospettive penali sull'inquadramento della IA nel processo.

Dopo il complesso percorso di analisi e approfondimenti, anche a carattere multidisciplinare[600] e geografico[601], la trattazione ha raggiunto una certa comprensione del funzionamento degli algoritmi di intelligenza artificiale. Ad opinione di chi scrive, comprendere e analizzare il funzionamento di tali tecnologie può risultare funzionale per un loro plausibile e positivo inserimento, secondo diverse prospettive, all'interno del processo penale. Si è quindi giunti al punto di formulare proposizioni che auspicabilmente siano di ausilio all'inquadramento dell'algoritmo di IA nel processo penale.

Sin qui sono state introdotte proposte operative[602] sugli strumenti di intelligenza artificiale e i suoi algoritmi per il riconoscimento facciale e per l'eventuale impiego nella sorveglianza di massa. Si ritiene che tali strumenti, attraverso una opportuna e fattibile progettazione, possano diventare elementi chiave di efficace ausilio alle autorità preposte alla pubblica sicurezza, nell'obiettivo del bilanciamento tra diritti, libertà degli individui e sicurezza. A partire da questi elementi progettuali si potrebbe, in prospettiva, ipotizzare un contributo in eventuali linee guida sul riconoscimento facciale e sorveglianza quale ausilio alla pubblica sicurezza, auspicando in una integrazione legislativa nel medio termine.

Si è giunti, anche attraverso queste proposizioni, ad un bagaglio di consapevolezza sistemica su benefici e rischi dell'impiego, anche illegittimo, dell'algoritmo. Tale consapevolezza, ad opinione di chi scrive, è foriera di un contributo propositivo al processo penale. In particolare, si ritiene che gli algoritmi di IA, sia del tipo convenzionale che di quello con caratteristiche predittive, potrebbero efficacemente far parte della fase del processo relativa alla *valutazione* e all'*apprezzamento* del giudice sull'impianto probatorio delineato nel corso delle indagini preliminari. L'ausilio arrecante maggior beneficio dell'algoritmo si ritiene che possa essere fornito nel corso delle attività che caratterizzano tale fase.

Secondo chi scrive, l'algoritmo di IA potrebbe essere di ausilio in tre modi diversi. Un primo contributo che l'algoritmo potrebbe fornire, in particolare, consiste nel corredare il materiale probatorio "tradizionale" con ulteriori e *nuovi* elementi elaborati e suggeriti dall'algoritmo, quindi corroborando il quadro probatorio. Un secondo contributo potrebbe consistere in una valutazione della possibilità che con il quadro probatorio a disposizione si giunga alla pronuncia di assoluzione per mancanza, insufficienza o contraddittorietà della prova, ai sensi dell'articolo 530 comma 2 c.p.p.[603]. Sempre in relazione all'impianto probatorio il terzo contributo potrebbe essere quello di *filtrare*[604]

[600] *supra* Capitolo I § 1; *supra* Capitolo II § 1
[601] *supra* § 1-5
[602] *supra* § 6
[603] articolo 530 co 2 c.p.p, *Sentenza di assoluzione*
[604] CANZIO G., *Intelligenza artificiale, algoritmi e giustizia penale*, in *Sistema Penale*, 2021, 4

ed eliminare quelle prove che non hanno una base scientifica a supporto, come verrà chiarito più avanti.[605] I tre contributi forniti dall'algoritmo potrebbero sia essere utilizzati separatamente oppure congiuntamente presumibilmente giungendo, in quest'ultima ipotesi, ad una maggiore efficacia sistemica della fase processuale nel suo complesso.

Prima di considerare come possa inquadrarsi il risultato di un sistema basato su algoritmi di intelligenza artificiale, è necessario analizzare in maggior dettaglio la sopracitata fase del processo penale in cui tale risultato possa essere impiegato. In quanto segue verranno analizzate queste tre possibilità di impiego dell'algoritmo di IA nella fase centrale del processo penale in cui si raccolgono e acquisiscono le prove, nel rispetto del contraddittorio delle parti, è il dibattimento. Prima dell'udienza dibattimentale, il Giudice dell'Udienza Preliminare (GUP) accerta che le parti si siano costituite ed effettua una valutazione generale del materiale probatorio conseguito attraverso le attività delle indagini preliminari. Quest'ultime sono attività di ricerca e raccolta di informazioni, successive alla acquisizione da parte del pubblico ministero della notizia di reato, effettuate dal medesimo pubblico ministero e dalla polizia giudiziaria.

Per quanto riguarda la prima possibilità, come anticipato, l'algoritmo può integrare le prove a disposizione grazie alle sue prestazioni in termini di velocità sia nell'esecuzione del calcolo dell'output che nell'accesso ad archivi elettronici di dati con estensione cronologica e di contenuti. Come già evidenziato spesso nella trattazione, l'algoritmo potrebbe, tuttavia, commettere errori e in questo si innesta la proposta di impiegare algoritmi capaci di una autovalutazione dei loro errori e, eventualmente, di correggerli migliorando le proprie prestazioni, come descritto in precedenza[606].

Per quanto concerne la seconda possibilità di impiego dell'algoritmo, su tale fase e in merito al ruolo del GUP sono sorti orientamenti giurisprudenziali relativi alla «ragionevole previsione di condanna», ai sensi dell'art. 425 c.p.p.[607], che richiama la *predictive policing*, la quale fornirebbe un ausilio a tale previsione attraverso l'algoritmo predittivo, come già illustrato in precedenza[608]. La susseguente questione, che è stata oggetto di interessanti discussioni, è relativa alla disponibilità di sufficiente materiale probatorio per sostenere l'accusa in dibattimento, quindi, ai fini della valutazione di innocenza o colpevolezza dell'imputato. Uno degli orientamenti ritiene che il GUP non possa valutare approfonditamente il materiale probatorio o dare un giudizio in merito alla colpevolezza dell'imputato. Tale ipotesi viene sostenuta in ragione del fatto che al giudice è inibito il proscioglimento, quando gli elementi di

[605] *infra* § 7.1
[606] *supra* § 6.2
[607] art. 425 co 3 c.p.p. «Il giudice pronuncia sentenza di non luogo a procedere anche quando gli elementi acquisiti non consentono di formulare una ragionevole previsione di condanna»
[608] *supra* Capitolo I § 2, 6.1

prova siano suscettibili di valutazioni alternative, aperte o suscettibili di valutazioni differenti in dibattimento, una volta che vi siano state ulteriori acquisizioni probatorie.[609]

Secondo un altro orientamento, ciò che ci si attende dal giudice dell'udienza preliminare, in sede di valutazione, è che quando vi siano concrete ragioni per ritenere che non si possa giungere ad una prova della colpevolezza dell'imputato nella fase dibattimentale, non rinvii a giudizio. Il GUP dovrebbe quindi valutare l'«effettiva consistenza del materiale probatorio»[610] alla base dell'accusa rivolta all'imputato, considerandola come una *condizione minima necessaria* a legittimare la sottoposizione dell'imputato al processo. In questo secondo caso si innesta la prospettiva di un utile impiego di una valutazione predittiva in merito all'astratto e potenziale esito del processo.

