UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Diritto Privato e Critica del Diritto

Corso di Laurea Magistrale in Giurisprudenza
Anno accademico 2022/2023

LE TECNOLOGIE DI RICONOSCIMENTO FACCIALE E IL LORO IMPIEGO A FINI DI PUBBLICA SICUREZZA

LA NECESSITÀ DI UNA PUNTUALE DISCIPLINA TRA RISCHI E BENEFICI

Relatore: Professor *CLAUDIO SARRA*

Laureanda: *VALENTINA AGNOLETTO*
Matricola numero: 1176832

INDICE

Capitolo II
Inquadramento storico e profili tecnici inerenti il funzionamento delle tecnologie di riconoscimento facciale

Capitolo III
Impiego dei sistemi di riconoscimento facciale per pubblica sicurezza
il paradigma di una nuova sicurezza di massa

Capitolo IV
Problematiche e criticità connesse all'impiego di tecnologie di riconoscimento facciale a fini di pubblica sicurezza

Introduzione

L'evoluzione tecnologica e informatica ha condotto l'esistenza umana in un'epoca che potremmo definire *digitale.* Il mondo analogico è stato profondamente trasformato, l'uomo ha iniziato, ormai da lungo tempo, ad essere coadiuvato da diversi strumenti, macchine e robot, fino all'introduzione dell'intelligenza artificiale che ha incentivato sempre più la presenza delle tecnologie nella nostra quotidianità. Ad oggi, viviamo e agiamo coadiuvati da strumenti intelligenti e con questi ci confrontiamo, tanto che la domanda che potremmo porci è: cosa non è in grado di fare l'intelligenza artificiale? Difficile trovare una risposta a questo quesito. L'uomo brama l'innovazione, vuole spingersi sempre oltre, ma qual è il limite? Lo sviluppo informatico ha condotto alla creazione e implementazione di sistemi sofisticati, in grado di compiere le più disparate funzioni, ma ciò non è esente da rischi, rischi per le persone fisiche e rischi per i diritti fondamentali, i quali richiedono un sempre più puntuale bilanciamento tra ciò che è giusto che l'IA faccia, e ciò che non è giusto lasciarle fare.

Tra le molte funzioni rimesse all'intelligenza artificiale vi rientra anche il riconoscimento facciale. La presente tesi è stata dedicata ad analizzare le tecnologie di riconoscimento facciale quando impiegate per fini di pubblica sicurezza, per fini, cioè, di prevenzione e repressione dei reati. L'indagine è stata volta a dimostrare che, a causa della potenza e della pervasività che contraddistinguono le dette tecnologie, queste si prestano a facili raggiri da parte delle autorità competenti (e incompetenti), astuzie che possono sfociare in sorveglianza di massa. Il pronostico di questa possibilità apre le porte alla necessità di individuare apposite garanzie, idonee tutele attribuite ai soggetti esposti al raggio d'azione delle telecamere di videosorveglia, ma la soluzione è tutt'altro che agevole. Al rischio concreto della sorveglianza di massa si aggiungono tutti i problemi connessi al funzionamento e alla logica algoritmica sottesa ai sistemi che integrano le tecnologie di riconoscimento facciale, le quali fanno emergere la lapalissiana necessità che il prorompente sviluppo tecnologico sia seguito da una altrettanto rapida evoluzione giuridica. L'impegno del legislatore, in particolare europeo, si prospetta come la soluzione per arginare usi pregiudizievoli e rischiosi di una tecnologia così all'avanguardia e, allo stesso tempo, così duttile.

Pertanto, la trattazione si apre con un'indagine prettamente giuridica che vuole mettere in luce, partendo dalla rilevazione della presente anomia normativa, il percorso che è stato fatto in ambito europeo per giungere alla Proposta di regolamento sull'intelligenza artificiale. Successivamente si indaga il piano tecnico-informatico, si spiegano prima le logiche algoritmiche sottese al funzionamento dei sistemi intelligenti, con particolare attenzione alle tecniche di *machine learning* e alla struttura delle reti neurali, poi si illustra il funzionamento del riconoscimento facciale in senso stretto. Di seguito, dopo aver posto le basi normative, tecniche e informatiche, si passa all'indagine centrale della trattazione, ossia quella dedicata a dimostrare quanto sia labile il confine tra uso idoneo e inidoneo delle TRF, e la conseguente illecita compressione del diritto alla *privacy* che decade in sorveglianza di massa quando si attua una troppo importante riduzione del nucleo forte di questo diritto. Si dedica anche attenzione al rapporto tra sicurezza 'primaria' e 'secondaria' al fine di indagare casi nazionali e comunali di uso illecito di queste tecnologie. L'ultima dell'elaborato pone l'attenzione alle criticità connesse a queste applicazioni di IA, in particolare all'opacità connessa alla medesima, ai *bias* quali distorsioni ingiustificate che si ripercuotono sul risultato, nonché sulle decisioni interamente automatizzate e sulla profilazione. Infine, il percorso si conclude con una piccola introduzione ai diversi e ulteriori settori di impiego di queste tecnologie all'avanguardia, di modo tale che il lettore possa avere la possibilità di comprendere a pieno l'ubiquità a queste collegata.

Il percorso di studio sopra descritto è stato sviluppato mediante l'indagine di documenti provenienti da diversi ambiti del sapere e della conoscenza. Si sono indagati atti normativi, interni ed europei, così come testi originari del mondo scientifico e informatico e talvolta è stato essenziale prendere in esame testi di sociologia. La metodologia utilizzata fa comprendere, pertanto, che la pervasività delle TRF si riversa in tutta la sua potenza in diversi e plurimi ambiti intellettuali, con la conseguenza che non si può restare indifferenti davanti a tutto ciò.

CAPITOLO I
VERSO L'APPROVAZIONE DEL REGOLAMENTO EUROPEO CHE STABILISCE REGOLE ARMONIZZATE SULL'INTELLIGENZA ARTFICIALE
RASSEGNA CROLOGICA DEGLI ATTI CHE HANNO CONDOTTO ALLA PROPOSTA DI REGOLAMENTO EUROPEO SULL'INTELLIGENZA ARTIFICIALE

1. Trovare rimedi alla presente anomia: il quadro normativo attuale tra GDPR e LED

Il quadro normativo vigente, in tema di sistemi di riconoscimento facciale, fa' emergere la presenza di una problematica anomia[1]; infatti né gli Stati Nazionali né l'Unione Europea hanno predisposto una disciplina giuridica omogenea ed unitaria che regoli l'impiego di queste tecnologie all'avanguardia e i rischi che vi sono connessi. Innanzi a questa mancanza emerge la presenza di diverse normative settoriali, tanto di rango interno[2] quanto di rango Comunitario[3], le quali necessitano di essere informate al rispetto della disciplina attualmente in vigore che si ritrova nel Regolamento generale sulla protezione dei dati. Ai fini della presente indagine rileva prendere in considerazione e analizzare la disciplina che si colloca a livello sovrannazionale europeo[4] e in particolare

[1] G. Mobilio, *Tecnologie di Riconoscimento Facciale. Rischi per i diritti fondamentali e sfide regolative,* Napoli, Editoriale Scientifica, 2021, cit. 119.

[2] Ad esempio, per rammentare una delle normative più recenti, il D.L 20 Febbraio 2017, n.14, convertito con modificazioni con la Legge 18 Aprile 2017, n.48, istituisce i cosiddetti 'Patti per l'attuazione della sicurezza urbana', sottoscritti tra il Prefetto e il Sindaco.

[3] E' il caso, ad esempio, della Direttiva (UE) 2015/2366 del 25 Novembre 2015, concernente i servizi di pagamento nel mercato interno, recepita dal D.lgs. 15 Dicembre 2017, n.218, che introduce il sistema di 'autenticazione forte del cliente', il quale prevede la possibilità di pagare attraverso l'autenticazione basata su più elementi, uno dei quali può essere biometrico (art.97).

[4] Al di là del 'quadro protezione dati', nel contesto sovranazionale europeo, possiamo anche ricordare l'importanza della Convenzione Europea, 28 Gennaio 1981, n.108, 'Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale', la quale è stata ratificata in Italia con la Legge 21 febbraio 1989, n.98. Successivamente è stato adottato un Protocollo di modifica, 18 Maggio 2018, che è stato firmato dall'Italia, ma non ancora ratificato; questo protocollo ha riformato profondamente la disciplina presente all'interno della Convenzione, per un maggiore approfondimento cfr. Luigi Montuori, '*Privacy: perché la Convenzione 108+ è cruciale per il libero flusso dei dati', in* Agenda Digitale, 28 Gennaio 2022, https://www.agendadigitale.eu/sicurezza/privacy-perche-la-convenzione-108-e-cruciale-per-il-libero-flusso-dei-dati/.

il 'quadro protezione dati'[5] che comprende il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio '*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*' (c.d. GDPR) e che abroga la direttiva 95/46/CE, e la Direttiva (UE) 2016/680 '*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*' (c.d. LED). Il GDPR essendo stato emanato nella forma di Regolamento[6], ha portata generale, è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri. Con tale atto Parlamento Europeo e Consiglio hanno perseguito l'intento di ridurre se non eliminare i limiti e la frammentazione della disciplina della protezione dei dati che scaturiva dalla previgente Direttiva. Originariamente la Direttiva 95/46/CE era stata adottata al fine di perseguire due obbiettivi ossia salvaguardare il diritto fondamentale alla protezione dei dati e garantire la libera circolazione dei dati tra gli Stati membri[7]. Successivi sviluppi tecnologici[8] tra i quali i più rilevanti sono l'aumento delle infrastrutture e il potenziamento della connessione internet con la nascita dell'ADSL; l'ascesa, a partire dal 1998, di Google quale grande '*gatekeeper'* [9]della Rete e l'inizio dell'era della condivisione del privato a partire dal 2004 con l'introduzione, nel mondo analitico, del Social-Media *Facebook*, queste innovazioni e molte altre ancora hanno avuto quale conseguenza la frammentazione, nei vari territori dell'Unione Europea, delle modalità di applicazione della disciplina a protezione dei dati personali, e con essa è

[5] Cfr. Camera dei Deputati, Documentazione Parlamentare, *Protezione dei dati personali,* 30 Settembre 2022,
https://temi.camera.it/leg18/temi/la_protezione_dei_dati_personali.html#:~:text=pacchetto%20protezione%20dati%20identifica%20gli,esigenze%20di%20tutela%20dei%20dati.

[6] Infatti, ai sensi dell'articolo 288, paragrafo 2, del Trattato sul funzionamento dell'Unione Europea: '*il Regolamento ha portata generale. Esso è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.'*

[7] M. Iaselli, *Protezione dei dati personali: le novità del nuovo Regolamento europeo, in* Altalex, 9 Maggio 2016, https://www.altalex.com/documents/news/2015/12/23/accordo-raggiunto-sul-regolamento-europeo-in-materia-di-protezione-dei-dati-personali.

[8] Cfr. C. Sarra, *Il Mondo-Dato. Saggi su datificazione e diritto,* Padova, CLEUP sc, 2019, pp 17-22.

[9] I c.d '*Gatekeeper'* sono i soggetti che forniscono i servizi informatici di 'di base' e che consentono di usufruire di altri servizi *online* e *offline* (come ad esempio: browser, motori di ricerca, social network…), per un più accurato approfondimento si veda, R. Berti, F. Zumerle, *Digital Markets Act:l'UE chiarisce le regole per individuare i Gatekeepers, in* Agenda Digitale, 11 Maggio 2023, https://www.agendadigitale.eu/mercati-digitali/digital-markets-act-lue-chiarisce-le-regole-per-individuare-i-gatekeeper/. L'articolo si propone di indagare le novità introdotte dal Regolamento (UE) 2022/1925, atto con il quale l'UE vuole regolare i cd. '*Gatekeepers.'*

persistita una forte preoccupazione, nel mondo dell'opinione pubblica, verso i rischi connessi alle operazioni *online.* Tutto ciò ha condotto alla necessità di adottare una normativa più solida e coerente in materia di protezione dei dati personali, che potesse consentire lo sviluppo dell'economia digitale interna, garantire il controllo dei dati personali alle persone fisiche e rafforzare la certezza giuridica e operativa per i soggetti economici privati e le pubbliche autorità.[10] Volendo intraprendere una breve analisi della disciplina individuata nel GDPR occorre specificare la portata dei principi di maggiore rilievo in esso prospettati ossia il Principio di Trasparenza, il Diritto all'Oblio, il Principio di *Accountability* e il Principio di *Privacy by design.*

Il Principio di Trasparenza[11], esplicato nell'articolo 5 paragrafo 1 lettera a) del GDPR[12], assume i caratteri della generalità e dell'essenzialità in ogni trattamento di dati personali. Questo principio è inteso come obbligo di rendere conoscibili le modalità con cui i dati sono raccolti, utilizzati e consultati grazie ad informazioni e comunicazioni facilmente accessibili e comprensibili, utilizzando un linguaggio semplice e chiaro[13]. A chiarire come tal principio deve essere applicato interviene il Considerando 39 che afferma '*qualsiasi trattamento dei dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati, o altrimenti trattati, dati personali che le riguardano nonché la misura in cui i dati saranno trattati*.[14]'

Passando al Diritto all'Oblio, sancito dall'articolo 17 del Regolamento[15], si qualifica come un diritto alla cancellazione dei propri dati personali in forma rafforzata in quanto sussiste l'obbligo, per i titolari del trattamento che abbiano reso pubblici i dati personali

[10] R. Berti, F. Zumerle op. cit.
[11] F. Pizzetti, *Trasparenza nel trattamento dei dati, cosa cambia col GDPR: l'alba di un nuovo valore sociale, in* Agenda Digitale, 31 Giugno 2018, https://www.agendadigitale.eu/sicurezza/trasparenza-nel-trattamento-dati-che-cambia-col-gdpr-lalba-di-un-nuovo-valore-sociale/.
[12] Il Principio di Trasparenza è enunciato nell'articolo 5, paragrafo 1 lett.a), che dispone: 'I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (<<liceità, correttezza e trasparenza>>).'
[13] Cfr. Considerando 39 Regolamento (UE) 2016/679.
[14] Cit. Considerando 39 Regolamento (UE) 2016/679.
[15] Art. 17 GDPR: '*l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti…*'; l'articolo prosegue indicando i motivi per cui il diritto alla cancellazione sussiste.

dell'interessato, di trasmettere la richiesta anche ad altri titolari che trattino o abbiano trattato i dati personali di cui si è chiesta la cancellazione[16].

Il Principio di *Accountability*, responsabilizzazione[17] volendo usare il termine italiano, di titolari e responsabili, chiede a tali soggetti di tenere comportamenti proattivi e che possano dimostrare che siano state concretamente adottate misure al fine di garantire l'applicazione del regolamento, in questo modo vengono affidate ai titolari del trattamento le decisioni relative alle modalità, alle garanzie e ai limiti del trattamento dei dati personali[18].

Infine il principio di *Privacy by design* stabilisce che '*la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento.*[19]' Il principio appena enunciato si applica a tutti i titolari del trattamento al fine di garantire un'idonea protezione dei dati personali, in conformità con le disposizioni contenute nel GDPR, e che tale garanzia si esplichi in relazione all'intero ciclo di vita della tecnologia impiegata, al fine del trattamento di detti dati personali, dalla prima fase di progettazione fino alla sua eliminazione[20].

---

[16] Il diritto all'oblio così come definito e disciplinato nel GDPR ha un ambito di applicazione più esteso rispetto alla rispettiva disciplina individuata nel D.lgs, 30 Giugno 2003, n.196, *Codice in materia di dati personali (cd. Codice della privacy),* ove il diritto all'oblio è disciplinato all'articolo 7, comma 3. Infatti come chiarisce il Garante per la protezione dei dati personali, secondo quanto dispone il Regolamento europeo, il diritto alla cancellazione può essere esercitato anche dopo la revoca del consenso. Per maggiori approfondimenti in materia si veda https://www.garanteprivacy.it/i-miei-diritti/diritti/oblio.

[17] Il termine *Accountability* non è semplice da tradurre in lingua italiana, nel testo si è adottata la traduzione individuata dal Garante per la Protezione dei Dati Personali, cfr. https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili. In questa sede è anche bene rammentare che il significato letterale del termine anglosassone è 'responsabilità', 'obbligo di rispondere', ma il legislatore italiano ha ritenuto più opportuno utilizzare il termine 'responsabilizzazione', sul punto vd. S. Aterno, *Il principio di Accountability nel GDPR, significato e applicazione, in* Agenda Digitale, 31 Luglio 2018, https://www.agendadigitale.eu/sicurezza/principio-di-accountability-nel-gdpr-significato-e-applicazione/.

[18] Cfr. Garante per la protezione dei dati personali, https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili

[19] Cit. Considerando 78 GDPR.

[20] C. Sarra *op. cit.*. Inoltre si vedano le Linee Guida dell'European Data Protection Board, 4/2019 sull'articolo 25, 20 Ottobre 2020, *Protezione dei dati fin dalla progettazione e per impostazione predefinita*, https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_it.pdf.

Il secondo atto del 'quadro protezione dati' è la Direttiva (UE) 2016/680,[21] ossia la c.d. LED. Detta Direttiva è speculare rispetto al GDPR e predisponendo la disciplina relativa alla protezione dei dati personali ai fini di prevenzione e repressione dei reati chiede un bilanciamento complesso tra un interesse privato, ossia quello facente capo alla persona fisica a ricevere un'adeguata tutela dei propri dati personali, e un'esigenza di natura pubblicistica e sociale volta a garantire l'ordine pubblico e la cooperazione informativa tra le autorità di contrasto[22]. Le norme contenute predispongono la disciplina specifica per i trattamenti posti in essere da autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati; esecuzione di sanzioni penali e salvaguardia e prevenzione di minacce alla sicurezza pubblica[23]. Come si desume dalle precedenti indicazioni, ai fini della LED, il trattamento è riservato alle sole autorità competenti come il titolare del trattamento, le autorità pubbliche competenti nelle materie oggetto del trattamento nonché altri organismi o entità ai quali lo Stato ha affidato il compito di esercitare l'autorità pubblica e i poteri ad essa connessi.[24] Allo scopo di garantire un'efficace cooperazione giudiziaria in materia penale e di polizia è necessario assicurare un'uniforme ed elevato grado di protezione dei dati a carattere personale nonché al fine di facilitare lo scambio di dati personali tra le autorità competenti degli Stati membri e proprio per questo si auspica un livello di tutela equivalente in tutti gli Stati membri[25]. Nella presente Direttiva si chiede, affinché non sia elusa, che la protezione delle persone fisiche sia neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate[26]. Nonostante la disciplina individuata all'interno della Direttiva (UE) 2016/680 sia volta a perseguire l'obiettivo della prevenzione e repressione dei reati diverse disposizioni in essa contenute echeggiano le norme contenute nel GDPR cosicché

[21] Nello stesso pacchetto di riforma UE sulla protezione dei dati, è stata adottata anche la Direttiva (UE) 2016/681, la quale predispone la disciplina per il trattamento dei dati del cd. codice di prenotazione (Passanger Name Record – PNR), per un confronto e un maggiore approfondimento si veda: G. Troiano, *Privacy, cosa sono le direttive 680 e 681 e quali rischi ci sono, in* Agenda Digitale, 14 Febbraio 2020, https://www.agendadigitale.eu/sicurezza/guglielmo-troiano-direttiva-680-e-681/.

[22] G. Mobilio *op cit*. 130

[23] Così come disposto dal considerando 4 della Direttiva (UE), 2016/680.

[24] G. Troiano, *in* Agenda Digitale *op cit.*

[25] Cfr. Considerando 7 della Direttiva (UE), 2016/680.

[26] In particolare la protezione garantita alle persone fisiche non dovrebbe variare in base al trattamento che ne viene fatto dei dati, che sia esso automatizzato o manuale, cfr. Considerando 18, Direttiva (UE) 2016/680.

i due regimi potranno essere unitamente richiamati, sempre avendo a mente le differenze che vengono in evidenza. [27]

1.1. La rilevanza della definizione e della puntuale disciplina dei dati biometrici

Per comprendere a pieno il funzionamento dei sistemi di riconoscimento facciale diviene fondamentale constatare la tipologia di dati che queste tecnologie sfruttano ossia i dati biometrici. Il dato biometrico, disciplinato tanto nel GDPR quanto nella LED,[28] viene definito in modo coincidente all'interno di entrambi i riferimenti normativi. All'articolo 4 paragrafo 1, n.14 del GDPR si chiarisce che sono i '*dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*.[29]' Affinché un dato sia qualificato come biometrico sono necessari tre requisiti, individuabili dalla definizione riportata, ossia: che presentino una specifica natura (la riproduzione delle caratteristiche fisiche, fisiologiche e comportamentali); che siano impiegati appositi mezzi e puntali modalità di trattamento (la loro sottoposizione ad un trattamento tecnico individuato); e che sia perseguita una finalità apposita con il loro trattamento (la facoltà di individuare in modo univoco una persona fisica)[30]. Questa specifica categoria di dati personali non dovrebbe costituire oggetto di trattamento in quanto configurati quali dati sensibili, salvo quando sia esplicitamente consentito e nei casi tassativamente individuati dalla normativa esplicata nel GDPR[31]. L'uso di dati biometrici, e in particolare il loro impiego per fini di identificazione biometrica, fa emergere elevati rischi per i diritti degli interessati ed è anche per questo motivo che laddove è consentito il trattamento, questo deve avvenire nel ligio rispetto dei principi di liceità, proporzionalità, necessità e minimizzazione dei dati.

---

[27] G. Mobilio *op. cit*. 135.

[28] Al fine di una esposizione legislativa quanto più completa, si può anche rammentare che la stessa definizione di dato biometrico, così come fornita nel GDPR e nella LED, è presente anche all'interno della Convenzione 108+. Inoltre il trattamento dell'immagine facciale è tutelato dall'articolo 8 della CEDU, il quale disciplina la protezione della vita privata.

[29] Cit. articolo 4, paragrafo 1, n.14 GDPR; ma la definizione è la medesima all'interno della LED, cfr. art. 3 par. 1, n.13.

[30] Cfr. Linee Guida della European Data Protection Board, 3/2019 *sul trattamento dei dati personali attraverso dispositivi video,* 29 Gennaio 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_it.pdf., p. 19.

[31] Il paragrafo 2 dell'articolo 9 del GDPR specifica in quali casi è consentito il trattamento dei dati biometrici, e con essi altri dati ritenuti tal volta sensibili, per i casi in specifico cfr. articolo 9 GDPR.

Gli Stati membri hanno la facoltà di predisporre disposizioni interne al fine di garantire un adeguato coordinamento tra le disposizioni presenti all'interno della normativa sovranazionale europea, un obbligo legale, l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento. È comunque idoneo individuare esplicitamente le deroghe al divieto di trattare tali dati personali specifici.[32] In base a quanto fino a questo momento riportato, si rileva che il regime dei dati biometrici trova esplicita applicazione se lo scopo perseguito è quello dell'identificazione di un soggetto attraverso un confronto uno-a-molti, mentre sorgono dubbi circa la possibilità di applicare detto regime al caso della verifica uno-a-uno[33]. Se le generalità della persona fisica sono sconosciute ma la TRF conserva dati riferiti a detto soggetto, anche solo al fine di utilizzarli quale modello di riferimento, con l'obiettivo, ad esempio, di tracciare l'interessato, allora si è, in ogni caso, in presenza di un trattamento di dati biometrici.[34] Al contrario, se vengono impiegati solo ed esclusivamente algoritmi di *face detection* e non di *face recognition,*[35] senza che avvenga alcuna conservazione del *template* biometrico, allora si esclude l'applicazione della disciplina riferita ai dati biometrici.

2. La consapevolezza della necessità di un intervento legislativo

L'Intelligenza artificiale (IA) si è particolarmente diffusa nell'epoca contemporanea e ciò ha contribuito a forgiare la sempre maggiore consapevolezza che non si tratta di astratta fantascienza ma di una solida realtà che fa sempre più parte delle nostre vite. Questa consapevolezza ha spinto l'Unione Europea a far fronte all'esigenza di predisporre un'adeguata disciplina in materia, che possa tenere in considerazione le implicazioni umane ed etiche che accompagnano le tecnologie emergenti nell'era digitale.[36] La conseguenza dell'anomia sopra evidenziata ha indotto l'Unione Europea a sviluppare

[32] Cfr. Considerando 51 GDPR.
[33] G. Mobilio *op cit.*. 139.
[34] Linee Guida della European Data Protection Board *op. cit*. 20.
[35] Se vengono impiegati solo ed esclusivamente algoritmi di *face detection* significa che svolgono la funzione di mero rilevamento del volto della persona; se invece si utilizzano algoritmi di *face recognition* allora vuol dire che l'algoritmo impiega i dati al fine di identificare uno specifico soggetto. Per un maggiore approfondimento si veda pag. 140 ss. Di G. Mobilio, *Tecniche di Riconoscimento facciale. Rischi per i diritti fondamentali e nuove sfide,* Napoli, Editoriale Scientifica, 2021.
[36] Cfr. P. Moro, *Intelligenza artificiale e tecnodiritto, in* Etica, Diritto e Tecnologia. Percorsi dell'informatica giuridica contemporanea, (a cura di) P. Moro, Milano, FrancoAngeli, 2022, p. 17.

azioni concrete, propedeutiche alla emanazione della proposta di Regolamento dell'UE che stabilisce regole armonizzate sull'intelligenza artificiale.

2.1. Dall'accettazione del cambiamento all'iniziativa UE per l'intelligenza artificiale: la Comunicazione (25 Aprile 2018) della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale Europeo e al Comitato delle Regioni

Il punto di partenza di questa disamina cronologica è la Comunicazione (25 Aprile 2018) della Commissione Europea. L'obiettivo perseguito dalla Commissione Europea è quello di condurre ad una sempre maggiore accettazione del cambiamento dettato dalla preponderante presenza di tecnologie dotate di intelligenza artificiale, tecnologie che hanno la capacità di apportare benefici all'uomo e alla società nel suo insieme, ma che al contempo sollevano nuove questioni da fronteggiare. Diversi fattori, come l'aumento della potenza di calcolo e della disponibilità di dati, nonché il progresso nello sviluppo e sfruttamento degli algoritmi, hanno fatto si che l'IA diventasse una delle tecnologie più strategiche del ventunesimo secolo, e proprio per questa ragione è necessaria una disciplina europea di riferimento[37]. Il quadro normativo che l'UE prospetta di emanare deve assicurare che l'IA sia creata, sviluppata e applicata in un contesto in cui vi sia la possibilità di una rapida risposta agli interrogativi etici e giuridici che da questi sistemi possono sorgere, nel rispetto dell'innovazione, dei valori dell'Unione nonché dei diritti fondamentali, oltre che dei principi etici di responsabilità e trasparenza.[38] La Comunicazione che si sta ora analizzando vuole lanciare un'iniziativa europea in tema di IA che persegue specifici obiettivi: incentivare la competenza tecnologica e industriale dell'UE e all'impiego dell'IA nei vari ambiti economici pubblici e privati[39]; organizzarsi ai mutamenti sociali ed economici scaturenti dal sempre maggiore utilizzo di sistemi

[37] Cit. Commissione Europea COM(2018) 237 final, *'L'intelligenza artificiale per l'Europa',* 25 Aprile 2018, p.2.

[38] Per maggiore completezza si veda la revisione intermedia della strategia per il mercato unico digitale, pubblicata dalla Commissione: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52017DC0228. Inoltre si può anche ricordare che il Consiglio europeo dell'Ottobre 2017 ha invitato l'UE a far fronte alle tendenze emergenti dall'IA e a presentare un approccio europeo all'IA: http://data.consilium.europa.eu/doc/document/ST-14-2017-INIT/en/pdf.

[39] Infatti l'IA può migliorare i pubblici servizi e prestarsi al raggiungimento degli obiettivi individuati nella dichiarazione ministeriale di Tallinn sull'e-governement (Ottobre 2017): https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovernment-tallinn-declaration.

tecnologici dotati di IA;[40] garantire un panorama etico e giuridico consono[41]. L'UE è consapevole che si sta inserendo in uno scenario internazionale fortemente competitivo nel quale la Cina[42] vuole ottenere la *leadership* mondiale entro il 2030 e a tal fine sta investendo in modo massivo, diversi paesi come il Giappone e il Canada si stanno impegnando per lo sviluppo di strategie di IA e allo stesso tempo gli Stati Uniti restano uno dei paesi più all'avanguardia in questo settore grazie agli importanti investimenti e allo sfruttamento di dati che diventa via via più ingente[43]. In relazione al contesto appena descritto l'UE è in ritardo sugli investimenti in ambito privato, che sono nettamente inferiori rispetto a quelli che si evidenziano in Asia e in America del Nord, ciò porta a comprendere che per poter competere a livello mondiale l'Unione Europea deve impegnarsi per creare un ambiente che stimoli gli investimenti e salvaguardi, oltre che sviluppi, i propri punti di forza[44]. L'UE ha inoltre promosso importanti iniziative tra le quali *chip* Neuromorfici,[45] computer ad elevate prestazioni di livello mondiale[46], nonché programmi sulle tecnologie quantistiche e sulla mappatura del cervello. Senza uno sforzo concreto da parte dell'Unione Europea e una stretta collaborazione con gli Stati membri, vi è il rischio che l'UE comprometta le prospettive offerte dall'IA. Inoltre potrebbe verificarsi una perdita di talenti qualificati oltre il fatto che l'UE rischia di trasformarsi in un acquirente passivo di tecnologie IA progettate altrove. Al fine di evitare tutto ciò la Commissione Europea mette in luce l'importanza di un effettivo aumento degli investimenti; del potenziamento della ricerca e dell'innovazione dal laboratorio al mercato[47]; di sostenere i preminenti centri di ricerca in ambito di IA; di consentire alle

[40] In tal senso la Commissione incoraggia il rinnovamento dell'istruzione, promuove il talento e vuole precedere i mutamenti del mercato del lavoro agevolando le transazioni e l'assestamento dei sistemi di protezione sociale.
[41] Cfr. pag. 4 della Comunicazione in questa sede analizzata, si specifica infatti che il quadro etico e giuridico deve ispirarsi ai valori dell'Unione Europea nonché alla Carta dei diritti fondamentali dell'UE.
[42] Il progetto con il quale la Cina vuole ottenere la *leadership* mondiale è il *'Piano di sviluppo dell'intelligenza artificiale di prossima generazione'*.
[43] Già nel 2018 la popolazione cinese generava enormi quantità di dati grazie all'1,4 miliardi di abbonati alla telefonia cellulare e agli 800 milioni di utenti della rete Internet.
[44] Bisogna rammentare che l'UE ospitava, già al tempo della Comunicazione, 100 tra gli istituti di ricerca più importanti al mondo, *start-up* ad importante contenuto tecnologico.
[45] Si tratta di *chip* plasmati sulla struttura biologica del cervello, nello specifico si tratta di microprocessori che sono in grado di imitare il funzionamento dei neuroni.
[46] Questa struttura diventerà la base del *cloud* europeo per la scienza aperta e metterà a disposizione dei ricercatori un mondo virtuale in cui archiviare, processare, condividere e riutilizzare i dati: https://ec.europa.eu/research/openscience/.
[47] Il criterio che ispira il sostegno alla ricerca sull'IA si specifica che sarà lo sviluppo dell'Intelligenza Artificiale responsabile volta al rispetto degli esseri umani, per un maggiore approfondimento si veda

piccole imprese e agli ipotetici consumatori l'accesso a sistemi di intelligenza artificiali[48]; di incentivare i *test* e la sperimentazione[49]; incrementare gli investimenti da parte di soggetti privati e infine di consentire un sempre maggiore accesso ad una sempre più ingente quantità di dati[50].

Un settore in cui queste tecnologie influiscono particolarmente è quello lavorativo, nel quale da un lato l'IA può essere un valido aiuto per il lavoratore, e dall'altro lato determina la nascita di nuove mansioni e posti di lavoro[51]. Sulla base di ciò, tre sono le sfide da fronteggiare: la prima è quella di garantire alla società un'adeguata preparazione, avendo coscienza del fatto che ci sono capacità umane che non possono essere sostituite dalla macchina, come ad esempio il pensiero critico o la creatività[52]; la seconda sfida si concentra nell'apprestare aiuto ai lavoratori che ricoprono mansioni che o subiranno importanti trasformazioni o scompariranno del tutto a causa, non solo dell'IA, ma anche della robotica e dell'automazione[53]; la terza sfida si esplica nell'istruire più esperti di tecnologie all'avanguardia. Affinché l'UE possa affrontare queste tre sfide innanzitutto nessuno deve restare escluso e questo significa dare l'opportunità ai lavoratori di apprendere le competenze e le conoscenze per governare le tecnologie in questione e ricevere un adeguato sostegno nel caso di cambiamento del mercato del lavoro[54].

'*Ricerca e innovazione responsabile':* https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation. Inoltre la Commissione sosterrà il progetto pilota del Consiglio Europeo per l'innovazione: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/european-innovation-council-eic-pilot.

[48] Al fine di agevolare quanto più possibile l'accesso alle più innovative tecnologie IA da parte di tutti i potenziali utilizzatori, la Commissione sosterrà lo sviluppo della *'Piattaforma di IA on demand',* la quale costituirà un unico punto di accesso alle risorse IA inerenti all'UE e concernenti informazioni, archivi di dati, potenza di elaborazione, strumenti e algoritmi.

[49] I *test* e la sperimentazione svolgono la funzione di garantire la concordanza con gli *standard* e le norme di sicurezza, oltre il fatto che i sistemi dotati di intelligenza artificiale devono anche rispettare le norme di sicurezza fin dalla progettazione e devono inoltre consentire ai politici di predisporre quadri normativi adeguati al contesto.

[50] Commissione Europea *op. cit.* 7,8,9,10. Per completezza si rammenta che la Commissione aveva anche proposto una serie di progetti per ampliare i dati in ambito europeo: https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy.

[51] Commissione Europea, *op. cit*. 12.

[52] si veda P. Moro, *Intelligenza artificiale e tecnodiritto, in Etica, Diritto e Tecnologia. Percorsi dell'Informatica giuridica contemporanea,* Milano, FrancoAngeli, 2022, p. 11 e seguenti.

[53] Questo significa anche assicurare, a tutti i cittadini, l'accesso alla protezione sociale dato che l'automazione spinge ad interrogarsi sulla conformità dei sistemi di sicurezza sociale rispetto alle innovazioni che vanno via via profilandosi, grazie al continuo sviluppo dell'IA.

[54] Infatti nel 2016 la Commissione aveva approvato un programma generale per incentivare le persone ad acquisire le giuste competenze per il mercato del lavoro che era ed è ancora ad oggi in continua evoluzione

Parimenti, ciò implica la necessità di stimolare l'emergere di nuovi talenti, incrementando il numero di persone aventi una formazione specifica in materia di intelligenza artificiale, nonché incentivando la diversità al fine di evitare che si insidi un'IA discriminatoria. Questo obiettivo può essere perseguito aumentando le persone che collaborano allo sviluppo dell'IA provenienti da situazioni tra loro diverse. Infine significa anche promuovere l'interdisciplinarietà[55].

È imprescindibile poi assicurare un panorama etico e giuridico consono, a livello giuridico il quadro si compone dei valori individuati nell'articolo 2 del Trattato sull'Unione europea[56], della Carta dei diritti fondamentali dell'UE che incasella in un unico testo normativo i diritti fondamentali di cui godono le persone che fanno parte dell'UE, nonché il Regolamento generale sulla protezione dei dati personali[57]. Plurime proposte sono poi state introdotte per promuovere il mercato unico digitale come per esempio il Regolamento sulla libera circolazione dei dati non personali; ma anche proposte volte a rafforzare la fiducia nel mondo online come il Regolamento sulla *e-privacy.* La Commissione ribadisce più volte che affinché i cittadini e le imprese possano maturare fiducia nei sistemi basati sull'IA con cui si relazionano è necessario che questi siano comprensibili o comunque spiegabili e per questo è fondamentale accrescere la trasparenza e ridurre esponenzialmente il rischio di condizionamenti o errori[58].

ossia *la Nuova Agenda per le competenze per l'Europa:* http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52016DC0381.

[55] Commissione Europea (*l'intelligenza artificiale per l'Europea) op.cit*. 12-14. Inoltre, a tal proposito, la Commissione aveva promosso l'iniziativa '*Digital Opportunity Trainership'* volta ad appoggiare i tirocini per il conseguimento di capacità digitali avanzate.

[56] Cfr. disposto normativo dell'articolo 2 del Trattato sull'Unione Europea: *'L'Unione si fonda sui valori del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze. Questi valori sono comuni agli Stati membri in una società caratterizzata dal pluralismo, dalla non discriminazione, dalla tolleranza, dalla giustizia, dalla solidarietà e dalla parità tra donne e uomini.'*

[57] Commissione Europea, '*l'intelligenza artificiale per l'Europea*', *op cit.* 15

[58] Al fine di raggiungere tale obiettivo diviene fondamentale una continua ricerca nella spiegabilità dei sistemi di IA dato che spesso accade che siano oscuri i processi sottesi al risultato emergente dall'intelligenza artificiale, ma per poter minimizzare gli errori è necessario prima individuarli e comprenderli.

Un ulteriore aspetto rilevante si concretizza nell'individuazione di un quadro normativo europeo sulla sicurezza che sia in grado di far fronte agli imprevedibili modi di agire di una tecnologia dotata di IA che per la prima volta viene messa in funzione[59].

Perché gli obiettivi individuati nella Comunicazione ora analizzata possano essere effettivamente raggiunti è necessario, da ultimo, coinvolgere quanto più possibile gli Stati membri e proprio per questo si evidenzia la necessità di un accordo per la pianificazione di una strategia sull'IA. In conclusione, si può notare come al tempo della Comunicazione, la Commissione Europea già fosse consapevole che erano presenti tutti gli elementi affinché l'UE occupasse una posizione di tutto rilievo nella rivoluzione dettata dall'intelligenza artificiale e anche perché, questa tecnologia, fosse messa a disposizione del progresso umano[60].

2.2 L'Alleanza Europea per l'Intelligenza Artificiale

L'Alleanza Europea per l'Intelligenza artificiale è un'iniziativa lanciata dalla Commissione Europea nel 2018 e in particolare all'interno della Comunicazione analizzata nel paragrafo precedente. In quest'ultima si specifica la volontà di creare una piattaforma multilaterale che sia in grado di dedicarsi a tutti i più svariati aspetti dell'IA e che possa facilitare il dialogo tra la stessa Alleanza e il Parlamento Europeo, gli Stati membri, il Comitato economico e sociale europeo, il Comitato delle regioni e le organizzazioni internazionali. L'Alleanza è nata come forum online ma è mutata in una e vera e propria comunità in cui la società civile, le organizzazioni delle imprese e dei consumatori, i sindacati, il mondo accademico e gli esperti possono interagire e guidare il lavoro del gruppo di esperti sull'intelligenza artificiale[61]. Ad oggi la si può definire come una aperta e multidisciplinare comunità di scambio[62], attraverso la quale si ha la possibilità di reperire gratuitamente documenti e altre risorse afferenti ai svariati aspetti politici dell'IA.

---

[59] Commissione Europea, *'L'intelligenza artificiale per l'Europea'*, *op. cit.* 17.
[60] Ibidem 59, cit. 20.
[61] Cfr. http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52016DC0381.
[62] Si veda anche A. Carleo, *Che cosa è l'alleanza europea sull'intelligenza artificiale?, in* Cyberlaw, 15 Ottobre 2018, https://www.cyberlaws.it/2018/che-cose-lalleanza-europea-sullintelligenza-artificiale/ .

3. Creare fiducia nell'intelligenza artificiale antropocentrica: la Comunicazione (8 Aprile 2019) della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale Europeo e al Comitato delle Regioni

Un atto di rilevante importanza nella disamina cronologica che si sta ora affrontando è la Comunicazione (8 Aprile 2019) della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale Europeo e al Comitato delle Regioni. Fin dal principio si puntualizza che il presupposto per dar vita ad una intelligenza artificiale antropocentrica è la fiducia, e questo significa che l'IA deve costituire un dispositivo volto a migliorare la vita degli esseri umani e perché questo accada è necessario dare vita ad un'intelligenza artificiale affidabile. Sviluppare un'IA affidabile è però difficile soprattutto tenendo in considerazione le sfide che da essa nascono, infatti l'IA permette alle macchine di 'imparare', di decidere e di fare ciò senza che sia necessario l'aiuto dell'uomo, ma al contempo le decisioni prese da un dispositivo dotato di IA e quindi dagli algoritmi possono basarsi su dati incompleti o manomessi e quindi inaffidabili e questo può portare i cittadini a non fidarsi di queste tecnologie. Si specifica che deve essere rispettata la diversità in ogni suo aspetto, sesso, razza, origine etnica, religione o convinzioni personali, disabilità ed età, e questo in ogni fase di sviluppo dell'IA, è di lapalissiana chiarezza l'esigenza di mettere a punto orientamenti etici sviluppati sul quadro normativo esistente[63]. Proprio a questo fine è stato istituito un gruppo di esperti di alto livello sull'IA[64] e allo stesso tempo è stata istituita anche l'Alleanza europea per l'IA[65].

Il punto di partenza per il gruppo di esperti di alto livello sull'IA è costituito dalle ricerche portate avanti dal Gruppo europeo sull'etica nelle scienze e nelle nuove tecnologie (GEE) e dall'Agenzia dell'Unione europea per i diritti fondamentali (FRA). Per aversi

[63] Cfr. Commissione Europea COM(2019)168 final, *'creare fiducia nell'intelligenza artificiale',* 8 Aprile, p. 2,3. Inoltre si confronti il paragrafo 1 del presente capitolo '*Trovare rimedi alla presente anomia:il quadro normativo attuale tra GDPR e LED'*, in esso si delinea il quadro normativo vigente e la sussistenza dell'attuale anomia; l'attenzione è posta in particolare sugli aspetti salienti del GDPR e della LED.