In tal senso, secondo questa linea di pensiero, si potrebbero ottimizzare le risorse e ridurre il carico dibattimentale, permettendo un'ottimizzazione generale del sistema processuale penale.[611] Quest'ottica consentirebbe, quindi, escludere dalla dinamica processuale quelle cause che hanno un impianto probatorio, il quale verosimilmente porterebbe a mostrarne l'insufficienza per la condanna dell'imputato, sulla base del calcolo dell'algoritmo predittivo[612]. Tale esclusione creerebbe, quindi, l'opportunità di convogliare risorse, mezzi, personale e soprattutto attenzione alle cause in cui sia attendibile l'affermazione di una responsabilità penale. Su questa linea di pensiero si colgono gli effetti positivi che tale sistema porterebbe all'imputato, che potrebbe essere considerare, grazie alle valutazioni non vincolanti del proprio difensore, i probabili risvolti di un processo e le sue implicazioni. Il rapporto di trasparenza tra imputato e difensore verrebbe così ad affinarsi e "responsabilizzerebbe", in una modalità da definire, il difensore che non presenti le indicazioni predittive di un esito sfavorevole del processo all'imputato che viene condannato.[613] Le opposizioni a tale prospettiva, quali la rigidità di un sistema così impostato, la possibile limitazione dei diritti dei soggetti offesi dal reato e la decisione del giudice meno "umana", si ritengono superabili in ragione dei vantaggi che comporterebbe nel processo.

7.1. *(Segue):* l'algoritmo come prova scientifica e il "filtro di accesso".

In ragione della "irruzione" della tecnologia e della scienza nell'ambito giuridico, è di rilievo la terza possibilità di impiego dell'algoritmo che prospetta la realizzazione di un «filtro di accesso», che consentirebbe una selezione più rigorosa delle prove

[609] Cass. Pen., sez. II, sent. 5 novembre 2015, n. 46145, CED 265246
[610] Cass. Pen, sez. VI, 30 aprile 2015, n. 33763, CED 264427
[611] PARODI C. – SELLAROLI V., *Sistema penale e intelligenza artificiale:molte speranze e qualche equivoco*, in *Diritto Penale Contemporaneo*, 6/2019, 65
[612] *supra* Capitolo I § 6
[613] PARODI – SELLAROLI, *Sistema penale e intelligenza artificiale*, cit., 66

ammesse al dibattimento, come illustrato dal magistrato Giovanni Canzio.[614] Per analizzare tale prospettiva che, a parere di chi scrive, sembra essere la strada migliore per introdurre nel contraddittorio prove generate dall'utilizzo di sistemi algoritmici o di IA, il punto di partenza è l'inquadramento come prova della «*electronic evidence*».

La nascita di discussioni da parte dei giuristi in merito agli algoritmi può ricondursi alle decisioni delle Corti statunitensi, che evidenziavano l'opacità, la difficile comprensibilità, le distorsioni e la discriminazione a cui tali strumenti potevano condurre. Venne quindi posto l'accento sull'esigenza di bilanciamento con le garanzie del processo nell'ottica di giustizia e attribuzione di responsabilità[615]. In tal senso si ricorda la Carta etica sull'intelligenza artificiale nei sistemi giudiziari e nel loro ambiente"[616] che è intervenuta in tale scenario fornendo delle linee guida[617], tra cui la necessità, già citata e sostenuta da chi scrive, che il giudizio non si fondi esclusivamente sui dati algoritmici, essendo necessaria la presenza del giudice "umano", e che essi possano essere utilizzati come elementi di prova.

L'inquadramento della prova generata attraverso l'algoritmo di un sistema di IA può trovare idonea collocazione, per alcuni, nella categoria della *prova scientifica*, la cui nascita è riconducibile alla sentenza Franzese[618]. Tale categoria contempla l'impiego di una legge scientifica o di una metodica a carattere tecnologico per l'accertamento del fatto e non viene ritenuta diversa da altri tipi di prove. Prima della sentenza citata, la giurisprudenza discuteva a proposito del grado di probabilità che richiede la legge scientifica per essere considerata tale. La sentenza Franzese interviene in merito alla questione, distinguendo tra la probabilità statistica e quella logica. Nel caso della probabilità *statistica* esiste una verifica a livello empirico della frequenza che un data condotta causi un determinato evento. La frequenza, in termini generali, indica quante volte su un determinato numero di prove si verifichi un certo evento. Quando l'evento si verifica in tutte le prove si ha la certezza dal punto di vista probabilistico, mentre quando non si verifica mai si ha l'impossibilità in termini probabilistici. Tuttavia, la probabilità statistica non può essere il criterio valutativo sia della prova che del giudizio in quanto deve essere considerato quale elemento di prova. In tal senso, la probabilità statistica, desunta dalla legge scientifica di copertura, deve essere valutata insieme alle altre prove concernenti il caso concreto al fine di esclude la rilevanza di ulteriori fattori interagenti.[619] Per cui, nonostante possa esserci una bassa probabilità in cui l'evento si verifichi a seguito di una determinata causa, la stessa causa può essere significativa nello stabilire che la sua verifica nel caso concreto abbia determinato l'evento in esame,

[614] CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, cit.
[615] *supra* Capitolo I § 5
[616] CEPEJ, 31ª Riunione plenaria, 3-4 dicembre 2018, Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti connessi, cit., 48
[617] *supra* Capitolo I § 6.1
[618] Cass. Pen., SS. UU., sent. 10 luglio 2002, n. 30328, *Franzese*
[619] OLIVIERO M., *Il ragionevole dubbio nella teoria della decisione*, in *Discrimen – Criminalia*, 2012, 361

con l'esclusione di qualsiasi ulteriore spiegazione alternativa. La sentenza Franzese evidenzia quindi che singolarmente né la probabilità statistica né il convincimento soggettivo del giudice possano essere sufficienti per determinare la causa dell'evento. Pertanto, ciò che è cruciale è il grado di probabilità fornito dalle prove che confermano la verificazione dell'evento dal punto di vista oggettivo[620], unitamente all'approccio del giudice di valutazione delle medesime prove.

È qui che viene in rilievo la distinzione con la probabilità logica. Essa è definita come il processo induttivo nel ragionamento probatorio in grado di confermare l'ipotesi relativa allo specifico fatto da provare e che include una ulteriore verifica. La verifica *aggiuntiva* si fonda sull'intero materiale probatorio disponibile e concerne l'«attendibilità dell'impiego della legge statistica per il singolo evento e [la] persuasiva e razionale credibilità dell'accertamento giudiziale»[621].

Si giunge così, pertanto, alla individuazione del rapporto di causalità tra condotta ed evento in concreto quando, al di là di ogni ragionevole dubbio, la condotta sia stata causa dell'evento e che quindi è ragionevolmente esclusa l'inferenza di alternativi fattori causali che avrebbero potuto determinare l'evento in questione. Il giudice, quindi, dovrà ragionare partendo dal caso concreto, che viene descritto nell'evento, che indentifichi le condotte penalmente rilevanti in linea con una legge scientifica per spiegare il nesso causale, e secondo il suo apprezzamento.

La prova scientifica sopra delineata[622], costituita da elementi forniti dall'algoritmo di IA, essendo una prova come le altre richiede l'apprezzamento da parte del giudice. Tale condizione pone questioni relative alla sua implementazione, alla qualità della decisione del giudice e a come possa essere rispettato il diritto di difesa e il contraddittorio "sulla" prova.[623] Secondo la linea di pensiero sopramenzionata, un filtro di accesso preventivo consentirebbe un contradditorio "per" la prova cosicché si possa escludere l'accesso all'impianto probatorio di informazioni che non siano basate su una legittimata base scientifica e non generare un contraddittorio "sulla" prova, quando ormai le parti si sono costituite in dibattimento e la prova è stata già ammessa ed acquisita. Per poter proteggere i principi di tutela processuali è necessario che nella valutazione della prova vengano rispettate delle linee guida che garantiscano che la prova scientifica, individuata attraverso l'impiego di strumenti di IA, rispetti i diritti fondamentali dell'individuo.

L'origine di tali linee guida si fa risalire alla sentenza Daubert[624] della Corte Suprema americana, considerata il caposaldo in materia di valutazione della prova scientifica. I

---

[620] CAPRIOLI F., *L'accertamento della responsabilità penale "oltre ogni ragionevole dubbio"*, in *Rivista Italiana di Diritto e Procedura Penale*, 2009, 62
[621] Cass. Pen., SS. UU., sent. *Franzese*, 8
[622] *supra* § 7
[623] CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, cit., 4
[624] US Supreme Court, *Daubert v. Merrel Dow Pharmaceuticals*, Inc., 509 U.S. 579, 1993

criteri dell'affidabilità di tale prova sono la sua verificabilità e il tasso di errore conoscibile del metodo impiegato. Inoltre, è richiesta l'accettazione generale da parte degli *esperti* del settore della prova che, con regolarità, essi controllano ai fini dell'accertamento della sua accuratezza. Un ulteriore criterio è la falsicabilità della prova scientifica, che prevede che essa sia stata scientificamente testata. A tali principi si accosta l'affermazione della imprescindibilità di una argomentazione ispirata alla razionalità, che, a parere di chi scrive, è certamente la base di un apprezzamento della prova in un auspicato clima di accettazione della continua innovazione.

In tale quadro si inserisce il contributo della Carta Etica[625] volto ad assicurare che l'ausilio apportabile dall'intelligenza artificiale non pregiudichi le garanzie del giusto processo. In tal senso è necessario il rispetto dei diritti fondamentali garantiti dalla CEDU e dalla Convenzione 108[626] e, nell'ordinamento italiano, dalla Costituzione[627]. In particolare, i diritti garantiti dalla CEDU a un equo processo e al rispetto della vita privata e familiare[628]. Quest'ultimo diritto si innesta nel quadro della privacy e delle difficoltà che sorgono dall'incontro con la tecnologia di IA[629]. Inoltre, tornano imperiosi i requisiti sull'algoritmo di IA, in particolare in termini di neutralità, quindi di non discriminazione e imparzialità, nonché di qualità come attendibilità del risultato. L'algoritmo deve anche rispettare i dettami della sicurezza, della trasparenza e dell'equità che rappresentano, unitamente alle altre caratteristiche, il punto di riferimento per l'integrazione delle tecnologie nell'ordinamento a carattere migliorativo.

I criteri definiti dalla sentenza Daubert sono stati arricchiti dalla sentenza Cozzini[630]della Corte di Cassazione italiana in relazione alla valutazione da parte del giudice. Gli ulteriori criteri da considerare sono relativi alla finalità e al dibattito critico, rigoroso ed estensivo sulla ricerca, nonché alla capacità esplicativa. Inoltre, come già detto nella trattazione, la figura dell'esperto risulta rilevante ai fini di una corretta integrazione della prova scientifica originata dalla IA, purché sia affidabile e indipendente ma anche con un'appropriata e profonda conoscenza delle nuove tecnologie e delle loro potenzialità e dei connessi rischi[631].

A questo punto sono stati delineati gli elementi che dovranno essere verificati dal giudice e che, per alcuni[632], sottolineano la necessità di una maggiore garanzia del

[625] CEPEJ, Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti connessi, cit., 48
[626]Consiglio d'Europa, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, Strasburgo, 28 gennaio 1981, STE 108
[627] Costituzione Italiana, art. 111, *principio del contradditorio*
[628] CEPEJ, Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti connessi, cit., 14
[629] *supra* Capitolo II § 3
[630] Cass. Pen, sez. IV, 17 settembre 2010, n. 43786, *Cozzini*
[631] *supra* Capitolo II § 3
[632] CONTI C., *La prova scientifica alle soglie dei vent'anni dalla sentenza Franzese: vette e vertigini in epoca di pandemia*, in *Sistema Penale*, 2021

diritto alla prova contraria[633], di cui all'articolo 468 c.p.p. comma 4, citando «testimoni, periti e consulenti tecnici non compresi nella propria lista», incluso l'esperto.

Un'ulteriore garanzia è il ragionevole dubbio, di cui sopra, che, ai sensi dell'articolo 533 c.p.p[634], si basa sulle informazioni acquisite nel corso del processo e rappresenta uno dei criteri di valutazione della prova in cui si ipotizza che la probabilità di condanna dell'imputato sia comunque elevata. Per riepilogare, la prova, anche se scientifica, deve rispondere alle garanzie processuali previste per la valutazione della prova ed inoltre, si può sostenere che la prova scientifica introduca un vincolo di razionalità maggiore rispetto al quella "tradizionale".[635]

La finalità che il citato filtro di accesso, anticipato a un contraddittorio "*per*" la prova[636], consentirebbe l'anticipazione della conoscenza delle parti dei metodi che saranno utilizzati per l'accertamento della prova scientifica.

La norma su cui si potrebbe incardinare tale filtro di accesso è, come riportato da Canzio[637] riportando la Relazione al Progetto preliminare del nuovo codice di procedura penale[638], l'articolo 189 c.p.p. ai sensi del quale occorre «evitare eccessive restrizioni ai fini dell'accertamento della verità, tenuto conto del continuo sviluppo tecnologico che estende le frontiere dell'investigazione, senza mettere in pericolo le garanzie difensive».[639] Basarsi su tale articolo assicura, anche, la presenza di un utile e necessaria flessibilità nell'approccio alla prova scientifica.

Su tali basi, il giudice, dopo aver sentito le parti sulle modalità di assunzione della prova, la ammette con ordinanza fissando sia le modalità per la corretta applicazione dei metodi e delle relative procedure tecniche dell'acquisizione della medesima prova.

Oltre a quanto esposto, va considerato, nonostante le varie perplessità e criticità descritte in precedenza[640], l'impiego dell'algoritmo con l'approccio *evidence-based* volto alla valutazione della pericolosità dell'imputato si ritorna al problema della qualità dei dati utilizzati e la necessità che la decisione, che ha un impatto dirompente nella vita del soggetto, sia comunque centrale il ruolo dell'operatore umano[641].

---

[633] *prova contraria* ha ad oggetto l'inesistenza del fatto che la controparte intende provare

[634] Art. 533 c.p.p. «Il giudice pronuncia sentenza di condanna se l'imputato risulta colpevole del reato contestatogli al di là di ogni ragionevole dubbio»

[635] BARTOLI R., *Diritto penale e prova scientifica*, in *Diritto Penale Contemporaneo*, 2018

[636] CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, cit., 4

[637] CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, cit., 5

[638] Ministerio di Grazia e Giustizia, *Relazione al progetto preliminare del codice di procedura penale*, 1989, 60

[639] articolo 189 c.p.p., *Prove non disciplinate dalla legge* «Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova».

[640] *supra* Capitolo I § 6.1

[641] *supra* § 6.1

8. Conclusioni.

La tesi ha affrontato il tema del complicato equilibrio tra diritti e sicurezza rispetto all'impiego dell'intelligenza artificiale e, in particolare, degli algoritmi di riconoscimento facciale e della delicata questione della sorveglianza di massa. La ricerca di soluzioni idonee ad assicurare un simile bilanciamento si è rivelata complessa, alla luce della autonomia che caratterizza gli algoritmi ad apprendimento automatico.

Un algoritmo che identifica le persone attraverso il riconoscimento biometrico del volto necessita di livelli di affidabilità e accuratezza adeguati, considerando le conseguenze sull'interessato in caso di errori nell'ambito del processo penale. Ma è anche necessario che l'algoritmo sia "onesto", senza pregiudizi ed etico perché le azioni su esso basate non siano affette dagli stessi difetti. Difetti che l'algoritmo può solo ereditare dal modo e dalle persone da cui è stato programmato e dal tipo di dati su cu è stato addestrato e da cui dipende la sua evoluzione. Quindi se i dati sono viziati da *bias*, l'algoritmo non potrà che restituire *outcome* del pari contaminati. Ne consegue che, al fine di garantire un corretto utilizzo dei sistemi in questione, occorre innanzi tutto che gli utilizzatori adottino tutte le cautele necessarie per evitare simili effetti distorsivi.