[64] Per un maggiore approfondimento circa i progetti del gruppo di esperti di alto livello sull'IA si veda il primo progetto di orientamenti etici che è stato pubblicato per la prima volta nel Dicembre del 2018 e successivamente alla consultazione di soggetti portatori di interessi e a riunioni con i rappresentanti degli Stati membri, il documento è stato ripresentato modificato nel marzo del 2019: https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/it/pdf.

[65] Si veda il paragrafo 2.2 del presente capitolo '*L'Alleanza Europea per l'Intelligenza Artificiale',* in cui si spiega che cosa è e come nasce l'Alleanza Europea per l'IA.

un'intelligenza artificiale affidabile è importante che l'IA sia conforme alla legge, ai principi e deve manifestare robustezza, sulla base di ciò nonché sulla base dei valori europei[66], gli orientamenti etici precisano i sette requisiti che permettono di qualificare una intelligenza artificiale come affidabile.

3.1. I requisiti fondamentali per un'Intelligenza Artificiale affidabile

I requisiti che in questo paragrafo si andranno ad analizzare sono applicabili ai diversi sistemi di intelligenza artificiale a prescindere dal contesto e dai settori in cui l'IA è impiegata, ma è bene tenere anche presente l'ambito concreto in cui il sistema si inserisce, anche al fine di valutare l'impatto che ne scaturisce.

Il primo requisito individuato e spiegato all'interno della Comunicazione 8 Aprile 2019 e che la Commissione appoggia è definito come *'intervento e sorveglianza umani'*. Partendo dal presupposto che il benessere dell'essere umano è al centro dell'attenzione per quanto concerne l'efficienza del sistema di IA, si consta come la sorveglianza umana svolge la funzione di evitare che detti sistemi siano la causa di conseguenze negative. Le misure di controllo sono rapportate al tipo di sistema a cui si applicano in concreto e al puntuale contesto di utilizzo del medesimo. La sorveglianza umana può essere attuata attraverso meccanismi di governance che consentono un approccio con intervento umano, con supervisione umana o con controllo umano[67].

[66] Come si specifica nella sezione 2 della Comunicazione 8 Aprile 2019 che si sta in questa sede analizzando, l'UE si basa su valori quali quelli indicati nell'articolo 2 del TUE ossia il rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze. Inoltre, come si specifica nella sezione 2 della presente Comunicazione, la Carta dei diritti fondamentali dell'UE racchiude tutti i diritti personali, civici, politici, economici e sociali delle persone all'interno dell'UE.

[67] Commissione Europea, *'Creare fiducia nell'intelligenza artificiale'*, *op cit.*. 4 e 5. Inoltre sono qui indicate tre forme di sorveglianza che richiedono una spiegazione più approfondita, infatti con il termine *human-in-the-loop* (in italiano approccio con intervento umano) ci si riferisce all'intervento umano in ogni ciclo decisionale del sistema, bisogna però tenere a mente che ciò in molti casi non solo non è possibile ma nemmeno sperabile; invece con l'espressione *human-on-the-loop* (in italiano approccio con supervisione umana) si intende la possibilità di intervento umano durante la fase di progettazione del sistema e di monitoraggio del funzionamento del medesimo; infine con l'espressone *huma-in-command* (in italiano approccio con controllo umano) si intende da un lato la capacità di sorvegliare l'attività complessiva del sistema IA, dall'altro la capacità di decidere quando e come utilizzare il sistema in una particolare situazione.

Il secondo requisito è *'robustezza tecnica e sicurezza'*. Con il termine robustezza si fa riferimento alla necessità che i sistemi di IA siano in grado contrastare errori o distorsioni e perché ciò sia possibile l'IA non solo deve essere affidabile ma anche resiliente, tanto agli attacchi evidenti tanto ai tentativi celati di raggiri di dati o algoritmi, e deve anche prevedere un piano di emergenza per fronteggiare i problemi che in concreto possono nascere. Inoltre, sempre avendo riguardo il sopra riportato requisito, nella comunicazione si aggiunge che devono essere previsti meccanismi di sicurezza a partire dalla fase di progettazione[68].

Il terzo requisito che rende un'intelligenza artificiale affidabile è la *'riservatezza e governance dei dati'*, queste due caratteristiche chiedono che sia garantita la riservatezza e la tutela dei dati gestiti dal sistema di IA e che ciò avvenga in ogni fase in cui questi sono impiegati. Bisogna avere coscienza del fatto che l'IA ha la facoltà di desumere le preferenze, l'età e il genere, come anche l'orientamento sessuale, politico e religioso e ciò attraverso l'analisi degli atteggiamenti degli individui.[69] È inoltre bene tenere in considerazione che dai dati che vengono sfruttati dal sistema IA possono derivare condizionamenti sociali così come anche inesattezze, errori e vizi materiali, poiché se i dati raccolti e impiegati presentano tali caratteristiche, allora verranno riprodotte negli *output* dall'IA. Per questa ragione i problemi menzionati devono essere risolti prima che il set di dati venga impiegato per istruire il sistema stesso e perché ciò sia garantito è anche essenziale che i dati usati siano integri e che sia regolato in modo completo l'accesso ai medesimi[70].

Il quarto requisito imprescindibile è la *'trasparenza'*. Trasparenza significa necessità di tracciare i processi che sono stati svolti dall'algoritmo per giungere ad una specifica ed individuata decisione, ma anche necessità di registrare le decisioni a cui il sistema di IA

[68] Commissione Europea, *'Creare fiducia nell'Intelligenza artificiale', op. cit* 5. In questo contesto deve anche prospettarsi la possibilità di ridurre, quanto più possibile, e rendere reversibili gli effetti non voluti o gli errori nel funzionamento dell'IA, è anche bene individuare meccanismi che siano capaci di chiarire e valutare i rischi scaturenti dall'impiego dei sistemi stessi, in relazione alla loro concreta applicazione.
[69] E' fondamentale che i cittadini europei possano riporre fiducia nei sistemi di intelligenza artificiale e perché ciò sia possibile deve essere loro assicurata la totale gestione dei dati personali e inoltre deve essergli garantito che dall'impiego di tali dati non ne derivino danni o discriminazioni.
[70] Commissione Europea, *'Creare fiducia nell'Intelligenza artificile' op cit.* 5, 6.

è pervenuto[71]. In questo contesto dovrebbe essere poi messo in conto che l'algoritmo dovrebbe essere spiegabile e che tale spiegazione deve essere commisurata alle persone destinatarie della decisione assunta[72]. Da ultimo bisogna tenere a mente che è importante la comunicabilità delle competenze e dei limiti del sistema IA ai titolari di interessi coinvolti anche solo latamente.

Passando ora al quinto requisito questo è individuato nella necessità di *'Diversità, non discriminazione ed equità'.* Per comprendere che cosa questo presupposto di affidabilità richiede al sistema di IA è bene aver presente che tanto per l'addestramento quanto per il funzionamento dell'IA viene impiegato un set di dati che può essere inficiato da condizionamenti storici, carenza e campioni di governance di dati che non sono adeguati, e se tali problematiche persistono possono sfociare in discriminazioni, dirette o indirette.[73] Sono state pensate diverse soluzioni alle difficoltà ora evidenziate, come ad esempio gruppi di progettazione diversificati e la creazione di meccanismi per assicurare la partecipazione dei portatori di interessi allo sviluppo dell'IA.

Il penultimo requisito è *'Benessere sociale e ambientale[74]'.* È fondamentale considerare il fatto che il sistema di IA può avere un impatto ambientale e che tale impatto può essere valutato in una prospettiva individuale oppure collettiva cioè l'impatto che l'intelligenza artificiale ha sulla società nel suo complesso. Le applicazioni di IA possono contribuire ad apportare un miglioramento delle competenze sociali ma può essere anche la causa di

[71] La trasparenza del sistema di IA è garantita anche attraverso un'ulteriore azione ossia deve essere fatta una descrizione della raccolta e dell'etichettatura dei dati, inoltre deve anche essere descritto l'algoritmo che l'IA impiega. Un problema concernente la trasparenza è data dalla difficoltà di spiegabilità, proprio per questo dovrebbero essere previste delle spiegazioni circa il come e in che misura l'IA influenza il processo decisionale, le scelte circa la progettazione dell'applicazione di IA nonché circa il criterio della sua diffusione, in questo modo si assicura anche la trasparenza dei modelli di business.

[72] Commissione Europea, *'Creare fiducia nell'Intelligenza artificiale', op cit.* 6. Inoltre si specifica che la ricerca è in questo campo incentrata nel voler individuare meccanismi di spiegabilità degli algoritmi e di come e in che misura l'applicazione di IA incide sul processo decisionale organizzativo. Sul punto, per un maggiore approfondimento si veda: A. Facchini, A. Termine, *'Explainable AI: come andare oltre la black box degli algoritmi', in* Agenda Digitale, 20 Gennaio 2022, https://www.agendadigitale.eu/cultura-digitale/explainable-ai-come-andare-oltre-la-black-box-degli-algoritmi/.

[73] Ibidem nota 72, cit. 6. È anche bene precisare che causa di un danno può essere una sleale concorrenza, l'abuso dei condizionamenti dei consumatori dell'applicazione di IA nonché i condizionamenti che si sono insidiati nel processo di sviluppo dell'IA; come precisa la Commissione, le preoccupazioni connesse a tali cause dovrebbe essere prese in considerazione fin dal principio.

[74] Per un maggiore approfondimento si veda: L. Floridi, *'In poche batture. Brevi riflessioni su cultura e digitale 2011-2021'*, Gennaio 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3998228; in particolare pp. 335-339.

un loro danneggiamento. Un'intelligenza artificiale affidabile dovrebbe, quindi, rispettare l'ambiente in cui si inserisce e gli esseri senzienti coinvolti dal suo funzionamento[75].

Da ultimo viene indicato, quale requisito ai fini del raggiungimento dell'obiettivo di predisporre sistemi di IA affidabili, l'*'Accountability'*. Con questo requisito si chiede che siano individuati meccanismi volti ad assicurare la responsabilizzazione dei sistemi e dei risultati raggiunti da essi. In questo contesto si chiede che il sistema sia verificabile tanto a livello interno quanto esterno, la verificabilità esterna dovrebbe essere maggiormente garantita per le attuazioni di IA che condizionano i diritti fondamentali degli individui. Da questo punto di vista, uno degli obiettivi che deve essere perseguito e raggiunto è la minimizzazione dei potenziali impatti negativi, tenendo in considerazione che questo sviluppo è agevolato dall'utilizzo di valutazioni di impatto che dovrebbero essere rapportate ai rischi che possono derivare dal sistema di IA concretamente utilizzato[76]. Quanto detto non impedisce che possano emergere dei conflitti tra i vari requisiti ma questi dovrebbero essere risolti con l'uso della ragione e seguendo un metodo oggettivo. Il requisito ora definito è volto a rendere affidabile il sistema IA come gli altri sopra elencati e descritti, ciò nonostante non si può escludere la possibilità che si verifichi un impatto negativo, e proprio per questo dovrebbero anche essere ipotizzati idonei mezzi di riparazione.

4. Il libro Bianco sull'intelligenza artificiale (Commissione Europea 19.02.2020)- *un approccio europeo all'eccellenza e alla fiducia*

Il 19 Febbraio 2020 è stato pubblicato, dalla Commissione, il Libro Bianco sull'intelligenza artificiale con il duplice obiettivo di immettere nel mercato sistemi di intelligenza artificiale affidabili e di far fronte ai rischi connessi a determinate applicazioni dei medesimi[77]. Il Libro Bianco che si vuole analizzare promuove strategie

[75] Commissione Europea, *'Creare fiducia nell'intelligenza artificiale'*, *op. cit.* 6, 7. Con essere senziente la Commissione intende non soltanto gli esseri umani che si interfacciano nel presente con l'IA ma anche le future generazioni le quali devono aver la possibilità di godere della biodiversità di un habitat, di conseguenza le applicazioni di IA devono essere sostenibili e la responsabilità ecologica dovrebbe essere incentivata.

[76] Ibidem nota 75, cfr. p 7-8.

[77] Nel Libro Bianco la Commissione indica in modo puntale i soggetti che godono dei benefici che derivano dai sistemi di IA e che di conseguenza sono esposti ai rischi del loro utilizzo, questi soggetti sono i cittadini, le imprese che li potranno impiegare per agevolare il loro sviluppo e i servizi di pubblico interesse.

comuni, a livello europeo, in ambito di IA volte ad impedire la frammentazione del mercato unico[78]. È fondamentale intervenire su più livelli se si vogliono raggiungere gli obiettivi appena individuati, quindi affinché sia creato un ambiente idoneo a promuovere lo sviluppo e l'adozione dell'IA vengono indicati, all'interno del Libro Bianco, gli aspetti che devono essere migliorati.

Tra le azioni più rilevanti individuate dalla Commissione Europea, vi è quella volta a concentrare gli sforzi della Comunità della ricerca e dell'innovazione per creare un centro di ricerca, innovazione e competenza in grado di collegare gli sforzi delle diverse Nazioni e impedire che si mantenga l'attuale frammentazione dei centri in questione, nessuno dei quali è in grado di concorrere con quelli presenti a livello mondiale. Di pari importanza è anche la prospettazione di siti per la sperimentazione che consentono la futura diffusione di nuove forme di Intelligenza Artificiale[79]. Come pure prestare attenzione alle Piccole e Medie Imprese di modo tale che possano usufruire dei benefici derivanti dai sistemi di IA, e perché ciò sia possibile bisogna consolidare i poli di innovazione digitale[80] e la piattaforma di IA on demand[81] oltre che incentivare la cooperazione tra le stesse. Deve anche essere istituito un partenariato pubblico-privato per consentire il pieno coinvolgimento del settore privato nell'esplicazione dell'agenda per la ricerca e l'innovazione e anche perché possa contribuire ai coinvestimenti, i quali hanno un ruolo più che fondamentale per la creazione e lo sviluppo di nuove applicazioni di IA. Come nel settore privato, anche nel settore pubblico deve essere promosso l'uso di sistemi di IA, in particolare è importante che siano adottati dalle pubbliche amministrazioni, dagli ospedali, dai servizi di utilità pubblica e di trasporto e dalle autorità che si occupano di vigilanza finanziaria. Essendo l'Intelligenza Artificiale una tecnologia che accosta dati, algoritmi e potenza di calcolo, tra le azioni fondamentali per il raggiungimento degli obiettivi sopra riportati vi è anche la necessità di assicurare l'accesso ai dati e alle strutture

[78] Per completezza si confrontino i due documenti allegati al presente che si sta analizzando, ossia la strategia europea per i dati che vuole rendere l'economia agile europea quanto più attraente, sicura e dinamica. E la relazione della Commissione che accompagna sempre il medesimo libro bianco e nella quale si analizzano le complicazioni legate all'IA, all'internet delle cose e ad altre tecnologie digitali, di modo tale che sia predisposta un'adeguata disciplina in materia di sicurezza e responsabilità.

[79] Anche la PESCO ossia il Fondo europeo per la difesa e la cooperazione strutturata permanente permetterà di fare ricerca in ambito di intelligenza artificiale.

[80] Cfr.: ec.europe.eu/digital-single-market/en/news/digital-innovation-hubs-helping-companies-across-economy-make-most- digital-opportunities.

[81] Cfr.: www.Ai4eu.eu.

di calcolo, di conseguenza deve essere migliorato l'accesso ai medesimi così come il loro controllo, e nel fare ciò devono essere rispettati i principi di FAIR[82], in caso contrario diviene difficile dar vita ad una IA affidabile. Bisogna anche ricordare che quanto svolto, fino al momento della stesura del Libro Bianco dall'Unione Europea, ha influenzato il dibattito internazionale, infatti, il gruppo di esperti di alto livello, per sviluppare gli indirizzi etici si è avvalso del parere di diverse organizzazioni internazionali nonché di osservatori governativi. A sua volta l'Unione Europea è stata chiamata in aiuto per coadiuvare l'OCSE nell'individuazione dei principi etici per l'IA, approvati in seguito dal G20. Anche in questo contesto la Commissione ritiene che la collaborazione internazionale debba rispettare i diritti fondamentali con lo scopo di promuovere i valori propri dell'UE in tutto il mondo. L'azione principale ai fini della trattazione e promossa dalla Commissione all'interno del Libro Bianco è creare un ecosistema di fiducia e per fare ciò è necessario dar vita ad un quadro normativo in grado di regolare in modo efficiente l'intelligenza artificiale. Come più volte specificato le applicazioni dotate di intelligenza artificiale implicano sia benefici che rischi[83], e questi ultimi in particolare fanno emergere la necessità di un intervento legislativo; ad oggi sono presenti normative ma prestano tutela solo per alcuni aspetti concernenti tali tecnologie, basti pensare alla regolamentazione in materia di Privacy o a tutela dei dati, le quali devono essere applicate da coloro che sviluppano e applicano l'IA. Anche per la tutela dei consumatori è presente una normativa, nonché norme attinenti la responsabilità e la sicurezza dei prodotti, in forza di queste i consumatori pretendono la medesima protezione sia che il prodotto o il sistema si basi sull'IA sia che non si basi sulla medesima. Tale pretesa non tiene conto delle difficoltà che sono connesse a tale tecnologica, infatti è bene ricordare che peculiari aspetti dell'IA rendono impossibile garantire la medesima protezione, basti pensare al

[82] I principi cui allude la Commissione sono quelli indicati nel piano d'azione predisposto dal gruppo di esperti della Commissione, confrontabile al presente link: https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf. In particolare i dati devono essere reperibili, accessibili, interoperabili e riutilizzabili nel rispetto cioè dei principi di *Findable, Accessible, Interoperable and Reusable.*

[83] I principali timori dei cittadini, quali fruitori di queste tecnologie, sono legati alla paura di non aver a disposizione un adeguato mezzo di tutela giuridica per i loro diritti e la loro sicurezza quando questi siano messi a rischio dalle asimmetrie informative che si palesano nel processo decisionale dell'algoritmo; inoltre hanno anche il timore che questa tecnologia venga sfruttata per causare effetti non voluti o per scopi dolosi. Le imprese dal canto loro temono per l'incertezza giuridica.

problema dell'opacità[84]. I problemi legati alle applicazioni di IA spingono a porsi diversi interrogativi, se cioè la legislazione presente è idonea e applicata in modo efficace o se invece siano opportune modifiche o la prospettazione di una nuova legislazione in materia[85]. Le considerazioni ora riportate fanno emergere la consapevolezza che un quadro normativo adeguato può efficacemente tutelare i cittadini europei oltre che eliminare le frammentazioni del mercato che favorirà a sua volta lo sviluppo e l'adozione dell'IA.

4.1. I rischi connessi all'utilizzo di sistemi di Intelligenza Artificiale

Importante argomento oggetto dell'analisi della Commissione nel Libro Bianco sull'Intelligenza Artificiale, sono i rischi che possono emergere dall'applicazione di specifici sistemi di IA. Prima di analizzare i tipi di rischi nello specifico la Commissione Europea rammenta che dalle applicazioni di IA possono derivare danni alla persona che ne fa' uso, questi danni si dividono in due tipologie, da un lato si può trattare di danni materiali i quali colpiscono la salute e la sicurezza dell'individuo, dall'altro lato può verificarsi un danno immateriale dal quale possono afferire una pluralità di rischi.

Andando ad analizzare in concreto i rischi, innanzitutto l'impiego di IA può compromettere i valori su cui si fonda l'UE nonché i diritti fondamentali[86]. Diverse le cause dei rischi appena richiamati, ci possono essere dei vizi derivanti da un problema di progettazione del sistema, ma il rischio può anche scaturire dal fatto che l'IA sfrutta dati dai quali non sono state eliminate le distorsioni. Così i dati utilizzati, le procedure di

[84] Quando si allude al problema dell'opacità dell'Intelligenza artificiale si fa riferimento al fatto che la struttura dei modelli che vengono impiegati per addestrare l'applicazione di IA, in particolare il *machine learning,* è molto complessa e rende difficile, e in alcuni casi impossibile, la sua comprensione da parte dell'utente umano, di conseguenza ne è difficile anche la spiegazione del funzionamento. Cfr.: A. Facchine e A. Termine, *'Explainable AI: come andare oltre la Black box degli algoritmi.', in* Agenda Digitale, 20 Gennaio 2022, https://www.agendadigitale.eu/cultura-digitale/explainable-ai-come-andare-oltre-la-black-box-degli-algoritmi/.

[85] Cfr. paragrafo 1 del presente capitolo, *' Trovare rimedi alla presente anomia: il quadro normativo attuale tra GDPR e LED.*

[86] L'impatto che l'intelligenza artificiale ha sui diritti fondamentali sarà meglio preso in considerazione nel paragrafo 5 del presente capitolo. Si tenga in questa sede presente che sono compresi il diritto alla libertà di espressione e di riunione, la dignità umana, la non discriminazione fondata sul sesso, sulla razza, sull'origine etnica, sulla religione o sulle convinzioni personali, sulla disabilità, sull'età o sull'orientamento sessuale, la protezione dei dati personali e della vita o il diritto a un ricorso giurisdizionale effettivo e a un giudice imparziale, nonché la tutela dei consumatori. A riguardo del diritto alla protezione dei dati personali la Commissione si si incarica di monitorare la corretta applicazione e il rispetto del Regolamento generale sulla protezione dei dati personali (GDPR), cfr. paragrafo 1 del presente capitolo.

progettazione e applicazione e l'intervento umano possono a loro volta influire su diritti fondamentali come la libertà di espressione, la tutela dei dati personali e della privacy ma anche sulle libertà politiche. Attinente in modo specifico alla analisi che si sta portando avanti, si può evidenziare come certe applicazioni di IA di analisi facciale rispecchiano le distorsioni connesse al genere e alla razza, è per questo che sono più facilmente in grado di riconoscere il genere maschile di pelle chiara, e incorrono in un numero maggiore di errori quando il sistema deve esaminare il volto di una donna di pelle scura.[87] Per comprendere a pieno i problemi connessi ai rischi che scaturiscono dalle applicazioni di IA si può ragionare in tal senso, quando un essere umano è chiamato a prendere una decisione c'è la possibilità che commetta errori, se questo avviene e questi errori o distorsioni vengono trasmesse al sistema di IA, l'Intelligenza Artificiale li amplifica esponenzialmente.[88] L'opacità, la complessità, l'imprevedibilità e la scarsa partecipazione umana rendono molto complicato il rispetto della legislazione UE in tema di diritti fondamentali[89].

I rischi per i diritti fondamentali non sono i soli che possono derivare dalle applicazioni di IA e che vengono evidenziati dalla Commissione Europea, infatti possono anche sussistere rischi per la sicurezza e il funzionamento vantaggioso di un idoneo regime di responsabilità. I rischi per la sicurezza sorgono da Intelligenze Artificiali che sono inserite in prodotti e servizi[90] e ciò è anche causa della mancanza di disposizioni in materia, da questo può anche derivare incertezza giuridica per le imprese che diffondono sistemi intelligenti nel territorio dell'Unione Europea. Con riferimento ai rischi che si stanno ora vedendo si pone il medesimo problema che si pone nel contesto dei rischi per i diritti fondamentali perché anche in questo ambito è difficile se non impossibile risalire alle decisioni dannose prese dai sistemi dotati di IA, infatti per aver chiaro ciò basti tener

[87] J. Buolamwini, T. Gebru, '*Proceedings of the 1st Conference on Fairness, Accountability and Transparency'* (Atti della 1ª conferenza sull'equità, sulla responsabilità e sulla trasparenza), PMLR 81:77-91, 2018.

[88] Per questa ragione sono presenti meccanismi di controllo sociale volti a regolare il comportamento umano, ad esempio l'Unione Europea ha adottato una strategia per le pari opportunità 2020-2024 che si concentra sul rapporto tra IA e parità di genere.

[89] Cfr. Commissione Europea COM(2020) 65 final, *'Libro Bianco sull'intelligenza artificiale- un approccio europeo all'eccellenza e alla fiducia',* 19 Febbraio 2020, p. 12-13.

[90] Basti pensare alla macchina a guida automatica, la quale può causare un incidente per un errore nella progettazione della tecnologia di riconoscimento degli oggetti e portare l'auto a male identificare un oggetto in strada.

presente che in molte situazioni è arduo per la persona ottenere gli elementi probatori necessari per agire in giudizio, ad aggravare il quadro descritto vi è il fatto che i rischi di cui si sta dicendo si ampliano con l'aumento della circolazione di applicazioni di IA[91].

4.2. Ambito di applicazione del futuro quadro normativo dell'UE e le intelligenze artificiali ad alto rischio

Questione cruciale è individuare l'ambito di applicazione del futuro quadro normativo dell'UE, per far ciò è necessario aver presente che ad oggi è vigente un quadro giuridico volto ad assicurare la tutela dei consumatori, fornire una protezione innanzi a pratiche commerciali sleali, ma anche salvaguardare i dati personali e la privacy dell'individuo, di conseguenza quanto disciplinato nella regolamentazione attuale, orizzontale e di settore, verrà ancora disciplinato da questa, una volta apportate le giuste modifiche di adeguamento al contesto.

Il nuovo quadro normativo, a disciplina dell'IA, che verrà istituito dall'Unione Europea seguirà un approccio basato sui rischi di modo tale da poter creare un equilibrio tra la necessità di raggiungere specifici obiettivi e non imporre oneri troppo gravosi. Tale approccio distingue tra le diverse applicazioni di intelligenza artificiale cioè a seconda che l'IA sia '*ad alto rischio'* o meno.[92] Gli elementi che la Commissione ritiene fondamentali per qualificare un sistema di IA come ad alto rischio sono: gli interessi in gioco in relazione all'ambito di impiego dell'applicazione di IA e l'uso a cui questa è destinata, se cioè questo coinvolge rischi rilevanti o meno. In particolare il sistema di IA è qualificato ad alto rischio se presenta due criteri, entrambi i quali devono essere soddisfatti, la presenza di uno ma non dell'altro non consente di definire l'IA ad alto rischio. In primo luogo è il settore in cui viene impiegata l'applicazione a consentire di definirla ad alto rischio, se cioè vi sono connessi rischi rilevanti allora è tale, in caso contrario no[93]. In secondo luogo è il modo in cui l'applicazione viene impiegata nel

[91] Commissione Europea, *'Libro Bianco sull'intelligenza artificiale- un approccio europeo all'eccellenza e alla fiducia', op. cit.* 13-14.

[92] Ibidem nota 91, p. 19. Inoltre per completezza è bene specificare che i rischi possono essere classificati anche diversamente da come qui indicato, infatti la legislazione dell'UE può procedere ad una loro qualificazione in base al settore in cui vengono in essere e quindi in cui vengono impiegate le applicazioni di IA.

[93] La Commissione specifica che i settori che comportano l'individuazione di IA ad alto rischio dovrebbero essere puntualmente indicati nel nuovo quadro normativo, in particolare quali esempi sono riportati i settori

settore specifico a determinare il modo in cui la medesima viene identificata, se cioè comporta, il modo in cui viene utilizzata, rischi significativi allora è un'intelligenza artificiale ad alto rischio. La sussistenza di entrambi i criteri sopra descritti permette di individuare l'ambito di applicazione del futuro quadro normativo e a far si che questo sia volto ad assicurare la certezza del diritto. Per completezza è bene far presente che vi sono sistemi di IA che devono essere, a prescindere, considerati ad alto rischio, senza l'esigenza di verificare in concreto la sussistenza dei due criteri rammentati[94], tra queste applicazioni vi è anche il sistema di identificazione biometrica da remoto[95]; di conseguenza si tratta di sistemi intelligenti che necessitano sempre e comunque dell'applicazione della disciplina che si andrà ora ad esaminare e approfondire.

Andando a prendere in considerazione le prescrizioni che devono essere applicate ai sistemi di IA ad alto rischio, i primi elementi essenziali che abbisognano di una disciplina puntuale sono i dati utilizzati per l'addestramento dell'IA. I dati sono una componente fondamentatale nel funzionamento di un'intelligenza artificiale, infatti il set di dati impiegato influenza il *modus operandi* dell'applicazione nonché le decisioni che da questa vengono prese, di conseguenza è essenziale prevedere disposizioni che siano in grado di tutelare i valori e la regolamentazione UE. Così nel Libro Bianco vengono indicate tre prescrizioni che si potrebbero adottare con riferimento al richiamato elemento essenziale e cioè, in primo luogo, regole che introducano garanzie per mettere in sicurezza l'utilizzo successivo che, di prodotti e servizi incentrati sull'IA[96], si fa'. In secondo luogo prescrizioni che prevedano l'obbligo di individuare misure che hanno l'obiettivo di

dell'assistenza sanitaria, dei trasporti; dell'energia e del settore pubblico, quest'ultimo potrebbe ricomprendere anche ambiti ulteriori quali il diritto di asilo, la migrazione… La Commissione specifica anche l'importanza di un continuo aggiornamento di detto elenco.

[94] A seconda del settore di impiego del sistema di IA, congiuntamente al quadro normativo di specifica applicazione per le IA ad alto rischio, potrebbero essere applicate anche altre normative dell'Unione Europea, basti, ad esempio, pensare all'uso dell'intelligenza artificiale inserita in prodotti di consumo, in questo caso può essere applicata anche la Direttiva sulla sicurezza generale.

[95] Quando si fa riferimento all'identificazione biometrica da remoto, questa deve essere tenuta distinta dall'autenticazione biometrica che è una tecnica utilizzata per verificare che la persona sia chi effettivamente afferma di essere. L'identificazione biometrica è invece volta a constatare l'identità attraverso l'analisi di identificatori biometrici, come ad esempio l'iride, il volto, immagini del volto…, e questo può avvenire anche da remoto come ad esempio in uno spazio pubblico, in questo modo i dati raccolti vengono poi confrontati con quelli conservati in una banca dati.

[96] La Commissione chiarisce che in questo caso è richiesto il rispetto degli standard stabiliti dalla disciplina dell'Unione Europea in materia di sicurezza, le quali sono disposizioni volte a garantire che le applicazioni di IA siamo addestrate attraverso set di dati vasti e che tengano in considerazione di quante più situazioni possibili.

assicurare che tale uso successivo di queste tecnologie non conduca a discriminazioni.[97] In terzo luogo la Commissione ritiene sia necessaria una disciplina peculiare per la tutela della privacy e dei dati personali quando si fa uso di sistemi dotati di IA[98].

Proseguendo nella disamina degli elementi essenziali dell'intelligenza artificiale, la Commissione ritiene debbano anche essere istituite prescrizioni per regolare la tenuta dei registri, concernenti la programmazione dell'algoritmo impiegato dall'IA, i dati impiegati per il suo addestramento quando è ad alto rischio e per la conservazione dei dati stessi (ma questo solo in taluni casi). Date le difficoltà legate alla complessità e all'opacità dell'intelligenza artificiale, questa disciplina vuole agevolare l'individuazione delle azioni nonché delle decisioni, che sono causa di problemi, per poterle verificare. La tenuta dei registri non può essere illimitata ma deve avvenire solo per un periodo circoscritto e adeguato a garantire che sia rispettata la legislazione di riferimento[99].

Un terzo elemento essenziale per promuovere un uso responsabile dell'IA, per incrementare la fiducia dei fruitori e facilitare la riparazione del danno, è la predisposizione di una disciplina volta a far rispettare gli obblighi di informazione, e a tal fine potrebbero essere presi in considerazione due esempi di prescrizioni, da un lato quelle che garantiscano che siano fornite le giuste informazioni circa ciò di cui è capace il sistema di IA e ciò di cui non è capace. Dall'altro lato, devono essere previste prescrizioni per garantire che i cittadini siano messi al corrente del fatto che si stanno relazionando con un'intelligenza artificiale[100], oltre il fatto che tali informazioni devono essere comprensibili al destinatario e appropriate al contesto.

---

[97] Tali disposizioni potrebbero imporre l'obbligo di utilizzo di set di dati di addestramento che siano rappresentativi in modo da contemplare i diversi generi, etnie…

[98] Commissione Europea, *'Libro Bianco sull'intelligenza artificiale- un approccio europeo all'eccellenza e alla fiducia', op. cit.* 21. Inoltre si tenga presente che in questo caso la normativa di riferimento è il Regolamento generale sulla protezione dei dati personali (GDPR) e la Direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (LED).

[99] Ibidem 98, p. 21-22.

[100] Ibidem nota 99, p. 22. La disciplina contenuta nel GDPR è insufficiente in diversi casi e potrebbe quindi essere necessaria una disciplina più specifica e ulteriore, infatti l'articolo 13, paragrafo 2, lettera f), del GDPR, stabilisce che nel momento in cui i dati personali sono ottenuti, il titolare del trattamento è tenuto a fornire agli interessati ulteriori informazioni necessarie a garantire un trattamento corretto e trasparente in relazione all'esistenza di un processo decisionale automatizzato, oltre a determinate informazioni aggiuntive.

Il quarto elemento essenziale di un sistema di IA, e in particolare dei sistemi ad alto rischio, è la robustezza e la precisione, così la Commissione specifica la necessità che questi due elementi siano adeguatamente regolamentati al fine di garantire che l'IA sia affidabile e perché sia minimizzata la possibilità di danni. Per raggiungere questo scopo, nel Libro Bianco, si identificano degli elementi rilevanti e che potrebbero essere presi in considerazione, tra questi si configurano le disposizioni che consentono che i risultati siano riproducibili e altre che consentono ai sistemi di IA di gestire errori ed incongruenze.

Procedendo nell'analisi delle prescrizioni, la Commissione evidenzia il fondamentale ruolo svolto dalla sorveglianza umana per evitare che si infici l'autonomia dell'uomo, chiaro è che il livello di sorveglianza dipende dall'uso a cui l'applicazione di IA è destinata e dalle conseguenze che possono scaturire per coloro che le utilizzano[101]. Prescrizioni specifiche sono previste per l'identificazione biometrica da remoto, la quale avviene, ad esempio, attraverso sistemi di riconoscimento facciale che vengono disposti in luoghi pubblici, tali sistemi raccolgono e impiegano i dati biometrici[102] e mediante queste azioni l'intelligenza artificiale è in grado di identificare[103] la persona. È bene ricordare che le norme dell'Unione Europea a tutela dei dati vietano che i dati biometrici siano impiegati per identificare un soggetto univocamente, in particolare la normativa di riferimento è il GDPR che ponendo il divieto di cui si è appena detto provvede a consentire tale azione dell'intelligenza artificiale soltanto a determinate e specifiche condizioni.[104] Di conseguenza l'identificazione biometrica da remoto è vietata in termini generali dalla normativa europea vigente, ma può essere impiegata quando il suo utilizzo sia motivato, proporzionato e siano applicate le idonee garanzie. I principali timori a

[101] La Commissione, nel Libro Bianco, ipotizza diversi modi in cui può svolgersi la sorveglianza umana e questi sono: porre a condizione, a che la decisione presa dall'applicazione di IA divenga effettiva, la necessità che sia rivista e approvata da un essere umano; altrimenti la sorveglianza umana può svolgersi successivamente ossia dopo che la decisione presa dal sistema sia divenuta effettiva; ancora L'intelligenza artificiale può essere supervisionata in tempo reale dall'essere umano che ha la facoltà di disattivarla quando ritiene che ciò sia opportuno; infine possono essere previsti vincoli operativi al sistema in fase di progettazione.

[102] Cfr. paragrafo 1.1 *'La rilevanza della definizione della puntuale disciplina dei dati biometrici',* del presente capitolo.

[103] L'identificazione avviene attraverso il confronto tra il *template* (ossia il modello) dell'immagine del viso di un soggetto e i diversi altri riferimenti contenuti in una banca dati con l'obiettivo di far emergere una corrispondenza.

[104] Cfr. articolo 9 GDPR e l'articolo 10 della LED.

livello sociale, in relazione all'utilizzo dell'IA di cui si è appena detto, è relativo all'impiego di tali sistemi in luoghi pubblici ed è per questo che la Commissione si era posta l'obiettivo di intraprendere un dibattito europeo per individuare le condizioni al verificarsi delle quali è consentito tale uso e le garanzie che dovranno necessariamente essere apprestate ai cittadini.

5. La Carta dei diritti fondamentali nel contesto dell'intelligenza artificiale e della trasformazione digitale: conclusioni del Consiglio dell'Unione Europea (21 Ottobre 2020)

In tale paragrafo si apre la prospettiva di un'analisi dettagliata dell'impatto che l'Intelligenza artificiale ha sui diritti fondamentali, previsti all'interno della Carta dei diritti fondamentali, e dei valori su cui l'UE si fonda, individuati all'interno dell'articolo 2 del Trattato sull'Unione Europea. Il documento che si prende in considerazione individua le conclusioni della Presidenza del Consiglio dell'UE in relazione alla Carta dei diritti fondamentali nel contesto dell'intelligenza artificiale e della trasformazione digitale. In fase introduttiva il gruppo FREMP[105] puntualizza la necessità di assicurare il rispetto dell'articolo 21 della Carta, il quale vieta ogni forma di discriminazione[106]; rinnova l'adesione dell'Unione Europea alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali; inoltre l'UE si impegna a supportare la parità di genere, i diritti delle donne e a far fronte alla violenza sulle donne e domestica; infine si ricorda l'importanza della Convenzione di Istanbul del Consiglio d'Europa, che al tempo in cui fu' pubblicato il documento in analisi era stata ratificata da 21 Stati membri (ad oggi sono 32). Il Consiglio sottolinea l'apprensione relativa alla possibile emersione di rischi per i diritti fondamentali, la democrazie e lo stato di diritto, derivanti da un utilizzo inadeguato dei sistemi dotati di IA, di conseguenza si evidenzia l'importanza di

[105] Il Gruppo FREMP è il gruppo diritti fondamentali, diritti dei cittadini e libera circolazione delle persone. Tratta le questioni relative alla Carta dei diritti fondamentali dell'Unione Europea e gestisce i negoziati inerenti l'adesione dell'UE alla Convenzione Europea dei diritti dell'uomo (CEDU). Per maggiori informazioni si può consultare la pagina al presente link: https://www.consilium.europa.eu/it/council-eu/preparatory-bodies/working-party-fundamental-rights-citizens-rights-free-movement-persons/.

[106] L'articolo 21 della Carta dei diritti fondamentali dispone: *'1. È vietata qualsiasi forma di discriminazione fondata, in particolare, sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, gli handicap, l'età o le tendenze sessuali. 2. Nell'ambito d'applicazione del trattato che istituisce la Comunità europea e del trattato sull'Unione europea è vietata qualsiasi discriminazione fondata sulla cittadinanza, fatte salve le disposizioni particolari contenute nei trattati stessi.'*

far fronte alle principali preoccupazioni connesse all'impiego dell'Intelligenza artificiale e cioè le sfide più rilevanti date dall'opacità, la complessità, la faziosità, l'imprevedibilità e una condotta quasi del tutto autonoma, che caratterizzano questa tecnologia. Proteggere e promuovere i diritti fondamentali permette che l'approccio europeo alla trasformazione digitale, e nello specifico all'IA, ponga al centro dell'attenzione l'individuo, consentendo lo sviluppo di un'IA antropocentrica, e la tutela oltre che la promozione dei diritti fondamentali, di modo tale che si dia vita ad applicazioni di IA affidabili.

Per promuovere un approccio antropocentrico dell'IA e che rispetti i diritti fondamentali deve essere osservato l'articolo 52, paragrafo 1, della Carta. Tale articolo chiede che quando siano disposte limitazioni all'esercizio dei diritti e delle libertà fondamentali, tali limitazioni siano conformi ad una finalità di interesse generale riconosciuta dall'UE, siano rispettosi dei diritti e delle libertà altrui oltre che dei diritti e delle libertà fondamentali, del principio di proporzionalità, e infine devono anche essere disposte per legge.

Entrando nel vivo dell'analisi del rapporto che vi è tra l'intelligenza artificiale e i vari diritti fondamentali, in primo luogo la Presidenza del Consiglio d'Europa rimarca l'importanza che l'individuo ha in relazione alle applicazioni dotate di IA, e per creare un'intelligenza artificiale antropocentrica diviene fondamentale osservare la normativa in tema di diritti fondamentali ed in particolare rispettare e tutelare la dignità umana.[107] Per quanto concerne il rapporto tra l'IA e libertà è bene far presente che peculiari applicazioni di intelligenza artificiale consentono a piattaforme online e motori di ricerca di raccogliere e associare i dati stabilendo i contenuti di principale importanza, in questo modo vengono messi a rischio, da un lato il pluralismo e la diversità informativa, e dall'altro lato la facoltà di individuare liberamente i contenuti e le informazioni di interesse. La tutela della libertà di parola, di scambio di vedute, della facoltà di accedere a informazioni diverse e quindi la tutela della società libera richiede un controllo puntuale

[107] Come fa presente Luciano Floridi, la dignità umana è un valore rispettato e tutelato nella disciplina predisposta dalla Proposta di regolamento sull'intelligenza artificiale, e anzi di pone come fondamento etico e fine ultimo. Per un più ampio approfondimento si veda: L. Floridi, *'In poche battute. Brevi riflessioni su cultura e digitale 2022-2021',* Gennaio 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3998228.

di tali applicazioni affinché la libertà non venga da esse pregiudicata. Al contempo tanto in ambito privato, ossia le imprese, quanto in ambito pubblico, in particolare i governi, massificano l'impiego di dati personali e dei sistemi di intelligenza artificiale al fine di svolgere diverse funzioni, e in particolare per analizzare e quindi prevedere il comportamento di un gruppo di soggetti[108]. Il rischio, alla tutela della libertà, che in questi casi può derivare dalle applicazioni di IA è palese e per minimizzare detti rischi è necessario, come evidenza il Consiglio d'Europa, individuare e allestire le adeguate garanzie, le quali consentano il rispetto del GDPR e delle norme nazionali a tutela dei dati personali e dei diritti fondamentali. In tale parte delle Conclusioni che si stanno ora analizzando, la presidenza del Consiglio d'Europa specifica anche l'importanza di individuare i requisiti giuridici che devono necessariamente essere soddisfatti per poter impiegare intelligenze artificiali volte alla sorveglianza di massa e al riconoscimento facciale. Nello specifico devono essere rispettate le norme disposte nel GDPR nonché le disposizioni a tutela della vita privata, in caso contrario non sarebbero rispettati i diritti e le libertà fondamentali, e devono comunque essere assicurati rimedi giurisdizionali effettivi. È infine fondamentale garantire la libertà di espressione e la libertà di informazione e per fare ciò è necessario predisporre meccanismi contro i contenuti illegali online e i reati che sorgono dall'odio[109]. Quanto appena detto consente di creare uno spazio unico europeo in cui i cittadini abbiano la sicurezza di essere tutelati e di vedere rispettati i propri diritti e libertà fondamentali[110].