Tali dettami sarebbero auspicabili in ogni dominio applicativo dell'algoritmo, ma nel delicato settore dei reati e del processo penale assurgono a requisiti irrinunciabili. La consapevolezza del rischio associato all'impiego del riconoscimento facciale basato su intelligenza artificiale deve essere nota sia a livello qualitativo che quantitativo a chi impiega questa risorsa. Il rischio quantificato consente scelte mirate e consapevoli, quindi con impatto negativo contenuto e, qualora esso sia presente, valutato come accettabile nella specifica circostanza.

L'approfondimento di come il riconoscimento facciale e la sorveglianza di massa siano accettate, impiegate, più o meno diffusamente, e normate, in altre parti del mondo fuori dall'Unione europea, è stato cruciale per soppesare il rischio operativo e gli abusi perpetrati o potenzialmente perpetrabili con questa tecnologia. Si è dedicato spazio al "modello" cinese che assurge a caso esemplificativo dei rischi e degli aspetti negativi collegati all'impiego del riconoscimento facciale basato su intelligenza artificiale. Abbiamo invero ampiamente illustrato l'ampia diffusione di tale tecnologia nelle città della Cina, il conseguente controllo della popolazione nonché le contraddizioni e gli abusi nel suo utilizzo. Ne è emerso un quadro allarmante, tuttavia proprio questa loro caratteristica li ha resi uno stimolo per giungere in modo ancora più consapevole agli aspetti propositivi della presente ricerca.

Si ritiene che nelle attività di pubblica sicurezza e nel processo penale l'operatore umano non sia sostituibile, anche se può trarre un valido ausilio dai sistemi di intelligenza artificiale. Sono stati presentati possibili scenari operativi, dove il tema della responsabilità e dell'autoria è centrale. Sono stati anche individuati elementi di

progettualità per i dati personali associati alla rilevazione dell'algoritmo, per migliorare il tema del bilanciamento tra diritti e sicurezza, che potrebbero tradursi in raccomandazioni se non, in prospettiva, in elementi integrativi della normativa vigente. Ulteriori aspetti di rilevo concernono il ruolo dell'algoritmo in termini di apprezzamento della prova; sul punto si è visto come la formazione degli operatori e la presenza di esperti di ausilio alle attività di pubblica sicurezza e nei tribunali siano cruciali per aumentare l'efficacia dell'impiego degli algoritmi.

L'essere umano è centrale sia nello sviluppo della intelligenza artificiale che nel suo impiego. Impiegare in modo diffuso ed efficace gli algoritmi e il rilevamento facciale, senza compromettere il bilanciamento tra diritti e sicurezza, è complicato ma è possibile. Considerare l'intelligenza artificiale come strumento di ausilio per la pubblica sicurezza, come parte dell'impianto probatorio nel processo penale, come strumenti per la profilazione del reo, non significa mettere da parte le autorità a ciò preposte, bensì conferirgli uno *tool* di supporto per assurgere a livelli di garanzia dell'imputato ancora maggiori; purché naturalmente i moderni sistemi rispettino talune condizioni.

In tal modo, il processo potrebbe beneficiare dei vantaggi delle nuove tecnologie e, in particolare, delle straordinarie capacità di analisi degli algoritmi, come nel caso dell'apprezzamento della prova. Gli esempi negativi in tali ambiti applicativi dello scenario penale sono un impegnativo ma utile punto di partenza per sviluppare un approccio sistemico all'impiego della intelligenza artificiale, robusto ma flessibile e resiliente agli errori non solo dell'algoritmo ma, se non soprattutto, a quello della "componente umana".

BIBLIOGRAFIA

116th Congress (2019-2020): *Commercial Facial Recognition Privacy Act,* 14 marzo 2019, S.847, Congress.gov, Library of Congress.

117th Congress, *American Data Privacy and Protection Act*, H.R.8152, 2022.

ABATE A.F. – NAPPI M. – RICCIO D. – SABATINO G.*, 2D and 3D face recognition: A survey*, in *Elsevier Pattern Recognition Letters*, 28, 2007, 1885–1906.

ABDERRAHMANE N. – LEMAIRE E. – MIRAMOND B., *Design Space Exploration of Hardware Spiking Neurons for Embedded Artificial Intelligence*, in *Elsevier*, vol. 121, 366 e ss., 2020.

ACLU of Vermont, *Enactment of s.124, the nation's strongest statewide ban on law enforcement use of facial recognition technology*, in *ACLU of Vermont*, 2020.

ADRIAN J., *Informational Inequality: How High Frequency Traders Use Premier Access To Information To Prey On Institutional Investors*, in *Duke Law & Technology Review*, 2016, 14, 256-279.

AGATA C. – MANGIAMELI A Algortimi e big data. Dalla carta sulla robotica in *Riv. fil. dir.*, 2019, 107, 124.

AgID, *Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino*, 2018, 8, 38.

ALETTI B., in *Enciclopedia Treccani della Scienza e della Tecnica*, 2008.

ALÙ A., *Sorveglianza di massa: così la Cina attua il suo modello "orwelliano"*, in *Agenda Digitale*, 2022.

ALVERONE G., *La DPIA sui trattamenti per finalità di polizia e di giustizia penale*, in *Diritto.it*, 2022.

AMBESI A. – CICCARELLI M., *GDPR e cifratura: concetti base e approcci pratici*, in *ICT Security Magazine*, 2019.

AMIDEI, *Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo*, in RUFFOLO (a cura di) *Intelligenza artificiale e responsabilità*, 2017, 92.

AMISANO M., *Prevedere -e non predire- attraverso gli algoritmi e le loro insidie*, in *Archivio penale*, 2022, 2, 3.

Amnesty International, *Ban The Scan Hyderabad*, in *Ban The Scan*, 2022.

Amnesty International, *Rapporto annuale del 2021 - 2022 sulla Cina*, 2022.

Amnesty International, *Why we're taking the UK government to court over mass spying*, in *Amnesty International UK/Mass surveillance*, 2020.

AMOROSO D. – TAMBURRINI G., *I sistemi robotici ad autonomia crescente tra etica e diritto: quale ruolo per il controllore umano*, in *Rivista di BioDiritto*, 2019, 51.

ANDOLINA E., *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della privacy e onde eversive*, in *Archivio Penale*, 2015, fascicolo 3, 916.

ANDORNINO B. G. (a cura di), *La Cina: sviluppi interni, proiezione esterna*, in *Torino World Affairs Institute*, 2020, 59, 60, 67, 69, 72, 79.

ASIMOV I., *Runaround*, *in Astounding Science Fiction*, 1942.

BANSAL V., *The Hyderabad model of CCTV surveillance*, in *Livemint*, 2020.

BARMANN B., *Intelligenza artificiale e law enforcement*, in *Istituto di Ricerche sulla Pubblica Amministrazione*, 2020.

BARRETT L., *Reasonably Suspicious Algorithms: Predictive Policing at the United States Border*, in *N.Y.U. Review of Law & Social Change*, 2017, 41 (3).

BARTOLI R., *Diritto penale e prova scientifica*, in *Diritto Penale Contemporaneo*, 2018.

BASILE F., *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine* in *Diritto Penale e Uomo*, 2019, 4, 16-18, 26, 31, 32.

BASSINI M. – L. LIGUORI L – O. POLLICINO O., *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in PIZZETTI F.(a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 356.

BELFI M., *PIPL, cosa dice la Legge privacy i Cina: ecco le regole per adeguarsi*, in *Cybersecurity 360*, 2021.

Belt and Road Forum for International Cooperation, Beijing, May 14 -15, 2017.

BERTOLESI R., *Intelligenza artificiale e responsabilità penale per danno da prodotto*, Tesi dottorato Diritto Penale, Milano, 2019, 236.

Big Brother Watch Team, *Big Brother Watch Files Legal Complaint Against Co-Op's "Orwellian" Facial Recognition,* in *Big Brother Watch*, 2022.