Il documento in analisi procede considerando il rapporto tra IA e uguaglianza. Anche da questo rapporto si possono trarre, dai sistemi di IA, vantaggi ma anche nuovi rischi a cui dover far fronte, infatti da un lato consente di verificare l'osservanza dei diritti fondamentali in tema di uguaglianza, dall'altro lato si può verificare l'eventualità che

[108] Attraverso i sistemi di intelligenza artificiale è possibile profilare ossia è possibile raccogliere informazioni su un individuo, o un gruppo di individui, per analizzarne e le caratteristiche, suddividerli in gruppi o categorie e poi procedere a valutazioni e previsioni. Per un maggiore approfondimento si veda: M. Di Giulio, *'Profilazione: tutte le sfide dell'intelligenza artificiale affrontate dal GDPR, 'in'* Agenda Digitale, https://www.agendadigitale.eu/sicurezza/privacy/profilazione-tutte-le-sfide-dellintelligenza-artificiale-affrontate-dal-gdpr/.

[109] Relativamente ai reati che scaturiscono dall'odio si può vedere, per un maggiore approfondimento, C. Sarra, *'Il mondo-dato. Saggi su datificazione e diritto',* Padova, Cleup, 2022, pp- 167-210.

[110] Cfr. Presidenza del Consiglio dell'Unione Europea, *'Conclusioni della Presidenza- La Carta dei diritti fondamentali nel contesto dell'Intelligenza artificiale e della trasformazione digitale',* 21 Ottobre 2020, p.7-9.

siano amplificate le discriminazioni.[111] La Presidenza del Consiglio evidenzia che è di rilevante importanza rispettare i principi di uguaglianza e non discriminazione durante l'intero ciclo di vita delle applicazioni dotate di intelligenza artificiale. Questo include la fase di progettazione, di sviluppo, diffusione, utilizzo e la fase finale di valutazione dell'intelligenza artificiale. Tale impegno è volto ad assicurare che siano fronteggiate le possibili distorsioni e che il set di dati impiegato per l'addestramento dell'IA sia conforme allo scopo previsto. Inoltre, le tecnologie dotate di IA, hanno un impatto positivo nel garantire il rispetto dei diritti sociali, ad esempio potenziando la protezione della salute, ma anche in questa possibilità di impiego, come già si è evidenziato, deve essere impiegato un idoneo set di dati di addestramento, che possa cioè assicurare il rispetto della dignità umana, della vita privata e l'integrità fisica, morale e mentale dei soggetti coinvolti, infine si richiede anche il rispetto delle norme a protezione dei dati personali, della privacy e della sicurezza dei dati impiegati[112].

L'ultimo aspetto che in questo documento viene valutato è dato dal rapporto tra IA e giustizia, infatti il Consiglio d'Europa afferma che le applicazioni di IA possono concorrere concretamente a migliorare l'accesso alla giustizia in generale[113]. Nonostante questo, sarà sempre e comunque assicurato l'accesso analogico al diritto e alla giustizia al fine di difendere lo Stato di diritto nell'UE e nei suoi Stati membri.[114]

6. La proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (21 Aprile 2021)

[111] Per un maggiore approfondimento si veda: Opinion of Advisory Committee on Equal Opportunities for Women and Men, 18 March 2020, *'Opinion on Artificial Intelligence- opportunities and challenges for gender equality'*, https://commission.europa.eu/system/files/2020-04/opinion_artificial_intelligence_gender_equality_2020_en.pdf.

[112] Presidenza del Consiglio dell'Unione Europea, *'Conclusioni della Presidenza- La Carta dei diritti fondamentali nel contesto dell'Intelligenza artificiale e della trasformazione digitale', op. cit.* 11.

[113] Con accesso alla giustizia in generale si fa riferimento alla necessità di assicurare la trasparenza e la spiegabilità dei processi giudiziari nonché del processo decisionale; significa anche indipendenza del giudice e certezza giuridica.

[114] Presidenza del Consiglio dell'Unione Europea, *'Conclusioni della Presidenza- La Carta dei diritti fondamentali nel contesto dell'Intelligenza artificiale e della trasformazione digitale', op. cit.* 12-14. Inoltre Cfr. Conclusioni del Consiglio, 14 Ottobre 2020, *'Accesso alla giustizia – Cogliere le opportunità della digitalizzazione'*, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:C:2020:342I:FULL&from=EN.

La rassegna cronologica in questo capitolo analizzata culmina nella proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (*Artificial Intelligence Act),* pubblicata dalla Commissione Europea il 21 Aprile 2021. Tale proposta di Regolamento rappresenta una svolta cruciale in materia di Intelligenza Artificiale poiché costituisce, attraverso un atto di portata generale, vincolante in tutti i suoi elementi e per tutti gli Stati membri, un quadro normativo comune, volto al perseguimento di specifici e puntuali obiettivi, ma prima di prenderli in analisi è anche bene rammentare che l'Unione Europea ha scelto la non territorialità della legislazione, il che comporta che l'UE sia considerata come unico interlocutore anche per le applicazioni di intelligenza artificiale, questo ha come conseguenza che i colossi del settore dovranno dimostrare direttamente all'UE di aver dato vita ad un sistema di IA conforme alla legislazione europea[115]. Passando ora agli obiettivi perseguiti dall'AIA, questo atto si propone di: garantire che i sistemi di IA immessi ed utilizzati nel mercato unico Europeo siano sicuri e rispettino tanto i valori su cui si fonda l'Unione Europea quanto i diritti fondamentali degli individui; assicurare la certezza del diritto in modo da facilitare le innovazioni e gli investimenti in ambito di IA; migliorare la governance così come l'effettiva applicazione della disciplina esistente e infine facilitare lo sviluppo di un mercato unico per le applicazioni di IA lecite, sicure e affidabili anche al fine di prevenire ed evitare la frammentazione del mercato stesso[116]. In primo luogo è importante specificare la struttura in cui tale Proposta di Regolamento si articola: è questo diviso in 12 titoli che contengono un totale di 85 articoli preceduti da 89 considerando.[117] La prima parte della proposta di Regolamento si compone del solo Titolo I -*Disposizioni Generali*- dedicato all'oggetto, all'ambito di applicazione della normativa in esso prospettata e all'indicazione delle definizioni fondamentali ai fini della presente disciplina. La seconda parte si estende in tre Titoli (II -*Pratiche di Intelligenza artificiale vietate*-; III -*Sistemi ad alto rischio*-; IV -*Obblighi di trasparenza per determinati sistemi di IA*-), in essi si predispone la disciplina delle diverse tipologie di sistemi di Intelligenza artificiale identificati e categorizzati dal legislatore attraverso un

[115] L. Floridi, *'In poche battute. Brevi riflessioni su cultura e digitale 2011-2021',* Gennaio 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3998228. Pp: 335-339.

[116] Sono questi gli obiettivi individuati nella Relazione alla proposta di Regolamento. Cfr p.3 della Proposta di Regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione.

[117] Per completezza si specifica che la proposta di Regolamento è accompagnata da 9 allegati tecnici.

approccio basato sul rischio[118]. La terza parte della Proposta di Regolamento si sviluppa in 8 Titoli (V -*Misure a sostegno dell'innovazione*-; VI -*Governance*-; VII -*Banca dati dell'UE per i sistemi di IA indipendenti ad alto rischio*-; VIII -*Monitoraggio successivo all'immissione sul mercato, condivisione delle informazioni, vigilanza del mercato*-; IX -*Codici di condotta*-; X -*Riservatezza e sanzioni*-; XI -*Delega di Potere e procedura di Comitato*-; XII -*Disposizioni finali-)* i quali individuano norme sulla governance, sul controllo delle applicazioni di IA ma anche norme che garantiscano la corretta attuazione della disciplina prevista nella proposta in esame. Come pocanzi ricordato, la disciplina prospettata dal Parlamento Europeo e dal Consiglio è stata concepita tramite un approccio cd. *Risk-based* che porta a categorizzare i sistemi di IA a seconda del rischio che può scaturire dal loro impiego e in particolare si distingue tra: le applicazioni di IA che comportano un rischio inaccettabile, un rischio alto e un rischio medio o basso. Il Considerando 32 specifica quando un sistema di intelligenza artificiale indipendente[119] è ad alto rischio e infatti stabilisce che '*è opportuno classificarli come ad alto rischio se, alla luce della loro finalità prevista, presentano un alto rischio di pregiudicare la salute o la sicurezza o i diritti fondamentali delle persone, tenendo conto sia della gravità del possibile danno, sia della probabilità che si verifichi, e sono utilizzati in una serie di settori specificatamente predefiniti indicati nel Regolamento[120].'* L'Allegato III alla proposta di Regolamento individua le 8 macro-aree [121]nelle quali l'impiego di sistemi di IA si presume essere ad alto rischio e per tutte le categorie di sistemi di IA così qualificabili, la Proposta di Regolamento stabilisce una serie di regole che devono essere necessariamente rispettate: l'articolo 9 della proposta chiede che sia '*istituito, attuato, documentato e mantenuto un sistema di gestione dei rischi'[122];* l'articolo 10 stabilisce

[118] Cfr. paragrafo 4.2 del presente capitolo *'Ambito di applicazione del futuro quadro normativo dell'UE e le intelligenze artificiali ad alto rischio.'*

[119] Il Considerando 32, della Proposta di Regolamento sull'IA, specifica che un sistema di IA indipendente è un sistema di IA ad alto rischio distinto da quello che è una componente di sicurezza di prodotti o che è esso stesso un prodotto, e il considerando si riferisce esclusivamente a sistemi di IA ad alto rischio e indipendenti.

[120] Cit. Considerando 32 dell'AI Act.

[121] Le macro-aree nelle quali un sistema di IA si considera ad alto rischio sono: l'identificazione biometrica, l'accesso ai servizi pubblici e privati, l'attività di contrasto, l'amministrazione della giustizia, la gestione e il funzionamento delle infrastrutture, l'istruzione e formazione professionale, l'occupazione, la gestione dei lavoratori e l'accesso al lavoro autonomo, la gestione della migrazione, dell'asilo e del controllo delle frontiere. Queste sono individuate dall'allegato III *'Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2'* della Proposta di regolamento sull'IA.

[122] Cit. articolo 9 rubricato *'Sistema di gestione dei rischi'* della Proposta di Regolamento sull'IA.

regole attinenti i dati e la governance dei dati, sono questi, obblighi di qualità e accuratezza dei set di dati impiegati per l'addestramento, la convalida e la prova dei sistemi di IA[123]; l'articolo 11 prevede che sia redatta una documentazione tecnica '*in modo da dimostrare che il sistema di IA ad alto rischio è conforme ai requisiti di cui'* all'articolo 8[124]; l'Articolo 12, a sua volta, stabilisce un obbligo di conservazione delle registrazioni, questo perché *'i sistemi di IA ad alto rischio sono sviluppati e registrati con capacità che consentono la registrazione automatica degli eventi ('log'[125]) durante il loro funzionamento[126];* l'articolo 13 stabilisce obblighi di trasparenza e fornitura di informazioni agli utenti; l'articolo 14 chiede che sia garantita la sorveglianza umana cioè '*strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui il sistema di IA è in uso'[127];* infine l'articolo 15 dispone che i sistemi di IA ad alto rischio siano *'progettati e sviluppati in modo tale da conseguire un elevato livello di accuratezza, robustezza e cibersicurezza'.*[128]

Seguendo l'approccio che è stato scelto per predisporre la disciplina contenuta nella Proposta in esame, ossia l'approccio basato sul rischio, dopo avere introdotto e brevemente analizzato i sistemi di IA ad alto rischio, è ora bene prendere in considerazione i cd. 'sistemi a medio rischio'. Il Titolo IV comprende il solo articolo 52 rubricato '*Obblighi di trasparenza per determinati sistemi di IA',* i sistemi di IA per cui sono stabiliti obblighi puntali di trasparenza sono quelli che presentano problemi inerenti la loro capacità manipolativa, così proprio per questa loro peculiare caratteristica, il

---

123 Cfr. articolo 10 rubricato *'Dati e Governance dei dati'* dell'AI Act.

124 Cit. articolo 11 rubricato *'Documentazione tecnica'* della Proposta. Mentre l'articolo 8 rubricato *'Conformità ai requisiti'* dispone: *'1. I sistema di IA ad alto rischio rispettano i requisiti indicati nel presente capo. 2. Nel garantire conformità a tali requisiti si tiene conto della finalità prevista del sistema di IA ad alto rischio e del sistema di gestione dei rischi di cui all'articolo 9.'*

125 I *'log'* rappresentano la registrazione sequenziale e cronologica delle operazioni effettuate da un sistema, e queste procedure possono essere effettuate o da un utente o essere automatizzate. Quindi le operazioni di *logging* sono quelle attività attraverso cui un sistema operativo o un'applicazione registrano gli eventi e li memorizzano. Per un maggiore approfondimento si veda: L. Zanotti, *'Cosa sono i file log e perché con il log menagement si garantisce la sicurezza informatica, 'in'* Network Digital 360, 6 Settembre 2022, https://www.zerounoweb.it/techtarget/searchsecurity/che-cosa-sono-i-file-log-e-perche-non-c-e-sicurezza-senza-log-management/.

126 Cit. articolo 12 rubricato *'Conservazione delle registrazioni.*

127 Cit. articolo 14 rubricato *'Sorveglianza umana'.*

128 Cit. articolo 15 rubricato *'Accuratezza, robustezza e cibersicurezza'.* In più, cfr. paragrafo 4.2 *'Ambito di applicazione del futuro quadro normativo dell'UE e le intelligenze artificiali ad alto rischio.'* Del presente capitolo. Da questo paragrafo si comprende la continuità che sussiste tra gli atti che hanno preceduto l'emanazione della Proposta e la Proposta stessa.

legislatore ha deciso di imporre un obbligo di trasparenza che deve essere assolto nei confronti della persona fisica che interagisce con il tipo di sistema in questione. L'articolo 13 della medesima proposta introduce a sua volta un obbligo di trasparenza riferito ai sistemi ad alto rischio, ma è bene sottolineare che i due obblighi non coincidono, infatti l'articolo 13 introduce un obbligo di 'spiegabilità' mentre l'articolo 52 chiede che chi interagisce con un sistema di intelligenza artificiale sia messo a conoscenza di ciò[129]. I primi tre paragrafi dell'articolo 52 indicano i gruppi di applicazioni di IA che sono classificate 'a medio rischio', il primo paragrafo si riferisce ai *'sistemi di IA destinati a interagire con le persone fisiche'*[130], procede però individuando una puntale situazione di eccezione, che pertanto deroga all'applicabilità dell'obbligo in questione, cioè per il caso in cui il sistema sia impiegato per accertare, prevenire, indagare e perseguire reati. Il secondo insieme di sistemi di IA individuati dall'articolo 52 come a medio rischio sono i sistemi di riconoscimento delle emozioni o di categorizzazione biometrica[131], e anche in questo caso il legislatore puntualizza che l'obbligo non si applica quando i sistemi di categorizzazione biometrica sono autorizzati dalla legge per accertare, prevenire e indagare i reati. L'ultima categoria di IA a medio rischio indicata nell'articolo 52 è quella che *'genera o manipola immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti*[132]*'*; il problema che con riferimento a questi sistemi si può palesare è quello del cd. '*deepfake'*[133]. Anche con riferimento a dette applicazioni vale la deroga ricordata con riferimento alle due precedenti categorie di IA a medio rischio. Un ultimo aspetto su cui concentrare l'attenzione, in quanto rilevante ai fini della presente trattazione, è il sistema di *Governance* introdotto dalla Proposta di regolamento. Detto sistema di *Governance* si

---

[129] G. Contissa, F. Galli, F. Godano & G. Sartor, *'Il Regolamento europeo sull'intelligenza artificiale', 'in'* i-lex, Dicembre 2021, Fascicolo 2, Rivista semestrale on-line: www.i-lex.it. P. 27.

[130] Cit. articolo 52 rubricato *'obblighi di trasparenza per determinati sistemi di IA'.* Cfr. il testo dell'articolo 52 inserito nella Proposta di Regolamento sull'IA.

[131] Non deve essere confusa la categorizzazione biometrica con l'identificazione biometrica, infatti la prima è un'applicazione di IA che interpreta i dati biometrici e fa valutazioni sugli individui, ma non sono sistemi finalizzati all'identificazione della persona fisica. Cfr. G. Contissa, F. Galli, F. Godano, G. Sartor, *'Il Regolamento europeo sull'intelligenza artificiale', 'in'* i-lex, Dicembre 2021, Fascicolo 2, rivista semestrale on-line: www.ilex.it. P. 28.

[132] Cit. paragrafo 3 dell'articolo 52 della Proposta di Regolamento.

[133] Il Garante per la protezione dei dati personali spiega cosa è il *deepfake:* si tratta di foto, audio e video creati mediante l'impiego di applicazioni di intelligenza artificiale, le quali manipolano contenuti reali per modificare o ricreare le caratteristiche e i movimenti di un corpo o la voce di un individuo. Cfr. Garante della Privacy scheda informativa: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9512278.

sviluppa su due livelli, a livello europeo la Proposta istituisce un 'Comitato europeo per l'intelligenza artificiale' con diverse funzioni: contribuire all'efficace cooperazione delle autorità nazionali di controllo e della Commissione; coordinare e contribuire agli orientamenti e all'analisi della Commissione, delle autorità nazionali di controllo e di altre autorità competenti in relazione alle questioni che emergono nel mercato interno con riferimento alle materie disciplinate dal presente Regolamento; assistere le autorità nazionali di controllo e la Commissione nel garantire un'uniforme applicazione della presente Proposta[134]. A livello nazionale, gli Stati membri dovranno poi designare una o più autorità competenti al fine di garantire l'applicazione e l'attuazione della disciplina in questione[135]. Per i soli sistemi ad alto rischio, l'articolo 60 predispone l'istituzione di una banca dati dell'Unione Europea; mentre l'articolo 69 prevede che la Commissione e gli Stati membri promuovano l'elaborazione di codici di condotta al fine di promuovere l'applicazione volontaria dei sistemi di IA diversi da quelli ad alto rischio.

6.1. Uno speciale *focus* sull'articolo 5 della Proposta di Regolamento: pratiche di intelligenza artificiale proibite e in particolare l'identificazione biometrica a distanza e 'in tempo reale'

L'articolo 5[136] dell'Artificial Intelligence Act è il solo di cui è composto il Titolo II della Proposta di regolamento ed è dedicato alle pratiche di intelligenza artificiale proibite, si tratta dei sistemi di IA contraddistinti da un livello di rischio estremamente alto, per le quali è stabilito un divieto generale derogabile al sussistere di specifiche condizioni e in presenza di particolari situazioni. In detto articolo, il legislatore si occupa di pratiche che prevedono l'utilizzo di sistemi di IA che causano o potrebbero causare effetti inaccettabili in quanto violano i valori o i diritti fondamentali dell'Unione Europea[137]. In particolare ci si vuole concentrare sull'identificazione biometrica remota (in spazi pubblici o accessibili al pubblico) 'in tempo reale' per attività di contrasto, pratica di intelligenza artificiale vietata dall'articolo 5(1), lett. d. Innanzitutto è bene specificare che detti sistemi

[134] Cfr. articolo 56 rubricato '*Istituzione del Comitato europeo per l'intelligenza artificiale'* della Proposta di Regolamento.
[135] In base a quanto disposto nell'articolo 59 rubricato *'Designazione delle autorità nazionali competenti'* della Proposta di Regolamento.
[136] L'articolo 5 della Proposta di Regolamento rubricato '*pratiche di intelligenze artificiali vietate'* dispone quali sono le pratiche di intelligenza artificiale proibite e disciplina le eccezioni.
[137] G. Contissa, F. Galli, F. Godano & G. Sartor, *'Il Regolamento europeo sull'intelligenza artificiale'*, *op. cit.* 11.

sono definiti al punto 37 dell'articolo 3 della Proposta come sistemi *'di identificazione biometrica remota in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi. Sono incluse non solo le identificazioni istantanee, ma anche quelle che avvengono con brevi ritardi limitati al fine di evitare l'elusione della normativa'.*[138] Come si è poc'anzi rammentato, si tratta di ipotesi di pratiche di IA vietate, ma il cui impiego è consentito in specifici casi eccezionali, i quali sono indicati ai punti i, ii, iii lettera d. dell'articolo 5 ossia: i. per la ricerca mirata di potenziali vittime da reato; ii. per prevenire una minaccia specifica, sostanziale e imminente per la vita o l'incolumità delle persone fisiche o di un attacco terroristico; iii. per il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato tra quelli indicati nell'articolo 2, paragrafo 2, della decisione quadro 2002/583/GAI del consiglio. Perché però, in presenza di una di queste eccezioni, si possano impiegare tali pratiche di IA, è necessario che siano adottate idonee garanzie procedurali: devono essere valutati i presupposti che consentono l'impiego di detti sistemi e l'impatto che hanno sui diritti e le libertà dell'individuo; devono essere apposte adeguate limitazioni geografiche, temporali e personali che necessariamente devono essere rispettate per il corretto uso dei sistemi in questione; infine deve sempre, il loro impiego, essere preventivamente autorizzato o dall'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro, rilasciata a seguito della presentazione di un'apposita domanda motivata[139]. L'analisi appena riportata permette di evidenziare alcuni aspetti problematici della disciplina riferita ai sistemi di identificazione biometrica remota 'in tempo reale', in particolare bisogna evidenziare che si tratta di un divieto, quello dell'articolo 5, che si esplica solo ed esclusivamente nei confronti di sistemi *identificazione* delle persone fisiche[140], ma spesso tali applicazioni vengono impiegate per il *riconoscimento* degli individui ai fini di una loro *categorizzazione,* con ciò correndo il rischio che taluni vengano 'isolati' dalla restante parte della massa della popolazione[141].

---

[138] Cit. articolo 3 n.37 rubricato '*Definizioni'* della Proposta.

[139] Cfr. articolo 5. Nonostante quanto detto, ci sono casi in cui l'impiego di sistemi di identificazione biometrica non deve essere preventivamente autorizzato dall'autorità, cioè quando sussiste una situazione di estrema urgenza debitamente giustificata, è infatti data la possibilità di iniziare ad usare il sistema senza autorizzazione, purché questa sia richiesta o durante o dopo l'utilizzo.

[140] La distinzione tra riconoscimento e identificazione biometrica è stata riportata nella nota 85. Mentre la distinzione tra identificazione e categorizzazione è stata indicata in nota 119.

[141] G. Contissa, F. Galli, F. Godano & G. Sartor, *'Il Regolamento europeo sull'intelligenza artificiale'*, *op. cit.* 18 e ss.

6.2. Alcune conclusioni in merito all'*AI ACT*

Nonostante la Proposta di regolamento rappresenti un fondamentale punto di svolta, ponendosi in modo pioneristico, come prima legislazione al mondo in tema di Intelligenza artificiale, e sebbene i benefici che da essa possono trarsi siano evidenti, non è esente da limiti. Il primo limite che può essere evidenziato è dato dal fatto che la disciplina in tale atto predisposta si basa su un approccio *top-down.* Attraverso questo approccio il rischio, connesso ad una data applicazione di IA, viene stabilito ex ante, e così vengono poi individuate le tecnologie che sono vietate o altamente rischiose, per poter in seguito constatare la disciplina che puntualmente deve essere applicata[142]. L'approccio *top-down* (dall'alto verso il basso), è un metodo di progettazione degli algoritmi che vuole individuare il problema dapprima in via generale per poi passare al caso pratico. [143]Seguendo questo approccio si corre un rischio concreto, ossia quello di dare vita a categorie normative astratte che difficilmente possono rappresentare le singolarità e i rischi pragmatici che sono connessi a ciascuna diversa applicazione di IA.[144] Per evitare tali problematicità sarebbe stato più consono adottare un approccio *bottom-up,* considerato un approccio migliore con riferimento a queste tecnologie all'avanguardia. L'approccio in questione prende le sue mosse dai problemi singolarmente individuati e affrontati, i quali vengono tra loro connessi e riuniti in più grandi e generiche categorie di problemi e questo avviene attraverso il metodo induttivo[145]. In questo modo il legislatore può individuare le caratteristiche specifiche di ciascuna applicazione di IA e dell'ambito in cui questa viene adottata e impiegata. Il secondo limite che si può evidenziare è strettamente connesso al primo, infatti se il legislatore avesse intrapreso un approccio bottom-up avrebbe, probabilmente, meglio tutelato l'individuo e i diritti fondamentali che ad esso fanno capo. Tale affermazione deriva dal fatto che l'obiettivo della Proposta, come già si era evidenziato nel corso della rassegna cronologica in questo capitolo affrontata, era quello di predisporre una disciplina volta a garantire l'immissione

[142] G. Contissa, F. Galli, F. Godano & G. Sartor, *'Il Regolamento europeo sull'intelligenza artificiale', op. cit.* 31,32,33.

[143] Da Treccani, *Metodo top-down*, https://www.treccani.it/enciclopedia/metodo-top-down_%28Enciclopedia-della-Matematica%29/#:~:text=metodo%20top%2Ddown%20(ingl.,che%20segue%20il%20percorso%20inverso.

[144] G. Contissa, F. Galli, F. Godano & G. Sartor, *'Il Regolamento europeo sull'intelligenza artificiale'*, *op. cit.*

[145] Treccani, *op. cit.*

nel mercato di intelligenze artificiali antropocentriche, eppure l'individuo, quale soggetto che si interrelaziona con tali tecnologie, non riceve specifici strumenti di difesa. Vero è, da un lato, che la disciplina in commento si inserisce in un quadro normativo più ampio, nel quale maggiore attenzione deve essere rivolta al GDPR, ma dall'altro lato è anche vero che, con riguardo a quest'ultimo ci sono questioni non del tutto chiarite, una delle quali riguarda il diritto a ricevere una spiegazione, che si ricorda non essere espressamente previsto dal GDPR ma solo nel Considerando 71.[146]

7. Un freno all'impiego di sistemi di videosorveglianza dotati di riconoscimento facciale: il divieto dell'Italia, la legge n.205 del 3 Dicembre 2021

Conclusa la rassegna cronologica, avente ad oggetto atti di valenza sovra-nazionale, che ha condotto fino all'analisi dell'AI Act, si può ora prendere in considerazione un atto di valenza nazionale, ossia la legge n.205 del 3 Dicembre 2021. Tale legge è di fondamentale importanza ai fini della trattazione poiché è la conversione del decreto legge Capienze con il quale l'Italia ha vietato l'impiego di sistemi di riconoscimento facciale in luoghi pubblici. Con un emendamento del Pd è stata, il 1 Dicembre 2021, approvata la legge di conversione del decreto Capienze, nella quale fu introdotta una sospensione dei trattamenti di riconoscimento facciale nei luoghi pubblici o aperti al pubblico da parte dei soggetti pubblici e privati[147]. Con detta legge l'Italia vieta tale pratica di IA fino al 31 Dicembre 2023, data entro la quale dovrebbe essere approvata la Proposta di Regolamento sull'intelligenza artificiale. Si tratta di un divieto generalizzato stabilito sulla base di quanto disposto nel Regolamento (UE) 679/2016, alla Direttiva (UE) 680/2016 e nel rispetto dell'articolo 52 della carta dei diritti fondamentali che dispone il principio di proporzionalità, di conseguenza non si impedisce in generale l'uso di videocamere ma solo quando queste siano predisposte alla funzione di riconoscimento facciale attraverso dati biometrici. Nonostante il divieto, la legge prevede specifiche eccezioni, che pertanto consentono l'impiego di videocamere dotate di riconoscimento facciale, l'utilizzo è consentito al fine di prevenire e reprimere i reati, da parte delle autorità competenti, nonché per l'esecuzione delle sanzioni previste nel decreto

[146] C. Sarra, *'Il mondo-dato. Saggi su datificazione e diritto',* Padova, Cleup, 2022, Pp. 127-165.
[147] M. Borgobello, '*Riconoscimento facciale vietato in Italia: ma solo per ora e con eccezioni', 'in'* Agenda Digitale, 2 Dicembre 2021, https://www.agendadigitale.eu/sicurezza/privacy/riconoscimento-facciale-vietato-in-italia-ma-per-ora-e-con-eccezioni/.

legislativo n.51 del 2018, in presenza del parere positivo del Garante per il trattamento dei dati personali[148]. Il divieto di cui si sta ora dicendo è stato prorogato, con l'approvazione del decreto legge n.51 del 2023, che estende la moratoria concernente i sistemi di riconoscimento facciale, fino al 31 Dicembre 2025. Ad oggi il decreto legge è stato convertito nella legge n.87 del 3 luglio 2023, la quale conformemente a quanto era disposto nella precedente legge del 2021, prevede un divieto esplicito per l'impiego delle tecnologie di riconoscimento facciale, tuttavia i Comuni hanno la possibilità di procedere all'istallazione previo parare favorevole del Garante per la protezione dei dati personali[149]. Il divieto posto dall'Italia permette di constatare il timore del governo a che si concretizzino i rischi che sono connessi allo sfruttamento di tale pratica di IA, questi hanno infatti spinto il legislatore a fare un passo avanti ed impedire che un impiego errato di detti sistemi possa pregiudicare i diritti fondamentali degli individui, in particolare emerge il timore di discriminazioni, non accettabili secondo quanto disposto dall'articolo 21 della Carta dei diritti fondamentali. Dall'altra parte è anche bene evidenziare che la disciplina che stabilisce il divieto pecca di essere approssimativa poiché necessita di un'apposita interpretazione da parte del Garante, che può acconsentire a che i comuni procedano all'istallazione di detti sistemi in luoghi pubblici o aperti al pubblico.[150]

[148] Cfr. testo della legge n.205 del 3 Dicembre 2021.

[149] A. Lepore, '*Confermato fino al 2025 il divieto di installare sistemi di riconoscimento facciale in Italia', 'in'* Smartworld, 23 Giugno 2023, https://www.smartworld.it/news/divieto-installazione-sistemi-riconoscimento-facciale-2025.html.

[150] A. Longo, *'Italia primo Paese a vietare il riconoscimento facciale (con eccezioni), 'in'* Il sole 24 ore, 2 Dicembre 2021, https://www.ilsole24ore.com/art/italia-primo-paese-vietare-riconoscimento-facciale-con-eccezioni-AEFLRY0.

CAPITOLO II
INQUADRAMENTO STORICO E PROFILI TECNICI INERENTI IL FUNZIONAMENTO DELLE TECNOLOGIE DI RICONOSCIMENTO FACCIALE

1. Nascita ed evoluzione delle Tecnologie di Riconoscimento facciale: i dati come *nuova valuta* dell'economia digitale alla base della crescente diffusione di tale tecnologia

Come si è avuto modo di specificare nel Capitolo precedente, le tecnologie di riconoscimento facciale sono una delle svariate applicazioni dell'Intelligenza artificiale cosicché, volendosi trattare della nascita ed evoluzione di dette tecnologie, non si può non avere riguardo, quanto meno brevemente e in generale, del quadro storico in cui si inserisce l'Intelligenza artificiale.

Prima di entrare nel vivo della questione, vorrei riportare una prima definizione di Intelligenza artificiale, ossia quella individuata da Somalvico nel 1987. Marco Somalvico è stato docente presso la facoltà di ingegneria del Politecnico di Milano e definisce l'IA come *'una disciplina che studia i fondamenti teorici, le metodologie e le tecniche che permettono di progettare sistemi hardware e sistemi di programmi software capaci di fornire all'elaboratore elettronico prestazioni che, a un osservatore comune, sembrerebbero essere di pertinenza esclusiva dell'intelligenza umana'.*[151]

Il termine Intelligenza artificiale è stato coniato da John McCarthy in occasione del seminario estivo tenutosi presso il Dartmouth College, in questa sede si può dire sia stata fondata programmaticamente questa nuova disciplina. In detta conferenza vengono affrontati temi all'epoca considerati di grande attualità quali le reti neurali, la teoria della computabilità, la creatività e l'elaborazione del linguaggio naturale;[152] ma sono proprio le basi poste nei secoli precedenti che consentono la discussione concernetemene detti argomenti. Grazie alla formalizzazione delle scienze e della matematica, è stato possibile

[151] Cit. M. Somalvico, *'Intelligenza artificiale',* Milano, Rusconi, 1987.
[152] Cfr. J. McCarthy, M. L. Minsky, N. Rochester and C. E. Shannon, *'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence',* August 31, 1955.

prospettare una costruzione artificiale dell'intelligenza cosicché, con l'avvento dei calcolatori elettronici avutasi a metà del XX secolo[153], fu possibile attribuire concretezza al nuovo programma di ricerca denominato Intelligenza artificiale.

Nonostante il 1956 sia la data convenzionalmente accettata nella comunità scientifica quale data di nascita dell'Intelligenza artificiale, è necessario fare un passo indietro fino al 1943, anno in cui Warren McCulloch e Walter Harry Pitts propongono il primo modello matematico di una rete neurale. Ancora ad oggi la rappresentazione formale di un singolo neurone, così come da loro concretizzata, è lo standard utilizzato nel campo delle reti neurali ed è stato denominato *neurone di McCulloch-Pitt[154]:* infatti è questa la prima formalizzazione di ciò che equivale tra il sistema nervoso umano e un calcolatore elettronico.

Il 1947 è un anno altrettanto importante poiché 'nasce' la Cibernetica, definita dal suo padre fondatore Norbert Wiener come lo studio unitario dei processi che riguardano *'la comunicazione e il controllo nell'animale e nella macchina'[155].* Molti degli strumenti utilizzati in ambito cibernetico sono legati all'elaborazione dell'informazione, e in particolare si tratta di tecnologie che ebbero grande impulso dallo sviluppo e dalla conseguente diffusione di dispositivi elettronici. Ciò detto, la stretta commistione tra Intelligenza artificiale e Cibernetica è evidente, infatti il progetto cibernetico vede alla propria base lo studio dei meccanismi di autoregolazione e controllo che sono presenti tanto nell'essere umano, quanto nelle macchine capaci di retroazione.[156]

---

[153] Per un maggiore approfondimento circa la storia dei calcolatori elettroni si veda: *'Chi ha inventato il Computer?', 'in'* Focus, https://www.focus.it/cultura/storia/chi-ha-inventato-il-computer#:~:text=Il%20primo%20calcolatore%20interamente%20elettronico,stanzone%20di%20140%20metri%20quadrati.

[154] Cfr. W. S. McCulloch, W. Pitts, *'A logical calculus of the ideas immanent in nervous activity',* Bulletin of mathematical biophysics, volume 5, 1943.

[155] Cfr. N. Wiener, *'Cybernetics, or Control and Communications in the animal and the machine',* Cambridge, MIT press, 1948.

[156] Il concetto di retroazione (*feed-back)* è stato definito da W. R. Ashby nel suo libro '*Introduzione alla Cibernetica'*(1971) come: '*una sorta di circolarità d'azione tra le diverse parti di un sistema dinamico'...* prosegue poi affermando: '*il concetto di retroazione, così semplice e naturale in certi casi elementari, diventa artificioso e difficilmente adoperabile quando le interconnessioni diventano più complesse.'*

Si è già detto che il successo dell'Intelligenza artificiale è collegato all'avvento dei calcolatori elettronici e questo perché l'IA necessita di un sistema artificiale-informatico nel quale possano essere riprodotti e quindi emulati i processi e le funzioni dell'intelligenza umana, e proprio il calcolatore elettronico fu individuato come sistema che meglio potesse adempiere a questa funzione. Ciò ci porta al concetto di *macchina* prospettato da Alan Turing, quale concetto sul quale vengono sviluppati i moderni calcolatori elettronici. La *macchina di Turing* è stata inventata dal matematico, nonché uno dei padri fondatori dell'informatica Alan Turing, nel 1936, e la si può definire come un modello astratto di macchina in grado di elaborare i dati, e quindi le informazioni, che sono riportati su un nastro. Essendo la *macchina di Turing* un concetto astratto, la lunghezza del nastro deve essere considerata potenzialmente infinita, e tal macchina sarebbe in grado di attuare detta manipolazione, dei dati sul nastro riportati, seguendo le istruzioni di un insieme predefinito di regole, cioè eseguendo algoritmi[157].

Sempre ad Alan Turing è attribuito il merito del noto *Test di Turing,* da lui elaborato in un celeberrimo articolo del 1950. Il Test in questione viene utilizzato come parametro per comprendere se sussiste o meno 'intelligenza' nella macchina con cui ci si confronta. Volendone fornire una descrizione, il Test si basa su *'il gioco dell'imitazione',* tal gioco si sviluppa attraverso la presenza di tre persone distinte che possiamo denominare A, B e C; la persona C viene tenuta separata dalle persone A e B e attraverso una serie di domande deve riuscire a stabile chi, tra i due, sia l'uomo e chi la donna. Affinché il gioco vada a buon fine sono attribuiti dei compiti anche ad A e B, infatti A ha il compito di indurre in errore C, conducendolo ad una risposta sbagliata; mentre il compito di B è quello di aiutare C a fornire una corretta identificazione. A questo punto possiamo comprendere come si svolge il Test, ossia attraverso una sostituzione: la persona A viene rimpiazzata da una macchina e se la percentuale di volte in cui la persona C giunge alla giusta risposta, e quindi ad individuare correttamente chi sia l'uomo e chi la donna, è molto vicina alla percentuale antecedente alla sostituzione di A, allora la macchina che

[157] Il concetto di macchina di Turing qui riportato e brevemente spiegato è preso da: A. M Turing, *'On computable number , with an application to the Entscheindungproblem',* November 12, 1936.

ha sostituito A deve essere considerata intelligente, in quanto non sarebbe distinguibile, nello svolgimento del compito assegnatogli, da un essere umano[158].

Gli anni successivi al 1956 furono gli anni delle grandi aspettative, le quali sono state alimentate dal forte miglioramento dei sistemi informatici che si ebbe durante la Seconda guerra mondiale. Ciò nonostante, dopo un primo momento di enfasi, si assiste ad un arresto e ad un accantonamento dello studio dei modelli a reti neurali, e ciò soprattutto a seguito di importanti critiche sollevate da M. Minsky e S. Paper nei confronti del modello *Perceptron,* elaborato da Frank Rosenblatt. Il *Perceptron* si può ritenere il primo schema a reti neurali, cioè il primo modello logico-matematico del cervello, lo si può descrivere un classificatore binario[159] avente due strati, uno di entrata e uno di uscita, e dotato di una regola di apprendimento *error back-propagation,* ossia volta alla minimizzazione degli errori. In questo primo modello l'apprendimento avviene mediante la retroazione, adattando cioè i pesi numerici fino ad ottenere il risultato, in uscita, desiderato[160]. Nonostante *Perceptron* possa essere definito 'un buco nell'acqua[161]' apre le porte alla possibilità di utilizzare l'intelligenza artificiale al fine di riconoscimento facciale, in quanto si tratta di un'applicazione di IA che opera, prevalentemente, mediante il modello a reti neurali.

Tenendo presente che tra il 1958 e il 1970 vengono immessi nel mondo analogico i primi linguaggi di programmazione specifici per l'IA, approdiamo al 1966 anno importante per l'evoluzione del riconoscimento facciale. Nel 1966, nonostante fossero passati dieci anni dal famoso seminario di Dartmouth, gli studi in ambito di intelligenza artificiale non erano ancora giunti all'invenzione di un algoritmo in grado riconoscere e classificare i

---

[158] Cfr. A. M. Turing, *'Computing machinery and intelligence', 'in'* Mind: A Quarterly Review of Psychology and Philosophy, Vol. LIX, number 236, October, 1950.

[159] Un classificatore binario è un tipo di algoritmo o modello di *machine learning* che è progettato al fine di affrontare e risolvere problemi di classificazione in cui ci sono solo due categorie o classi di output possibili. Le due classi vengono comunemente indicate come 'positiva' e 'negativa' oppure come '1' e '0'. L'obiettivo che persegue un classificatore binario è di riuscire ad assegnare correttamente un'istanza di input a una di queste due classi.

[160] Per un maggiore approfondimento su '*perceptron'* si veda: F. Rosenblatt, *'The Perceptron:. A probabilistic model for information storage and organization in the brain', 'in'* Psychological Review, volume 65, number 6, 1958.