BOCACCINI P. – PRELATI S., *Trasferimenti internazionali di dati: le nuove disposizioni cinesi sulle clausole contrattuali standard*, in *Cybersecurity 360*, 2022.

BOLDRINI N., *Reti neurali: cosa sono e a cosa servono*, in *AI4business*, 2022.

BONOMI S., *Personal Information Protection Law (PIPL): la Cina approva la prima legge in materia di data protection*", in *CyberLaws*, 2021.

BONTA J. – ANDREWS D.A., *Risk-Need-Responsivity. Model for Offender Assessment and Rehabilitation*, in *Public Safety Canada*, 2007.

BUOLAMWINI J, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in *Proceedings of Machine Learning Research,* 81 (Conference on Fairness, Accountability, and Transparency), 2018, 1, 6.

BURGIO E. – DE SIMONE L., *Intelligenza Artificiale e responsabilità civile*, in MediaLaws, 2021.

BURRELL J., *How the machine "thinks": Understanding opacity in machine learning algorithms*, in *Big Data & Society*, 2016, 3, 3.

CALDERINI B., *Sorveglianza di massa, la Cina è un sistema a "diritti affievoliti": perché lo tolleriamo e cosa rischiamo*, in *Agenda Digitale*, 2022.

California State, *The California Privacy Rights Act (CPRA)*, 2020.

CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale*, in *Sistema Penale*, 2021, 4, 5.

CAPPELLINI A., *Machina delinquere non potest?*, in *Discrimen*, 2019, 14-15, 18.

CAPRIOLI F., *L'accertamento della responsabilità penale "oltre ogni ragionevole dubbio"*, in *Rivista Italiana di Diritto e Procedura Penale*, 2009, 62.

CARBONI K., *La nuova frontiera del controllo in Cina è il riconoscimento delle emozioni*, in *Security*, 2021.

CARBONI K., *Come è andata a finire la prima causa sul riconoscimento facciale in Cina*, in *Wired*, 2021.

Carta dei diritti fondamentali dell'Unione europea (CDFUE o Carta di Nizza), 18 dicembre 2000, C 364/01.

Cass. Pen., sez. II, Sent. 5 novembre 2015, n. 46145, CED 265246.

Cass. Pen, sez. IV, 17 settembre 2010, n. 43786, *Cozzini*.

Cass. Pen, sez. VI, 30 aprile 2015, n. 33763, CED 264427.

Cass. Pen., SS. UU., Sent. 10 luglio 2002, n. 30328, *Franzese*, 8.

CATANIA P. – ALLEN C., *Facial recognition technology: a model law*, in *Corrs Chambers Westgarth*, 2022.

CEE, *Direttiva del Consiglio relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri in materia di responsabilità per danno da prodotti difettosi*, 25 luglio, n. 85/374/CEE, 1985.

CEPEJ, 31ª Riunione plenaria, 3-4 dicembre 2018, *Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti connessi*, CEPEJ (2018)14, 48.

Chinese Courts and Internet Judiciary, *Chinese Courts and the Internet Judiciary*, December 2019.

CGUE, Grande Sez., sent. 8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, The Attorney General*, causa (C-293/12).

CGUE, Grande Sez., sent. 16 luglio 2020, *Data Protection Commissioner c. Facebook Ireland Ltd, Maximillian Schrems,*, causa C-311/18.

CGUE, Grande Sez., sent. 6 ottobre 2020, *État luxembourgeois c. B*, causa C-254/19.

CGUE, Grande sez., sent. 6 ottobre 2020, *La Quadrature du Net c. Premier ministre e a.*, causa C-511/18 e C-512/18.

CGUE, Grande Sez., sent. 2 marzo 2021, *H.K. c. Prokuratuur*, causa C-746/18.

CGUE, Grande Sez., sent. 12 maggio 2021, *Bundesamt für Fremdenwesen und Asyl*, C-505/19.

CGUE, Prima Sezione, sent. 24 marzo 2022, *X, Z c Autoriteit persoonsgegevens*, Paesi Bassi, C-245/20.

Codice del consumo, d.lgs. 6 settembre 2005, n. 206.

Codice della Privacy, *Codice in materia di protezione dei dati personali,* d.lgs. 30 giugno 2003 n. 196, con le modifiche apportate da d-l 8 ottobre 2021, n. 139 convertito da l. 205/2021 e dal d-l 30 settembre 2021, n. 132 convertito da l. 178/2021.

COLACURCI M., *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema Penale*, 13-14.

Commissione Europea, Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni - L'intelligenza artificiale per l'Europa, COM (2018) 237 final.

Commissione Europea - Proposta di Regolamento del Parlamento Europeo e del Consiglio, "*che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione"*, 206 final, 2021/0106 (COD).

Commissione Europea, 206 final, 2021/0106 (COD), Relazione, (71), 4.

Commissione Europea, *Il pacchetto Digital Services Act*, in *Sito Ufficiale dell'Unione Europea,* 2023.

Consiglio d'Europa, *Adesione dell'Unione europea alla Convenzione europea dei diritti dell'uomo – Domande e risposte*, in *sito Consiglio d'Europa*, 2023.

Consiglio d'Europa, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, Strasburgo, 28 gennaio 1981, STE 108.

Consiglio Europeo - Riunione speciale del Consiglio europeo, Conclusioni EUCO 13/20, 2020.

Consiglio dell'Unione europea, *Conclusioni del Consiglio dell'Unione europea sulla conservazione dei dati per finalità di lotta contro la criminalità*, 27 maggio 2019, 9663/19.

Constitution of India, 1949.

CONSULICH F., *Il nastro di Mobius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, 2007, 203, 204, 206, 232.

CONTI C., *La prova scientifica alle soglie dei vent'anni dalla sentenza Franzese: vette e vertigini in epoca di pandemia*, in *Sistema Penale*, 2021.

Corte EDU, Grande Sez., sent. 4 dicembre 2008, S. and Marper v. United Kingdom, ric. n. 30562/04 and 30566/04).

Corte EDU, Grande Sez., sent. 25 maggio 2021, Big Brother Watch and others c. The *United Kingdom,* ric. n. 58170/13, 62322/14, 24960/15, 301/92, 323/98.

Corte EDU, sez. I, sent. 24 maggio 2016, *Biao c. Danimarca*, ric. n. 38590/10, 103.

Costituzione Italiana, 1948.

D'AGOSTINO L., *Sorveglianza di massa, algoritmi e intelligenza artificiale: lo stato dell'arte al livello nazionale ed europeo*, in *Relazione al Seminario "Stati Generali del Diritto di Internet"*, 2021, 1, 3.

D'AGOSTINO L., *Gli algoritmi predittivi per la commisurazione della pena*, in *Diritto Penale Contemporaneo*, 2019, 2, 354. 358, 359, 365.

DAVIS N., PERRY L., SANTOW E., *Facial recognition technology: Towards a model law*, in *Human Technology Institute, The University of Technology Sydney*, 2022.

DE LUCIA A., *Intelligenza artificiale e processo tributario: l'algoritmo "studia" un milione di sentenze*, in *Altalex*, 2022.

DE SIMONE G., *La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi) d'imputazione*, in *Diritto Penale Contemporaneo*, 2010, 1, 3.

D.l. del 30 settembre 2021 n. 132, convertito in l. 23 novembre 2021, n. 178, *misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP*.

DEL PIZZO A., *Privacy by design: il ponte tra diritto e tecnica nella tutela dei dati personali*, in *Cammino Diritto*, 2020, 7, 18.

Digital Markets Act (DMA), proposto dalla Commissione nel dicembre 2020, accordo politico il 25 marzo 2022.

Digital Services Act (DSA), proposto dalla Commissione nel dicembre 2020, accordo politico il 23 aprile 2022.

DIMOCK S., *Actio libera in causa*, in *Crini. Law and Philos.*, 2013, 7, 550.

Direttiva 2014/65/UE, *Market in financial instruments directive* (MiFID II), del 15 maggio 2014, art. 48, *Resilienza dei sistemi, interruttori di circuito e negoziazione elettronica*.

D.lgs. 14 marzo 2013, n. 33, *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*.

ECO U., *Apocalittici e integrati. Comunicazioni di massa e teorie della cultura di massa,* Milano, 1964.

European Lawyers Foundation, *Guide on use of Artificial Intelligence-based tools by lawyers and law firms in the EU*, 2022.

FABBRI F., *"IA, quest'anno nel mondo saranno monitorati da remoto 75 milioni di pazienti"*, in *Key4biz*, 2023.

FEINER L. – PALMER A., *Rules around facial recognition and policing remain blurry*, in *CNBC*, 2021.

FERGUSON A., *Policing Predictive Policing*, in *Washington University Law Review*, 2017, 1148.

FINOCCHIARO G., *Riflessione su intelligenza artificiale e protezione dei dati personali* in RUFFOLO (a cura di) *Intelligenza artificiale e responsabilità*, 2017, 237.

FLACKS M. – SONGY M., *The Uyghur Forced Labor Prevention Act Goes into Effect*, in *Center for International Foreign Studies*, 2022.

FONSEKA T. M. - BHAT V. - KENNEDY S. H., *The utility of artificial intelligence in suicide risk prediction and the management of suicidal behaviours*, in *Sage*, 2019, 53 (10).

FREEMAN K., *Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in State v. Loomis*, in North Carolina Journal of Law & Technology, 2016, 18, 65, 98.

FUSSELL S., *The NYPD Had a Secret Fund for Surveillance Tools*, in *Wired,* 2021.

GALGANI B., *Giudizio penale, habeas data e garanzie fondamentali*, in *Archivio Penale,* 2019, 3, 7-9, 23.

Garante per la protezione dei dati personali, *Organigramma*, in *GPDP*, 2021.

GARITO E., *Dall'algoritmo egoista all'algoritmo responsabile (e forse anche generoso)*, in *Econopoly*, 2022, 2.

GAROFALO L., *Riconoscimento facciale. Il branco di Milano identificato con il software 'Sari'*, in *key4biz*, 2022.

GHIGLIA A., componente del Garante per la protezione dei dati personali, in *Invervista di Coccorese P., È sottile il confine tra la sicurezza e la sorveglianza di massa*, in *GPDP*, 2021.

GIALUZ M., *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *Diritto Penale Contemporaneo*, 2019, 7.

GPDP, *Convegno "la protezione dei dati: da 25 anni la bussola del futuro". I quattro componenti dell'Autorità intervistati su AI, sanità digitale, sorveglianza di massa,* in *Metaverso,* 2022.

GPDP, *Regolamento 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali*, 2000.

GRANDE E., "*La condanna di Derek Chauvin per la morte di George Floyd: giustizia è fatta*", Questione Giustizia, 2021.

GROTHER P., NGAN M., HANAOKA K., *Face Recognition Vendor Test (FVRT). Part 3: Demographic Effects*, NISTIR 8280, 2019.

Gruppo di lavoro "Articolo 29" per la protezione dei dati, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, in *European Commission Guidelines*, 2018, 8.

HALLEVY G., *Liability for Crimes Involving Artificial Intelligence Systems* in *Springer International Publishing AG*, 2014, 41.

HALLEVY G., *The Basic Models of Criminal Liability of AI Systems and Outer Circles*, in *Elsevier* SSRN, 2019, 1, 4, 8.

Hangzhou Fuyang District Court, *Bing Guo v Hangzhou Safari Park*, Zhejiang 0111, Civil No. 6971, 20 November 2020.

HANNACHI A.*, Patterns identification and Data mining in weather and climate*, in *Springer*, 2021.

HASSAN T., *A New Model for Global Leadership on Human Rights*, in *Human Right Watch World Report*, 2023, 6, 9, 71, 80.

HERSEY F., *China to have 626 million surveillance cameras within 3 years*, in *TechNode*, 2017.

High Court of Justice, Queen's Bench Division, Divisional Court, September 4, 2019, Judgment *R (Bridges) v. CCSWP e SSHD*, Case n. CO/4085/2018.

High-Level Expert Group on Artificial Intelligence, *Ethic guidelines for trustworthy AI*, 2019.

HOSSAIN M.S. – MUHAMMAD G. – GUIZANI N., *Explainable AI and Mass Surveillance System-Based Healthcare Framework to Combat COVID-19 Like Pandemics*, in *IEEE Network*, 2020, 128, 129.

HUQ A.Z., *Racial Equity in Algorithmic Criminal Justice*, in *Duke Law Journal*, 2019, 1076.

Illinois, *Biometric Information Privacy Act (BIPA)*, 740 ILCS 14/1 et seq. (West 2016), 2008.

Illinois Supreme Court, Judgment *Rosenbach v. Six Flags Entertainment Corp.*, 2018, docket n. 123186.

JACOBS P. – PATTERN T., *Natural language processing*, in IEEE Expert, 1994, 9, 1, 35.

JAKUBOWSKA E., *Ban Biometric Mass Surveillance A set of fundamental rights demands for the European Commission and EU Member States*" in *European Digital Rights (EDRI)*, 2020, 10.

KAPLAN J., *Intelligenza artificiale. Guida al futuro prossimo* in *Luiss University Press*, II, 2018, 126.

KETH D. – PRISCILLA G. – KESSLER S., *Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing,* in *Responsive Communities Initiative*, *Berkman Klein Center for Internet & Society*, 2017, 16.

KLEIBERG J. – LAKKARAJU H. – LESKOVEC J.et al., *Human Decision and Machine Predictions*, in *The Quarterly Journal of Economics*, 2018, 237.

KNOX L., *NYPD, told it can't use "Glomar" denial, now claims it has no records on Millions March cell phone surveillance* in *Muckrock,* 2019.

KOLEKAR S. – GITE S. – PRADHAN B., *Behavior Prediction of Traffic Actors for Intelligent Vehicle Using Artificial Intelligence Techniques: A Review*, in *IEEE Access*, 2021, 9, 1, 35.

KOLODNER J. L., *An Introduction to Case-Based Reasoning*, in *Artificial Intelligence Review*, 1992, 4.

L. 31 dicembre 1996, n. 675. *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*.

LAVORGNA A. – SUFFIA G., *La nuova proposta europea per regolamentare i Sistemi di* Intelligenza, 92-94, 97-99.

Law Commission of India, *The Identification of Prisoners Act*, 9 settembre 1920, act n. 33, in *Indian Kanoon*.

LECHER C., *Shareholders are pushing Amazon to stop selling its facial recognition tool*, in *theverge*, 2019.

LEPRINCE-RINGUET D., *Facial recognition tech is supporting mass surveillance. It's time for a ban, say privacy campaigners*, in *ZDNET*, 2021, 2.

LEVY A., *Microsoft says it won't sell facial recognition software to police until there's a national law 'grounded in human rights'*, in *CNBC,* 2020.

LI X., MU X., LI S., PENG H., *A Review of Face Recognition Technology* in IEEE Access, 8, 2020, 139113.

LIU T. – YANG B. – GENG Y. – DU S., *Research on Face Recognition and Privacy in China—Based on Social Cognition and Cultural Psychology*, in Frontiers in Psychology, 12, 2021, 1, 3, 5, 10.

LIVELLI F.M.R., *La Ue sceglie un approccio basato sul rischio per regolare l'intelligenza artificiale*, in *Network digital 360 – Risk-managment*, 2021.

LIVIO M., *Il Regolamento europeo sulla intelligenza* artificiale, in *Altalex*, 2022.