[161] Nonostante il Perceptron sia qualificabile come un'invenzione innovativa per il tempo in cui si colloca presentava diverse criticità, le quali furono ampiamente evidenziate da M. Minsky e S. Papert in '*Perceptron: an introduction to Computational geometry',* 1969.

volti umani in modo del tutto autonomo, ciò nonostante è un anno da ricordare grazie agli studi pioneristici di Woodrow Wilson Bledsoe, Charles Bisson e Helen Chan Wolf.[162] Questi tre precorritori dell'Intelligenza artificiale collaborarono presso la *Panoramic Research* al fine di riuscire ad addestrare un computer a svolgere la funzione di riconoscimento dei volti umani, funzione nota come '*Automated facial recognition'.* Il programma allora creato richiedeva una stretta collaborazione tra uomo e macchina, infatti era proprio l'uomo che si occupava di inserire manualmente le caratteristiche, inerenti ad un volto umano, nel sistema e dopodiché il computer si occupava del riconoscimento. Questo metodo sfruttava la *Rand tablet,* un dispositivo impiegato al fine di inserire in una apposita griglia, tramite uno stilo che emetteva impulsi elettromagnetici, le coordinate delle caratteristiche del viso quali la bocca, la linea dei capelli, il naso o ancora, gli occhi. Una volta eseguita questa mansione, le metriche potevano poi essere inserite in un *database,* cosicché quando veniva aggiunta, nel programma, una nuova fotografia ritraente il volto umano, il programma era in grado di estrarre, dallo stesso *database,* l'immagine che più assomigliava all'individuo[163]. Nonostante sia una conquista importante bisogna anche tenerne presente i limiti, i quali derivano principalmente dalla tecnologia impiegata e dalla scarsa potenza di elaborazione del computer stesso. Nonostante le diverse problematiche connesse, rappresenta un primo passo verso il riconoscimento facciale come è noto oggi e mostra le potenzialità dell'impiego dei dati biometrici.

Nel 1973 viene pubblicata la tesi di dottorato dello studioso e informatico giapponese Takeo Kanade, il quale sviluppa una ricerca volta all'elaborazione di algoritmi per il riconoscimento facciale automatico. Al tempo la ricerca era ancora ai primi stadi, e pertanto si trattava di algoritmi che sfruttavano semplici modelli geometrici in grado di elaborare distanza, angoli e punti del volto umano[164].

---

[162]Chi interessato ad un approfondimento circa la biografia di questi studiosi, si possono visitare i seguenti link, per W. W. Bledsoe: https://www.historyofinformation.com/detail.php?id=2126. Per H. C. Wolf: https://en.wikipedia.org/wiki/Helen_Chan_Wolf.

[163] Cfr. '*The brief history of Face Recognition', 'in'* FaceFirst, August 1, 2017, https://www.facefirst.com/post/a-brief-history-of-face-recognition. Si può inoltre vedere: W. W Bledsoe, I. Browing, *'Pattern Recognition and Reading by Machine',* 1959 Proceedings of the Eastern Joint Computer Conference. E ancora: W. W. Bledsoe, *'Some Results on Multicategory Pattern Recognition', 'in'* Journal of the Association for Computing Machinery, Vol. 13, number 2, 1966.

[164] Cfr. T. Kanade, *'Picture Processing System by Computer Complex and recognition of Human Face',* Tesi di dottorato, Università di Kyoto, Department of Information and Science, November 1973.

Si dovrà attendere fino al 1988 per assistere ad un ulteriore avanzamento nelle ricerche in tema di riconoscimento facciale, è questo l'anno in cui Sirovich e Kirby elaborano l'approccio *Eigenface,* approccio questo sviluppato attraverso l'applicazione dell'algebra lineare al problema del riconoscimento facciale. Si tratta di un approccio che si basa sull'estrazione di un insieme di caratteristiche di base da una serie svariata di immagini del volto umano, le caratteristiche di base estratte (appunto le *Eigenpictures* o *Eigenface)* venivano a loro volta combinate in modo lineare per riprodurre le immagini nel *training-set*, quindi gli stessi *Eigenface,* che costituiscono, nel loro complesso, il set base di tutte le immagini, venivano utilizzate per creare la matrice di covarianza, e così la classificazione avveniva attraverso il confronto delle caratteristiche del volto presenti nel set di base.[165] Quindi attraverso l'applicazione dell'algebra lineare (analisi delle componenti principali, PCA) si ottennero importanti risultati, si tratta infatti di un algoritmo di apprendimento che *'cerca di estrarre i fattori tipici di un dataset per focalizzarsi sulle variazioni rispetto al pattern calcolato. Nel riconoscimento facciale, si utilizza PCA per definire quali sono i tratti del volto in grado di caratterizzarlo, portando a massimizzare le differenze tra i volti'*[166]. L'approccio *Eigenface* è stato successivamente migliorato e ulteriormente sviluppato da Turk e Pentland, i quali aprono le porte alla possibilità non solo di realizzare la funzione di riconoscimento facciale, ormai appurata, ma di fare ciò automaticamente e in tempo reale.[167]

Nel 1993 fu avviato il programma FERET (*facial recognition tecnologies*), si tratta di un progetto lanciato dalla Defense Advanced Research Projects Agency (DARPA) e il National Institute of Standards and Technology (NIST), con l'obiettivo di promuovere l'utilizzo del riconoscimento facciale. Questo si sviluppò in tre fasi, l'obiettivo con cui fu avviata la prima fase era di quello di verificare la fattibilità degli algoritmi di riconoscimento facciale, nonché quello di stabilire *performace* di base, attraverso le quali ponderare gli sviluppi futuri. L'obiettivo delle due fasi successive era quello di sviluppare ulteriormente gli algoritmi di *face recognition.* Un aspetto importante di questo

[165] Cfr. M Kirby, L. Sirovich, *'Low-dimensional procedure for the characterization of human face', 'in'* Journal of the Optical Society of America A, Volume 4, March 1987.
[166] Cit. M. Bacci, *'Metodi e tecnologie per il riconoscimento facciale',* Tesi di laurea, Alma Mater Studiorum Università di Bologna, 2016, p.10.
[167] Cfr. M. A. Turk, A. P. Pentland, *'Face Recognition Using Eigenfaces', 'in'* Journal of Cognitive Neuroscience, Vol. 3, number 1, 1991.

programma fu la creazione di un *database* di immagini facciali, che al tempo si considerò fondamentale per il successo del progetto, questo permetteva di raccogliere, classificare e conservare immagini del volto, poi impiegate dai ricercatori per lo sviluppo degli algoritmi, nonché per la conseguente verifica degli stessi. Prima dell'avvio di detto programma, i *database* avevano, salvo alcune eccezioni, dimensioni estremamente ridotte, tanto che potevano conservare le foto di meno di 50 individui, mentre il *database* in questione conteneva, già al momento dell'avvio del programma, un totale di 14.126 immagini, riconducibili a 1199 individui differenti, di cui solo 365 erano set duplicati di immagini[168]. La nascita del *database* di cui si sta dicendo, rappresenta un momento cruciale nell'evoluzione del riconoscimento facciale e lo si consta agevolmente se si tiene presente la modalità con cui vengono addestrate le macchine intelligenti, è infatti fondamentale un idoneo *training set* costituito da un numero quanto più elevato possibile di dati, della specie di cui si necessita (in questo caso immagini del volto degli individui). Il modo con cui viene costruito il *set* di addestramento determina, di conseguenza, l'affidabilità dell'IA poiché più sono i dati, sulla base dei quali l'algoritmo viene addestrato, minore sarà la probabilità di errore[169]. Questo non significa che i dati siano l'unico fattore che incide sull'efficienza di un algoritmo, in particolare, con riferimento al riconoscimento facciale, svariati sono gli elementi che inducono o comunque possono indurre l'IA ad un risultato errato, possiamo ricordare, come esemplificazione, l'incidenza che la razza, il genere o la provenienza etnica del soggetto hanno sulla qualità del risultato, così come l'età o l'espressione facciale[170].

Sulla base di quanto evidenziato, l'avvento dell'era dei Social-network rappresenta un ulteriore passo nell'evoluzione del riconoscimento facciale e, ancora prima, nella raccolta di dati utilizzabili per l'addestramento degli algoritmi. L'anno di riferimento è il 2004, ossia l'anno in cui Facebook viene messo nella disponibilità di utilizzazione di chiunque avesse un computer, e soprattutto in modo del tutto gratuito, ma è davvero così? Non è

[168] Si confronti sul punto il sito del NIST- National Institute of Standards and Technology. US Department of Commerce al presente link: https://www.nist.gov/programs-projects/face-recognition-technology-feret. Dove viene spiegato approfonditamente il programma FERET.
[169] Non soltanto la quantità di dati incide sull'efficacia dell'addestramento dell'algoritmo, ma anche la tipologia e la qualità dei dati che venivano in concreto impiegati per la costruzione del *training set.*
[170] Cit. G. Mobilio, *'Tecnologie di Riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative',* Napoli, Editoriale Scientifica, 2021, p.34.

richiesta alcuna moneta di scambio? O è solo un modo per incentivarne l'uso, tenendone nascoste le implicazioni? Cosa significa, in concreto, creare un profilo sul *social-network* Facebook? Per rispondere a quest'ultima domanda, e le stesse considerazioni possono estendersi anche agli altri prodotti del gruppo Meta Platform Inc., basta leggere l'informativa sulla Privacy, alla quale ciascuno di noi acconsente nel momento in cui da vita al proprio profilo digitale.[171] L'informativa sulla Privacy adottata dal gruppo Meta, spiega come vengono raccolte, usate e condivise le informazioni facenti capo a ciascun utente, ma prima ancora, quali sono le informazioni che noi decidiamo di mettere nella disponibilità dei colossi social, ossia l'indirizzo e-mail, il numero di telefono, l'attività che svolgiamo sui social stessi (i contenuti che visualizziamo o a cui mettiamo 'Mi piace', post, foto ma anche i messaggi che inviamo), chi sono i nostri 'amici' o '*followers'* e le attività da questi svolte sulle piattaforme, le informazioni del telefono, computer o tablet che viene utilizzato per il programma in questione e infine le informazioni che sono provenienti da *Partner* circa le attività svolte sia all'interno che all'esterno del *social*. E queste informazioni vengono impiegate nei più svariati modi, dalla personalizzazione dell'esperienza dell'utente alla trasmissione internazionale di dati personali[172]. Ma perché e dove, i nostri dati vengono trasmessi? Come appena puntualizzato, i dati sono oggetto di trasmissione internazionale e mondiale, ma ci si vuole in questa sede concentrare sulla trasmissione di dati che avviene tra l'Unione Europea e Stati Uniti d'America[173], ma perché ciò è necessario? Ciò è necessario perché il progresso economico dipende dall'impiego massivo di dati, e se questa trasmissione fosse repentinamente interrotta le conseguenze sarebbero disastrose, basti pensare alla piccola *Start-up* avente sede in Germania che utilizza *cloud* con sede negli USA, questa non potrebbe più utilizzare codesto *cloud,* ed è una conseguenza che coinvolgerebbe tutte le aziende europee che

[171] Altra questione rilevante che deve tenersi a mente è che la lettura della normativa sulla Privacy impegna gli utenti in una lettura lunga e complicata (per gli utenti medi) e che spesso induce ad acconsentire a trattamenti senza essersi effettivamente ed adeguatamente informati su che cosa comporta la nostra azione.
[172] Si può confrontare sul punto la Normativa Privacy del gruppo Meta, dove viene spiegato più nel dettaglio quanto esposto nel presente paragrafo, la si trova aggiornata al 7 settembre 2023 al seguente link: https://mbasic.facebook.com/privacy/policy/printable/#2-HowDoWeUse.
[173] È però bene ricordare, come si evidenzia nella stessa normativa sulla Privacy citata nella precedente nota, che i dati non sono solo oggetto di scambi transatlantici tra UE e US, ma vi sono anche altri luoghi in cui vengono inviati e, in particolare, luoghi in cui il gruppo Meta ha infrastrutture o data center fra cui ci sono gli Stati Uniti, Irlanda, Danimarca e Svezia; possono poi essere trasmessi in Paesi in cui i prodotti delle aziende di Meta sono disponibili e infine anche in paesi in cui i Partner del gruppo Meta, nonché i provider di servizi e altri terzi operano al di fuori del paese di residenza dello specifico utente i cui dati sono trasmessi.

impiegano cloud americani.[174] Il passaggio dei dati da un continente all'altro necessita però di essere regolato da un accordo sulla privacy tra Unione Europea e Stati Uniti, il quale ad oggi è il UE-U.S Data Privacy Framework[175], entrato in vigore il 10 Luglio 2023, dove per la prima volta, dopo l'invalidazione dei due accordi precedenti, la Commissione Europea afferma che gli Stati Uniti hanno raggiunto un livello adeguato di protezione verso i dati personali che vengono trasmessi. Ma se solo nel 2023, anno corrente, l'Unione Europea ha affermato la liceità del trattamento da parte degli U.S, questo vuol dire che prima ne derivava un trattamento illecito, quanto meno per gli standard europei[176]. Di conseguenza se i dati sono la nuova valuta dell'economia digitale[177], i social rappresentano l'avvento della *'participatory surveillance'.*[178]

Le considerazioni fino a questo momento evidenziate possono essere applicate specificatamente anche al Riconoscimento facciale[179], infatti tra i dati che l'utente carica

---

[174] Cit. S. Cosimi, *'Facebook, l'Irlanda blocca il trasferimento dei dati verso gli USA: i rischi per il social senza un nuovo Privacy Shield', 'in'* La Repubblica, 10 Settembre 2020, https://www.repubblica.it/tecnologia/social-network/2020/09/10/news/facebook_l_irlanda_blocca_il_trasferimento_dei_dati_verso_gli_usa_i_rischi_per_il_social_senza_un_nuovo_privacy_shield-266805870/.

[175] Commission implementing decision, 10 Luglio 2023, C(2023) 4745 final, *'Pursuant to Regulation (UE) 2016 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework'.* Lo si può agevolmente consultare al presente link: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.

[176] Plurime sono le sanzioni erogate nei confronti del gruppo Meta per la violazione della normativa sulla Privacy, che per l'UE è racchiusa nell'importante Regolamento 679 del 2016 conosciuto come GDPR: si può ricordare la multa di 1 milione di euro impartita dal Garante della Privacy a Facebook per illeciti compiuti nel caso Cambridge Analytica, infatti il garante aveva accertato che 57 italiani avevano scaricato l'applicazione Thisisyourdigitallife attraverso la funzione Facebook-login, funzione che consentiva di condividere i dati degli 'amici' e attraverso la quale sono stati recepiti di dati di 214.077 utenti italiani, e senza che loro avessero in concreto scaricato l'applicazione, si confronti sul punto: Garante per la protezione dei dati personali, *'Cambridge Analytica: il Garante privacy multa Facebook per 1 milione di euro',* 28 Giugno 2019, file:///Users/valentina/Downloads/GarantePrivacy-9121352-2.0.pdf. Non è questa l'unica violazione rilevata, venendo a tempi quanto più recenti, cioè proprio al 2023, il Garante della privacy Irlandese ha impartito a Meta una multa pari 1,2 Milioni di euro per la violazione della normativa sulla Privacy europea, cfr: *'Meta, multa record di 1,2 miliardi dell'autorità per la privacy irlandese', 'in'* Rai News 24, 22 Maggio 2023, https://www.rainews.it/articoli/2023/05/meta-multa-record-di-12-miliardi-di-euro-dallautorita-per-la-privacy-irlandese-1eb1fe09-3a09-4b4b-93a4-d1e133c677b9.html#:~:text=L'Autorit%C3%A0%20garante%20della%20privacy,Garante%20europeo%20per%20la%20privacy.

[177] Infatti i dati ricoprono un ruolo fondamentale nell'economia digitale contemporanea, tanto che si può legittimamente pensare che il prezzo dell'iper-connessione e quindi della gratuità dei social sia proprio la continua messa a disposizione, da parte degli utenti usufruitori, di dati personali e non.

[178] A. Albrechtslund, *'Online social networking as Participatory surveillance', 'in'* First Monday, Vol. 13, N. 3, March 2008.

[179] Si tenga presente che il GDPR definisce il dato personale, all'articolo 4, come '*qualsiasi informazione riguardante una persona fisica identificata o identificabile'* e più in particolare i dati utilizzati dall'IA

sui *social*, vi sono anche quelli biometrici. Ne deriva che l'avvento di Facebook, e di tutte le successive piattaforme, ha contribuito ad una maggiore e sempre più semplice reperibilità di ciò che è necessario per il miglioramento della funzione di Riconoscimento facciale, così come per il suo impiego massivo, tanto in ambito privato quanto in quello pubblico, pur non risolvendo importanti problematiche che si analizzeranno nei capitoli successivi.[180] In ambito pubblico, il Riconoscimento facciale veniva e viene impiegato per incrementare la pubblica sicurezza nonché per la prevenzione e repressione dei reati. A questo ultimo proposito, si può ricordare che nel 2011 il governo di Panama, in collaborazione con Janet Napolitano (l'allora Segretario della Sicurezza Nazionale degli Stati Uniti), ha autorizzato l'impiego di un programma pilota della piattaforma di riconoscimento facciale *FaceFirst,* al fine di ridurre reati quali il traffico di droga e la criminalità organizzata.[181]

Il XXI secolo, e in particolare gli anni dal 2010 in poi, ha visto una forte implementazione dell'utilizzo del riconoscimento facciale, sia in ambito privato che pubblico. Con riferimento al settore privato possiamo ricordare il suo impiego, da parte di Facebook, per identificare il volto delle persone che potrebbero essere presenti nelle foto che gli utenti pubblicano e aggiornano con cadenza quasi quotidiana, fino alla possibilità di usarlo per sbloccare il nostro *smart-phone* (2017-IphoneX). Per quanto concerne invece gli impieghi per pubblici fini delle tecnologie di riconoscimento facciale, questi sono incrementati oltre aver involto sempre più ambiti, ma questo non vuol dire che le criticità e i problemi

---

quando si esplica in un'applicazione di riconoscimento facciale sono i dati biometrici,[179] definiti nello stesso articolo come '*i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*'.

[180] Ad accreditare quanto riportato si può anche citare il Privacy Shield del 2020, ossia l'accordo alla base della trasmissione dei dati dall'UE agli U.S che era in vigore prima di quello vigente, dove per la prima volta si pone una limitazione alla reperibilità e all'utilizzo dei dati personali da parte delle pubbliche autorità americane. Essendo Facebook del 2004, e l'accordo in questione del 2020, nulla impedisce di ipotizzare che antecedentemente le pubbliche autorità americane impiegassero, avendone libero accesso, i dati personali degli utenti tra cui le immagini del volto che la persona utilizzava quale immagine del profilo, o come semplice post, per ampliare i database di addestramento dell'IA, soprattutto perché, in ambito pubblico, il riconoscimento facciale veniva e viene impiegato per incrementare la pubblica sicurezza nonché la prevenzione e repressione dei reati. Per un maggiore approfondimento si veda sul punto: Garante per la protezione dei dati personali, *Privacy Shield,* https://www.garanteprivacy.it/documents/10160/0/Privacy+shield.+Lo+Scudo+per+la+privacy+fra+Ue+e+USA+-+Infografica.

[181] R. Tomkins, *'Panama expands use of facial recognition system at the airport', 'in'* UPI, 18 Settembre 2014, https://www.upi.com/Defense-News/2014/09/18/Panama-expands-use-of-facial-recognition-system-at-airport/6521411050216/.

connessi al suo utilizzo si siano vanificati o siano stati risolti, in particolare si discute della possibilità che questa tecnologia venga installata in luoghi pubblici o aperti al pubblico, utilizzo ad oggi vietato in Italia.[182]

2. Concetti e definizioni fondamentali per comprendere il funzionamento del Riconoscimento facciale: la *Computer Vision* come punto di partenza

Prima di procedere a descrivere e spiegare come funziona l'Intelligenza artificiale quando preposta al Riconoscimento facciale, è fondamentale riportare alcuni concetti e definizioni basilari, estranee al mondo giuridico, ma propedeutiche ad una comprensione quanto più esaustiva.

Il quadro storico, preso in considerazione nel precedente paragrafo, ha mostrato come il progresso informatico e gli studi cibernetici abbiano contribuito a rendere concretamente possibile tale applicazione di IA, in particolare il Riconoscimento facciale si inserisce nell'ambito della *Computer vision* (visione artificiale). La *Computer vision* è un campo dell'Intelligenza artificiale che consente al computer e ad altri sistemi di ricavare informazioni da immagini digitali, video e altri input visivi, e di elaborare detti dati al fine di prendere decisioni o comprendere l'ambiente o la situazione da cui detti impulsi scaturiscono. Di conseguenza se si può affermare che l'IA permette al computer di pensare, allora si può anche asserire che la *computer vision* permette a questo di vedere[183]. È quest'ultima un'affermazione avventata perché così come, per lungo tempo gli studiosi si sono e si stanno ancora ad oggi, interrogando sull'annosa questione: 'Possono le macchine pensare[184]?', allo stesso modo, gli studiosi che hanno concentrato le loro ricerche nel settore della Computer vision, si sono chiesti: 'Può la macchina vedere?'. Ma dire che la *Computer vision* è la branca dell'intelligenza artificiale che consente alla

[182] Cfr. Capitolo I, paragrafo 7 *'un freno all'impiego di sistemi di videosorveglianza dotati di riconoscimento facciale: il divieto dell'Italia, la legge n.5 del 3 Dicembre 2021',* della presente tesi.
[183] Cfr. *'Che cos'è la Computer Vision', 'in'* IBM, https://www.ibm.com/it-it/topics/computer-vision. E anche B. Marr, *'7 Amazing Examples of Computer and Machine Vision in practice', 'in'* Forbes, 8 Aprile 2019, https://www.forbes.com/sites/bernardmarr/2019/04/08/7-amazing-examples-of-computer-and-machine-vision-in-practice/#3dbb3f751018.
[184] Per un maggiore approfondimento sulla questione si può consultare: A. Turing, *'Computing machinery and Intelligence', 'in'* Mind a Quarterly review of Psychology and Philosophy, Vol. LIX, No. 236, October 1950; e: L. Floridi, *'The Ethics of Artificial intelligence. Principles, Challenges, and Opportunities' (Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide.),* a cura di M. Durante, Milano, Raffaello Cortina Editore, 2022.

macchina di vedere, significa affermare che le macchine possono emulare il processo compiuto dal cervello umano quando compie l'azione di '*vedere'* (qualcosa o qualcuno). Ad oggi è possibile, grazie ai progressi compiuti nello sviluppo dei modelli a reti neurali, consentire alla macchina di vedere, deve però tenersi sempre a mente che, seppur possibile, i margini di errore sono molto alti poiché molteplici sono i fattori che incidono sulla qualità del risultato, oltre al fatto che anche se molto avanzate, le tecnologie non sono, per loro natura, il cervello umano, a sua volta non esente dal commettere errori. Il processo che il nostro cervello compie per vedere è complesso, e l'algoritmo volto ad emularlo deve essere a ciò addestrato, prima di entrare in questo ambito vediamo brevemente il sistema visivo umano.

Innanzitutto, il sistema visivo umano è costituito da due componenti principali: l'occhio (formato a sua volta da sistema ottico e retina) e il Sistema Nervoso Centrale, che ha la funzione di elaborare le informazioni visive dando un significato a ciò che vediamo intorno a noi. L'occhio reperisce le radiazioni elettromagnetiche provenienti da diverse fonti di luce, e il cervello processa le informazioni che l'occhio recepisce e forma la scena così come noi la percepiamo. Tra l'occhio e il cervello c'è un meccanismo che agevola la funzione di analisi, e infatti ha la funzione di filtrare le radiazioni elettromagnetiche prima che giungano al cervello, e la connessione con quest'ultimo avviene tramite il nervo ottico (che è un fascio di fibre)[185]. Ciò spiegato, sembra impossibile riprodurre detto processo attraverso i sistemi di funzionamento di una macchina, ma la *Computer vision* si propone proprio di individuare metodi e modelli attraverso i quali una macchina possa estrarre autonomamente informazioni da immagini[186], non si vuol in tal contesto eguagliare l'essere umano, ma raggiungere un risultato ottimale, minimizzando gli errori e i rischi connessi a tale procedura. I metodi e i modelli che vengono sviluppati nella *Computer Vision* possono essere schematizzati su tre livelli: basso, medio e alto livello, ed è proprio quest'ultimo quello in cui si inserisce il riconoscimento facciale. Il *low-level* ossia il livello più basso è quello nel quale l'immagine viene acquisita, tale procedimento si svolge attraverso trasduttori che consentono di tradurre ciò che si manifesta nel mondo

[185] Cit. G. Naldi, *'Matematica, immagini e visione computazionale: gioie, dolori e possibili sfide',* Conferenza nell'ambito di '*Matematica, che passione'* dell'Università degli Studi di Milano, 15 febbraio 2012.
[186] L. Shapiro, G. Stockman, *'Computer Vision',* Prentice Hall, March 2000.

analogico, in immagini in versione digitale, dando così vita a dati grezzi in un linguaggio comprensibile alla macchina. In questa prima fase l'obiettivo è quello di pre-processare informazioni utili, ma primitive, come forma, profondità, o i contorni degli oggetti, e i risultati ottenuti saranno poi impiegati nelle fasi successive. Nella fase successiva, ossia quella intermedia, si esplicano procedimenti di estrazione di informazioni a partire dall'immagine digitale precedentemente acquisita, in questo caso si tratta di informazioni come linee, contorni, texture, luminosità e molte altre, cioè appunto tutto ciò che concerne la struttura dell'immagine. Infine, l'ultima fase in cui si sviluppano i modelli suddetti è il cosiddetto alto livello, ossia il livello dedicato alla comprensione semantica, nel quale l'immagine viene analizzata, attraverso il vaglio delle caratteristiche prima estrapolate, per fini diversi tra i quali il riconoscimento del volto di una persona determinata, in questo caso attraverso l'impiego dei dati biometrici connessi al soggetto stesso[187].

2.1 La definizione di Intelligenza artificiale e gli ulteriori concetti di reti neurali artificiali, *machine learning* e *deep learning*

Prima di poter spiegare il funzionamento dell'Intelligenza artificiale risulta necessario riprenderne la definizione, seppur questa non debba essere considerata in modo univoco e universale. Nel paragrafo 1 del presente capitolo, è stata riportata la definizione di IA formulata da Marco Somalvico nel 1987, ma non è Somalvico lo studioso che per primo fornì detta definizione; è necessario, infatti, tornare indietro di qualche anno fino al 1956, quando uno dei padri fondatori della disciplina 'Intelligenza Artificiale', nonché colui che ne coniò la denominazione, Jhon McCarthy, elaborò la prima definizione di IA rispondendo alla domanda '*che cosa è l'intelligenza artificiale?': 'It is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable.*[188]'

Se nel mondo scientifico la definizione di IA risale all'anno in cui la disciplina fu fondata programmaticamente, il mondo del diritto se ne interessò solo recentemente, infatti

[187] Cfr. A. Fusiello, *'Visione computazionale. Tecniche di ricostruzione tridimensionale',* Milano, FrancoAngeli, 2018.
[188] Cit. J. McCarthy, *'What is Artificial Intelligence?',* Formal Reasoning Group Stanford university, November 2007.

questa fu predisposta dalla Commissione Europea nella Comunicazione del 2018 '*L'intelligenza artificiale per l'Europa',* qui viene definita come: *'i sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi*[189]*'.* Successivamente la Proposta di Regolamento che predispone regole armonizzate sull'intelligenza artificiale, all'articolo 3 n.1, formalizza la definizione di IA disponendo che è: *'un software sviluppato con uno o più 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*[190]*'.* L'Allegato I della proposta di Regolamento indica tre modelli generali attraverso i quali un *software* può essere sviluppato e cioè: l'apprendimento automatico (che a sua volta si divide in apprendimento supervisionato e non; e apprendimento per rinforzo); approcci basati su logica e modelli espliciti della conoscenza (es. i sistemi esperti); e approcci statistici (es. stima *bayesiana*[191]). Giungiamo così a spiegare il funzionamento dell'IA[192], limitandoci ai *Software* sviluppati attraverso l'apprendimento automatico, perché sono quelli che prevalentemente vengono impiegati per la creazione e lo sviluppo di applicazioni di Riconoscimento facciale.[193]

---

[189] Comunicazione della Commissione Europea, 25 Aprile 2018, COM(2018) 237 final, *'L'intelligenza artificiale per l'Europa'.* Per un maggiore approfondimento della citata Comunicazione si rimanda al Capitolo I, paragrafo 2.1 della presente Tesi.

[190] Cit. Proposta di Regolamento del Parlamento europeo e del consiglio, 21 Aprile 2021, COM(2021) 206 final, *'Che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione.* Per un maggiore approfondimento a riguardo si veda Capitolo I, Paragrafo 6 della presente Tesi.

[191] Cfr. Allegato I Proposta di Regolamento del Parlamento europeo e del Consiglio, 21 Aprile 2021, COM(2021) 206 final, *'Che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione.* Sul punto si veda anche: G. Contissa, F. Galli, F. Godano, G. Sartor, *'Il regolamento europeo sull'intelligenza artificiale', 'in'* i-lex, fascicolo 2, Dicembre 2021, cit pp. 8 ss.

[192] Per semplificare si tenga a mente che l'Intelligenza artificiale è un insieme di tecnologie che combina dati, algoritmi e potenza di calcolo (Cit. Comunicazione della Commissione europea, 19 Febbraio 2020, COM(2020) 65 final, *Libro Bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla sfida,* p. 2). Gli algoritmi sono: '*una serie di istruzioni codificate che un computer deve seguire per svolgere un dato compito: quello per cui gli algoritmi sono impiegati è prendere decisioni, ossia selezionare e rendere visibile in modo 'sensato' l'enorme quantità di dati prodotti e disponibili sul web'* cit. presa da E. Garzonio, *'L'algoritmo: obiettivi ed implicazioni dello spazio digitale europeo', 'in'* Rivista italiana di informatica e diritto, fascicolo 2, 2021, DOI: 10.32091/RIID0037.
Cit. Comunicazione della Commissione europea, 19 Febbraio 2020, COM(2020) 65 final, *Libro Bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla sfida,* p. 2.

[193] Per poter spiegare il *Machine learning* bisogna innanzitutto ricordare che l'IA è un complesso sistema formato da *hardware* e *software,* il primo è la parte del sistema che consente il *training* delle reti neurali artificiali, mentre il secondo è definibile come l'insieme dei programmi che permettono lo svolgimento di funzioni al sistema di IA stesso.

Il *machine learning* (ML), in italiano conosciuto anche come apprendimento automatico, è una tecniche base dell'Intelligenza artificiale, che ne costituisce un suo sottogruppo. Nello specifico il ML è la tecnica impiegata per l'addestramento delle reti neurali artificiali. Quindi, prima di tutto, bisogna comprendere che cosa sono le reti neurali artificiali, le quali possono essere definite come un sistema di elaborazione dell'informazione, che si ispira, per il suo funzionamento, alle reti neurali biologiche (umane o animali). La loro struttura è assai complessa, sono infatti composte da una molteplicità di unità semplici, diversamente connesse tra di loro, con la funzione di elaborare l'informazione recepita. Le unità che costituiscono le reti neurali si dividono a loro volta in tre categorie: le unità di ingresso (*input*) che svolgono la mansione di recepimento dell'informazione, proveniente dall'ambiente esterno; le unità di uscita (*output*) che invece emettono risposte attraverso l'elaborazione delle informazioni recepite dalle unità di *input;* infine vi sono le unità nascoste (*hidden*) che comunicano solo ed esclusivamente con le unità poste all'interno della struttura neurale, senza mai entrare in contatto, né in entrata né in uscita, con l'ambiente esterno. Affinché una rete neurale sia in grado di fornire una risposta idonea allo stimolo in entrata ricevuto, è necessario che sia addestrata attraverso regole di apprendimento[194]. Il *Machine learning* consente l'apprendimento delle reti neurali*,* e ciò può avvenire attraverso modelli differenti, che si distinguono in base al grado di incidenza del programmatore[195]. Generalmente, cioè a prescindere dal tipo specifico di addestramento impiegato, nel ML gli algoritmi apprendono in modo autonomo come adempiere al compito loro impartito, più nello specifico si tratta di una modalità di apprendimento che si basa sul riconoscimento di *patterns,* posti all'interno di dati non strutturati i quali a loro volta vengono utilizzati per addestrare gli algoritmi, così gli algoritmi stessi, attuando delle comparazioni tra i nuovi dati e i *patterns* antecedentemente riconosciuti, sono in grado di predire nuove correlazioni.[196]

---

[194] Cit. D. Floreano, C. Mattiussi, *'Il manuale delle reti neurali',* Bologna, il Mulino, 2002, pp. 16 ss.
[195] Cfr. N. Boldrini, *'Reti neurali: cosa sono e a cosa servono', 'in'* AI4Business, 2 Luglio 2023, https://www.ai4business.it/intelligenza-artificiale/deep-learning/reti-neurali/.
[196] Cit. G. Mobilio, *'Tecnologie di Riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative',* Napoli, Editoriale Scientifica, 2021, pp 52,53.

I differenti prototipi impiegati nell'ambito del ML per l'addestramento degli algoritmi sono: l'addestramento supervisionato che è il modello in cui il programmatore (ossia l'essere umano) interviene non soltanto fornendo all'algoritmo i dati di entrata (*input*), attraverso i quali essere addestrato in concreto, ma anche indicando quali sono nello specifico i risultati (*output*) attesi dall'elaborazione dell'informazione e questo per consentire al sistema di riconoscere i *patterns.* Il secondo è l'addestramento non supervisionato, dove non interviene in alcun caso il programmatore, cioè il sistema viene lasciato apprendere da sé, di modo tale che possa autonomamente riconoscere gli schemi, senza che ciò sia stimolato dalle correzioni predisposte dall'essere umano; infine, il terzo modello di apprendimento è quello per rinforzo, il quale si basa a sua volta sull'intervento del programmatore, il quale fornisce una serie di *feedback,* che hanno la funzione di far comprendere al sistema quando ha tenuto un comportamento corretto e quando sbagliato[197]. Infine, per una completa trattazione, si evidenzia che le continue ricerche in ambito di reti neurali artificiali hanno condotto al c.d. *deep learning* (apprendimento profondo)*,* qualificabile come una sottocategoria del *machine learning* che ha consentito importanti sviluppi nelle applicazioni di IA per il riconoscimento facciale grazie alle sue peculiari ed innovative caratteristiche. Si tratta di una IA che sfrutta sempre le reti neurali artificiali, ma in questo caso multistrato, e i *patterns* che sono presenti nei dati, cioè nelle informazioni in entrata (*input*), vengono estratti in modo autonomo dall'algoritmo, cioè avviene per gradi successivi di astrazione e classificazione non lineare, al fine di ottenere determinati e specifici dati in uscita (*output*)[198].

3. Come funziona il riconoscimento facciale

I concetti che sono stati spiegati e approfonditi nei paragrafi precedenti pongono le basi per comprendere come funzionano le tecnologie di riconoscimento facciale (TRF). Innanzitutto, il riconoscimento facciale può essere inteso come un ambito specifico di ricerca in seno alla *Computer vision,* il quale si occupa di creare e sviluppare sistemi *software* in grado di analizzare volti umani presenti in immagini e video. I sistemi di

[197] Cfr. M. A. Boden, Traduzione a cura di F. Calzavarini, *'L'intelligenza artificiale',* Bologna, il Mulino, 2019.
[198] G. Mobilio, *'Tecnologie di Riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative', op. cit.* 55; e cfr. C Accotto, *'Il mondo-dato. Cinque brevi lezioni di filosofia della programmazione',* Milano, EGEA, 2017, cit. p 75

riconoscimento facciale, ad oggi più all'avanguardia, sono costruiti attraverso l'impiego del *deep learning,* il quale permette di dar vita a programmi software in grado di trasformare le immagini facciali nel linguaggio computazionale, ossia in espressioni numeriche che possono essere poste a confronto al fine di estrapolare le somiglianze[199]. Le tecnologie in questione possono essere impiegate per diversi scopi, le stesse funzioni cui sono preposte si intendono dalla definizione, concettualizzata in ambito europeo, degli *automatic facial recognition system (AFRS),* cioè sistemi che permettono di analizzare '*immagini digitali che contengono volti di individui, ai fini di identificazione, autenticazione/verifica, o categorizzazione di tali persone'*[200]. Prima di vederne i differenti impieghi, è bene constatare il procedimento compiuto dai sistemi in questione per raggiungere lo scopo di identificazione piuttosto che di verificazione o categorizzazione. Si tratta di un procedimento che si sviluppa in più fasi, l'una strettamente connessa all'altra, che si susseguono al fine di fornire il risultato atteso.

La prima fase di questo complesso procedimento è quella di *Acquisizione dell'immagine:* attraverso tale passaggio iniziale vengono rilevati i tratti del volto di un soggetto e convertiti in formato digitale. L'acquisizione può avvenire in modo differente, o attraverso i c.d. sistemi biometrici interattivi, o mediante i c.d. sistemi biometrici passivi: i primi sono detti interattivi o partecipativi in quanto la raccolta dei dati biometrici avviene mediante la cooperazione consapevole del soggetto interessato; al contrario i secondi sono detti passivi perché la raccolta dei dati di interesse avviene senza l'effettiva e consapevole partecipazione dell'interessato[201]. A seconda che sia usato uno o l'altro sistema, non varia solo la consapevole partecipazione dell'interessato, ma anche la qualità dei dati che vengono effettivamente raccolti dalla tecnologia impiegata.

La seconda fase è quella di *individuazione di un volto:* è questo il processo di separazione del volto rispetto all'immagine complessiva in cui si trova.

---

[199] Cit. J. Buolamwini, V. Ordóñez, J. Morgenstern, E. Learned-Miller, *'Facial recognition technologies: A Primer',* May 29, 2020.

[200] La definizione qui riportata è data dal Gruppo di lavoro articolo 29, cit. Parere 16/2011 del Gruppo di lavoro articolo 29 per la protezione dei dati, adottato il 22 Marzo 2012, WP 192, *Parere relativo al riconoscimento facciale nell'ambito dei servizi online e mobili.* p.2.

[201] La distinzione tra sistema biometrico interattivo e passivo è stata presa da: Garante per la protezione dei dati personali, *'Linee-guida in materia di riconoscimento biometrico e firma grafometrica. Allegato A al provvedimento del Garante del 23 Novembre 2014,* 12 Novembre 2014, p. 6.

Segue poi la terza fase, cioè quella di *normalizzazione:* questa è volta ad attenuare le varianti presenti nelle regioni del viso umano, in concreto ciò si può realizzare in modo differente come ad esempio attraverso procedure di conversione ad una dimensione standard piuttosto che mediante l'allineamento della distribuzione dei colori.

Dopo questa si ha la fase di *estrazione delle caratteristiche:* attraverso specifici meccanismi vengono recuperati gli elementi distintivi dell'immagine digitale di un soggetto, i meccanismi impiegati si distinguono in estrazione olistica e basata sui tratti oppure i due metodi possono essere combinati. L'estrazione olistica si sostanzia in '*una rappresentazione matematica dell'intera immagine come risulta dall'analisi dei principali componenti',* mentre l'estrazione delle caratteristiche mediante i tratti è la *'localizzazione delle specifiche caratteristiche del volto quali occhi, naso e bocca*[202]*':* questi due possono essere combinati dando così vita al metodo di estrazione ibrido delle caratteristiche. Questa fase consente di elaborare il c.d. *template,* ossia il modello che in concreto è suscettibile di confronto con le immagini presenti nei *database*[203].

Viene, in seguito, la fase di *registrazione:* l'immagine digitale di un individuo, per la prima volta esposto al riconoscimento facciale, viene conservata al fine di successivi confronti.

L'ultima fase che si connota nel procedimento di funzionamento delle TRF è quella di *confronto:* si attua, in concreto, un confronto tra gli elementi identificativi del soggetto esposto al trattamento e una serie di caratteristiche registrate negli archivi a disposizione del sistema[204].

Tornando ora alla definizione dei AFRS sopra citata, questa evidenzia le funzioni cui possono assolvere queste tecnologie ossia: identificazione, autenticazione/verifica e categorizzazione. La principale distinzione tra autenticazione e identificazione consiste

[202] Ibidem nota 201, cit. note 2 e 3 p. 2.
[203] Cfr. J. Della Torre, *'Tecnologie di riconoscimento facciale e procedimento penale', 'in'* Rivista italiana di Diritto e Procedura Penale, n. 3, 2022.
[204] Gruppo di lavoro articolo 29, *op. cit.* lo schema riportato che spiega il funzionamento del riconoscimento facciale è ripreso dallo stesso parare 16/2011 del gruppo di lavoro articolo 29, p 2.

nel fatto che nel primo caso viene operato un confronto '*uno-a-uno',* nel secondo caso invece si esplica un confronto *'uno-a-molti'*. L'analisi comparativa uno-a-uno avviene tra i dati biometrici riferiti ad una persona specifica e il modello (di identificazione biometrica) presente in un *database.* Nel secondo caso invece, il confronto avviene tra il *template* registrato e quelli disponibili, è questo un raffronto che ha come obiettivo l'identificazione del soggetto esposto al trattamento, del quale non si conosce l'identità[205].

Un'ultima puntualizzazione è necessaria al fine della presente trattazione, ossia il fatto che i sistemi di *facial recognition* possono essere predisposti a due modalità di funzionamento distinte e cioè sia *Real Time* che in differita. Il riconoscimento facciale in differita (o ex post) viene per lo più impiegato nel contesto di indagini giudiziarie per attuare un confronto tra le foto identificative di individui di interesse per l'indagine, le quali vengono recepite tramite videocamere o attraverso documenti, e le immagini digitali contenute in un *database* di riferimento, le quali ritraggono soggetti identificati e conosciuti. Dall'altro lato la modalità *Real Time* sfrutta video *live* dai quali estrapola, in modo istantaneo, fotografie di individui al fine di porle a raffronto con le immagini digitali di persone identificate e presenti in un apposito archivio[206]. Molte riserve sono state espresse con riferimento al riconoscimento facciale *Real Time,* dette perplessità sono strettamente connesse ai fattori che incidono sull'esattezza dei risultati prodotti, che se già presenti nella modalità 'in differita', si ampliano e incremento nella modalità *Real Time.* Le tecnologie in questione si basano su algoritmi che svolgono calcoli probabilistici che permettono di individuare un *match,* nel caso in cui vi sia, tra gli elementi posti a confronto, e questo fa constatare che alle operazioni svolte è sempre connessa una certa percentuale di errore, nonostante si sia cercato, e si cerchi tutt'ora di minimizzare i c.d. *falsi positivi*[207]. In particolare si verifica un falso positivo quando il sistema evidenzia un'analogia non rispondente alla realtà, ma può verificarsi anche il caso contrario ossia i c.d. *falsi negativi,* cioè l'algoritmo ritiene, anche in questo caso in modo inesatto, che non

[205] Cfr. G. Borgia, *'Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuri sviluppi normativi sul fronte eurounitario', 'in'* La legislazione penale, ISSN: 2421-552X, 11 Dicembre 2021. E anche: E. Currao, *'Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?', 'in'* Diritto Penale e Uomo, si può prendere visione dell'articolo completo al seguente link: https://dirittopenaleuomo.org/wp-content/uploads/2021/05/Currao_DPU.pdf.

[206] Cfr. Greens/EFA, '*Biometric and Behavioural Mass Sourveillance in EU Member States*', October 1, 2021, link: https://www.greens-efa.eu/biometricsurveillance/.

[207] Cit. G. Mobilio, *op. cit.* 35,36.

vi sia alcuna corrispondenza tra l'immagine campione e i modelli biometrici presenti nei *database* a disposizione del sistema, ma una corrispondenza invece sussiste. Gli errori, come sopra preannunciato, dipendono da diversi fattori, ma si può affermare che il punto chiave sta nel fatto che nessuna tecnologia è in grado di creare un unico *faceprint* (modello facciale) per ciascun soggetto di riferimento e questo perché, nella produzione del modello, l'algoritmo valuta una molteplicità di fattori tra cui i capelli, l'angolazione della telecamera, la luce, la risoluzione dell'immagine, il *make-up* e molti altri ancora[208]. Si può anche segnalare l'irrisolto problema dei gemelli, infatti allo stato attuale dello sviluppo tecnologico non vi è possibilità per una macchina di non commettere errori quando sia chiamata a decidere circa soggetti fratelli gemelli (nello specifico omozigoti). In ultima battuta vorrei accennare brevemente al problema connesso ai dati che vengono utilizzati per addestrare gli algoritmi preposti al riconoscimento facciale, che a loro volta incidono sui risultati e sulla loro correttezza. Più precisamente i modelli impiegati per progettare gli algoritmi, nonché le variabili prese in considerazione possono produrre un effetto discriminatorio e dare origine a *Bias*[209]. Di questo argomento nello specifico ci si occuperà in seguito, basti qui rammentare che i problemi presenti nel riconoscimento facciale 'in differita' si amplificano in maniera esponenziale nella versione in tempo reale e questa è solo una delle ragioni per cui l'Italia ne ha proibito l'adozione e istallazione.

[208] J. Buolamwini, V. Ordóñez, J. Morgenstern, E. Learned-Miller, *op. cit.* 12.
[209] Cfr. S. Barocas, E. W. Felten, J. Huey, J. A. Kroll, J. R. Reidenberg, D. G. Robinson, H. Yu, *'Accountable Algorithms', 'in'* University of Pennsylvania Law Review, Vol. 165: 633.

CAPITOLO III
IMPIEGO DEI SISTEMI DI RICONOSCIMENTO FACCIALE PER FINI DI PUBBLICA SICUREZZA
IL PARADIGMA DI UNA NUOVA SORVEGLIANZA DI MASSA

1. Pubblica sicurezza e sorveglianza di massa: le fondamenta della *Dataveillance*

Come si è avuto modo di evidenziare nei capitoli precedenti, si è assistito ad un sempre più frequente impiego dei sistemi di riconoscimento facciale e ciò soprattutto grazie agli importanti sviluppi tecnologici e informatici che, dalla metà del XX secolo ad oggi, hanno reso possibile la diffusione di detti sistemi. Se è facile constatare quali siano i meriti del progresso tecnologico lo stesso non si può dire del mondo giuridico, dove l'assenza di una disciplina puntale volta a regolare gli equilibri di utilizzo dell'IA, fa emergere le difficoltà connesse ad un suo uso improprio, nonché il difficile bilanciamento fra i diritti della persona e la pervasività di un impiego massivo[210]. Ciò nonostante, le tecnologie che sfruttano l'IA sono sempre più onnipresenti, sia in ambito sociale che giuridico, e questo porta sia i soggetti privati che le pubbliche autorità a farvi affidamento così da determinarsi un legame inestricabile tra mondo reale e mondo virtuale[211]. L'era dei *Big Data* ha consentito di sfruttare i vantaggi di dette tecnologie nei più svariati contesti, tanto appartenenti al settore pubblico quanto a quello privato, dalla Ricerca online (i motori di ricerca imparano da enormi quantità di dati al fine di fornire risultati sempre più efficienti alla ricerca effettuata dall'utente), alla traduzione automatica (Google translate è un chiaro esempio di miglioramento dell'efficienza dell'IA, le traduzioni fornite in passato rispetto a quelle che possono ottenersi oggi evidenziato l'importanza che i dati e la loro analisi hanno per l'addestramento degli algoritmi che permettono il funzionamento di queste tecnologie), e ancora in ambito di Cyber sicurezza, per la creazione di case, città e

[210] Si veda, per un maggiore approfondimento circa la disciplina che regola l'IA e il riconoscimento facciale, il Cap. I par. 1 ss. Della presente tesi.
[211] Cfr. L. Floridi, *'La quarta rivoluzione. Come l'infosfera sta trasformando il mondo',* Milano, Raffaello Cortina Editore, 2014, p. 55 ss.

infrastrutture intelligenti, per consentire ai veicoli la guida automatica, ma anche per migliorare le diagnosi mediche e nell'ambito delle pubbliche amministrazioni etc[212]…

Preso atto della pervasività dell'utilizzo delle tecnologie di riconoscimento facciale, l'analisi verrà ora incentrata sull'uso di queste tecnologie per fini di sicurezza da parte delle pubbliche autorità. In particolare si vuole evidenziare come un uso pregiudizievole dei diritti della persona, e nello specifico del diritto alla *privacy,* possa far evolvere le competenze connesse alla pubblica sicurezza in sorveglianza di massa, e quindi in *Dataveillance.*

1.1 Declinazione pluralistica del concetto di *sicurezza* nell'ordinamento italiano

Su delucidazione della giurisprudenza costituzionale si può oggi affermare che il concetto di *sicurezza* ha una declinazione pluralistica, potendosi distinguere una sicurezza *'primaria'*, che esprime l'accezione tradizionale di sicurezza pubblica; da una sicurezza *'secondaria',* che deve intendersi come un insieme di operazioni strettamente connesse l'una all'altra, che coincidono ad una pluralità differenziata di funzioni.[213]

La sicurezza in senso tradizionale è disciplinata dall'articolo 117, comma secondo, lettera h), e dall'articolo 118, comma terzo della Costituzione[214], così come novellati dalla riforma del Titolo V avutasi nel 2001. La riforma costituzionale ha riconfermato che tale declinazione di sicurezza è di competenza legislativa dello Stato, rientrante nelle mansioni di polizia giudiziaria e di pubblica sicurezza, escludendo esplicitamente la competenza della polizia amministrativa locale. L'articolo in

[212] Cfr. Parlamento europeo 'Attualità', *'Che cos'è l'intelligenza artificiale?',* ultimo aggiornamento: 28/06/2023, https://www.europarl.europa.eu/news/it/headlines/society/20200827STO85804/che-cos-e-l-intelligenza-artificiale-e-come-viene-usata#:~:text=L'intelligenza%20artificiale%20%C3%A8%20largamente,i%20rifornimenti%20e%20la%20logistica.

[213] Cit. G. Mobilio, *'Profilare tramite riconoscimento facciale: il caso della sicurezza urbana', 'in' 'Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche',* a cura di A. Adinolfi e A. Simoncini, Napoli, Edizioni Scientifiche Italiane, 2022, p. 187.

[214] L'articolo 117, comma 2, lettera h, della Costituzione, dispone: *'Lo Stato ha legislazione esclusiva nelle seguenti materie: … h) Ordine pubblico e sicurezza, ad esclusione della polizia amministrativa locale.'*

questione deve però essere letto in combinato disposto con il riformato terzo comma dell'articolo 118 Cost., nel quale si ammette la possibilità di disciplinare con legge statale il coordinamento tra Stato e Regioni nelle materie di 'ordine pubblico e 'sicurezza' e 'immigrazione'. Volendo fornire una definizione oggettiva di pubblica sicurezza questa è *'la funzione che consente agli individui di vivere tranquillamente nella comunità e di agire in essa per manifestare la propria individualità e per soddisfare i propri interessi*[215]*'.* Ad essa si devono pertanto ricollegare quelle attività, preventive e repressive, volte al mantenimento dell'ordine pubblico al fine di garantire una convivenza ordinata e civile all'interno dello Stato nazionale, oltre che per tutelare le istituzioni, i cittadini e i loro beni[216].

Se si prende ora in considerazione il concetto di sicurezza *'secondaria'*, tenendo presente quanto detto a riguardo poc'anzi, questa ricomprendere in generale tutte le competenze che vogliono assicurare un miglioramento degli ambiti sociali e territoriali nei quali gli enti locali operano, questo al fine di aumentare la possibilità che siano sussistenti le precondizioni volte a rendere più efficiente l'esercizio delle funzioni di ordine pubblico tradizionali[217]. Un momento importate, ai fini della presente trattazione, è rappresentato dal decreto legge n. 14 del 20 febbraio 2017 in quanto in esso viene formalizzata la definizione di *sicurezza urbana*[218]*,* ponendo le basi per un'azione coordinata tra Stato ed enti territoriali, ha infatti dato la possibilità di riqualificare gli strumenti consensuali per mezzo dei quali dar vita a politiche di

---

[215] Cit. F. Paolozzi, *'FOCUS sulla GIURISPRUDENZA COSTITUZIONALE in materia di SICUREZZA PUBBLICA', 'in'* Servizio Affari legislativi e qualità dei processi normativi (Direzione Generale Affari istituzionali e legislativi della Giunta della Regione Emilia Romagna, 2011, p. 2.

[216] Cfr. Corte Costituzionale, sentenza n. 290 del 2001, inoltre sul punto si veda P. Bonetti, *'La giurisprudenza costituzionale sulla materia 'sicurezza' conferma la penetrazione statale nelle materie di potestà legislativa regionale', 'in'* Forum di Quaderni Costituzionali, 2010, p. 1 ss, https://www.forumcostituzionale.it/wordpress/images/stories/pdf/old_pdf/1138.pdf.

[217] Ibidem nota 216. Inoltre G. Mobilio, *'Profilare tramite riconoscimento facciale: il caso della sicurezza urbana', 'in' 'Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche', op. cit.*

[218] La definizione di sicurezza urbana è individuata nell'articolo 4 del decreto legge n.14 del 2017, il quale dispone: *'Ai fini del presente decreto, si intende per sicurezza urbana il bene pubblico che afferisce alla vivibilità e al decoro delle città, da perseguire anche attraverso interventi di riqualificazione (anche urbanistica, sociale e culturale) e recupero delle aree o dei (siti degradati), l'eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio, la promozione (della cultura) del rispetto della legalità e l'affermazione di più elevati livelli di coesione sociale e convivenza civile, cui concorrono prioritariamente, anche con interventi integrati, lo Stato, le Regioni e province autonome di Trento e di Bolzano e gli enti locali, nel rispetto delle rispettive competenze e funzioni'.*

sicurezza volte a garantire la collaborazione tra Stato centrale e i vari livelli di governo[219]. Di particolare importanza è la disposizione contenuta nell'articolo 5[220], comma secondo, lettera a), del decreto in analisi poiché apre le porte all'utilizzo capillare e sempre più pervasivo dei sistemi di videosorveglianza; è infatti a questo momento che si può ricondurre l'inizio dell'impiego di sistemi di sicurezza dotati di tecnologie di riconoscimento facciale nelle realtà territoriali comunali.[221]

A questo punto è bene evidenziare i problemi connessi a quanto appena rilevato. Da un lato non era presente alcuna specifica normativa che autorizzasse le amministrazioni locali all'impiego di queste tecnologie, definendone la disciplina e i relativi limiti di utilizzo[222]; dall'altro lato si apre la possibilità che siano queste sfruttate per l'adempimento di funzioni non riconducibili all'ambito della sicurezza *'secondaria',* ma quanto più a quella *'primaria'*, emergendo l'utilità ai fini di prevenzione e repressione dei reati, funzione rimessa alla competenza statale[223]. Tenendo in considerazione quanto fino ad ora evidenziato, oltre alla mancanza di una normativa statale, Parlamentare o Governativa, che disciplini in modo compiuto le TRF, nonché l'importante impatto che i sistemi di riconoscimento facciale hanno sul diritto al rispetto della vita privata e sul diritto alla protezione dei dati personali, si prospetta la possibilità di travalicare i limiti connessi alla tutela della privacy per dar

---

[219] Cfr. M. Bonazzi, *'La videosorveglianza ai fini della tutela dell'ordine e della sicurezza pubblica, con particolare riferimento alle novità introdotte dalla legge 18 Aprile 2017, n. 48 (Disposizioni urgenti in materia di sicurezza delle città), 'in'* Rivista di Polizia, 2018, p. 545 ss.

[220] L'articolo 5, comma secondo lettera a), del decreto legge 14 del 2017, dispone: *'I patti per la sicurezza urbana di cui al comma 1, perseguono, prioritariamente, i seguenti obiettivi: a) prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria, attraverso servizi e interventi di prossimità, in particolare a vantaggio delle zone maggiormente interessate da fenomeni di degrado, anche coinvolgendo, mediante appositi accordi, le reti territoriali di volontari per la tutela e la salvaguardia dell'arredo urbano, delle aree verdi e dei parchi cittadini e favorendo l'impiego delle forze di polizia per far fronte ad esigenze straordinarie di controllo del territorio, nonché attraverso l'installazione di sistemi di videosorveglianza'*

[221] G. Mobilio, *'Profilare tramite riconoscimento facciale: il caso della sicurezza urbana', 'in' 'Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche', op. cit.* 191

[222] Infatti a livello legislativo vi sono solo riferimenti indiretti come quello contenuto nel decreto legge n.14 del 2017, che all'articolo 7, comma 1-*bis,* dispone: *'Al fine di conseguire una maggiore diffusione delle iniziative di sicurezza urbana nel territorio, nonché per ulteriori finalità di interesse pubblico, i patti di cui al comma 1 possono riguardare…sistemi di sorveglianza tecnologicamente avanzati, dotati di software di analisi video per il monitoraggio attivo per l'invio di allarmi automatici a centrali delle forze di polizia o di istituti di vigilanza privata convenzionati.'*

[223] G. Mobilio, *'Profilare tramite riconoscimento facciale: il caso della sicurezza urbana', 'in' 'Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche', op. cit.*

vita ad una società sorvegliata[224], aprendosi quindi la strada al tramutarsi delle tecnologie di riconoscimento facciale in tecnologie di controllo della vita quotidiana.

1.2 Dalla garanzia di uno Stato sicuro alla sorveglianza di massa: il bilanciamento tra diritto alla Privacy e sicurezza pubblica

Le considerazioni che emergono nel paragrafo precedente aprono le porte alla necessità di indagare l'evenienza che, attraverso la garanzia di una pubblica sicurezza, si esplichi, al contrario, una vera e propria sorveglianza di massa.

Prima di tutto pare opportuno tenere presente il complesso rapporto sussistente tra sicurezza e libertà. Nell'ambito di questo rapporto uno dei campi in cui si evidenziano le principali e più gravi tensioni è quello in cui il diritto alla *privacy*[225] può rappresentare un ostacolo per la tutela della sicurezza, tanto dei singoli quanto della società nel suo complesso[226]. Ciò che rende particolarmente complicata la relazione suddetta si identifica nel ruolo ambivalente che la sicurezza svolge nel nostro ordinamento, essendo tanto 'garanzia dei diritti' quanto un 'limite' all'esercizio dei medesimi e, in particolare, può diminuire lo spazio lasciato al diritto alla *privacy* fino al verificarsi di un'illecita compressione del medesimo[227]. Parte della dottrina mette in luce l'estesa correlazione che sussiste tra il diritto alla privacy e l'apparato delle libertà, al fine di evidenziare che solo se si garantisce un'adeguata protezione del primo può assicurarsi un libero esercizio di tutte le altre libertà. Così affermando, la riservatezza si qualificherebbe come il presupposto necessario affinché un cittadino possa sentirsi libero nella sfera collettiva, oltre che 'sicuro' in quella privata[228]. Allo

---

[224] Cit. D. Lyon, *'La Società Sorvegliata. Tecnologie di controllo della vita quotidiana',* Milano, Feltrinelli Editore, 2001.

[225] Il diritto alla *privacy* è sancito quale diritto fondamentale dell'individuo all'articolo 8 della Convenzione EDU, si tenga già presente che è un diritto mutevole che ha affrontato diverse stagioni, infatti nella Convenzione EDU si parla di diritto alla riservatezza ma ad oggi, nell'era dell'informazione, questo coincide con il diritto alla protezione dei dati personali sancito all'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea.

[226] Cfr. C. Barone, *'Privacy, Sicurezza e Libertà nell'era della sorveglianza di massa e dell'emergenza terrorismo',* Tesi di Dottorato di Ricerca in Pluralismi giuridici, Università degli studi di Palermo, 2019, p. 100 ss.

[227] Cfr. S. Scagliarini, '*La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica', 'in'* Consulta online, periodico telematico fascicolo 2, 9 Luglio 2021, ISSN 1971-9892, p. 564 ss.

[228] Sul punto si esprimono in tal senso: S. Rodotà, '*Privacy, libertà e dignità, discorso conclusivo della Conferenza internazionale sulla protezione dei dati', 'in'* Garante per la protezione dei dati personali,

stesso tempo, questa visione è stata ampiamente criticata da differente parte della dottrina che evidenzia come, attraverso tale accezione del diritto alla *privacy*, si ammetta la possibilità per i singoli di esigere la non interferenza nella loro vita privata, venendo così a confondere il diritto alla riservatezza con la pretesa di segretezza totale, qualificabile a sua volta come un ostacolo insormontabile per la vita in società nonché per l'impiego di tecnologie come strumento di prevenzione e repressione dei reati.[229]

Avendo posto l'attenzione su queste due tesi contrapposte pare necessario chiedersi quale sia il confine, oltrepassato il quale, la compressione del diritto alla privacy si trasforma in violazione illegittima. La risposta a questo quesito deve essere ricercata con la consapevolezza che nella contemporaneità si sono inseriti fattori in grado di incidere significativamente e irreversibilmente sul modo di intendere tanto il diritto alla privacy quanto la sicurezza quale bene costituzionalmente garantito, e in particolare si deve avere a mente l'incessante progresso tecnologico e la sempre più pervasiva diffusione di strumenti di sorveglianza di massa. Per poter comprendere quale sia un adeguato bilanciamento tra sicurezza e diritto alla *privacy* occorre indagare quale sia il nucleo essenziale di quest'ultimo, operazione tutt'altro che agevole se si considera la mutevolezza che lo caratterizza[230]. Fin dagli anni '80 inizia a profilarsi, in ambito europeo, il diritto alla protezione dei dati personali il quale era originariamente concepito come controllo dei propri dati, il che comportava la qualifica della riservatezza in termini di conoscenza esclusiva delle proprie vicende private[231]. Se inizialmente il diritto alla protezione dei dati personali aveva una valenza circoscritta, ad oggi non è più così, infatti l'evoluzione tecnologica e tutti gli effetti ad essa connessi, ha attribuito una valenza centrale a quel diritto che diviene il

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293. Inoltre v. C. Cocq and F. Galli, *'The Catalasing effect of serious crime on the use of surveillance technologies for prevention and investigation purposes', 'in'* New Journal of European Criminal Law, Vol. 4, 2013, p. 275 ss.

[229] Cfr. A. Pintore, *'Diritto e sicurezza ai tempi del terrore', 'in'* Quaderni di Scienza Politica, 2007.

[230] Il diritto alla *privacy* è stato recepito nel nostro ordinamento attraverso, da un lato, l'articolo 2 della Carta Costituzionale il quale consente, ponendo la persona al centro dell'ordinamento, il riconoscimento di diritti anche posti al di fuori di quelli enunciati dal catalogo costituzionale; e dall'altro lato su lettura congiunta degli articoli 13, 14, 15, 21 Cost.

[231] Cfr. F. Pizzetti, *'Privacy e diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo regolamento europeo',* Torino, Giappichelli, 2016, p. 36 ss.

modello europeo di tutela della riservatezza[232]. Nell'era dell'informazione si può infatti affermare che il diritto alla riservatezza si viene a configurare con il diritto alla protezione dei dati personali. A ciò si deve aggiungere che con l'entrata in vigore del Trattato di Lisbona e, con esso, della Carta dei diritti fondamentali dell'Unione Europea, il diritto alla protezione dei dati personali viene identificato come un diritto fondamentale autonomo, enunciato all'articolo 8, che si pone in posizione simmetrica rispetto all'articolo 8 della Convenzione EDU che afferma il diritto alla riservatezza[233]. Di conseguenza una restrizione del diritto in analisi, nonché di ogni altro diritto previsto dalla Carta, deve essere attuata nel rispetto del disposto normativo di cui all'articolo 52[234] il quale impone che sia espressamente prevista dalla legge, che non leda il contenuto essenziale del diritto di cui si vuole apportare una restrizione e, infine, deve rispondere ad una esigenza generale dell'Unione Europea. L'aspetto problematico connesso alla norma in questione consiste, come sopra anticipato, nell'individuazione del c.d. 'contenuto essenziale' del diritto alla *privacy*. Più precisamente l'unico aspetto problematico rimane l'individuazione del nucleo forte solo se la sicurezza pubblica viene perseguita mediante l'impiego di strumenti tradizionali, ma nel momento in cui vengono utilizzati dispositivi ad alta innovazione tecnologica e specialmente dotati della funzione di riconoscimento facciale, l'indagine volta a constatare quali siano le situazioni che, integrando i requisiti chiesti dall'articolo 52 della Carta europea dei diritti fondamentali, consentono un tale uso e legittimo diviene gravosa.

Ma prima di concentrarci su tale aspetto, a chi scrive pare appropriato inserire qualche considerazione in merito al contenuto essenziale del diritto alla privacy. Innanzitutto, pare opportuno chiarire che non è possibile identificare in modo certo e definitivo il

[232] Cit. M. Orofino, *'Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione', 'in'* Media Laws (Rivista di diritto dei media), 2/2018, p. 14-15

[233] L'articolo 8 della Convenzione EDU sancisce il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza; del pari l'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea garantisce il diritto alla protezione dei dati personali. I due possono essere letti simmetricamente poiché, come specificato nella nota 212, il diritto alla *privacy* è un diritto mutevole e camaleontico, di conseguenza, nell'era digitale, il diritto alla vita privata coincide con il diritto alla protezione dei dati personali.

[234] Come si specificherà nelle prossime pagine, l'articolo 52 della CDFUE deve essere letto unitamente alla disciplina individuata nel GDPR e nella LED, inoltre deve aversi riguardo del fatto che è stata avanzata la proposta di Regolamento sull'Intelligenza Artificiale, a tal proposito si rimanda al Cap. I della presente tesi.

contenuto essenziale del diritto alla privacy, poiché si tratta di un diritto che per sua natura è mutevole, avendo la capacità di adattarsi all'evoluzione sociale e alle necessità del vivere in società. Di conseguenza dovrà essere ricercato di volta in volta, attraverso un puntuale bilanciamento tra il diritto in questione e il potere suscettibile di causarne la compressione come, per l'appunto, la sicurezza pubblica che lo Stato si prefigge di garantire[235]. Proprio per queste ragioni il bilanciamento è l'operazione che consente di constatare una possibile violazione, suscettibile di qualificarsi come sorveglianza di massa quando le situazioni a confronto siano la tutela dei dati personali da un lato e la sicurezza pubblica dall'altro[236]. Da questo punto di vista, il bilanciamento è '*la tecnica per l'individuazione e la tutela del contenuto'* poiché '*attraverso il sindacato intorno al ragionevole bilanciamento, il giudice delle leggi realizza propriamente le sue funzioni: quella di fornire tutela al loro nucleo di valore[237]'*. Da questo punto di vista, pare conforme ritenere che, dove finisce il bilanciamento si individua il contenuto essenziale del diritto alla riservatezza, cioè ove il giudice giudica sbagliato il bilanciamento in questione si può individuare il contenuto essenziale del diritto alla *privacy* e quindi quel contenuto incomprimibile senza che si individui una violazione illecita[238].

1.3 Il diritto alla tutela dei dati personali a confronto con le tecnologie di riconoscimento facciale: la *Dataveillance*

Nel paragrafo precedente si è ricercato il contenuto essenziale del diritto alla *privacy* nel difficile rapporto con il potere dello Stato di garantire pubblica sicurezza, ciò da un punto di vista tradizionale, ora non resta che chiedersi quale sia la naturale declinazione di quanto detto se vengono impiegate tecnologie che sfruttano l'IA, e in particolare il Riconoscimento facciale. Come precedentemente affermato, dato che l'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea riconosce il diritto alla protezione dei dati personali come un diritto fondamentale autonomo, la

---

[235] Cfr. G. Pino, *'Diritto e società. Proporzionalità, diritti, democrazia'* (estratto), Editoriale Scientifica, Napoli, 2014.
[236] Cfr. A. Morrone, *'Il custode della ragionevolezza',* Giuffrè, Milano, 2001.
[237] G. Pino, *op.cit*. 372.
[238] Cit. C. Barone, *'Privacy, Sicurezza e Libertà nell'era della sorveglianza di massa e dell'emergenza terrorismo',* Tesi di Dottorato di Ricerca in Pluralismi giuridici, Università degli studi di Palermo, 2019, p. 190. Per un maggiore approfondimento si possono vedere sul punto le sentenze 22 Luglio 1999 n. 341 e 26 Luglio 1988 n. 27 della Corte Costituzionale.

sua compressione deve essere effettuata secondo la regola riportata nell'articolo 52 della Carta medesima, valutando quindi che la restrizione del diritto sia espressamente prevista dalla legge, che non leda il suo 'contenuto essenziale' e che risponda ad una esigenza generale dell'Unione Europea. L'unico aspetto non problematico è quello concernente l'individuazione di un'esigenza generale, in quanto non vi è dubbio che la garanzia di pubblica sicurezza sia tale. Ciò lo si comprende analizzando due ulteriori normative, infatti proprio per il fatto che ad oggi, nell'era digitale, il diritto alla *privacy* si qualifica nel diritto alla protezione dei dati personali, la Carta dei diritti fondamentali deve essere messa a confronto con il GDPR (Regolamento n. 679/2016) e con la LED (Direttiva n. 680/2016[239]), tenendo a mente l'esistenza della proposta di Regolamento sull'Intelligenza Artificiale, non ancora approvato. Questi atti normativi confermano la possibilità di restringere il diritto alla protezione dei dati personali quando ciò sia necessario per garantire la sicurezza pubblica, ma allo stesso tempo la fattispecie viene delimitata in maniera puntuale e stringente[240]. A tal proposito l'articolo 23 del GDPR prevede esplicitamente la possibilità di apporre restrizioni al diritto alla protezione dei dati personali per ragioni di *sicurezza nazionale, difesa, sicurezza pubblica*[241]… ciò, però, deve avvenire tramite apposite misure legislative, deve rispettare l'essenza dei diritti e delle libertà fondamentali e deve essere effettuata in misura necessaria e proporzionata alla società democratica in cui si esplica. L'articolo preso in analisi individua specificatamente gli elementi che devono essere riportati nella legislazione adottata al fine della restrizione e in particolare: : *a) le finalità del trattamento o le categorie di trattamento; b) le categorie di dati personali; c) la portata delle limitazioni introdotte; d) le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti; e) l'indicazione precisa del titolare del trattamento o delle categorie di titolari; f) i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento; g) i rischi per i diritti e le libertà degli interessati; e h) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa*[242]. Si comprende facilmente la pervasività delle

[239] Si rimanda al Capitolo I della presente tesi.
[240] M. Orofino *op. cit*. 15.
[241] Cit. articolo 23 GDPR.
[242] Ibidem nota 241.

indicazioni richieste dal legislatore europeo per poter effettuare compressioni al diritto alla vita privata.

Accanto a questa disposizione si pongono anche numerosi interventi della Corte EDU (che si pronuncia sul rispetto o meno del diritto alla riservatezza sancito nell'articolo 8 della Convenzione EDU), le quali, pur non trattando in principio delle tecnologie di riconoscimento facciale, forniscono importanti indicazioni sul bilanciamento tra il diritto alla *privacy* e le tecnologie di videosorveglianza[243]. Particolarmente rilevante a tal proposito è la sentenza Peck v. UK (2003). Tutto ebbe inizio quando il Brentwood Borough Council approvò, nel febbraio del 1994, le linee guida per l'operatività e l'installazione di un sistema di videosorveglianza CCTV a Brentwood. Dette direttive davano la possibilità di conservare le registrazioni sul nastro CCTV per un massimo di 90 giorni, e una volta terminato il periodo dovevano essere cancellate. Già nel Luglio del medesimo anno il sistema era completamente operativo e nell'anno successivo si colloca il fatto preso in considerazione dalla Corte EDU. Goeffrey Peck (l'instante) soffriva di forte depressione per circostanze personali e famigliari che lo portarono alla decisione di togliersi la vita, così prese un coltello da cucina e lungo una delle vie principali del centro di Brentwood iniziò a tagliarsi i polsi. Durante il compimento di questo atto venne ripreso dal sistema di videosorveglianza CCTV a sua insaputa e l'operatore che, al tempo, si occupava delle registrazioni avvisò tempestivamente gli agenti di polizia, i quali, una volta arrivati sul posto, gli impediscono di proseguire fino a causarsi la morte. Il signor Peck venne portato in centrale di polizia dopo che fu accuratamente medicato, i documenti di custodia riportavano la situazione quale che era, infatti dichiaravano che l'istante aveva cercato di togliersi la vita procurandosi ferite ai polsi, subito dopo è stato rilasciato senza accuse. Successivamente il gruppo di lavoro CCTV del Consiglio autorizzò la pubblicazione regolare di servizi stampa sul sistema CCTV, e ciò portò alla pubblicazione di fotografie statiche che riprendevano l'istante, ciò per accompagnare un articolo intitolato '*Scongiurato – La collaborazione tra CCTV e polizia impedisce*

[243] Tra le sentenze della Corte EDU circa l'utilizzo di sistemi di videosorveglianza, oltre a quella trattata di seguito, si può vedere anche la sentenza Khmel v. Russia (2013).

una situazione potenzialmente pericolosa'. Le stesse immagini furono anche utilizzate per un articolo volto a mettere in risalto i benefici connessi all'uso del sistema CCTV. Sempre in questo periodo il Consiglio decise di fornire le riprese ai produttori di 'Crime Beat' una serie trasmessa su BBC, e nel Marzo del 1996 gli amici del Signor Peck lo riconobbero nel trailer della serie citata. A seguito di questi eventi l'istante presentò una serie di reclami, prima alla Broadcasting Standards Commission, che rinvenne la sussistenza della violazione della *privacy* dell'istante; successivamente presentò reclamo contro l'Independent Television Commission che giunse alla stessa conclusione della BSC. La questione giunse, infine, innanzi alla Quarta Sezione della CEDU, la quale si concentrò sul constatare la possibile violazione del diritto alla *privacy* dell'istante, affermato nell'articolo 8 della Convenzione EDU. L'istante si appellò alla Corte sostenendo che erano state trasmesse immagini dalle quali era identificabile e che, nonostante non mostrassero l'atto da lui compiuto, riprendevano comunque un momento privato, divulgato senza il suo consenso e senza un idoneo occultamento del volto. L'appello del signor Peck venne presentato alla Corte perché precedentemente il Governo del Regno Unito aveva negato che le immagini oggetto delle riprese documentassero parte della sua vita privata. Ciò in base a quanto era stato filmato, alla posizione e alle circostanze, quindi si sostenne che aveva di sua sponte deciso di rinunciare alla *privacy* di quel momento, non avendo nemmeno lamentato di essere stato ripreso. La Corte, in questa sede, afferma che l'uso di attrezzature fotografiche che non riprendono dati visivi non costituisce in sé una violazione del diritto alla vita privata vantato dall'istante, tuttavia il fatto che i dati venivano registrati in maniera sistematica o permanente poteva profilare la violazione in questione, in particolare perché il signor Peck non lamentava l'impiego del sistema CCTV, avendone a sua volta riconosciuto il beneficio che ne è derivato a suo favore, ciò che da lui è stato lamentato era la successiva divulgazione, che non sarebbe mai potuta essere prevista, delle immagini catturate dal sistema e dalle quali era facilmente riconoscibile. In considerazione di quanto riportato la Corte ritenne[244] che la divulgazione delle riprese, in cui compariva il signor Peck, fosse sproporzionata, la mancanza delle garanzie menzionate insieme alle tutele per il

[244] La Corte EDU fa riferimento a diverse sentenze dalle quali riprende i punti salienti e queste sono: Herbecq v. Belgio (1988), Rotaru v. Romania (2000) e Amann v. svizzera (2000).

rispetto della vita privata dell'istante è, cioè, un sufficiente motivo per ritenere violato l'articolo 8 della Convenzione EDU[245].

Ciò preso in considerazione occorre ora valutare quali sono le ulteriori complicazioni che emergono quando si utilizzano sistemi di videosorveglianza dotati della funzione di Riconoscimento facciale, tenendo presente la pervasività e la potenza connessa alla natura stessa delle tecnologie involte. Occorre quindi valutare quando si possa verificare una violazione del diritto alla protezione dei dati personali, potendosi così configurare il diritto alla *privacy* nell'era dell'informazione.

Da un lato è necessario rispettare l'articolo 52 della Carta dei diritti fondamentali dell'UE affinché non derivi una compressione illecita del diritto alla *protezione dei dati personali* attraverso l'impiego di tali tecnologie, dall'altro lato è bene anche avere a mente che se è presente una disciplina puntale e specifica per la tutela dei dati personali, la quale si ritrova nel, più volte citato, GDPR, non è presente una normativa vigente e specifica che regoli l'impiego di tecnologie dotate di IA e soprattutto di funzioni pervasive come il riconoscimento facciale. La mancanza di una disciplina specifica che possa arginare i possibili abusi dell'autorità, la difficoltà di garantire il rispetto del principio di proporzionalità chiesto dall'articolo 52, nonché la pervasività e la diffusione dei sistemi di Riconoscimento facciale che sta sempre più caratterizzando l'era digitale, apre le porte al possibile sfruttamento di queste tecnologie per fini di sorveglianza di massa, o per meglio dire, abilita la *Dataveillance (*ossia la *Data-surveillance[246]).* David Lyon già nel lontano 2001 poneva l'attenzione sulla incessante diffusione di infrastrutture avanzate per l'informazione (tra le quali vi rientra il riconoscimento facciale), e sulle conseguenze connesse a tale propagazione. In tutto il mondo si assiste, ormai da tempo, ad una crescente attività di sorveglianza, e le caratteristiche delle tecnologie di riconoscimento facciale fanno facilmente comprendere la possibilità di un loro sfruttamento in tal senso[247]. Questo lo si capisce ancora meglio se si considera cosa si intende con il termine

[245] Cfr. Chamber Judgment in the case of Peck v. The United Kingdom (28.1.2003), European Court of Human Rights, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22003-687182-694690%22]}.
[246] G. Mobilio, *'Profilare tramite riconoscimento facciale: il caso della sicurezza urbana', op. cit.* 183.
[247] D. Lyon *op. cit.* 5-6.

Dataveillance. Il primo a parlarne fu Roger Clarke che già nel 1988 riconduce a questo termine il monitoraggio e la sorveglianza degli individui, delle loro azioni nonché dei loro comportamenti mediante la raccolta e la conseguente analisi di dati, soprattutto nell'ambito delle tecnologie dell'informazione e della comunicazione[248].

A questo punto non resta che prendere in considerazione due casi verificatisi nel nostro ordinamento giuridico che rappresentano un importante punto di svolta tanto nell'impiego dei sistemi di Riconoscimento facciale da parte delle pubbliche autorità, quanto nella consapevolezza delle autorità regolatrici della pervasività e della pericolosità che deriva da questi strumenti di sorveglianza di massa.

2. Il caso SARI: il sistema automatico di riconoscimento facciale utilizzato dalla Polizia di Stato Italiana

S.A.R.I è l'acronimo che sta per Sistema Automatico Riconoscimento Immagini, il quale permette di '*effettuare ricerche nella banca dati A.F.I.S (Automated Fingerprint Identification System) attraverso l'inserimento di un'immagine fotografica di un soggetto ignoto che, elaborata da due algoritmi di riconoscimento facciale, fornisce un elenco di immagini ordinato secondo un grado di similarità[249]'*. Si tratta di uno strumento impiegato dalla Polizia di Stato nella lotta alla criminalità di cui l'opinione pubblica viene a conoscenza nel Settembre del 2018 quando la Polizia di Brescia riesce a sfruttare le sue funzioni per l'arresto di due uomini, accusati di aver commesso un furto in un appartamento[250].

---

[248] Cit. R. Clarke, '*Information Technology and Dataveillance',* November 1987, http://www.rogerclarke.com/DV/CACM88.html#PDV.

[249] Cit. D. Fioroni, *'Brescia: ladri d'appartamento scoperti grazie al riconoscimento facciale',* Comunicato stampa della Polizia di Stato, 07/09/2018, https://www.poliziadistato.it/articolo/pdf/135b92536bb3957899899171.

[250] Cfr. V. Bontempi, *'Un'interrogazione parlamentare sull'uso del riconoscimento facciale in Italia: il caso S.A.R.I.', 'in'* IRPA (Istituto di ricerche sulla pubblica amministrazione), 07/05/2020, https://www.irpa.eu/uninterrogazione-parlamentare-sulluso-del-riconoscimento-facciale-in-italia-il-caso-s-a-r-i/.

2.1. La funzione *Enterprise* di S.A.R.I.

S.A.R.I si compone di due sistemi diversi, per funzionamento e possibilità di sfruttamento, infatti da un lato c'è S.A.R.I *Enterprise* e dall'altra parte S.A.R.I *Real Time.*

È bene prima prendere in considerazione la funzione *Enterprise.* Lo scenario *Enterprise* viene in auge quando vi è la necessità di ricercare l'identità di una persona che è ritratta in una fotografia. Si tratta di una funzione che viene utilizzata dal 2017 e attraverso la quale è possibile eseguire un confronto comparativo tra le immagini che vengono 'catturate' da un sistema di videosorveglianza, e quelle contenute nella banca dati A.F.I.S. Più precisamente la banca dati A.F.I.S è in grado di comparare, una volta codificate, le c.d. *minutiae* ossia i dettagli particolari delle impronte digitali degli individui, con le informazioni riguardanti la criminalità e l'identità delle persone che sono archiviate nel Casellario Centrale d'Identità della Polizia Criminale[251]. Tra le informazioni conservate in questo registro ufficiale vi possono essere cartellini foto-segnaletici, condanne, impronte digitali, informazioni personali nonché altri dettagli rilevanti concernenti la vita criminale di un soggetto[252]. Nella funzione *Enterprise* il sistema sfrutta specifici algoritmi per effettuare in modo automatico la comparazione, la quale viene resa quanto più specifica e puntuale attraverso limiti di ricerca che vengono inseriti manualmente dall'operatore come, ad esempio, il sesso, la razza, l'altezza ecc.., ossia informazioni generalmente riferite all'immagine che consentono un'indagine più efficace.[253]

Sul legittimo utilizzo di S.A.R.I. *Enterprise* da parte della Polizia Scientifica si è pronunciato il Garante della Privacy, il quale ha espresso un parere favorevole all'utilizzo, per contrasto alla criminalità, della tecnologia in questione. Il Garante infatti rileva che la funzione *Enterprise* rappresenta *«un mero ausilio all'agire umano, avente lo scopo di velocizzare l'identificazione, da parte dell'operatore di polizia, di*

[251] Cfr. Ministero dell'Interno (Dipartimento della pubblica sicurezza), *'Capitolato tecnico. Procedura volta alla fornitura della soluzione integrata per il sistema automatico di riconoscimento immagini S.A.R.I.',* https://www.poliziadistato.it/statics/06/20160627-ct-sari--4-.pdf.
[252] Cfr. Polizia di Stato, *'Identità',* 10/05/2013, https://www.poliziadistato.it/articolo/identita-1.
[253] Ministero dell'Interno *op. cit*.

un soggetto ricercato della cui immagine facciale si disponga, ferma restando l'esigenza dell'intervento dell'operatore per verificare l'attendibilità dei risultati prodotti dal sistema automatizzato[254]*»*. Quindi come osservato dal Garante per la protezione dei dati personali non vi sono rilevanti problemi connessi a questa modalità di impiego di S.A.R.I, ma lo stesso non si può dire della sua funzione *Real Time.*

2.2. S.A.R.I *Real Time* e l'intervento del Garante per la protezione dei dati personali

I veri problemi vengono in essere quando ad essere sfruttata è la funzione *Real Time* di S.A.R.I. Attraverso l'applicazione *Real Time* è possibile comparare, in tempo reale, il volto di un individuo che viene catturato dal sistema di riconoscimento facciale, seppur in una zona geografica ristretta e ben delimitata, con una banca dati denominata *watch-list.* Se si verifica un *match* allora il sistema genera un *alert* che richiama l'attenzione delle forze di polizia, il quale viene generato attraverso un apposito algoritmo. Questa funzione è stata pensata per specifiche operazioni di tutela del territorio, in particolare in occasione di eventi e manifestazioni pubbliche[255].