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

LOVERGINE S., *Breve disamina degli algoritmi di intelligenza artificiale. Aspetti tecnologici e metodologici*, Rapporto dell'Istituto Nazionale per Analisi Politiche Pubbliche (INAPP), 2022, 7, 8.

MAESTRI E., *Giustizia digitale Tecnologia giudiziaria e accesso alla giustizia nell'era della digitalizzazione*, in *Archivio Penale*, 2020.

MAGRO M.B., *A.I.: la responsabilità penale per la progettazione, la costruzione e l'uso dei robot*, in *Altalex*, 2018.

MAGRO M. B., *Robot, cyborg e intelligenze artificiali* in CAPODOPPI A. – CANESTRARI S. et al., *Trattato di diritto penale - Cybercrime*, Milano, 2019, 1207.

Maine House and Senate, *An Act to Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials*, 2021.

MARAS M. H., *The social consequences of a mass surveillance measure: What happens when we become the 'others'?*, in *Elsevier International Journal of Law, Crime and Justice*, 40, 2012, 66.

MARIA M., *Riconoscimento facciale: che cos'è e perché rivoluzionerà gli smartphone*, in Network Digital 360, 2022.

MARMO R., *Algoritmi per l'intelligenza artificiale*, Milano, 2020, 8.

MARTORANA M. – PINELLI L., *Data retention, impatto critico sui procedimenti già aperti*, in *Altalex,* 2021.

MASCELLINO A., *Researchers pitch model law for facial recognition to Australian government*, in *Biometric*, 2022.

Massachusetts, *Facial and Other Remote Biometric Recognition*, 2021.

MASSI S., *Affidamento sull'intelligenza artificiale e "disimpegno morale" nella definizione dei presupposti della responsabilità penale* in GIORDANO R. et al. (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Milano, 677, 678.

MASSI S., *A.I.: la responsabilità penale per la progettazione, la costruzione e l'uso dei robot*, in *Altalex - Ip, It e Data* Protection, 2018.

MAUGERI A.M*., L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra evidence based practices e tutela dei diritti fondamentali, in Archivio Penale*, 2021, 1, 13, 14.

MAURO G., *L'intelligenza artificiale sta per essere regolamentata*, in *Econopoly*, 2021.

MELONI C., *Droni armati in Italia e in Europa: problemi e prospettive*, in *Diritto Penale Contemporaneo*, 2017, 1.

MCCARTHY J., "*What Is Artificial Intelligence*", Standford, 2007.

MILANO L., *Il Regolamento europeo sull'intelligenza artificiale*, in *Altalex*, 2022.

MINELLI C., *La responsabilità "penale" tra persona fisica e corporation alla luce della Proposta di Regolamento sull'Intelligenza Artificiale*, in *Diritto Penale Contemporaneo*, 2022, 50-53, 59.

Ministero della Giustizia*, XVIII LEG – Schema di D.Lgs. – Attuazione della direttiva (UE) 2016/680/UE protezione delle persone fisiche con riguardo al trattamento dei dati personali,* Relazione di accompagnamento, 23.

Ministerio di Grazia e Giustizia, *Relazione al progetto preliminare del codice di procedura penale*, 1989, 60.

Ministry of electronics and information technology, *The Digital Personal Data Protection Bill*, 2022.

Ministry Of Law, Justice and Company Affairs (Legislative Department), *Information Technology Act*, n. 2, DL-33004/2000.

MONTAG L. et al, *The rise and rise of biometric mass surveillance in the EU - Legal analysis of biometric mass surveillance practices in Germany, the Netherlands, and Poland*, in *European Digital Rights (EDRI)*, 2021, 10.

MULLER C. (relatrice), *Parere del Comitato economico e sociale europeo (CESE) sulla proposta di Regolamento*, 2021, C 517/62, 65.

NAJIBI A., *Racial Discrimination in Face Recognition Technology*, in *Harward University- SITN*, 2020.

National Crime Records Bureau (NCRB), in *ncrb.gov*, 2020.

National Crime Records Bureau*, Request For Proposal To procure Automated Facial Recognition System*, 02/001, 2018.

NINO M., *La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE* in *Il diritto dell'unione europea*, 2021, 1, 93-124.

OHRI N., *India lets banks use face recognition, iris scan for some transactions - sources*, in *Reuters,* 2023.

OLIVIERO M., *Il ragionevole dubbio nella teoria della decisione*, in *Discrimen – Criminalia*, 2012, 361.

Organisation for Economic Co-Operation and Development, *National Innovation Systems*, ai sensi Convention of Paris against Discrimination in Education, December 14, 1960.

PAGALLO U., *Etica e diritto dell'Intelligenza Artificiale nella governance del digitale: il Middle-out Approach* in RUFFOLO (a cura di) *Intelligenza artificiale e responsabilità*, 2017, 31.

PANCHANKIS Y, *Mass Surveillance, Behavioral Control, and Psychological Coercion The Moral Ethical Risks in Commercial Devices*, in *AIRCC Publishing Corporation*, 2022, 151.

PAREKH D. – PODDAR N. – RAJPURKAR A. – CHAHAL M. – KUMAR N. – JOSHI G.P. – CHO W., *A Review on Autonomous Vehicles: Progress, Methods and Challenges*, in *Electronics*, 2022, 11 (14), 2162.

PARODI C. – SELLAROLI V., *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto Penale Contemporaneo*, 6/2019, 65*,* 66.

Parlamento Europeo, *Che cos'è l'intelligenza artificiale e come viene usata*, in *Sito web ufficiale del Parlamento Europeo,* 2020.

Parlamento Europeo, Risoluzione del 16 febbraio 2017 recante *raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, P8 TA(2017)0051, C 252/242, 249.

Parlamento europeo, Risoluzione del 19 dicembre 2019 sulla *situazione degli uiguri in Cina («China Cables»)*, (2019/2945(RSP)), C 255.

Parlamento Europeo e Consiglio, Direttiva CE, 8 giugno 2000, n. 31, *relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno*, «Direttiva sul commercio elettronico».

Parlamento europeo e Consiglio, Direttiva del 12 luglio 2002, n. 58, *relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)*.

Parlamento Europeo e Consiglio, Direttiva del 27 aprile 2016 n. 680, *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*.

Parlamento Europeo e Consiglio, Direttiva del 27 aprile 2016, n. 681*, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi*.

Parlamento Europeo e Consiglio, Direttiva del 24 ottobre 1995, 95/46/CE, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, n. l. 281 (attualmente non in vigore).

PASCERI G. – BIBBOLINO C. – STASI M. – COPPOLA F. et al., *Intelligenza artificiale e radiologia*, in *Sirm*, 7.

PAULESU P.P., *Intelligenza artificiale e giustizia penale. Una lettura attraverso i principi*, in *Archivio Penale*, 2022, 21, 22.

PEASLEE E., *Massachusetts Pioneers Rules For Police Use Of Facial Recognition Tech*, in *NPR*, 2021.

PECORA L. – STAGLIANÒ G., (curatore LEANTE M.), *Massimario 1997-2001. I principi affermati dal Garante nei primi cinque anni di attività*, 2004, 23.

People's Republic of China, Constitution, December 4, 1982, artt. 51, 53, 54.

People's Republic of China, Cybsersecurity Law, November 7, 2016.

People's Republic of China, Data Security Law of the, June 10, 2021.

People's Republic of China, Personal Information Protection Law, August 20, 2021.

PESCE G., *Sul rapporto tra atto del privato inserito sulla piattaforma tecnologica "sicura ed irretrattabile" (blockchain) e atto pubblico. Riflessi sul procedimento e sul processo* in *Judicium*, 2021, 1.

PIERGALLINI C., *Il paradigma della colpa nell'età del rischio: prove di resistenza del tipo*, in *Rivista italiana di diritto e procedura penale*, 2005, 1684.

PIERGALLINI C., *Intelligenza artificiale: da mezzo a autore del reato?*, in *Rivista italiana di diritto e procedura penale*, 2020, 4, 1767.