Il parere rilasciato dal Garante per la Protezione dei dati personali al Ministero degli Interni circa questa specifica applicazione di S.A.R.I è diametralmente opposto a quanto affermato dalla medesima Autorità con riferimento alla funzione *Enterprise.* Si tratta cioè di un parere sfavorevole ad un suo uso, in quanto manca, totalmente, una base legale adeguata che consenta un appropriato e proporzionato utilizzo. Oltre all'assenza di un'apposita disciplina, è inoltre necessario il rispetto dell'articolo 7 della CEDU, dell'articolo 52 della CDFUE, oltre che dell'articolo 10 della LED e 9 del GDPR, volendo infine fare riferimento all'ordinamento giuridico interno deve essere poi conforme all'articolo 7 del decreto legislativo 51 del 2018[256]. La base

[254] Cit. Garante per la protezione dei dati personali, *'Sistema automatico di ricerca dell'identità di un volto',* provvedimento n. 440 del 26 Luglio 2018. Inoltre cfr. sul punto M. Colacurci, *'Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini', 'in'* Sistema Penale, 9/2022, cit. pag. 37 ss.

[255] Ministero dell'Interno *op. cit*. 6.

[256] Cit. G. Mobilio, '*Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative',* Editoriale Scientifica, Napoli, 2021 p. 245 ss. Inoltre si rammenta che l'articolo 7 della CEDU esprime il principio secondo cui nessuno può essere per un'azione o omissione che, al momento in cui è stata commessa, non costituiva reato secondo il diritto interno o internazionale. L'articolo 52 è stato più volte ricordato (si vedano le pagine precedenti). L'articolo 10 della LED pone la distinzione tra i dati

legislativa che legittimi e disciplini l'impiego di S.A.R.I *Real Time* è per il Garante fondamentale perché deve imprescindibilmente valutare e ponderare i diritti e le libertà personali coinvolte al fine di '*rendere adeguatamente prevedibile l'uso di tali sistemi senza conferire una discrezionalità così ampia che il suo utilizzo dipenda in pratica da coloro che saranno chiamati a disporlo*[257]*'*. Il Garante della Privacy ha sottolineato la delicatezza del trattamento di immagini per l'identificazione di persone in un contesto pubblico, e afferma che *«realizza un trattamento automatizzato su larga scala che può riguardare, tra l'altro, anche coloro che siano presenti a manifestazioni politiche e sociali, che non sono oggetto di "attenzione" da parte delle forze di Polizia*», potendo determinare *«una evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui*[258]*».* Attraverso le parole del Garante per la protezione dei dati personali si concretizza l'eventualità di una sorveglianza di massa, laddove non sia presente alcun limite alla discrezionalità delle Autorità circa l'impiego di sistemi di riconoscimento facciale così pervasivi, la possibilità di un passaggio dalla sorveglianza individuale alla sorveglianza di massa si profila come una logica conseguenza, violandosi in tal modo il diritto alla riservatezza di ciascun individuo si trovi nel raggio di operatività della TRF. Per evitare che questo sia l'esito dell'uso delle TRF è necessario anche garantire che il loro impiego sia necessario e proporzionato alla finalità perseguita, come prescrive l'articolo 52 CDFUE, obiettivo non sempre agevole da raggiungere. Le pronunce della Corte di Giustizia [259] sul punto, se lette unitamente al parere del Garante della privacy in questo paragrafo analizzato, permettono di affermare che soltanto nel caso in cui siano prospettate stringenti cautele, allora il principio di proporzionalità è rispettato e le TRF possono essere usate al fine di prevenzione e repressione dei reati, e quindi per perseguire la funzione di pubblica sicurezza. Tutto ciò deve anche essere messo in relazione ad una normativa interna che vieta l'impiego

personali e verifica della qualità dei dati personali. L'articolo 9 del GDPR dispone la disciplina per il trattamento di categorie particolari di dati personali (e per l'appunto riguarda anche i dati biometrici). Infine l'articolo 7 del decreto legislativo 51/2018 che dando attuazione alla Direttiva europea 680/2016 riprende la disciplina circa il trattamento di categorie particolari di dati personali.

[257] Cit. Garante per la protezione dei dati personali, *'Parere sul sistema S.A.R.I Real Time',* 25 Marzo 2021

[258] Ibidem nota 257.

[259] Sul punto si possono confrontare diverse sentenze della Corte di Giustizia tra le quali alcune di particolare rilevanza sono: C-291/12, Schwarz e le sentenze C-293/12 e C-594/12, Digital Rights Ireland.

di sistemi di videosorveglianza dotati di riconoscimento facciale, ossia la legge 51 del 2023, e tal divieto è valido fino a Dicembre 2025. Inoltre, pur non essendo ancora stato approvato, l'Ai Act pone un divieto generale all'impiego dei sistemi di riconoscimento facciale da remoto in tempo reale, se non alle condizioni e nei casi in detto articolo stabilite.

3. Sicurezza urbana e sistemi di videosorveglianza: i problemi connessi all'impiego delle tecnologie di riconoscimento facciale da parte delle amministrazioni comunali

All'inizio del presente capitolo si è avuto modo di evidenziare che la Sicurezza pubblica si declina in *'primaria'* e '*secondaria*[260]*'*. Se nei paragrafi precedenti si è presa in considerazione l'utilizzazione delle TRF in relazione alla sicurezza '*primaria'* e quindi al fine precipuo di prevenire e reprimere i reati, è ora bene chiedersi se un tale uso sia possibile da parte degli enti locali, al fine di ottemperare alla funzione di sicurezza '*secondaria*'.

Una risposta, seppur parziale, è già stata fornita, poiché si è messo in luce che un impiego in tal senso delle TRF da un lato non è supportato da un'apposita normativa, né Governativa né Parlamentare, dall'altro lato non è nemmeno possibile ricondurre all'ambito della sicurezza *'secondaria'* il fine di prevenire e reprimere i reati attraverso le tecnologie in questione, essendo tuttalpiù detta finalità ascrivibile alla sfera della sicurezza *'primaria'*.

Le osservazioni qui riprese devono essere messe in relazione con quanto riportato a riguardo dell'impiego delle TRF da parte della Polizia di Stato. Quindi trattandosi di sistemi di riconoscimento facciale, ossia di tecnologie pervasive che facilmente possono comportare un'illecita compressione del diritto alla protezione dei dati personali, oltre ad essere necessaria un'apposita normativa che ne legittimi l'impiego, è anche richiesto il rispetto delle condizioni di cui all'articolo 52 CDFUE. E così, come anche specificato dal Garante per la protezione dei dati personali, è

[260] V. paragrafo 1.1 Cap. III.

fondamentale che siano utilizzate solo in modo proporzionato allo scopo perseguito, e inoltre si chiede che siano prescritte le idonee garanzie.

Il percorso seguito permette di giungere alla conclusione che difficilmente le TRF possono conciliarsi con la funzione di sicurezza *'secondaria'* rimessa agli enti locali, sono infatti solo le finalità riconducibili ad un interesse primario dello Stato che consentono *'una forte compressione dei diritti alla privacy e alla protezione dei dati personali, come si evince dal confronto tra le diverse discipline del d.lgs. n. 51 del 2018 e del GDPR*[261]*'*.

Ciò nonostante, poco dopo la manifestazione della contrarietà al Ministero dell'Interno da parte del Garante della Privacy sull'impiego di S.A.R.I *Real Time,* sono state formulate plurime richieste, da parte di diversi Comuni, per poter incrementare il numero di videocamere al fine di garantire una maggiore sorveglianza. Ciò consente di aprire un'ulteriore questione critica, ossia: ma i dati che vengono raccolti dai diversi comuni che utilizzano sistemi di videosorveglianza dotati di riconoscimento facciale, dove vengono conservati, per quanto tempo e da chi vengono custoditi? E soprattutto: a cosa servono questi dati ai Comuni? Questa domanda appare di particolare importanza poiché, in base a quanto evidenziato, il Comune ha poteri di sicurezza secondaria che non gli consentono di svolgere indagini, e in base ai principi cardine a tutela dei dati personali, ossia il principio di proporzionalità e di minimizzazione dei dati, la conservazione deve essere proporzionata alle finalità perseguite e se questo già emerge nel GDPR, è quanto più lampante nella proposta di Regolamento sull'Intelligenza Artificiale la quale richiede anche una valutazione d'impatto preventiva[262].

[261] G. Mobilio *'Profilare tramite riconoscimento facciale: il caso della sicurezza urbana' op. cit*. 197.
[262] V. A. Ghiglia (Componente del Garante della Privacy) Intervento in occasione dell'executive webinar: *'Intelligenza artificiale e riconoscimento facciale in Real Time, i vantaggi e i rischi del Regolamento europeo',* Webinar organizzato da Privacy Italia, ASSO Dpo e Key4biz, https://www.youtube.com/watch?v=zOZdz2WvVJU&t=144s.

3.1. I Comuni si avvicinano alla *smart security*: il caso di Udine e di Como

Agostino Ghiglia, componente del Garante per la protezione dei dati personali, afferma che la sorveglianza di massa è '*una questione di percezione*[263]'. Questo significa che il modo in cui i soggetti valutano la presenza di sistemi di riconoscimento facciale dipende dalle loro esigenze personali. Così i cittadini che vivono in quartieri con un alto tasso di criminalità o di spaccio e quindi generalmente malavitosi, hanno un maggiore interesse all'installazione di telecamere di videosorveglianza perché possono garantire un maggior grado di sicurezza. Se però il medesimo cittadino si sposta in un quartiere non più afflitto da queste problematiche, allora non avrà più lo stesso grado di interesse a che siano queste montate in specifiche aree, e anzi potrebbe non volere affatto essere 'seguito' da un occhio elettronico.

Ciò premesso, sempre più città in Italia stanno sviluppando progetti che comportano il loro avvicinamento alla *smart security*[264] e a tal proposito sono interessanti i casi di Udine e Como, i quali non sono isolati. Nonostante sia dagli anni Duemila che i Comuni hanno iniziato ad incrementare la presenza di telecamere lungo le vie delle città, i Comuni di Udine e Como si pongono in maniera peculiare poiché avanzano progetti per l'installazione di sistemi di videosorveglianza dotati di riconoscimento facciale, in tempo reale.[265] La Città di Udine delibera un progetto per il posizionamento di videocamere lungo via Roma, ossia una delle vie principali del centro-città. Essendo vicino alla Stazione è una zona ad alta presenza di senzatetto, di persone con problemi di alcol o droga… e sono state, dai cittadini, avanzate diverse lamentele al riguardo, tanto che il Comune ha varato il progetto in questione. Quelle di Udine non sono però videocamere normali, cioè finalizzate alla mera ripresa della zona interessata, ma sono invece dotate della funzione di riconoscimento facciale in tempo reale, di conseguenza sono in grado acquisire, sempre in tempo reale, i dati biometrici di tutte le persone che passeggiano lungo la via. Inoltre, la delibera del progetto specifica che la tecnologia che verrà installata avrà anche la possibilità di

[263] A. Ghiglia *op. cit.*.

[264] Quando si parla di *smart security,* ossia di sicurezza intelligenze, si fa riferimento all'impiego di tecnologie avanzate (anche munite di IA) per migliorare la sicurezza.

[265] Cfr. I. Invernizzi, *'I sistemi di riconoscimento facciale stanno arrivando nelle città italiane', 'in'* Il Post, 16 Settembre 2021, https://www.ilpost.it/2021/09/16/riconoscimento-facciale-comuni-telecamere/.

creare da sé un allarme al fine di segnalare la presenza di soggetti oggetto di attenzione, direttamente alle forze dell'ordine[266].

Prima della delibera del progetto in questione, il Garante della Privacy si era già pronunciato su un progetto simile ma presentato dal Comune di Como, il quale quando fu oggetto della pronuncia del Garante aveva già proceduto all'installazione di telecamere fornite della funzione di riconoscimento facciale presso l'area verde denominata 'parco Tokamakhi', ossia un parco che si trova nelle vicinanze della principale Stazione ferroviaria della città, la stazione San Giovanni, con l'intento di identificare persone oggetto di indagine e/o scomparse, individuare automaticamente situazioni che siano sospette, potenzialmente pericolose o al fine di rilevare furti nonché ingressi e uscite da zone oggetto di indagine[267]. Ciò che il Garante rileva è che le normative che vengono invocate dal Comune, al fine di reperire una legittimazione alla raccolta e conservazione di dati biometrici, in realtà non lo consentono, e constata che una simile raccolta sarebbe lecita solo ed esclusivamente in presenza di un'apposita previsione normativa, ai sensi dell'articolo 7 del Decreto Legislativo 51/2018 che la richiede quando la suddetta conservazione sia finalizzata a identificare soggetti interessati e nei soli casi indicati dall'articolo 349 c.p.p. Inoltre, il Garante rileva che non sussistono nemmeno le condizioni presenti con riferimento al sistema S.A.R.I *Enterprise*[268].

Tutto ciò constatato e letto unitamente a quanto previamente rilevato, si può affermare che, allo stato attuale, tal uso dei sistemi di riconoscimento facciale si presta ad una pervasiva sorveglianza di massa in quanto si configura come un illecito impiego da parte degli enti locali che a ciò non sono legittimati, in assenza di un'apposita normativa che ne consenta l'utilizzo e in violazione dei principi di proporzionalità e minimizzazione dei dati che comporta, come conseguenza, la violazione del diritto alla *privacy* e alla protezione dei dati personali quali diritti fondamentali degli individui.

---

[266] Cfr. Delibera del progetto di videosorveglianza della città di Udine, https://www.comune.udine.it/it/sicurezza-22643/polizia-locale-50372/videosorveglianza-89669.
[267] Cfr. Garante per la protezione dei dati personali, Provvedimento n.54 del 26 Febbraio 2020.
[268] Ibidem nota 267.

CAPITOLO IV
PROBLEMATICHE E CRITICITA' CONNESSE ALL'IMPIEGO DI TECNOLOGIE DI RICONOSCIMENTO FACCIALE AI FINI DI PUBBLICA SICUREZZA

1. La non comprensibilità degli algoritmi e il sempre più difficile controllo da parte dell'uomo: il problema delle *Black Box*

Questo capitolo è dedicato a mettere in luce le problematiche che sono connesse all'impiego di sistemi di riconoscimento facciale, quelle criticità solo accennate nei capitoli precedenti e che meritano una più accurata indagine. La prima questione su cui pare rilevante porre attenzione è quella dell'opacità algoritmica. L'opacità è una caratteristica intrinseca della società in cui viviamo tanto che si parla di *Black Box Society:* assistiamo ad una incessante crescita dell'uso dei nostri dati personali per alimentare strumenti intelligenti, ormai in grado di sostituire l'uomo in moltissimi contesti, ma non siamo in grado di comprendere il procedimento seguito per raggiugere uno specifico risultato[269]. La rivoluzione delle *Information and Communication Technologies* ha avuto come risultato la digitalizzazione dei flussi di informazione e ciò ha fatto emergere l'esigenza di rilevare uno strumento in grado di elaborare le enormi quantità di dati prodotti, reperiti e conservati[270]. Così, le dette funzioni, sono state rimesse agli algoritmi[271], metodologie di risoluzione di problemi dalle enormi potenzialità, in grado di compiere le mansioni che gli sono impartite, in tempi ridotti e senza l'intervento dell'uomo. Ma, nonostante i benefici siano plurimi, non sono esenti da rischi, infatti è particolarmente gravoso comprendere le modalità attraverso le quali operano e di conseguenza gli errori che questi commettono.

[269] Cit. F. Pasquale, '*The Black Box Society*. *The secret Algorithms That Control Money and Information'*, Harvard University Press, Cambridge-London, 2015, p. 3

[270] Cit. E. Campo, L. Ciccarese, A. Martella, *'Gli algoritmi come costruzione social. Neutralità, potere e opacità', 'in'* LQ The Lab's Quarterly, 2018, a. XX, n.4 (Ottobre-Dicembre), p. 7.

[271] Per un maggiore approfondimento su cosa sono gli algoritmi e come funzionano, specie nel riconoscimento facciale, si veda il Cap. II della presente tesi.

Innanzitutto è bene puntualizzare che i compiti che possono essere affidati agli algoritmi sono assai vari, qui ci si è concentrati su come vengono impiegati nelle applicazioni di riconoscimento facciale ma, più generalmente, questi possono eseguire tutte le funzioni che sono traducibili in linguaggio matematico: hanno la capacità di selezionare le informazioni importanti e al contrario di scartare ciò che è superfluo e inutile per il compito affidatogli, possono aiutare nei processi di ricerca e nel prendere decisioni.[272]Ciò nonostante, alle vastissime mansioni riconducibili agli algoritmi, corrisponde un altrettanto complesso problema di comprensibilità dei processi sottesi. Volendo indagare le ragioni che principalmente determinano l'opacità, queste sono riconducibili a tre categorie.

Un primo livello di opacità si evidenzia nella segretezza che avvolge tanto i dati con cui si alimentano gli algoritmi, tanto gli algoritmi stessi. Questo è l'effetto causato da un'intenzionale volontà delle aziende di autodifendersi da attacchi esterni, al fine di preservare la segretezza commerciale e i vantaggi competitivi connessi alla non divulgazione dei *design* degli algoritmi[273]. Un secondo livello di opacità sarebbe poi stato individuato nella difficile comprensione del linguaggio impiegato. Gli algoritmi vengono programmati da soggetti con competenze tecniche, attraverso un linguaggio di programmazione, di conseguenza per le persone prive di dette competenze è impossibile poter comprendere come da un *input* si sia giunti ad uno specifico *output.* Se ciò è impossibile per le persone che non rientrano nelle categorie di informatici o matematici, è comunque necessario puntualizzare che, talvolta, anche gli stessi tecnici che li hanno progettati hanno difficoltà nella loro comprensione, soprattutto quando

[272] E. Campo, L. Ciccarese, A. Martella, *op. cit*. 8.

[273] Se questa è la tesi sostenuta da J. Burrell, non manca chi, pur ritenendo ciò corretto, assimili questo primo livello di opacità ad un ulteriore ragione rispetto alla volontà delle aziende di mantenere la segretezza per ragioni di competitività nel mercato. In particolare F. Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Cambridge, Harvard University Press, 2015; sostiene che la preservazione delle informazioni concernenti il *design* degli algoritmi sia da un lato posta a garanzia di riservatezza, in funzione di una maggiore competitività, ma dall'altro lato non pone in questo una giustificazione, poiché sostiene che sia anche la causa di una regolamentazione scarsa e obsoleta. Secondo l'autore si sta cioè verificando una sorta di situazione avversaria in cui l'avversario però è il regolamento; proprio per questo Pasquale si chiede se l'opacità non sia il risultato di una nuova forma di occultamento regolamentare, provocato cioè dalle stesse aziende *i-tech.* Ciò che rileva è che se così fosse sarebbe possibile individuare una soluzione a detta forma di opacità attraverso la messa a disposizione del codice per l'ispezione. Sul punto si può anche vedere P. Dourish, '*Algorithms and their other: Algorithmic culture in context', 'in'* Sage Journals, August 2016, https://journals.sagepub.com/doi/10.1177/2053951716665128#bibr42-2053951716665128.

vengono impiegati il *machine* e il *deep learning*[274]. Quest'ultima osservazione apre le porte al terzo livello di opacità, ossia quello connesso alle peculiarità del *machine* e del *deep learning.* Per essere più specifici, il *machine* e il *deep learning* sono due modalità di apprendimento automatico degli algoritmi, altamente sofisticate e ampiamente utilizzate nel riconoscimento facciale. In termini generali si può constatare che spesso gli algoritmi sono sistemi multi-componenti in grado di generare un'opacità circa la quale gli stessi *'insiders'* devono confrontarsi e questo vede come conseguenza la necessità di ore e ore di lavoro, per poter districare la logica sottesa al codice usato in un sofisticato sistema *software*. Vengono in auge in tal senso sfide connesse al numero di pagine in cui si sviluppa il codice, il numero dei componenti del *team* che si impegna nella decodificazione e l'ingerente quantità di collegamenti tra i moduli che lo compongono. In ogni caso si comprende la gravosità dell'operazione di decriptazione del codice sorgente. I problemi connessi al terzo livello di opacità si amplificano esponenzialmente quando gli algoritmi, che sono sottoposti all'analisi, sono implementati dall'apprendimento automatico: *'the curse of dimensionality*[275]*'.* I problemi aumentano perché attraverso il *machine learning* le logiche interne degli algoritmi si modificano mentre gli stessi apprendono dai dati, attraverso i quali sono '*nutriti'*. Quindi, tenuto conto di quanto detto, ciò che è incomprensibile non sono le ingenti quantità di dati che vengono raccolte e usate, e nemmeno il codice di programmazione che a sua volta può essere comprensibile (così come può non esserlo), ma è l'interazione tra i due cioè tra il codice e i dati, poiché il primo si modifica mentre apprende dai dati che vengono elaborati.[276] Quanto riportato deve essere inserito in un contesto più ampio, infatti vi sono delle conseguenze connesse alla non possibilità di comprendere i processi sottesi agli algoritmi e quindi all'intelligenza artificiale che opera mediante i medesimi. Infatti, le tecnologie intelligenti possono commettere errori e agire in modo discriminatorio, ma come si può individuare la fonte dell'errore o della discriminazione se, ad un livello più

[274] Per un maggior approfondimento su cosa siano e come funzionano il *machine* e il *deep learning* si torni al Cap. II, paragrafo 2.1..

[275] Cit. P. Domingos, *'A few useful things to know about Machine Learning', 'in'* Communications of the ACM, October 2012, Vol. 55, no.10, DOI: 10.1145/2347736.2347755.

[276] Cfr. J. Burrell, *'How the machine thinks: Understanding opacity in machine learning algorithms', 'in'* Sage Journal, 2016, DOI: 10.1177/2053951715622512. Da qui è stata ripresa la tripartizione, nei tre livelli evidenziati, dell'opacità algoritmica.

elementare non è agevole, e alle volte assolutamente impossibile, comprendere la logica che viene sfruttata per produrre uno specifico risultato? E se si vuole proseguire nelle criticità attinenti l'opacità, nel momento in cui viene impiegato il *machine learning* diviene fondamentale concentrarsi anche sull'interpretazione degli *output* generati poiché sono il risultato, non di un'attività di programmazione posta in essere dall'uomo, ma di processi automatizzati, ma, nonostante ciò, vengono ricondotti a categorie preesistenti che non rispecchiano le logiche algoritmiche sottese, poiché ricondotti a logiche sociali tradizionali[277].

Una volta messo in luce le cause dell'opacità che portano a qualificare la società come *Black Box Society* è necessario indagare le possibili soluzioni di contrasto alla non comprensibilità degli algoritmi e quindi dell'intelligenza artificiale. Proprio a tal fine il 18 Aprile 2023 è stato inaugurato il Centro Europeo per la trasparenza algoritmica (ECAT), il quale riunisce *team* interdisciplinari composti da *data scientists,* esperti legali, sociali e di intelligenza artificiale al fine di garantire che l'impatto degli algoritmi e dell'IA sia più sicuro, prevedibile ed etico[278]. A questo fine pare necessario prendere in considerazione la regolamentazione volta a garantire il rispetto del principio di trasparenza ossia il GDPR, per poi vedere brevemente come tal principio viene disciplinato nella proposta di regolamento sull'intelligenza artificiale.

1.1. Come porre rimedio all'opacità algoritmica: tra soluzioni tecniche e tutele giuridiche

L'opacità è un problema che affligge la logica algoritmica e al quale il mondo giuridico ha cercato di fornire una soluzione, per poter vivere in una società digitale deve, infatti, poter essere data la possibilità di comprendere e 'controllare' la potenza e la pervasività che è connessa agli algoritmi e all'intelligenza artificiale. Non essendo ancora stato approvato l'AI Act, è bene pendere in mano il GDPR per valutare quale

[277] G. Bolin, J. A. Schwarz, '*Heuristics of the algorithm: Big Data, user interpretation and institutional translation', 'in'* Sage Journal, October 2015, DOI: 10.1177/2053951715608406.
[278] Cfr. European Commission, *'European Centre of Algorithmic Transparency'*, https://algorithmic-transparency.ec.europa.eu/index_en. Si tratta di un'iniziativa nata in seno al Regolamento UE 2022/2065 del 19 Ottobre (c.d. Digital Service Act).

sia il comportamento da tenere al fine di minimizzare i rischi derivanti dalla non comprensibilità.

Il principio che viene in aiuto è quello di Trasparenza, al quale si è brevemente accennato nel Capitolo I, ma è ora opportuno entrare nel merito della questione. L'articolo 5, lettera a) esplicita il principio in esame, le cui modalità di applicazione si trovano nelle disposizioni successive. Il GDPR prevede la normativa che deve essere applicata, tanto quando il trattamento dei dati sia interamente o parzialmente automatizzato, tanto quando non lo sia, ma in questa sede ci si concentra soltanto sulla prima ipotesi[279], infatti il riconoscimento facciale sfrutta algoritmi di *Machine e Deep learning,* i quali operano in maniera autonoma. La Trasparenza, pertanto, sembrerebbe l'antidoto all'opacità,[280] ma non è sempre così semplice, le questioni che a tal riguardo si aprono sono numerose. Innanzitutto non vi è un modo univoco per comprendere quale forma debba assumere la trasparenza. La soluzione scontata sembrerebbe quella di rivelare il codice sorgente, ossia il codice utilizzato per la programmazione dell'algoritmo, soltanto che così facendo si da la possibilità di comprendere, e quindi di godere dell'effettiva trasparenza, soltanto a coloro che abbiano le capacità tecniche per comprendere il linguaggio di programmazione, di conseguenza l'uomo comune resterebbe escluso dal godimento di questa tutela[281]. Così infatti non si riuscirebbe a porre rimedio a quello che, nel paragrafo precedente, è stato qualificato come il secondo livello di opacità. Non può nemmeno essere invocata, in soccorso, la tecnica di *auditing* poiché si tratta di un metodo che permette di verificare se il procedimento seguito per ottenere uno specifico *output,* dati certi

[279] Cfr. Gruppo di lavoro articolo 29 per la protezione dei dati personali, '*Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679',* emendamento del 6 febbraio 2018. Il Gruppo di lavoro articolo 29 (Gruppo di lavoro WP29), considerati gli interpreti per eccellenza della disciplina contenuta nel GDPR, fornisce una definizione puntuale e specifica di cosa debba intendersi per trattamento interamente e parzialmente automatizzato. Il trattamento interamente automatizzato consiste nella capacità di prendere decisioni impiegando esclusivamente mezzi tecnologici, senza cioè che intervenga un essere umano. Le decisioni che ne derivano possono essere basate sull'elaborazione di differenti tipologie di dati: su dati forniti direttamente dall'interessato, oppure su dati osservati riguardo ad una persona e infine sui dati derivati o desunti. Il trattamento parzialmente automatizzato è, al contrario, un trattamento che prevede anche solo in minimissima parte l'ingerenza umana.

[280] Cfr: F. Pasquale , *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 *Nw. U. L. Rev.* 160ss. (2010).

[281] Cfr. S. Barocas, E. W Felten, J. Huey, J. K Reidenberg, D. G Robinson, J. A Kroll, H. Yu, *'Accountable Agorithms',* 165 Un Pennsylvania L. R, 2017, p. 633 ss.

input, abbia seguito le procedure adeguate, quindi si tratta di un approccio che consente di constatare la presenza di manomissioni o interferenze esterne nel processo informatico, ma non di porre rimedio alle incomprensibilità delle logiche algoritmiche[282]. Inoltre, la domanda che pare opportuno porre è: è davvero una forma di garanzia testare, anche in modo molto approfondito, il codice dopo che è stato progettato e quindi sperimentato su ampia scala? La risposta è sicuramente negativa. Se non possono essere individuate apposite soluzioni nel mondo scientifico-informatico, volte ad eliminare l'opacità degli algoritmi, allora devono essere fornite adeguate tutele e garanzie nei confronti dell'interessato, ossia il soggetto nei cui confronti si esplica il trattamento automatizzato dei dati personali.

Questa garanzia è proprio fornita dal principio di trasparenza, sancito dal Regolamento 2016/679. Il principio di trasparenza non trova una precisa definizione nel testo normativo del Regolamento richiamato, a tal fine viene in soccorso il Considerando 39, il quale dispone che: '… *Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati i dati personali che le riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio di trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro…'* nella prosecuzione vengono individuate le informazioni che, essendo di massima rilevanza ai fini della garanzia ad un trasparente trattamento, devono essere fornite al destinatario[283]. Gli articoli che sono volti a tutelare la garanzia fornita dal principio di trasparenza si trovano nel Capo III, dedicato ai Diritti dell'interessato. In particolare la disposizione che rileva ai fini della presente trattazione è quella individuata nell'articolo 12 (paragrafo 1), dove si chiede che le informazioni fornite siano *'concise, trasparenti, intellegibili e facilmente comprensibili'* e inoltre devono essere predisposte mediante *'un linguaggio semplice e chiaro[284].'* Chiedere che le

[282] S. Barocas, W. W. Felten, J. Huey, J. K. Reidenberg, D. G. Robinson, J. A Kroll, H. Yu, *op. cit.* 660 ss.
[283] Cfr. versione completa del considerando 39 del GDPR, dove si dispone che le informazioni che devono essere fornite al destinatario del trattamento sono: '*l'identità del titolare del trattamento, finalità del medesimo nonché tutte le altre informazioni necessarie per garantire un trattamento corretto e trasparente*.'
[284] Cit. articolo 12 del GDPR.

informazioni siano fornite in modo conciso e trasparente significa che il titolare del trattamento deve impegnarsi al fine di evitare il subissamento informativo, e ciò si persegue trasmettendo le comunicazioni in modo efficace e succinto[285]. Allo stesso tempo l'articolo 12 chiede che le medesime informazioni siano *intellegibili,* requisito volto a garantire la comprensibilità, ad un soggetto medio, delle notizie che gli sono riferite, quindi si tratta di un elemento strettamente connesso all'obbligo di utilizzare un linguaggio *semplice e chiaro*[286]. Il Considerando 39 dispone inoltre che è '*opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali*[287]*',* in questo caso, ai fini del rispetto della disposizione rammentata, non è sufficiente riportare ai destinatari le informazioni di cui agli articoli 13 e 14 del GDPR[288], ma se il trattamento è particolarmente complesso, per motivi tecnici o inattesi, il titolare del trattamento deve anche permettere al destinatario di comprendere quelle che saranno le conseguenze del trattamento stesso, e quindi gli effetti che ne deriveranno sulla sua persona.

Il principio di trasparenza risponde ad una specifica esigenza se gli algoritmi vengono progettati per espletare la funzione di riconoscimento facciale, soprattutto se l'installazione dei sistemi di videosorveglianza avviene in luoghi pubblici o aperti al pubblico, nonché nella funzione *Real time,* e questa funzione è quella di informare i possibili destinatari del trattamento del fatto stesso che sono 'I' destinatari. Come rammentato, le TRF sono tecnologie altamente opache, poiché sfruttano algoritmi di *machine* e *deep learning*, in cui la complessità della logica è direttamente

[285] Cit. Gruppo di lavoro articolo 29 per la protezione dei dati personali, *'Linee guida sulla trasparenza ai sensi del regolamento 2016/679',* WP260 rev.01, versione emendata adottata l'11 Aprile 2018, p. 6 ss. In particolare il gruppo di lavoro articolo 29 fornisce anche un esempio di ottemperamento alla disposizione di cui all'articolo 12, infatti ritiene che gli obblighi indicati sarebbero rispettati se, nell'ambiente online, fosse predisposta un'informativa sulla privacy stratificata, poiché, in questo caso, l'utente avrebbe la possibilità di accedere direttamente alla sezione di suo interesse.

[286] Gruppo di lavoro articolo 29, *'Linee guida sulla trasparenza ai sensi del regolamento 2016/679', op. cit*. Inoltre con riferimento al requisito dell'intelligibilità, il gruppo di lavoro articolo 29, specifica che il linguaggio utilizzato per trasmettere le informazioni deve essere rapportato all'interlocutore, se cioè le informazioni devono essere fornite ad un gruppo di professionisti, si potrà ben immagine che presenti un livello di comprensione superiore rispetto all'interlocutore uomo comune.

[287] Cit. Considerando 39 Regolamento europeo 2016/679.

[288] L'articolo 13 del GDPR indica quali siano le informazioni da fornire qualora i dati personali siano raccolti preso l'interessato, mentre l'articolo 14 è dedicato alle informazioni che devono essere fornite se i dati non sono reperiti presso l'interessato.

proporzionale alla complessità della funzione cui sono preposte. Concludendo sul punto, se non è possibile, allo stato attuale dell'evoluzione informatica e scientifica, eliminare la non comprensibilità della metodologia risolutiva algoritmica, quanto meno devono essere fornite adeguate e proporzionate garanzie a coloro che rientrano nel raggio di operatività delle telecamere dotate di IA. Questo lo si comprende in modo più approfondito analizzando, nei paragrafi a seguire, i problemi connessi alla non neutralità degli algoritmi e alla possibilità di svolgere un'attività di profilazione tramite riconoscimento facciale.

1.1.1. Il principio di Trasparenza nella Proposta di Regolamento sull'Intelligenza Artificiale

Nonostante sia ancora una proposta, merita attenzione indagare come viene disciplinato il principio di trasparenza nell'AI Act, poiché in questo atto assume la qualifica di principio cardine del funzionamento dell'Intelligenza Artificiale[289]. La priorità del Parlamento è quella di assicurare, attraverso la disciplina in questo atto predisposta, che i sistemi di intelligenza artificiale immessi e circolanti nel mercato europeo siano sicuri, trasparenti, tracciabili, non discriminatori e rispettosi dell'ambiente[290]. Innanzitutto è bene ricordare che la Proposta di regolamento disciplina l'IA attraverso un metodo basato sul rischio, ciò vuol dire che i sistemi vengono qualificati e classificati in base al rischio che deriva dal loro impiego, nei confronti delle persone fisiche. In base a questa tecnica *risk-based,* il riconoscimento facciale è categorizzato tra i sistemi ad alto rischio, ma nel caso in cui detta applicazione operi nelle modalità 'in tempo reale' e 'a distanza' in luoghi pubblici o aperti al pubblico, allora il rischio è inaccettabile, infatti l'articolo 5 lettera d) pone un divieto generale al loro impiego, individuando, di seguito, le tassative eccezioni.
L'articolo 52 [291]rubricato '*Obblighi di trasparenza per determinati sistemi di IA'*, predispone la disciplina del principio di trasparenza, individuando le informazioni che

[289] La proposta di Regolamento in questione viene analizzata nel dettaglio nel Cap. I paragrafi 6 e seguenti della presente tesi, si rimanda per un maggiore approfondimento.
[290] Cfr. Parlamento Europeo- Attualità, *'Normativa sull'IA: la prima regolamentazione sull'intelligenza artificiale',* 13/06/2023, https://www.europarl.europa.eu/news/it/headlines/society/20230601STO93804/normativa-sull-ia-la-prima-regolamentazione-sull-intelligenza-artificiale.
[291] L'articolo 52 dell'AI Act dispone: '*1. I fornitori garantiscono che i sistemi di IA destinati a interagire con le persone fisiche siano progettati e sviluppati in modo tale che le persone fisiche siano informate del*

devono necessariamente essere fornite alle persone fisiche che si relazionano con il sistema intelligente, ma per comprenderne la portata bisogna prendere in considerazione il Considerando n. 47. Quest'ultimo specifica, in modo puntuale, che il principio di trasparenza deve essere rispettato, nei sistemi di IA ad alto rischio, al fine di porre rimedio all'opacità, che può avere come conseguenza l'incomprensibilità o l'insormontabile complessità per le persone fisiche. Il legislatore europeo prosegue indicando come deve essere assicurata la trasparenza, e cioè dando la possibilità all'utente di interpretare gli *output* del sistema, nonché di poterlo utilizzare in modo adeguato. A tal fine, i sistemi ad alto rischio, dovrebbero essere corredati da un'apposita documentazione che individua le istruzioni per l'uso, riporta in modo chiaro e specifico le informazioni e ciò anche in relazione ai possibili rischi per i diritti fondamentali e discriminazioni[292]. In ottemperanza a quanto indicato nel considerando 47 si pone l'articolo 13 *'Trasparenza e fornitura di informazioni agli utenti'*[293]. Il modo in cui il principio di trasparenza viene regolato nella Proposta di

fatto di stare interagendo con un sistema di IA, a meno che ciò non risulti evidente dalle circostanze e dal contesto di utilizzo. Tale obbligo non si applica ai sistemi di IA autorizzati dalla legge per accertare, prevenire, indagare e perseguire reati, a meno che tali sistemi non siano a disposizione del pubblico per segnalare un reato.

2. Gli utenti di un sistema di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica informano le persone fisiche che vi sono esposte in merito al funzionamento del sistema. Tale obbligo non si applica ai sistemi di IA utilizzati per la categorizzazione biometrica, che sono autorizzati dalla legge per accertare, prevenire e indagare reati.

3. Gli utenti di un sistema di IA che genera o manipola immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri per una persona ("deep fake") sono tenuti a rendere noto che il contenuto è stato generato o manipolato artificialmente.

Tuttavia il primo comma non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare e perseguire reati o se è necessario per l'esercizio del diritto alla libertà di espressione e del diritto alla libertà delle arti e delle scienze garantito dalla Carta dei diritti fondamentali dell'UE, e fatte salve le tutele adeguate per i diritti e le libertà dei terzi.

4. I paragrafi 1, 2 e 3 lasciano impregiudicati i requisiti e gli obblighi di cui al titolo III del presente regolamento.'

[292] Cfr. Considerando n. 47 della Proposta di Regolamento sull'Intelligenza artificiale.

[293] Il testo dell'articolo 13 dispone: '1. *I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utenti di interpretare l'output del sistema e utilizzarlo adeguatamente. Sono garantiti un tipo e un livello di trasparenza adeguati, che consentano di conseguire il rispetto dei pertinenti obblighi dell'utente e del fornitore di cui al capo 3 del presente titolo.*

2. I sistemi di IA ad alto rischio sono accompagnati da istruzioni per l'uso in un formato digitale o non digitale appropriato, che comprendono informazioni concise, complete, corrette e chiare che siano pertinenti, accessibili e comprensibili per gli utenti.

3. *Le informazioni di cui al paragrafo 2 specificano*:

a) *l'identità e i dati di contatto del fornitore e, ove applicabile, del suo rappresentante autorizzato;*

b) le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio, tra cui:

i) la finalità prevista;

Regolamento permette, da un lato di comprendere che vi sono rischi concreti che scaturiscono dall'impiego dei sistemi di intelligenza artificiale, i quali sono più o meno invasivi, per la persona fisica, a seconda delle concrete funzioni che svolge l'IA (come sopra detto, nel caso del riconoscimento facciale i rischi per la persona fisica, soprattutto legati a illecite compressioni dei diritti fondamentali -come nel caso del diritto alla protezione dei dati personali- sono ampiamente suscettibili di verificarsi); dall'altro lato il Centro Europeo per la trasparenza algoritmica, svolgerà un ruolo di fondamentale importanza una volta approvato ed entrato in vigore l'AI Act, questo perché, se il principio di trasparenza assume una posizione cardine, allora si dovranno cercare di minimizzare, quanto più possibile, i rischi connessi all'opacità algoritmica. Questo fa comprendere le sfide che l'ECAT dovrà affrontare perché, i sistemi di IA più sviluppati, sfruttano quasi tutti il *machine* e il *deep learning*, che se da una parte consentono di far svolgere all'IA i compiti più complessi, dall'altra parte sono anche qualificati per il più alto grado di opacità e di incomprensibilità.

2. La non neutralità degli algoritmi: i *Bias*

Un ulteriore problema che viene in auge quando si sfruttano le funzionalità algoritmiche nei sistemi di riconoscimento facciale sono i *bias,* i quali determinano la non neutralità degli algoritmi. La non neutralità assume una particolare importanza nel mondo giuridico poiché, se gli algoritmi possono dare luogo a discriminazioni vuol dire che possono causare un'illecita violazione del principio di uguaglianza.[294]

---

ii) il livello di accuratezza, robustezza e cibersicurezza di cui all'articolo 15 rispetto al quale il sistema di IA ad alto rischio è stato sottoposto a prova e convalidato e che ci si può attendere, e qualsiasi circostanza nota e prevedibile che possa avere un impatto sul livello atteso di accuratezza, robustezza e cibersicurezza;
iii) qualsiasi circostanza nota o prevedibile connessa all'uso del sistema di IA ad alto rischio in conformità alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, che possa comportare rischi per la salute e la sicurezza o per i diritti fondamentali;
iv) le sue prestazioni per quanto riguarda le persone o i gruppi di persone sui quali il sistema è destinato a essere utilizzato;
v) ove opportuno, le specifiche per i dati di input o qualsiasi altra informazione pertinente in termini di set di dati di addestramento, convalida e prova, tenendo conto della finalità prevista del sistema di IA;
c) le eventuali modifiche apportate al sistema di IA ad alto rischio e alle sue prestazioni, che sono state predeterminate dal fornitore al momento della valutazione iniziale della conformità;
d) le misure di sorveglianza umana di cui all'articolo 14, comprese le misure tecniche poste in essere per facilitare l'interpretazione degli output dei sistemi di IA da parte degli utenti;
e) la durata prevista del sistema di IA ad alto rischio e tutte le misure di manutenzione e cura necessarie per garantire il corretto funzionamento di tale sistema, anche per quanto riguarda gli aggiornamenti software.'

[294] Cfr. G. Mobilio, *'Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e nuove sfide regolative',* Napoli, Editoriale Scientifica, 2021, p.217.

Il percorso che è stato seguito dalle istituzioni europee e che ha condotto alla redazione della Proposta di Regolamento sull'IA, ha avuto come obiettivo la creazione di sistemi intelligenti affidabili. Al fine di evitare che si verifichi la situazione contraria è necessario che siano rispettati il principio di uguaglianza e non discriminazione, pertanto il funzionamento dei sistemi di IA non deve produrre risultati ingiustificatamente distorti. Per arginare queste distorsioni è fondamentale la creazione di sistemi più inclusivi e rappresentativi di gruppi di popolazione diversi, nel consueto rispetto delle persone e dei gruppi vulnerabili[295].

Nel mondo informatico i *bias* sono discriminazioni sistematiche e ingiustificate di determinati individui o gruppi, a favore di altri. Da questa definizione emergono due punti fondamentali, da un lato infatti una discriminazione ingiusta non può essere qualificata come *bias* a meno che non si verifichi in modo sistematico; dall'altro lato, la distorsione ingiustificata e sistematica deve essere la causa di un risultato ingiusto[296]. Esistono diversi tipi di *bias,* i quali sono riconducibili a tre categorie, cioè i *bias preesistenti*, quelli *tecnici* e quelli *emergenti*. I *bias preesistenti* sono radicati nelle istituzioni sociali così come nelle pratiche e nelle attitudini, di conseguenza si tratta di pregiudizi che vengono incorporati nel sistema informatico, quindi se vengono assimilati significa che preesistono alla sua creazione. In secondo luogo, posso esservi dei *bias tecnici* ossia generati da vincoli o considerazioni tecniche, i quali nascono dalla risoluzione di problemi che colpiscono i *design* tecnici. Infine, esistono i *bias emergenti,* i quali si differenziano poiché se i *bias preesistenti* e *tecnici* si collocano nel momento della nascita o dell'implementazione del sistema, i *bias emergenti* vengono in essere durante l'impiego dei sistemi informatici, si tratta, cioè, di distorsioni che normalmente dipendo da cambiamenti della conoscenza sociale[297].

---

[295] Cit. Gruppo indipendente di esperti di alto livello sull'intelligenza artificiale, *'Orientamenti etici per un'intelligenza artificiale affidabile',* 8 Aprile 2019.

[296] Cit. B. Friedman, H. Nissenbaum, *'Bias in Computer System', 'in'* ACT Transactions on Informations Systems, Vol. 14, No. 3, July 1996, p. 332-333. Un esempio di *bias* che viene riportato in queste pagine è il seguente: si verifica un *bias* quando un consulente creditizio automatizzato assegna, sistematicamente, cattive valutazioni a soggetti che hanno un cognome etnico diverso, in quanto discrimina su basi non rilevanti ai fini del riconoscimento del credito. Se da queste valutazioni dipende il diniego di un credito la distorsione è a tutti gli effetti un *bias* del sistema perché oltre a presentarsi una discriminazione ingiustificata e sistematica, da questa deriva anche un risultato ingiusto nei confronti del/dei soggetti che si sono sottoposti al trattamento automatizzato.

[297] B. Friedman, H. Nissenbaum, *op. cit.* 333 ss.

2.1. I diversi momenti in cui hanno origine i *bias:* dalla progettazione all'effettivo svolgimento del riconoscimento facciale

Nel paragrafo precedente si sono distinte tre tipologie di *bias,* ora si vogliono invece individuare i momenti in cui una distorsione si può verificare nel corso della 'vita' di un sistema di intelligenza artificiale[298]. È importante individuare i diversi archi temporali in cui può sostanziarsi un *bias,* soltanto in questo modo si può intervenire prima che la distorsione si concretizzi in un danno ingiusto verso i soggetti destinatari del trattamento e comunque questo risultato non è sempre possibile, ma dipende dal momento in cui la distorsione può verificarsi.

Ciò premesso, il primo momento rilevante è quello della programmazione, la fase dedicata alla progettazione dell'algoritmo. Questa prima tappa della vita di un sistema intelligente si concentra nell'individuazione della metodologia che seguirà il sistema di apprendimento, che nelle TRF normalmente è automatico, per localizzare le correlazioni presenti in uno specifico *set* di dati. Intervenire nel momento della programmazione ha notevoli risvolti positivi poiché da la possibilità di eliminare fin dal principio la distorsione, evitando cioè che si verifichi, ma è evidente che in questo caso si deve conoscere la ragione che condurrebbe il sistema ad una discriminazione totalmente ingiustificata. In questo caso si procede 'ordinando' al sistema di *machine learning* di considerare irrilevanti alcuni caratteri ricorrenti, che potrebbero essere la causa della distorsione[299]. I caratteri che devono essere esclusi dall'algoritmo sono i più vari: razza, colore, sesso, lingua, religione, opinione politica, nazionalità e origine sociale, *status* economico, nonché qualsiasi altra condizione sociale (le c.d. *categorie algoritmiche sospette*[300]*).* Se non si effettuasse questa esclusione allora si genererebbe una discriminazione algoritmica diretta, derivante cioè da un'analisi pregiudizievole dei dati sensibili. Ciò nonostante, è importante rilevare che alcune tra le più note banche dati, nell'ambito del riconoscimento facciale, si prestano a questa tipologia di

[298] Cfr. P. Zuddas, *'Intelligenza artificiale e discriminazioni', 'in'* Consulta Online – Liber Amicorum per Pasquale Costanzo, 16 Marzo 2020, p. 5 ss.
[299] Ibidem nota 298.
[300] Cit. D. U. Galetta, J. G. Corvalan, *'Intelligenza artificiale per una pubblica amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto', 'in'* Federalismi, 6 Febbraio 2019, p. 21-22.

discriminazioni, non si è esenti da casi in cui le TRF non sono in grado, ad esempio, di distinguere il colore della pelle dei destinatari del trattamento[301]. Inoltre, una ricerca ha dimostrato anche la possibilità che si verifichi una forma di razzismo scientifico. Tra gli altri casi, l'esempio che si riporta è quello della UTKFace *Dataset,* la quale raccoglie circa 20.000 immagini ritraenti persone classificate ed etichettate in base al genere, all'età e alla razza. Precisamente i problemi vengono in essere con riferimento al genere e alla razza, dati particolarmente sensibili. Per quanto concerne il genere, infatti, i programmatori si sono limitati ad etichettare i volti ritratti dalle immagini attraverso una classificazione binaria maschio/femmina; per quel che riguarda, d'altra parte, la razza, sono state adottate solo cinque categorie distintive entro le quali collocare i soggetti, ossia: Bianco, Nero, Asiatico, 'Altro[302]'. Si comprende facilmente da questa descrizione del caso, che la scelta delle etichette così effettuata può condurre a quello che è stato nominato poc'anzi come razzismo scientifico[303].

Nella fase che si sta analizzando possono verificarsi anche differenti tipi di *bias* e in particolare le discriminazioni algoritmiche indirette, ossia le c.d. *Proxy Discriminations.* I caratteri *proxy* sono tali perché, in modo indiretto, collegano ad una categoria protetta piuttosto che a caratteri specifici che però non sono consentiti. Si tratta di *bias* che con l'avvento dell'apprendimento automatico hanno trovato una nuova vita, in quanto, i suddetti caratteri, potrebbero essere direttamente individuati dal sistema[304]. Di conseguenza si connette, al problema della non neutralità, un ulteriore livello problematico dato dal fatto che, come messo in luce nel paragrafo 1, i modelli di apprendimento automatico sono opachi e difficilmente comprensibili, anche all'occhio di un esperto di IA[305].

---

[301] M. Merler, N. Ratha, R. S. Feris, J. R. Smith, *'Diversity in faces', 'in'* arXiv, 2019, https://arxiv.org/abs/1901.10436.

[302] Cfr. K. Crawford, T. Paglien, '*Excavating AI: The Politics of Training Set for Machine Learning',* 19 Settembre 2019, https://excavating.ai/.

[303] Cit. Ibidem nota 280.

[304] P. Zuddas *op. cit*.

[305] P. Zuddas *op. cit*. Per maggiore completezza si riporta che gli studiosi hanno individuato due tipi di problemi pratici che possono venire in essere quando si tratta di *proxy discrimination*. Da un lato l'opacità del modello di apprendimento automatico rende particolarmente gravoso individuare *proxies* discriminatorie; dall'altro lato è anche possibile che si sostanzi il problema del c.d. 'slittamento', si tratta di un fenomeno inevitabile che si verifica quando, a seguito del divieto impartito all'algoritmo di *machine learning* di poter usare i caratteri *proxies,* comunque il sistema giunge a categorie più 'lontane' e le quali sono collegate a quelle categorie per le quali sussiste un divieto. Per un maggiore approfondimento sul

Se questi sono i *bias* che possono caratterizzare la fase di programmazione del sistema e quindi la progettazione degli algoritmi di funzionamento, non sono gli unici tipi individuabili, infatti vi è un secondo stadio temporale a cui ricongiungere la possibilità che si formino distorsioni ingiustificate, e in questa seconda fase i pregiudizi sono la conseguenza dei dati scelti per costruire il *training set,* ossia il set di addestramento della TRF, e generalmente del sistema di IA. Per comprendere a fondo l'ubiquità dei problemi connessi a questa ultima forma di *bias,* è necessario avere presente le ulteriori difficoltà che sono legate alla lettura delle immagini. Le Tecnologie di riconoscimento facciale sono progettate per identificare, tramite la lettura dei dati biometrici, gli individui, ma si tratta di un'operazione molto gravosa perché le immagini sono per loro natura sfuggenti e cariche di incomprensioni. Diversi campi del sapere si sono, nel corso della storia, impegnati a dispiegare il significato legato ad una immagine, dalla storia alla filosofia, e ancora il mondo dell'arte e la teoria dei media, e se queste difficoltà vengono in auge già quando si osservano fotografie che rappresentano oggetti, queste aumentano esponenzialmente quando il soggetto dell'immagine non è un oggetto ma una persona[306]. Di conseguenza, tutti i problemi legati alla ricerca della giusta relazione tra significato e soggetto ritratto si ripresentano e si aggravano quando a dover effettuare questa ricerca non è più un uomo, bensì un sistema intelligente, il quale apprende in base alle istruzioni che gli sono impartite e riproduce i pregiudizi che gravano la mente umana (c.d. *Bias cognitivi).* Una volta compresa la complessità delle sfide legate alla lettura delle immagini, occorre analizzare le ulteriori questioni che si palesano con riferimento alle distorsioni legate alla scelta del *training set.* I programmatori hanno la libertà di adottare quale set di addestramento o una banca dati 'aperta' che reperisce i *big data* mediante la rete Internet, o un archivio 'chiuso' dove i dati che sono sfruttati sono circoscrivibili ad un insieme dai confini definiti. In entrambi i casi si possono adottare dati inquinati o dati incompleti che possono condurre a previsioni inadeguate, allora diviene necessario agire, fin dal principio, proprio per evitare che la scelta dei

punto si veda, nello specifico, A. Prince, D. B Schwarcz, *'Proxy Discrimination in theAage of Artificial Intelligence and Big Data', 'in'* Iowa Law Review, 5 Agosto 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3347959.

[306] K. Crawford, T. Paglien, *op. cit.* in particolare il paragrafo '*Training AI'.*

dati ricada su quelli di scarsa qualità, obsoleti o inesatti[307]. Una volta compreso che i problemi in termini di distorsioni ingiustificate sono causati dai dati incompleti e inquinati, sembra facile anche individuare la soluzione del problema, ma tale facilità è solo apparente. Se è l'uomo che sceglie i dati con cui istruire un sistema intelligente, allora saranno solo le informazioni da lui reputate 'inquinate' o 'incomplete' ad essere scartate, ma non vuol dire che siano le uniche con tali caratteristiche. I pregiudizi si annidano nel nostro pensiero e difficilmente se ne vanno, sono il frutto del luogo e di come siamo stati cresciuti, delle scuole che abbiamo frequentato, delle persone che abbiamo incontrato e del tempo in cui abbiamo vissuto, tutti questi sono fattori che incidono sul modo in cui pensiamo e agiamo, e di conseguenza si ripercuotono anche nella scelta dei dati che vengono impiegati per l'addestramento[308]. Ora, nel caso in cui sia adottato un *data set* 'chiuso' i veri problemi si evidenziano quando non sono adottati filtri ulteriori volti a limitare la scelta dei dati presenti, in questo caso, cioè, l'algoritmo viene alimentato con una statistica storica delle decisioni effettuate in passato[309], e quindi mediante dati che sono inquinati. Un caso storico in questo ambito è rappresentato dalla vicenda COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions).* Si tratta di un algoritmo ideato per scovare il rischio di recidiva in soggetti imputati in procedimenti penali, soltanto che diversi studi hanno dimostrato che presentava un pregiudizio ingiustificato nei confronti delle persone di colore, questo perché le successive verifiche evidenziarono che vennero impiegati, per l'addestramento, prevalentemente casi giudiziari giunti ad un risultato negativo verso questa categoria di soggetti[310]. Se quest'ultimo esempio si riferisce all'impiego di dati inquinati, sempre nell'ambito di banche dati 'chiuse', i problemi si esplicano anche se i dati usati sono incompleti, infatti in questo frangente ciò che

---

[307] Cit. Parlamento Europeo, *'Risoluzione del Parlamento Europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale', https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52019IP0081&from=EN*.

[308] Cfr. L. Cannito, *'Cosa sono i bias cognitivi?', 'in'* Economia comportamentale, 2017, https://www.economiacomportamentale.it/wp-content/uploads/2021/10/Cosa-sono-i-bias-cognitivi_.pdf. L'autrice, nell'ultima parte dell'articolo, evidenzia che è la possibilità di attuare un processo di *debiasing* volto ad eliminare la presenza di *bias cognitivi,* ma al contempo specifica che si tratta di un procedimento molto lungo e complesso. A tal proposito, per maggiori informazioni si può consultare '*A user's guide to debiasing'.*

[309] P. Zuddas, *op. cit.* 8.

[310] Cfr. G. Resta, *'Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza', 'in'* Forum disuguaglianze diversità. 15 proposte per la giustizia sociale, https://www.forumdisuguaglianzediversita.org/wp-content/uploads/2019/09/Resta.x89907.pdf. P. 222 ss.

incide in modo significativo sono i modi e/o gli strumenti attraverso i quali sono ottenute le informazioni[311]. Accanto ai problemi legati ai sistemi di addestramento 'chiusi' vi sono quelli legati alle banche dati 'aperte' che cioè fanno ricorso alla rete internet, in questo caso, evidentemente possono essere riprodotti tutti i pregiudizi che governano il web e di conseguenza anche i social network[312]. Un'ultima puntualizzazione rilevante con riferimento tanto ai *bias* che sorgono in riferimento ad un *training set* chiuso quanto a quelli che si verificano in un sistema aperto, è che in entrambi i casi possono essere distinti i *Bias di selezione* dai *Bias di conferma*[313]. I primi si verificano poiché è stata erroneamente scelta la fonte sorgente dalla quale reperire le immagini, i secondi invece sono causati dalle persone che si occupano della valutazione dei dati precedentemente selezionati. I *bias di conferma* sono un'ulteriore riprova di quanto affermato poc'anzi, ossia del fatto che la mente umana è carica di pregiudizi che portano l'uomo a porre maggiore attenzione e quindi ad accettare più facilmente le prove a supporto di ciò in cui credono, conducendolo invece a ignorare o sottovalutare quelle lo contraddicono e se questo influenza il processo decisionale, allo stesso modo può riprodursi in un'applicazione di IA, influenzando le stesse decisioni prese da quest'ultima, sempre per il fatto che è l'uomo che decide i canoni e le condizioni di apprendimento.

La trattazione fa emergere con evidenza l'importanza della scelta delle immagini, infatti la qualità degli *output,* quali risultati in uscita, dipende dall'apprezzabilità degli *input,* cioè dei dati che compongono il *training set:* questo è il principio che si esprime

---

311 Cfr. F. Z. Borgesius, *'Discrimination, Artficial intelligence and Algorithmic decision-making',* Published by Director General of Democracy, 2018, https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73. P. 15 ss.

312 I casi legati a queste forme di *bias* sono numerosi, si può ricordare il TAY, si tratta di un esperimento condotto da Microsoft nel 2016 al fine di creare un algoritmo in grado di replicare il linguaggio comunicativo degli adolescenti, si trattava di un sistema in grado di reperire tutte le informazioni necessarie dal mondo online, ma che allo stesso tempo si dimostrò razzista, misogino e per certi versi anche nazista; di conseguenza il progetto fu interrotto poco dopo l'avviamento della sperimentazione. Sul punto si può vedere, per un maggiore approfondimento: A. Venanzoni, *'La valle del perturbante: il costituzionalismo alla prova delle intelligenze artificiali e della robotica', 'in'* Scienze Politiche, 2019, p. 238 ss. Ma non è il solo caso che può essere ricordato, infatti F. Z Borgesius (ibidem nota 297) ricorda il caso di Google Images del 2016. In questo caso se veniva chiesto all'algoritmo di mostrare immagini ritraenti persone bianche allora venivano trovate foto ordinarie senza alcun problema, ma nel momento in cui veniva chiesto all'algoritmo di scovare immagini di ragazzi di colore, le foto che venivano proposte erano foto segnaletiche della polizia. P. 16 ss.

313 Cfr. Consultative Committee of the Convention 108, *'Report on Artificial Intelligence'*, 25 July 2019 p. 9 ss.

nella locuzione tecnica *garbage in, garbage out*[314]. In conclusione, tutto quanto sostenuto, se non si è disposti a rinunciare all'aiuto quotidiano che l'intelligenza artificiale ci offre e se non è possibile, allo stato attuale dell'evoluzione tecnologica, eliminare totalmente le distorsioni ingiustificate, allora è fondamentale, proprio come contro l'opacità, fornire adeguate tutele giuridiche conto la *AI-Driven discrimination.*

2.2. Gli automatismi del riconoscimento facciale

Si è chiuso il paragrafo precedente evidenziando la necessità di adeguate tutele contro l'*AI-Driven Discrimination,* ma prima di entrare nel vivo delle soluzioni è opportuno sottolineare che l'evoluzione tecno-informatica ha consentito ai sistemi di IA di raggiungere un grado di autonomia un tempo impensabile. È oggi un evento del tutto ordinario che un'applicazione intelligente sia in grado di agire in modo totalmente indipendente, infatti le TRF, come molte applicazioni di IA, sono in grado di prendere decisioni autonome, per questo si può affermare che si aprono le porte agli automatismi del riconoscimento facciale. Quando l'interessato è destinatario di una decisione completamente automatizzata vuol dire che il risultato è stato elaborato, senza alcun intervento umano, dall'algoritmo sotteso alla funzione di riconoscimento facciale, quindi attraverso un confronto tra le immagini presenti in *database* e le fotografie reperite dai sistemi di videosorveglianza, se è individuato un *match* il sistema emette la decisione, la quale consiste nell'identificazione biometrica[315].

L'incredibile autonomia che ad oggi contraddistingue l'intelligenza artificiale solleva rilevanti questioni. Da un lato vi è chi sostiene che sia un passo in avanti verso la c.d. *singolarità tecnologica,* dall'altro lato si amplificano esponenzialmente le problematiche connesse all'esistenza di *bias* nel processo logico di azione seguito dall'algoritmo. Per quel che riguarda la singolarità tecnologica si tratta di una prospettiva secondo la quale arriverà un momento storico in cui non sarà più possibile distinguere un automa da un essere umano, e anzi la macchina sarà in grado prima di integrare la mente umana per poi superarne le capacità di pensiero, dando vita ad una

[314] G. Resta, *op. cit.*. 208.
[315] Per un maggiore approfondimento su come funzionano i sistemi di riconoscimento facciale si veda il Capitolo II, paragrafo 3.

commistione biorobotica[316]. Per quanto concerne, dall'altro lato, i problemi scaturenti dalle discriminazioni algoritmiche è evidente che, se anche la decisione finale viene presa dal sistema intelligente, non vi è possibilità di intervento se non *ex-post,* ossia una volta che sia stato prodotto il risultato ingiusto verso il destinatario della decisione. È proprio in questa fase decisionale che si possono verificare delle *proxies* discriminatorie non volute, cioè si concretizza la possibilità che l'algoritmo individui nuove categorie di soggetti, in base a caratteristiche che per l'appunto sono individuate autonomamente dal sistema, che sono sottoposte a trattamento diverso e più gravoso rispetto a quello cui sono esposte altre categorie di soggetti.

3. Le tutele contro gli automatismi e le discriminazioni degli algoritmi di riconoscimento facciale

La panoramica presentata nei paragrafi precedenti impone di ricercare una base giuridica che offra un'adeguata tutela contro i *bias,* la quale deve essere integrata con la disciplina a protezione delle persone fisiche esposte a decisioni basate esclusivamente su un trattamento automatizzato (come nel caso delle TRF).

Il principio di non discriminazione è un principio cardine dell'Unione Europea, sancito all'articolo 21 della Carta dei diritti fondamentali dell'UE, il quale dispone: '*1. È vietata qualsiasi forma di discriminazione fondata, in particolare, sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, gli handicap, l'età o le tendenze sessuali. 2. Nell'ambito d'applicazione del trattato che istituisce la Comunità europea e del trattato sull'Unione europea è vietata qualsiasi*

[316] La singolarità tecnologica è una visione pessimistica che dipende dal modo in cui l'uomo si approccia all'intelligenza artificiale, se si aderisce alla tesi 'forte' dell'IA allora si aprono le porte a questa eventualità poiché questa visione sostiene che l'IA possa integrare taluni valori propri dell'essere umano. Se dall'altra parte si aderisce alla tesi 'debole' dell'IA questa eventualità è del tutto esclusa perché vi sarà sempre e comunque un elemento distintivo tra l'essere umano e gli automi ed è rappresentato dalla capacità di deliberare. Per maggiori approfondimenti si può consultare: V. Vige, *'The Coming Technological Singularity: How to Survive in the Post-Human Era, in Vision-21 Interdisciplinary Science and Engineering in the Era of Cyber-Space',* Proceedings of a symposium cosponsored by the NASA Lewis Research center and the Ohio Aerospace Institute and held in Westlake, Ohio, 1993. Ancora: R. Kurzweil, *'The singularity is near. When humans transcend biology',* New York, Viking, 2005. E infine: R. Kurzweil, *'Get ready for hybrid thinking',* TED talk, 2014.

discriminazione fondata sulla cittadinanza, fatte salve le disposizioni particolari contenute nei trattati stessi'. L'attuazione di questo principio avviene mediante la predisposizione e la successiva attuazione di diverse Direttive settoriali, le quali hanno la funzione di coordinare la legislazione nazionale in materia. In particolare si hanno: la Direttiva 2000/43/EC, la quale attua il principio della parità di trattamento fra le persone a prescindere dalla razza e dall'origine etnica; la Direttiva 2000/78/2000 (c.d. direttiva quadro), che sancisce il principio di parità di trattamento in materia di occupazione e lavoro, in questo caso si tratta di una disciplina che è volta a prevenire che si esplichino discriminazioni basate sulla religione o le convinzioni personali, gli handicap, l'età o le tendenze sessuali; possiamo poi ricordare la Direttiva 2004/113/EC relativa al principio di parità di trattamento tra uomini e donne con riferimento all'accesso a beni e servizi, nonché la loro fornitura; infine si cita qui la Direttiva 2006/54/EC riguardante il principio delle pari opportunità e della parità di trattamento tra uomini e donne in materia di lavoro e occupazione. La disciplina antidiscriminatoria che si individua in queste quattro Direttive ruota intorno ad una distinzione fondamentale, ossia quella tra discriminazione 'diretta' e 'indiretta[317]'. Si verifica una discriminazione 'diretta' quando un soggetto riceve un trattamento sfavorevole rispetto a quello ricevuto o che potrebbe ricevere un'altra persona, nella medesima situazione. Nel mondo dell'intelligenza artificiale questa tipologia si integra quando o l'algoritmo attribuisce rilevanza minore a dati sensibili, o quando la distorsione dipende da come sono state apposte le etichette che qualificano e classificano i dati in uno specifico *training set.* La discriminazione 'indiretta' si manifesta in un trattamento pregiudizievole che non è facilmente scrutabile, poiché dipende da come l'algoritmo valuta una disposizione, una prassi o un criterio che a primo impatto sembrano neutri, ma che producono un risultato distorsivo verso soggetti che sostengono una particolare religione o ideologia, verso persone portatrici

[317] Per essere specifici, le forme di discriminazione che sono individuate nelle Direttive citate sono quattro, oltre alla discriminazione 'diretta' e 'indiretta', si individuano anche la discriminazione che si sostanzia in molestie e le istruzioni a discriminare; ciò nonostante in questa sede ci si limita a prendere in esame le due forme di discriminazione 'diretta' e 'indiretta', poiché sono le forme di distorsioni cui possono dar vita i sistemi di intelligenza artificiale come si puntualizza nel paragrafo 2.1 del presente capitolo. Cfr. H. Sapeha, *'Le leggi anti-discriminazione nell'Unione Europea. Come funzionano le leggi anti-discriminazione nei paesi membri e come sono regolate dall'UE', 'in'* Europe Direct Emilia-Romagna, Assemblea legislativa, Febbraio 2008, https://www.assemblea.emr.it/europedirect/pace-e-diritti/archivio/i-diritti-umani-e-leuropa/2008/le-leggi-anti-discriminazione-nell2019unione-europea.

di handicap, di una determinata età o tendenza sessuale, rispetto ad altri soggetti.[318] Una volta evidenziata questa distinzione, si deve avere a mente che il diritto anti-discriminatorio agisce sulle *conseguenze degli atti*, cioè dopo che si è accertata la sussistenza di un nesso di causalità tra l'atto e il pregiudizio nei confronti di un soggetto o di un gruppo di persone svantaggiate, si tratta cioè di una forma di tutela *ex post*[319]. Se da un lato si comprende agevolmente la necessità di una garanzia *ex ante,* dall'altro lato deve anche chiedersi perché sia un'esigenza così sentita, soprattutto nel momento in cui il trattamento sfavorevole sia la conseguenza di un automatismo dell'IA. I soggetti che volessero lamentare di aver subito un trattamento sfavorevole devono fornire una prova quasi impossibile, improntata al principio di proporzionalità, cioè devono provare la sussistenza del nesso di causalità di cui si è detto sopra, ma perché ciò sia possibile è prima necessario risolvere il problema dell'opacità algoritmica, solo così si garantisce l'accesso alla *black box,* che non sarebbe più così qualificabile[320].

Date le rilevanti difficoltà nella concreta applicazione della legislazione antidiscriminatoria, come forma di tutela nei confronti dei *bias,* emerge l'esigenza di individuare una normativa che, seguendo un approccio diverso, si concretizzi in una effettiva tutela verso i soggetti destinatari del trattamento automatizzato. Ancora una volta l'attenzione deve essere rivolta verso il GDPR, e in particolare al Considerando 71 poiché esplicita il *principio di non discriminazione per via algoritmica*[321].

---

[318] Cit. G. Mobilio, *'Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative',* Editoriale Scientifica, Napoli, 2021, p. 225-226.

[319] Cfr. M. Barbera, *'Discriminazioni algoritmiche e forme di discriminazione', 'in'* Labour and Law Issues, Vol. 7, n. 1, 2021, https://labourlaw.unibo.it/article/view/13127/12679. P. 8-9.

[320] Cfr. P. Zuddas, *'Intelligenza artificiale e discriminazioni', 'in'* Consulta Online-Liber Amicorum per Pasquale Costanzo, 16 Marzo 2022.

[321] Cit. A. Simoncini, S. Suweis, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale, 'in'* Rivista di filosofia del diritto, VII, 1/2019, cit. p. 101. Inoltre Il Considerando 71 pur non avendo valenza normativa assume un'importanza di massima centralità e dispone: '*L'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani. Tale trattamento comprende la «profilazione», che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo*

L'efficacia di questo principio si individua sotto due profili, infatti da un lato rileva l'importanza che si pone sui *criteri* attraverso i quali devono essere considerati gli elementi interni della decisione algoritmica; dall'altro lato è rilevante l'importanza che il legislatore europeo attribuisce alle misure tecniche e organizzative che devono essere adottate dal titolare a tutela degli interessati.

Procedendo per gradi, ciò che contraddistingue il Considerando 71 dalla legislazione antidiscriminatoria è l'approccio seguito dal legislatore, infatti è la concretizzazione della consapevolezza per cui solo vietando che una decisione sia presa sulla base di caratteri sensibili, si può effettivamente prevenire l'esplicarsi di un effetto dannoso, non ci si deve cioè solo concentrare sul risultato, ossia sulla decisione prodotta automaticamente dall'algoritmo, ma sui parametri e dati che si pongono a fondamenta della decisione specifica. A questo proposito il Considerando 71 parla di '*aspetti personali che lo riguardano'* e sancisce il diritto dell'individuo a non essere sottoposto ad una decisione che si basi solo ed esclusivamente su questi, potendovisi ricongiungere, all'interno di questa categoria, tutti i dati sensibili, dall'origine razziale, alla religione, ideologia, orientamento politico… In questo modo si prevengono quelle che sono state qualificate come discriminazioni 'dirette'.
Resta da risolvere il problema legato alle discriminazioni 'indirette', quelle distorsioni precedentemente chiamate *proxies,* ciò perché, per loro natura, derivano da caratteri 'neutri', non collocabili nella categoria di dati protetti, inoltre non è nemmeno possibile evitare, attraverso un'idonea programmazione, che l'algoritmo non basi il suo operato sui caratteri dai quali generano le *proxies discriminations* perché, come

analogo significativamente sulla sua persona. Tuttavia, è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore.'

già ribadito, sono dati neutri. Così, il rimedio alle discriminazioni indirette, si ritrova nel secondo profilo di rilevanza del Considerando che si sta analizzando, infatti questo chiede che il titolare del trattamento adotti *misure tecniche e organizzative,* affinché, per il loro tramite, si possa assicurare un trattamento equo e non discriminatorio, oltreché rispettoso della disciplina contenuta nello stesso Regolamento 679/2016. Quanto più rilevanti sono le misure tecniche poiché in questa tipologia di interventi vi rientrano tutti i parametri che siano, a livello di programmazione e configurazione del *training set,* suscettibili di evitare il sostanziarsi di una decisione ingiusta e discriminatoria. Allo stesso tempo, si chiede inoltre che siano adottate adeguate *misure organizzative*[322]*,* tra le quali vi rientrano gli interventi di esperti al fine di integrare e implementare l'IA con sistemi intelligenti proveniente da altre culture, contesti o da altre discipline[323]. La disciplina analizzata permette di concludere sul punto affermando che, in assenza di una puntuale disciplina che regoli l'intelligenza artificiale e in assenza di soluzioni tecniche, scientifiche ed informatiche che possano eliminare l'opacità e la discriminazione algoritmica, non vi è altra soluzione che quella di attribuire idonee garanzie nei confronti dei soggetti interessati, tutele antidiscriminatorie che devono a loro volta essere integrate con la disciplina prevista dal GDPR per le decisioni completamente basate su un trattamento automatizzato.

Non resta che prendere in considerazione quest'ultima, e sempre con riferimento al Regolamento 679/2016, il punto di partenza è individuato nell'articolo 22. Innanzitutto viene in auge che se il Considerando 71 individua misure che hanno l'obiettivo di intervenire sul problema in via preventiva, al contrario la disciplina che si andrà d'ora in poi a prendere in esame consente di constatare la sussistenza di distorsione una volta che si siano già verificate.[324] L'articolo 22 del GDPR dispone: '***1.*** *L'interessato ha il diritto di non essere sottoposto a una decisione basata*

[322] Si occupano in modo specifico della disciplina antidiscriminatoria e delle tutele predisposte dal GDPR, nonché di un loro specifico confronto: P. Zuddas, *'Intelligenza artificiale e discriminazioni', 'in'* Consulta Online-Liber Amicorum per Pasquale Costanzo, 16 Marzo 2022, p 13, 14, 15. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative',* Editoriale Scientifica, Napoli, 2021, p. 224 ss. E ancora: A. Simoncini, S. Suweis, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale, 'in'* Rivista di filosofia del diritto, VII, 1/2019.

[323] Gruppo indipendente di esperti di alto livello sull'intelligenza artificiale, '*Orientamenti etici per un'intelligenza artificiale affidabile',* 8 Aprile 2019, cit 5.

[324] P Zuddas, *op. cit*. 16.

unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. ***2.*** *Il paragrafo 1 non si applica nel caso in cui la decisione:* ***a)*** *sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;* ***b)*** *sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;* ***c)*** *si basi sul consenso esplicito dell'interessato*[325]*.'* Il primo paragrafo dell'articolo riportato pone un divieto generale a che un soggetto sia sottoposto a decisioni completamente automatizzate, allo stesso tempo il paragrafo successivo individua delle eccezioni al verificarsi delle quali il divieto posto cessa di operare, ma chiede comunque che siano applicate le garanzie previste dal Considerando 71.[326] Si pone così un regime di non esclusività, assistito da ulteriori tutele, infatti l'interessato ha la facoltà anche di chiedere e ricevere notizie sulle logiche utilizzate, nonché sull'importanza e sulle conseguenze previste, inoltre ha il diritto di chiedere, in caso in cui sussistano specifiche condizioni, che non venga attuato il trattamento in questione[327]. Il secondo paragrafo individua le eccezioni, ossia i casi tassativi in cui le persone fisiche possono essere esposte ad un simile trattamento, e proprio queste eccezioni rappresentano il punto debole della disciplina poiché permettono di raggirare il divieto posto dal primo paragrafo. Si prenda l'eccezione di cui al secondo paragrafo lettera c), in questo caso, se è ottenuto il consenso dell'interessato, allora il divieto può essere sorvolato ma è evidente quanto sia facile ottenere un consenso in cambio dell'erogazione di servizi

[325] Sono qui stati riportati solo i primi due paragrafi dell'articolo poiché sono quelli rilevanti fini della trattazione, ma l'articolo 22 GDPR prosegue e dispone: '***3.*** *Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.* ***4.*** *Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.'*

[326] Il Gruppo di Lavoro articolo 29 specifica che la corretta interpretazione è quella riportata, non deve cioè intendersi il primo paragrafo dell'articolo 22 come un diritto che può essere invocato dal destinatario del trattamento, altrimenti non fungerebbe quale effettiva garanzia nei suoi confronti, ma è un divieto generale che non opera solo ed esclusivamente qualora si verifichi una delle eccezioni tassativamente riportate di seguito nel paragrafo 2. Cfr. Gruppo di lavoro articolo 29, *'Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679'* versione emendata del 6 Febbraio 2016, in particolare p. 21 ss.

[327] G. Mobilio, *'Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative', op. cit.* 196

basati su decisioni algoritmiche[328], pertanto viene in essere, senza dubbio, la labilità della disciplina in relazione alle eccezioni. Vero è che il soggetto destinatario ha ulteriori tutele invocabili, tra le quali ha la possibilità di chiedere l'intervento umano, e questo normalmente si verifica nelle TRF, ma è anche necessario sottolineare che i processi algoritmici sottesi sono complessi a tal punto che spesso e volentieri l'esperto si limita a confermare la soluzione raggiunta dal sistema[329], trasformandosi così la tutela da effettiva ad apparente. Simili critiche possono essere sollevate anche con riguardo agli ulteriori diritti invocabili dal destinatario del trattamento sanciti dallo stesso articolo 22, ossia il diritto di opinione e il diritto di contestare la decisione, infatti si pongono, sempre e comunque, come limiti evidenti l'opacità e la non comprensibilità dei processi di *machine learning.*

3.1. La profilazione al servizio della *Dataveillance*

L'articolo 22 del GDPR dispone, nel primo paragrafo, che *'l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione…'* ed effettivamente le Tecnologie di riconoscimento facciale sono un potente strumento ai fini della profilazione. Prima di entrare nel vivo della questione è necessario spiegare che cos'è la profilazione, la quale trova una puntuale definizione all'articolo 4, n. 4 del Regolamento 2016/679: *'qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica'.* Per il fatto che il legislatore utilizza il verbo valutare per indicare l'azione che viene compiuta sui dati personali, per lo svolgimento di attività di analisi o predittive, suggerisce che la profilazione sia una tecnica che sottende valutazioni o

[328] P. Zuddas, *op. cit.* 16-17.

[329] Per questa ragione vi è chi ritiene che debba attingersi ad una interpretazione sostanziale di processo decisionale, ricongiungendovi anche i casi in cui l'intervento umano sia meramente formale. Sul punto si veda: L.A. Bygrave, '*Automated Profiling: Minding the Machine: Article 15of the EC Data Protection Directive and Automated Profiling*', in Computer Law & Security Review, 17, 2001, 20.

giudizi circa una persona[330]. Le valutazioni effettuate si sostanziano in deduzioni statistiche, questo perché viene impiegata al fine di effettuare previsioni sulle persone fisiche in base alle qualità, statisticamente simili, presenti in altre persone[331].

La profilazione è una tecnica ampiamente usata nell'era dell'informazione, infatti ha a disposizione strumenti potentissimi che se combinati fanno comprendere la pervasività della procedura: il *machine learning* viene sfruttato, cioè, per la *valutazione* di enormi quantità di dati reperiti dalle più svariate fonti (*web, app* utilizzate sugli *smartphone,* dispositivi dell'*Internet of things…).* Una volta che i dati personali sono ottenuti si apre la seconda fase, volta al raggruppamento, in questo stadio tutti i dati delle persone che presentano tratti comuni vengono inseriti nella medesima classe, ad esempio per similarità nei comportamenti o nelle preferenze, e si da vita al profilo di ciascun soggetto; se un soggetto presenta lo stesso profilo di altri è questa una ragione bastevole per giungere alla conclusione che, molto probabilmente, condividerà ulteriori e altri attributi, e ciò sulla base di calcoli probabilistici[332]. Lo sviluppo di algoritmi in grado di apprendere automaticamente attraverso i dati che costituiscono il *training set,* ha consentito di incrementare l'uso della profilazione e allo stesso contribuisce a plasmare l'economia globale: l'automazione ha cioè consentito da un lato di diminuire i costi e dall'altro la difficoltà di reperimento dai dati necessari per svolgere la profilazione.[333]

Come anticipato nell'incipit del paragrafo anche le TRF si mettono al servizio della profilazione, in questo caso i dati che vengono valutati per analisi predittive sono le immagini catturate dalle telecamere. Se i risvolti dell'impiego di questa tecnica si esplicano in plurimi settori, da quello pubblico a quello privato, deve però aversi a mente la logica conseguenza dello sfruttamento di una così pervasiva tecnica

[330] Gruppo di lavoro articolo 29, *'Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento', op. cit*. 8.
[331] Ibidem nota 330, cit. 8.
[332] G. Mobilio, '*Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali', op. cit.* 201,202.
[333] Cfr. F. Lagioia, G. Sartor, '*profilazione e decisione algoritmica: dal mercato alla sfera pubblica', 'in'* Federalismi, 11/2020, https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=42114&dpath=document&dfile=23042020224508.pdf&content=Profilazione%2Be%2Bdecisione%2Balgoritmica%3A%2Bdal%2Bmercato%2Balla%2Bsfera%2Bpubblica%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B. P. 6,7.

predittiva, ossia i '*filter bubbles'*. Si tratta di un fenomeno che si riferisce alla tendenza che gli individui sottoposti a profilazione sono esposti principalmente ad informazioni e opinioni che risultano conformi e in linea con le loro convinzioni, in tal modo si personalizza l'informazione e si limitano esponenzialmente le possibilità degli individui di accrescere le loro conoscenze nonché di cambiare le loro opinioni, e questo rafforza il fenomeno delle *echo chamber.*. [334] Infine non devono essere dimenticati i problemi connessi alle TRF, i quali persistono e si moltiplicano quando si entra nell'ambito della profilazione, infatti accanto ai profili che si sono già evidenziati è necessario sottolineare che il diritto alla riservatezza e all'anonimato in spazi pubblici diventano diritti sempre più apparenti e meno effettivi. Nonostante le garanzie predisposte dal GDPR, i rischi di una illecita compressione dei diritti e delle libertà fondamentali sono dietro l'angolo e questo permette di comprendere a pieno l'esigenza di un'apposita normativa che regoli precipuamente ed esclusivamente l'intelligenza artificiale.[335] La breve analisi del tema della profilazione conduce ad affermare che si tratta di uno strumento al servizio della sorveglianza di massa, effettivamente nel momento in cui viene attuata mediante le TRF è possibile non solo identificare la persona e tracciarne i movimenti, ma anche creare un suo profilo personale approfondito che si configura come la ricostruzione delle abitudini e delle preferenze di ciascuno[336]

4. Oltre la sicurezza pubblica: i diversi impieghi del riconoscimento facciale

La presente tesi è stata dedicata ad analizzare come le tecnologie di riconoscimento facciale sono impiegate ai fini di sicurezza pubblica, ma si può ben immagine che siano plurimi i settori d'impiego dei sistemi di IA in questione. In questo paragrafo si

[334] Per un maggiore approfondimento sui *filter bubbles* e sulle *echo chamber* cfr.: A. Bruns, *'It's not the Technology stupid: How the echo chamber and filter bubbles metaphors have failed us',* 7 July 2019, https://eprints.qut.edu.au/131675/1/It%E2%80%99s%20Not%20the%20Technology%2C%20Stupid%20%28paper%2019771%29.pdf.

[335] Cfr. G. Mobilio, *op. cit.* 207-208.