PIVA D., *Machina discere, (deinde) delinquere et puniri potest*, in Giordano R. (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia,* Milano, 2022, 7, 683, 684.

PIVA D., *Spunti per una riscoperta della colpa per assunzione*, in BONDI A. – FIANDACA G. et al. (a cura di), *Studi in onore di Lucio Monaco*, Urbino, 1139.

PIZZETTI F. (a cura di), *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in PIZZETTI F. (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, 39.

POSPIELOV S., *Top 10 AI Development and Implementation Challenges*, in *Spiceworks*, 2022.

Press Trust of India, *Delhi police facial recognition software has only 2 per cent accuracy: HC told*, in *Business Standard*, 2018.

PTI News Agency, *Facial recognition technology introduced at 3 airports in India under Digi Yatra initiative*, in *The Indian Express*, 2022.

RAJENDRAN L., SHANKARAN R. S., *Bigdata Enabled Realtime Crowd Surveillance Using Artificial Intelligence and Deep Learning*, in *IEEE International Conference on Big Data and Smart Computing (BigComp)*, 2021.

Regio Decreto, 18 giugno 1931, n. 773, *Approvazione del testo unico delle leggi sulla pubblica* sicurezza, (TULPS), art. 1.

Regolamento (UE) 2016/679, *General Data Protection Regulation* (GDPR), agli art. 13, *Dati personali raccolti presso l'interessato: informazioni da fornire*, art. 15, *Diritto di accesso dell'interessato*.

Regolamento (UE) del 23 ottobre 2018, n.1725, sulla *tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati,* che ha abrogato Regolamento (CE) n. 45/2001.

RESTA F., *La Direttiva sulla protezione dei dati personali in ambito giudiziario penale e di polizia e la tutela dei terzi* in CIRIELLO A. – GRASSO G. (a cura di), *Il trattamento dei dati personali in ambito giudiziario,* 2021, 41.

RICCIO G., *Ragionando sulla intelligenza artificiale e il processo penale* in *Archivio Penale*, 2019, 11.

RICHARDS N. M., *The Dangers of Surveillance*, in *Harward Law Review*, 2013, 1937, 1964.

Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, P8 TA(2017)0051, C 252/242, AB, 53, 54, 56.

ROBERTS L.A. – RICHARDSON B. ET AL., *General Perspectives Toward the Impact of AI on Race and Society*, in *Social Justice and Education in the 21st Century*, 2021, 347-363.

ROSSI DAL POZZO F., *Alcune riflessioni a margine della nuova disciplina in materia di protezione dei dati personali di cui al Regolamento (UE) 2016/679/UE* in *Eurojust*, 2018, 17, 19.

RUFFOLO U. (a cura di), *Intelligenza artificiale e responsabilità*, Milano, 2017, 22, 25, 28, 87.

RUFFOLO U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, 130.

RUSSELL J. - NORVIG P., "*Artificial Intelligence. A Modern Approach*", New Jersey, 2010, 5, 6.

SACCHETTO E., *face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, in *Giustizia penale e nuove tecnologie*, 2020.

SALVADORI I., *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Rivista italiana di diritto e procedura penale*, 2021, 64, 1, 85.

SARKER I., *AI-Based modelling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems*, in SN Computer Science, 2022.

SARKER I., *AI Watch. European Landscape on the Use of Artificial Intelligence by the Public Sector,* in *JRC science for policy report science policing report*, EU Commission, 2022, 48.

SARTOR G., *L'intelligenza artificiale e il diritto*, Torino, 2022, 56.

SEVERINO P., *Intelligenza artificiale e diritto penale*, in RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, 531.

SIBILLA F. – GUERRESCHI E., *UE – DSA e DMA, strumenti chiave per correggere i limiti del GDPR*, in *Diritto di Internet*, 2022.

SPANO L., *Il ruolo e la responsabilità delle piattaforme di E-commerce*, in *Amministrazione in Cammino*, 2022, 7.

SRINIVASAN R. – SAN MIGUEL GONZÁLEZ B., *The role of empathy for artificial intelligence accountability*, in *Elsevier - Journal of Responsible Technology*, 6, 2022, 3.

STRAMPELLI G., *L'informazione societaria a quindici anni dal t.u.f: profili evolutivi e problemi,* in *Rivista societaria*, 2014, 1002.

Supreme Court of India, *Justice K. S. Puttaswamy (Retd.) vs. Union of India*, Writ Petition (Civil), n. 494 of 2012, (2017) 10 SCC 1.

Supreme Court of the State of New York, Judgment *Millions March NYC v. NYPD*, January 14, 2019, NYSCEF, doc. n. 21, index 100690/2017.

SUR A., *Hyderabad second most surveilled city in world, beats New York, London*, in *New Indian Express*, 2021.

Testo unico delle disposizioni in materia di intermediazione finanziaria (TUF), d.lgs. 24 febbraio 1998, n. 58, art. 185.

TEOH K.H. – ISMAIL R.C. – NAZIRI S.Z.M. – HUSSIN R. – ISA M.N.M. – BASIR M.S.S, *Face recognition and Identification using Deep Learning Approach* in *Journal of Physics: Conference Series*, 2021, 3, 4.

Texas Statute, *The Capture or Use of Biometric Identifiers Act* (CUBI) or *Business and Commerce Code*, title 11, *personal identity information,* subtitle a., *identifying information,* chapter 503, *biometric identifiers,* 2007.

The Human Rights Council, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, HR/PUB/11/04, 2011.

The International Criminal Police Organization (INTERPOL) – United Nations Interregional Crime and Justice Research Institute (UNICRI), *Artificial Intelligence and Robotic for law* enforcement, 2018.

The Personal Data Protection Bill, n. 373, 2019.

THORAT S.B. – NAYAK S. K. – DANDALE J. P., *Facial Recognition Technology: An analysis with scope in India*, in *International Journal of Computer Science and Information Security (IJCSIS)*, 8, 1, 2010.

Trattato di Lisbona, *Modifiche del trattato sull'Unione Europea e del Trattato che istituisce la Comunità Europea*, 2007/C 306/01.

Trattato sull'Unione Europea, C 326, 2007.

TURING A. M., "On computable numbers, with an application to the entscheidungs problem", Princeton, 1936.

UBERTIS G.*, Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Diritto Penale Contemporaneo* 2020, 78, 80.

UCCI M., «Il Grande Fratello vi guarda», in *Zeta LUISS*, 2022.

United States District Court, *Floyd v. City of New York*, 959 F. Supp. 2d 540, 2013.

United States District Court, *State of Minnesota v. Chauvin*, Court File n. 27-CR-20-12646, 2021.

United States Supreme Court, *Daubert v. Merrel Dow Pharmaceuticals*, Inc., 509 U.S. 579, 1993.

VETCH F., *UK supermarket uses facial recognition tech to track shoppers*, in *Coda*, 2023.

Vermont Statute S.124 Acts and Resolves n. 166. Sec. 14, *Moratorium On Facial Recognition Technology*, 2020.

Virginia, HB 2031, *Facial recognition technology; authorization of use by local law-enforcement agencies and public institutions of higher education*, in *LIS Virginia's legislative information system,* 2021.

Washington, House Bill 1493, 2021, app.leg.wa.gov.

White House Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*, 2022, 5-8.

Wisconsin Supreme Court, Judgement *State v. Loomis*, July 13, Wisconsin, 2016, § 53, 54.

ZANIRATO S., *La Vittoria di Pirro del diritto alla privacy*, in *Strategic Litigation (STRALI)*, 2021.

ZIROLDI A., *Intelligenza artificiale e processo penale tra norme, prassi e prospettive*, in *Questione di Giustizia*, 2019.

ZSARKER I.H., *Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions* in *SN COMPUT. SCI.,* 2, 420, 2021.