[336] Cit. G. Mobilio, *'Profilare tramite riconoscimento facciale: il caso della sicurezza urbana', 'in' Protezione dei dati personali e nuove tecnologie. Ricerche interdisciplinari sulle tecniche di profilazione e sulle loro conseguenze giuridiche',* (a cura di) A. Adinolfi e A. Simoncini, Napoli, Edizioni Scientifiche Italiane, 2021, p. 186. A livello mondiale l'esempio di più interessante e citato è quello del modello Cinese. Infatti in Cina è stato creato un sistema di credito sociale, quale vera a propria infrastruttura di sorveglianza di massa, anche mediante l'impiego di TRF, viene attribuito a ciascun soggetto un numero identificativo e un punteggio che determina la sua affidabilità e la sua reputazione pubblica come cittadino.

vuole aprire una prospettiva specifica, seppur riduttiva, sugli ulteriori e diversi utilizzi delle TRF per far si che il lettore possa avere una visione quanto più completa.

Innanzitutto si può ricordare che si tratta di un uso sempre più diffuso nel settore della difesa, in particolare ai fini dall'implementazione di droni, usati a loro volta per gli scopi più disparati, in particolare per effettuare un controllo pervasivo e per monitorare specifiche aree geografiche. Essendo i droni dispositivi che possono essere guidati a distanza, offrono la possibilità di identificare soggetti catturati dalle telecamere di riconoscimento facciale, e di fare ciò anche nei luoghi più difficili da raggiungere nonché particolarmente pericolosi, oltre che da una distanza rilevante[337].

Ancora, si può constatare come si tratti di una funzione di IA che si presta facilmente ad essere utilizzata anche in ambito privato e, in particolare, nel settore commerciale. In questo caso il riconoscimento facciale viene usato come un vero e proprio strumento di *markentig.* Le TRF permettono di automatizzare i processi aziendali e produttivi, di fornire servizi intelligenti ai clienti, ma possono anche svolgere un ruolo di mediazione tra venditore e acquirente[338]. Proprio in ambito commerciale si esplica la maggiore potenzialità della tecnica della profilazione, poiché attraverso la commistione di dati, reperiti dalle più diverse fonti (*web, social-media*, applicazioni telefoniche…), e dei sistemi intelligenti di cui sono dotate le tecnologie di riconoscimento facciale, è possibile effettuare delle indagini probabilistiche per prevedere i gusti e gli interessi dei clienti, anche al fine di inviare campagne pubblicitarie[339].

Passando ad un diverso impiego, l'*Internet of things* ha permesso di integrare questa funzione nei nostri dispositivi elettronici, i nostri smartphone sono quasi sempre

[337] Per maggiori informazioni sul punto si può confrontare: Hwai-Jung Hsu e Kuan-Ta Chen, '*Face Recognition on Drones: Issues and Limitations'*, *'in'* «Institute of Information Science- Academia Sinica», James Grebey, '*Video from military drone shows it can identify armed people*,' '*in'* «Inverse», 2016, https://www.inverse.com/article/22753-darpa-military-drone-ai-identify-armed-people.

[338] Cfr. . Paul Hackett e Selene Verri, '*Intelligenza artificiale: un'opportunità per le imprese europee', 'in'* «Euronews», http://it.euronews.com/2018/05/04/intelligenza-artificiale-un-opportunita-per-le-imprese-europee.

[339] Cfr. F. Lagioia, G. Sartor, *'Profilazione e decisione algoritmica: dal mercato alla sfera pubblica', 'in'* Federalismi, n. 11, 24 Aprile 2020.

'sbloccabili' tramite *face-id,* del pari avviene nei *tablet* e nei *computer* per l'accesso a specifiche applicazione in questi installate o per poter utilizzare, semplicemente, il dispositivo in questione.

Anche l'ambito sanitario non è esente da ripercussioni causate dall'arrivo irruente di queste tecnologie infatti si può, per il suo tramite, limitare l'accesso ad aree mediche sensibili o monitorare la presenza del personale medico sanitario. Per avere un esempio concreto di come il riconoscimento facciale è stato usato in ambito sanitario basta guardare con occhio critico gli anni della pandemia da Covid-19, basta cioè tornare al 2020 e pensare alle misure governative che furono adottate per combattere e limitare il numero dei contagi, veniva infatti impiegato per individuare le persone con sintomi, per rilevare la temperatura corporea, per trasportare merci evitando il contatto umano e in molti altri casi… [340]

Infine possiamo ricordare come sia stato impiegato per limitare l'accesso nelle scuole, e quindi per monitorare gli ingressi e le uscite, in quest'ultimo campo importante è l'esempio francese dove si voluto sperimentare in concreto i benefici, e con essi anche i difetti, di una simile installazione negli ambienti scolastici.[341]

Si sono voluti evidenziare i differenti settori d'impiego delle TRF per mettere in luce due caratteristiche peculiari che le contraddistinguono ossia la duttilità e l'ubiquità. L'evoluzione tecnico-informatica ha permesso di sviluppare sistemi sofisticatissimi, incomprensibili e dalle mille potenzialità, ora si rimette all'uomo la decisione circa quanto spazio lasciar 'loro' nella nostra vita quotidiana, certo è che deve essere ricercato il giusto compromesso tra ciò che è giusto che facciano e ciò che non lo è: l'attenzione, cioè, non è più posta su ciò che l'IA può e non può fare, le funzioni che

[340] Cfr. J. Scipione, *'L'intelligenza artificiale, protagonista silenzioso ed efficiente nella al Coronavirus', 'in'* CSI Review, n. 1, Giugno 2020, https://deliverypdf.ssrn.com/delivery.php?ID=243069124094101104023082100114119007000076081034060007022064071097005110122017080119005102039099016121119028116082111068079098020045006069064003111094000093066123076040065013111095117019010123085019118114116001007090099071005074118084092002005124022085&EXT=pdf&INDEX=TRUE.

[341] E. Falletti, *'Francia: bocciata la sperimentazione del riconoscimento biometrico negli edifici scolastici', 'in'* Il quotidiano giuridico, 25 Marzo 2020.

le possono essere demandate sono innumerevoli, ma questo non vuol dire che se un automa può essere istruito a farlo, per forza debba essergli consentito dall'uomo.

Conclusioni

L'analisi prospettata nella presenta tesi evidenzia l'importanza che i sistemi intelligenti stanno sempre più acquisendo nella nostra vita quotidiana. Il riconoscimento facciale è, allo stesso tempo, una delle diverse applicazioni riscontrabili in questi sistemi, e una delle più problematiche funzioni rimesse all'intelligenza artificiale. Emerge con chiarezza che si tratta di uno strumento molto potente di cui l'uomo gode, e del quale deve fare un giusto e proporzionato uso.

Il riconoscimento facciale è l'esempio perfetto per affermare la necessità di un intervento legislativo che regoli l'intelligenza artificiale in ogni funzione ad essa attribuita. Il percorso che le Istituzioni Europee hanno seguito fino a giungere alla Proposta di Regolamento sull'intelligenza artificiale mette in luce l'esigenza di dar vita e di sviluppare forme di IA affidabili e antropocentriche, dato che solo in tal modo può generarsi fiducia nell'uomo. Per queste ragioni, per creare un'IA affidabile si è scelto di adottare una disciplina che si basa sul metodo del rischio. Attraverso questo, le autorità del mondo giuridico hanno la possibilità di vietare a monte determinate funzioni. Si tratta, cioè, di quelle funzione che comportano un rischio inaccettabile per l'uomo, un rischio tale da legittimare un divieto generalizzato. In questo contesto l'Unione Europea adotta un approccio volto ad individuare soluzioni alle possibili e future conseguenze, vuole, cioè, predisporre rimedi applicabili a monte, al fine di ridurre la necessità di tutele a valle. È questo un bisogno più che una scelta, un'esigenza strettamente legata alle caratteristiche proprie di queste tecnologie sofisticate, sono infatti incomprensibili, opache e complesse, oltreché fortemente esposte al rischio di produrre risultati errati, distorti e discriminatori. Così, se la logica sottesa è incomprensibile, se cioè non è possibile comprendere come da un *input* l'automa sia giunto ad uno specifico *output,* allora diviene fondamentale arginare il problema aprioristicamente, per ridurre le conseguenze negative che possono prodursi per il tramite del loro 'agire'.

È logico che i sistemi di riconoscimento facciale si prestano ampiamente al perseguimento del fine di pubblica sicurezza. Al contempo, però, il binomio sicurezza-sorveglianza pare diverso agli occhi di chi guarda, dipende dalle esigenze di ciascuno di noi, ma non solo, dipende anche dal tempo in cui siano nati e cresciuti, il quale influisce

su quanto e cosa siamo disposti a condividere. Il diritto alla *privacy* è il diritto più toccato dal riconoscimento facciale, se accettiamo, per garantire una maggiore sicurezza pubblica, la presenza di telecamere di videosorveglianza, accettiamo di essere seguiti da un occhio elettronico, accettiamo di perdere la nostra pretesa di restare anonimi in spazi pubblici (e non solo), quindi rinunciamo alla nostra *riservatezza.* Ragion per cui, se accogliamo questa funzione si aprono le porte ad una vera e propria sorveglianza di massa, che può facilmente degenerare in sorveglianza individuale, e la profilazione ne è la riprova. Per questo servono dei limiti, dei confini specifici e puntuali entro i quali ricongiungere l'uso di queste potenti e innovative tecnologie, per questo serve l'approvazione dell'*AI Act*.

L'impegno del legislatore, se pur essenziale, non è bastevole. A chi scrive pare naturale sottolineare la necessità che il mondo giuridico e il mondo tecnico-informatico si evolvano di pari passo, attraverso un impegno reciproco e costante. E' necessaria un'azione congiunta tra gli esperti di intelligenza artificiale e gli esperti di diritto. Unicamente in questo modo è possibile controllare le ripercussioni positive e negative, soltanto in tal modo è possibile una commistione tra mondo analogico e digitale che argini rischi per la persona e tuteli i diritti fondamentali di cui godiamo.

Bibliografia & Sitografia

ACCOTTO C., *Il mondo-dato. Cinque brevi lezioni di filosofia della programmazione,* Milano, EGEA, 2017.

AlLBRECHTSLUND A., *Online social networking as participatory surveillance, 'in'* First Monday, Vol. 13, N. 3, March 2008.

ASHBY W. R., *L'introduzione alla cibernetica,* Londra, Chapman & Hall, 1956.

ATERNO S., *Il principio di Accountability nel GDPR, significato e applicazione, in* Agenda Digitale, 31 Luglio 2018, https://www.agendadigitale.eu/sicurezza/principio-di-accountability-nel-gdpr-significato-e-applicazione/.

BACCI M., *metodi e tecnologie per il riconoscimento facciale,* tesi di laurea, Alma Mater studiorum, Università degli studi di Bologna, 2016

BARBERA M., *'Discriminazioni algoritmiche e forme di discriminazione', 'in'* Labour and Law Issues, Vol. 7, n. 1, 2021, https://labourlaw.unibo.it/article/view/13127/12679.

BAROCAS S., FELTEN W., HUEY J., KROLL J. A., REIDENBERG J. R., ROBINSON D. G., Yu H., *Accountable Algorithms, 'in'* University of Pennsylvania Law Review, Vol. 165:633.

BARONE C., *'Privacy, Sicurezza e Libertà nell'era della sorveglianza di massa e dell'emergenza terrorismo',* Tesi di Dottorato di Ricerca in Pluralismi giuridici, Università degli studi di Palermo, 2019.

BERTI M., ZUMERLE F., *Digital Markets Act: l'UE chiarisce le regole per individuare i Gatekeepers, in* Agenda Digitale, 11 Maggio 2023, https://www.agendadigitale.eu/mercati-digitali/digital-markets-act-lue-chiarisce-le-regole-per-individuare-i-gatekeeper/

BLEDSOE W. W, Browing I., *Pattern recognition and reading by Machine,* Proceedings of the Eastern Joint Computer Conference, 1959.

BLEDSOE W. W., *Some result on Multicategory Pattern recognition, 'in'* Journal of the Association for Computing machinery, Vol 13, N. 2, 1966.

BODEN M. A., Traduzione a cura di F. Calzavarini, '*L'intelligenza artificiale',* Bologna, il Mulino, 2019

BOLDRINI N., *Reti neurali: cosa sono e a cosa servono, 'in'* AI4Business, 2 Luglio 2023, https://www.ai4business.it/intelligenza-artificiale/deep-learning/reti-neurali/.

BOLIN G., SCHWARZ J. A., '*Heuristics of the algorithm: Big Data, user interpretation and institutional translation', 'in'* Sage Journal, October 2015, DOI: 10.1177/2053951715608406.

BONAZZI M., *'La videosorveglianza ai fini della tutela dell'ordine e della sicurezza pubblica, con particolare riferimento alle novità introdotte dalla legge 18 Aprile 2017, n. 48 (Disposizioni urgenti in materia di sicurezza delle città), 'in'* Rivista di Polizia, 2018.
BONETTI P., *'La giurisprudenza costituzionale sulla materia 'sicurezza' conferma la penetrazione statale nelle materie di potestà legislativa regionale', 'in'* Forum di Quaderni Costituzionali, 2010, p. 1 ss, https://www.forumcostituzionale.it/wordpress/images/stories/pdf/old_pdf/1138.pdf.

BONTEMPI V., *'Un'interrogazione parlamentare sull'uso del riconoscimento facciale in Italia: il caso S.A.R.I.', 'in'* IRPA (Istituto di ricerche sulla pubblica amministrazione), 07/05/2020, https://www.irpa.eu/uninterrogazione-parlamentare-sulluso-del-riconoscimento-facciale-in-italia-il-caso-s-a-r-i/.

BORGESIUS F. Z., *'Discrimination, Artificial intelligence and Algorithmic decision-making',* Published by Director General of Democracy, 2018, https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73.

BORGIA G., *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuri sviluppi normativi sul fronte eurounitario, 'in'* La Legislazione penale, ISSN: 2421-552X, 11 Dicembre 2021.

BORGOBELLO M., '*Riconoscimento facciale vietato in Italia: ma solo per ora e con eccezioni', 'in'* Agenda Digitale, 2 Dicembre 2021, https://www.agendadigitale.eu/sicurezza/privacy/riconoscimento-facciale-vietato-in-italia-ma-per-ora-e-con-eccezioni/.

BOULAMWINI J., LEARNED-MILLER E., M. J., Ordóñez V., *Facial Recognition technologies: A primer,* May 29, 2020

BRUNS A., *'It's not the Technology stupid: How the echo chamber and filter bubbles metaphors have failed us',* 7 July 2019, https://eprints.qut.edu.au/131675/1/It%E2%80%99s%20Not%20the%20Technology%2C%20Stupid%20%28paper%2019771%29.pdf

BURRELL J., *'How the machine thinks: Understanding opacity in machine learning algorithms', 'in'* Sage Journal, 2016, DOI: 10.1177/2053951715622512.

BYGRAVE L. A., '*Automated Profiling: Minding the Machine: Article 15of the EC Data Protection Directive and Automated Profiling*', in Computer Law & Security Review, 17, 2001.

Camera dei Deputati, Documentazione Parlamentare, *Protezione dei dati personali,* 30 Settembre 2022, https://temi.camera.it/leg18/temi/la_protezione_dei_dati_personali.html#:~:text=pacchetto%20protezione%20dati%20identifica%20gli,esigenze%20di%20tutela%20dei%20dati.

CAMPO L., CICCARESE A., MARTELLA A., *'Gli algoritmi come costruzione social. Neutralità, potere e opacità', 'in'* LQ The Lab's Quarterly, 2018, a. XX, n.4 (Ottobre-Dicembre).

CANNITO L., *'Cosa sono i bias cognitivi?', 'in'* Economia comportamentale, 2017, https://www.economiacomportamentale.it/wp-content/uploads/2021/10/Cosa-sono-i-bias-cognitivi_.pdf.

CARLEO A., *Che cosa è l'alleanza europea sull'intelligenza artificiale?, in* Cyberlaw, 15 Ottobre 2018, https://www.cyberlaws.it/2018/che-cose-lalleanza-europea-sullintelligenza-artificiale/

Che cos'è la Computer Vision, 'in' IBM, https://www.ibm.com/it-it/topics/computer-vision.

CHEN K. T., HSU H. J., '*Face Recognition on Drones: Issues and Limitations'*, *'in'* «Institute of Information Science- Academia Sinica», James Grebey, '*Video from military drone shows it can identify armed people*,' 'i*n'* «Inverse», 2016, https://www.inverse.com/article/22753-darpa-military-drone-ai-identify-armed-people.

'Chi ha inventato il computer?', 'in' Focus, https://www.focus.it/cultura/storia/chi-ha-inventato-il-computer#:~:text=Il%20primo%20calcolatore%20interamente%20elettronico,stanzone%20di%20140%20metri%20quadrati.

CLARKE R. '*Information Technology and Dataveillance',* November 1987, http://www.rogerclarke.com/DV/CACM88.html#PDV.

COCQ C., GALLI F., *'The Catalasing effect of serious crime on the use of surveillance technologies for prevention and investigation purposes', 'in'* New Journal of European Criminal Law, Vol. 4, 2013.

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, 9/2022.

Commissione Europea, *Plasmare il futuro digitale dell'Europa. Un approccio europeo all'intelligenza artificiale,* https://digital-strategy.ec.europa.eu/it/policies/european-approach-artificial-intelligence.

Commissione Europea, *Ministerial Declaration on eGovernment - the Tallinn Declaration,* 6 Ottobre 2017, https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration.

Commissione Europea, *Research and innovation,* https://commission.europa.eu/research-and-innovation_en.

Commissione Europea, *Research and innovation. Horizon 2020*. https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en.

Commissione Europea, *a European AI on demand Platform and Ecosystem,* https://cordis.europa.eu/project/id/825619/it.

Commissione Europea, *A European Strategy for Data,* https://digital-strategy.ec.europa.eu/en/policies/strategy-data.

Consilio dell'Unione Europea, *Gruppo diritti fondamentali, diritti dei cittadini e libera circolazione delle persone (FREMP),* https://www.consilium.europa.eu/it/council-eu/preparatory-bodies/working-party-fundamental-rights-citizens-rights-free-movement-persons/.

CONTISSA G., GODANO F., SARTOR G., , *'Il Regolamento europeo sull'intelligenza artificiale', 'in'* i-lex, Dicembre 2021, Fascicolo 2, Rivista semestrale on-line: www.i-lex.it.

COSIMI S., *Facebook, l'Irlanda blocca il trasferimento dei dati verso gli USA: i rischi per il social senza un nuovo Privacy Shield, 'in'* La Repubblica, 10 settembre 2020, https://www.repubblica.it/tecnologia/social-network/2020/09/10/news/facebook_l_irlanda_blocca_il_trasferimento_dei_dati_verso_gli_usa_i_rischi_per_il_social_senza_un_nuovo_privacy_shield-266805870/.

CRAWFORD K., PAGLIEN T., '*Excavating AI: The Politics of Training Set for Machine Learning',* 19 Settembre 2019, https://excavating.ai/.

CURRAO E., *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?, 'in'* Diritto Penala e Uomo, https://dirittopenaleuomo.org/wp-content/uploads/2021/05/Currao_DPU.pdf.

DELLA TORRE J., *Tecnologie di riconoscimento facciale e procedimento penale, 'in'* Rivista italiana di Diritto e Procedura penale, N.3

DI GIULIO M., *'Profilazione: tutte le sfide dell'intelligenza artificiale affrontate dal GDPR, 'in'* Agenda Digitale, https://www.agendadigitale.eu/sicurezza/privacy/profilazione-tutte-le-sfide-dellintelligenza-artificiale-affrontate-dal-gdpr/.

DOMINGOS P., *A few useful things to know about Machine Learning', 'in'* Communications of the ACM, October 2012, Vol. 55, no.10, DOI: 10.1145/2347736.2347755.

DOURISH P., , '*Algorithms and their other: Algorithmic culture in context', 'in'* Sage Journals, August 2016, https://journals.sagepub.com/doi/10.1177/2053951716665128#bibr42-2053951716665128.

European Commission, *'European Centre of Algorithmic Transparency'*, https://algorithmic-transparency.ec.europa.eu/index_en. Si tratta di un'iniziativa nata in seno al Regolamento UE 2022/2065 del 19 Ottobre.

FACCHINI A., TERMINE A., *'Explainable AI: come andare oltre la black box degli algoritmi', in* Agenda Digitale, 20 Gennaio 2022, https://www.agendadigitale.eu/cultura-digitale/explainable-ai-come-andare-oltre-la-black-box-degli-algoritmi/.

FALLETTI E., *'Francia: bocciata la sperimentazione del riconoscimento biometrico negli edifici scolastici', 'in'* Il quotidiano giuridico, 25 Marzo 2020.

FIORONI D., *'Brescia: ladri d'appartamento scoperti grazie al riconoscimento facciale',* Comunicato stampa della Polizia di Stato, 07/09/2018, https://www.poliziadistato.it/articolo/pdf/135b92536bb3957899899171.

FLOREANO D., MATTIUSSI C., *Il manuale delle reti neurali,* Bologna, il Mulino, 2002

FLORIDI L., *'In poche batture. Brevi riflessioni su cultura e digitale 2011-2021'*, Gennaio 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3998228.

FLORIDI L., *The Ethics of Artificial intelligence. Principles, Challenges and Opportunities (Etica dell'intelligenza artificiale. Sviluppi, opportunità e sfide),* a cura di M. Durante, Milano, Raffaello Cortina Editore, 2022.

FLORIDI L., *'La quarta rivoluzione. Come l'infosfera sta trasformando il mondo',* Milano, Raffaello Cortina Editore, 2014.
FRIEDMAN B., NISSENBAUM H., *'Bias in Computer System', 'in'* ACT Transactions on Informations Systems, Vol. 14, No. 3, July 1996.

FUSIELLO A., *Visione Computazionale. Tecniche di ricostruzione tridimensionale,* Milano, FrancoAngeli, 2018

GALETTA D. U., CORVALAN J. G *'Intelligenza artificiale per un pubblica amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto', 'in'* Federalismi, 6 Febbraio 2019.

Garante per la Protezione dei dati personali, *Cambridge Analytica: il Garante privacy multa Facebook per 1 milione di euro,* 28 Giugno 2019, file:///Users/valentina/Downloads/GarantePrivacy-9121352-2.0.pdf.

GARZONIO E., *L'algoritmo: obiettivi ed implicazioni dello spazio digitale europeo, 'in'* Rivista italiana di informatica e diritto, fascicolo 2, 2021 DOI: 10.32091/RIID0037.

GHIGLIA A., (Componente del Garante della Privacy) Intervento in occasione dell'executive webinar: *'Intelligenza artificiale e riconoscimento facciale in Real Time, i vantaggi e i rischi del Regolamento europeo',* Webinar organizzato da Privacy Italia, ASSO Dpo e Key4biz, https://www.youtube.com/watch?v=zOZdz2WvVJU&t=144s.

Greens/EFA, *Biometric and Behavioural Mass Surveillance in EU Member States,* October 1, 2021, https://www.greens-efa.eu/biometricsurveillance/.

Garante per la protezione dei dati personali, *Approccio basato sul rischio e misure di Accountability (responsabilizzazione) di titolari e responsabili,* https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili.

Garante per la protezione dei dati personali, *Deepfake: dal garante una scheda informativa sui rischi dell'uso malevolo di questa nuova tecnologia,* https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9512278.

HACKETT P., VERRI S., *Intelligenza artificiale: un'opportunità per le imprese europee', 'in'* «Euronews», http://it.euronews.com/2018/05/04/intelligenza-artificiale-un-opportunita-per-le-imprese-europee.

IASELLI M., *Protezione dei dati personali: le novità del nuovo Regolamento europeo, 'in'* Altalex, 9 Maggio 2016, https://www.altalex.com/documents/news/2015/12/23/accordo-raggiunto-sul-regolamento-europeo-in-materia-di-protezione-dei-dati-personali.

INVERNIZZI I., *'I sistemi di riconoscimento facciale stanno arrivando nelle città italiane', 'in'* Il Post, 16 Settembre 2021, https://www.ilpost.it/2021/09/16/riconoscimento-facciale-comuni-telecamere/.

KANADE T., *Picture Processing System by Computer Complex and recognition of Human face,* Tesi di Dottorato, Università di Kyoto, Department of Information and Science, November 1973

KIRBY M., SIROVICH L., *Low-dimensional procedure for the characterization of human face, 'in'* Journal of the Optical Society of America A, Vol. 4, March 1987.

KURZWEIL R., *'The singularity is near. When humans transcend biology',* New York, Viking, 2005.

KURZWEIL R., *'Get ready for hybrid thinking',* TED talk, 2014.

LAGIOIA F., SARTOR G., , '*profilazione e decisione algoritmica: dal mercato alla sfera pubblica', 'in'* Federalismi, 11/2020,

https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=42114&dpath=document&dfile=23042020224508.pdf&content=Profilazione%2Be%2Bdecisione%2Balgoritmica%3A%2Bdal%2Bmercato%2Balla%2Bsfera%2Bpubblica%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B

LEPORE A., '*Confermato fino al 2025 il divieto di installare sistemi di riconoscimento facciale in Italia', 'in'* Smartworld, 23 Giugno 2023, https://www.smartworld.it/news/divieto-installazione-sistemi-riconoscimento-facciale-2025.html.

LONGO A., *'Italia primo Paese a vietare il riconoscimento facciale (con eccezioni), 'in'* Il sole 24 ore, 2 Dicembre 2021, https://www.ilsole24ore.com/art/italia-primo-paese-vietare-riconoscimento-facciale-con-eccezioni-AEFLRY0.

LYON D., *'La Società Sorvegliata. Tecnologie di controllo della vita quotidiana',* Milano, Feltrinelli Editore, 2001.

MARR B., *7 Amazing Examples of Computer and Machine Vision in practice, 'in'* Forbes, 8 Aprile 2019, https://www.forbes.com/sites/bernardmarr/2019/04/08/7-amazing-examples-of-computer-and-machine-vision-in-practice/#3dbb3f751018.

MCCARTHY J, Minsky M. L., Shannon C. E, *A Proposal for the Dartmounth Summer Research Project on Artificial Intelligence,* August 31, 1955.

MCCARTHY J., *What is Artificial Intelligence?,* Formal Reasoning Group Stanford University, November 2007.

MCCULLOCH W. S., PITTS W., *A logical calculus of the ideas immanent in nervous activity,* Bulletin of mathematical biophysics, Vol. 5, 1943.

Meta: multa record di 1,2 miliardi dell'autorità per la privacy Irlandese, 'in' RaiNews 24, 22 Maggio 2023, https://www.rainews.it/articoli/2023/05/meta-multa-record-di-12-miliardi-di-euro-dallautorita-per-la-privacy-irlandese-1eb1fe09-3a09-4b4b-93a4-d1e133c677b9.html#:~:text=L'Autorit%C3%A0%20garante%20della%20privacy,Garante%20europeo%20per%20la%20privacy.

MERLER M., RATHA N., FERIS R. S., SMITH J. R. *'Diversity in faces', 'in'* arXiv, 2019, https://arxiv.org/abs/1901.10436.

Ministero dell'Interno (Dipartimento della pubblica sicurezza), *'Capitolato tecnico. Procedura volta alla fornitura della soluzione integrata per il sistema automatico di riconoscimento immagini S.A.R.I.',* https://www.poliziadistato.it/statics/06/20160627-ct-sari--4-.pdf.

MINSKY M., PAPERT S., *Perceptron*: *An Introduction to computational geometry,* 1969

MOBILIO G., '*Profilare tramite riconoscimento facciale: il caso della sicurezza urbana', 'in' 'Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle*

tecniche di profilazione e sulle loro conseguenze giuridiche', a cura di A. Adinolfi e A. Simoncini, Napoli, Edizioni Scientifiche Italiane, 2022.

MOBILIO G., *Tecnologie di Riconoscimento Facciale. Rischi per i diritti fondamentali e sfide regolative,* Napoli, Editoriale Scientifica, 2021.

MONTUORI L., *Privacy: Perché la Convenzione 108+ è cruciale per il libero flusso dei dati, 'in'* Agenda Digitale, 28 gennaio 2022, https://www.agendadigitale.eu/sicurezza/privacy-perche-la-convenzione-108-e-cruciale-per-il-libero-flusso-dei-dati/.

MORO P., *Intelligenza artificiale e tecnodiritto, in* Etica, Diritto e Tecnologia. Percorsi dell'informatica giuridica contemporanea, (a cura di) P. Moro, Milano, FrancoAngeli, 2022

MORRONE A., *'Il custode della ragionevolezza',* Giuffrè, Milano, 2001.

NALDI G., *Matematica, immagini e visione computazione. Gioie, dolori e possibili sfide',* Conferenza nell'ambito di '*matematica, che passione'* dell'Università degli Studi di Milano, 15 Febbraio 2012.

NIST- National Institute of Standards and Technology: : https://www.nist.gov/programs-projects/face-recognition-technology-feret.

OROFINO M., *'Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione', 'in'* Media Laws (Rivista di diritto dei media), 2/2018.

PAOLOZZI F., '*FOCUS sulla GIURISPRUDENZA COSTITUZIONALE in materia di SICUREZZA PUBBLICA', 'in'* Servizio Affari legislativi e qualità dei processi normativi (Direzione generali affari istituzionali e legislativi della Giunta della Regione Emilia Romagna, 2011.

Parlamento Europeo- Attualità, *'Normativa sull'IA: la prima regolamentazione sull'intelligenza artificiale',* 13/06/2023, https://www.europarl.europa.eu/news/it/headlines/society/20230601STO93804/normativa-sull-ia-la-prima-regolamentazione-sull-intelligenza-artificiale

Parlamento Europeo 'Attualità', *'Che cos'è l'intelligenza artificiale?',* ultimo aggiornamento 28/06/2023, https://www.europarl.europa.eu/news/it/headlines/society/20200827STO85804/che-cos-e-l-intelligenza-artificiale-e-come-viene-usata#:~:text=L'intelligenza%20artificiale%20%C3%A8%20largamente,i%20rifornimenti%20e%20la%20logistica.

PASQUALE F., '*The Black Box Society*. *The secret Algorithms That Control Money and Information'*, Harvard University Press, Cambridge-London, 2015

PASQUALE F., *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 Nw. U. L. Rev., 2010

PENTLAND A. P., TURK M. A, *Face Recognition Using Eigenfaces, 'in'* Journal of Cognitive Neuroscience, Vol 1, 1991

PINO G., *'Diritto e società. Proporzionalità, diritti, democrazia'* (estratto), Editoriale Scientifica, Napoli, 2014.

PINTORE A., *'Privacy e diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo regolamento europeo',* Torino, Giappichelli, 2016.

PIZZETTI F., *Trasparenza nel trattamento dei dati, cosa cambia col GDPR: l'alba di un nuovo valore sociale, in* Agenda Digitale, 31 Giugno 2018, https://www.agendadigitale.eu/sicurezza/trasparenza-nel-trattamento-dati-che-cambia-col-gdpr-lalba-di-un-nuovo-valore-sociale/.

Polizia di Stato, *'Identità',* 10/05/2013, https://www.poliziadistato.it/articolo/identita-1.

PRINCE A., SCHWARCZ D. B., *'Proxy Discrimination in the Age of Artificial Intelligence and Big Data', 'in'* Iowa Law Review, 5 Agosto 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3347959.

RESTA G., *'Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza', 'in'* Forum disuguaglianze diversità. 15 proposte per la giustizia sociale, https://www.forumdisuguaglianzediversita.org/wp-content/uploads/2019/09/Resta.x89907.pdf

RODOTA' S., '*Privacy, libertà e dignità, discorso conclusivo della Conferenza internazionale sulla protezione dei dati', 'in'* Garante per la protezione dei dati personali, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293

ROSENBLATT F., *The Perceptron: A probabilistic model for information storage and organization in the brain, 'in'* Psychological review, Vol. 65, N. 6, 1958.

SARRA C., *Il mondo-dato. Saggi su datificazione e diritto,* Padova, Cleup, 2019.

SCAGLIARINI S., '*La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica', 'in'* Consulta online, periodico telematico fascicolo 2, 9 Luglio 2021, ISSN 1971-9892.

SCIPIONE J., *'L'intelligenza artificiale, protagonista silenzioso ed efficiente nella al Coronavirus', 'in'* CSI Review, n. 1, Giugno 2020, https://deliverypdf.ssrn.com/delivery.php?ID=243069124094101104023082100114119007000076081034060007022064071097005110122017080119005102039099016121119028116082111068079098020045006069064003111094000093066123076040065013111095117019010123085019118114116001007090099071005074118084092002005124022085&EXT=pdf&INDEX=TRUE

SEPAHA H., *'Le leggi anti-discriminazione nell'Unione Europea. Come funzionano le leggi anti-discriminazione nei paesi membri e come sono regolate dall'UE', 'in'* Europe Direct Emilia-Romagna, Assemblea legislativa, Febbraio 2008, https://www.assemblea.emr.it/europedirect/pace-e-diritti/archivio/i-diritti-umani-e-leuropa/2008/le-leggi-anti-discriminazione-nell2019unione-europea

SHAPIRO L., Stockman G., *Computer Vision,* Prentice Hall, March 2000.

SIMONCINI A., SUWEIS S., *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale, 'in'* Rivista di filosofia del diritto, VII, 1/2019

SOMALVICO M., *Intelligenza Artificiale,* Milano, Rusconi, 1987.

The Brief history of Face Recognition, 'in' FaceFirst, August 1, 2017, https://www.facefirst.com/post/a-brief-history-of-face-recognition.

TOMKINS R., *Panama expands use of facial recognition system at the airport, 'in'* UPI, 18 Settembre 2014, https://www.upi.com/Defense-News/2014/09/18/Panama-expands-use-of-facial-recognition-system-at-airport/6521411050216/.

TRECCANI, *metodo top-down,* https://www.treccani.it/enciclopedia/metodo-top-down_%28Enciclopedia-della-Matematica%29/#:~:text=metodo%20top%2Ddown%20(ingl.,che%20segue%20il%20percorso%20inverso.

TROIANO G., *Privacy, cosa sono le direttive 680 e 681 e quali rischi ci sono, in* Agenda Digitale, 14 Febbraio 2020, https://www.agendadigitale.eu/sicurezza/guglielmo-troiano-direttiva-680-e-681/.

TURING A. M., *On computable number, with an application of the Entscheindungproblem',* November 12, 1936.

TURING A. M., *Computing machinery and intelligence', 'in'* Mind: A Quarterly Review of Psychology and Philosophy, Vol. LIX, Number 236, October, 1950.

Unione Europea, 21 ottobre 2020, *Tirocini 'Digital Opportunity' per l'acquisizione di competenze digitali,* https://youth.europa.eu/go-abroad/traineeships/digital-opportunity-traineeships_it.

VIGE V., *'The Coming Technological Singularity: How to Survive in the Post-Human Era, in Vision-21 Interdisciplinary Science and Engineering in the Era of Cyber-Space',* Proceedings of a symposium cosponsored by the NASA Lewis Research center and the Ohio Aerospace Institute and held in Westlake, Ohio, 1993.

ZANOTTI L., *'Cosa sono i file log e perché con il log menagement si garantisce la sicurezza informatica, 'in'* Network Digital 360, 6 Settembre 2022,

https://www.zerounoweb.it/techtarget/searchsecurity/che-cosa-sono-i-file-log-e-perche-non-c-e-sicurezza-senza-log-management/.

ZUDDAS P., *'Intelligenza artificiale e discriminazioni', 'in'* Consulta Online – Liber Amicorum per Pasquale Costanzo, 16 Marzo 2020.

Garante per la protezione dei dati personali, *The Privacy Shield,* https://www.garanteprivacy.it/documents/10160/0/Privacy+shield.+Lo+Scudo+per+la+privacy+fra+Ue+e+USA+-+Infografica#:~:text=L'accordo%20detto%20Privacy%20Shield,%2C%20ossia%20%C2%ABPorto%20sicuro%C2%BB.

Legge della Camera dei Deputati e del Senato della Repubblica, 3 Dicembre 2021, n. 205, *Conversione in legge, con modificazioni, del decreto-legge 8 ottobre 2021, n. 139, recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali*

Recommendation of the Committee of ministers, 3 November 2021, n. 8, *Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling*

Proposta di Regolamento del Parlamento europeo e del Consiglio 21 Aprile 2021, COM(2021) 206 final, *che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione.*

Garante per la protezione dei dati personali, *'Parere sul sistema S.A.R.I Real Time',* 25 Marzo 2021

Linee Guida della European Data Protection Board, 29 Gennaio 2020, 3/2019, *sul trattamento dei dati personali attraverso dispositivi video,*

Linee Guida dell'European Data Protection Board sull'articolo 25, 20 Ottobre 2020, 4/2019, *Protezione dei dati fin dalla progettazione e per impostazione predefinita*.

Conclusioni del Consiglio dell'Unione europea, 21 Ottobre 2020, 11481/20, *Conclusioni della Presidenza. La Carta dei Diritti fondamentali nel contesto dell'intelligenza artificiale e della trasformazione digitale.*

Conclusioni del Consiglio europeo, 14 Ottobre 2020, (2020/C 342 I/01), *Accesso alla giustizia- Cogliere le opportunità della digitalizzazione.*
Commission implementing decision, 10 Luglio 2023, C(2023) 4745 final, *Pursuant to Regulation (UE) 2016 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework,* https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.

Garante per la protezione dei dati personali, provvedimento del 26 febbraio 2020 n. 54

Libro Bianco della Commissione Europea, 19 Febbraio 2020, COM(2020) 65 final, *sull'intelligenza artificiale - Un approccio europea all'eccellenza e alla fiducia.*

Consultative Committee of the Convention 108, *'Report on Artificial Intelligence'*, 25 July 2019

Comunicazione della Commissione Europea, 8 Aprile 2019, COM(2019) 168 final, *creare fiducia nell'intelligenza artificiale antropocentrica*

Gruppo indipendente di esperti di alto livello sull'intelligenza artificiale, *'Orientamenti etici per un'intelligenza artificiale affidabile',* 8 Aprile 2019

. Parlamento Europeo, *'Risoluzione del Parlamento Europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale', https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52019IP0081&from=EN.*

Conclusioni del Comitato dei rappresentanti permanenti, 11 Febbraio 2019, n. 6177/19, *Conclusioni relative al piano coordinato sull'intelligenza artificiale.*

Gruppo di lavoro articolo 29 per la protezione dei dati personali, '*Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679',* emendamento del 6 febbraio 2018

Gruppo di lavoro articolo 29 per la protezione dei dati personali, *'Linee guida sulla trasparenza ai sensi del regolamento 2016/679',* WP260 rev.01, versione emendata adottata l'11 Aprile 2018

Decreto Legislativo, 10 Agosto 2018, n.101, *Decreto Legislativo che adegua la normativa italiana alle disposizioni del Regolamento Generale sulla Protezione dei Dati (GDPR)*

Comunicazione della Commissione europea, 7 Dicembre 2018, COM(2018) 795 final, *piano coordinato sull'intelligenza artificiale.*

Garante per la protezione dei dati personali, provvedimento 26 Luglio 2018 n. 440, *'Sistema automatico di ricerca dell'identità di un volto.'*

Comunicazione della Commissione Europea al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, 25 Aprile 2018, COM(2018) 237 final, *L'intelligenza artificiale per l'Europa.*

Decreto Legislativo, 8 Giugno 2018, n. 51, *Attuazione Direttiva (UE)2016/680 su trattamenti di pubblica sicurezza.*

Delibera del progetto di videosorveglianza della città di Udine, https://www.comune.udine.it/it/sicurezza-22643/polizia-locale-50372/videosorveglianza-89669.

Direttiva (UE), 25 Novembre 2015, 2015/2366, *concernente i servizi di pagamento nel mercato interno*, recepita dal D.lgs. 15 Dicembre 2017, n.218

Direttiva (UE) del Parlamento europeo e del Consiglio, 27 Aprile 2016, n.680, *relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai 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*

Regolamento (UE) Europeo, 27 Aprile 2016, n.679 *Regolamento generale sulla protezione dei dati personali*

Comunicazione della Commissione Europea, 10 Maggio 2017, COM(2017) 228 final, *Sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti.*

Decreto Legge, 20 Febbraio 2017, n.14, convertito con modificazioni con la Legge 18 Aprile 2017, n.48, istituisce i cosiddetti *'Patti per l'attuazione della sicurezza urbana'*, sottoscritti tra il Prefetto e il Sindaco.

Comunicazione della Commissione europea, 10 Giugno 2016, COM(2016) 381 final, *Una nuova agenda per le competenze per l'Europa. Lavorare insieme per promuovere il capitale umano, l'occupabilità e la competitività.*

Direttiva (UE) del Parlamento europeo e del Consiglio, 27 aprile 2016, 2016/681, *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.*

Linee guida del Garante dei dati personali, 12 Novembre 2014, *Linee-guida in materia di riconoscimento biometrico e firma grafometrica. Allegato A al provvedimento del garante del 23 Novembre 2014.*

Corte Europea dei diritti dell'uomo, sentenza *Khmel v. Russia*, 2013

Parere 16/2011 del Gruppo di Lavoro articolo 29 per la protezione dei dati, 22 Marzo 2012, WP 192, *Parere relativo al riconoscimento facciale nell'ambito dei servizi online e mobili.*

Corte di Giustizia, sentenza C-291/2012, *Schwarz*.

Corte di Giustizia, sentenze C-293/12 e 594/12, *Digital Rights Ireland*

Normativa sulla Privacy del Gruppo meta inc.: https://mbasic.facebook.com/privacy/policy/printable/#2-HowDoWeUse.

Trattato sul funzionamento dell'Unione Europea, 13 Dicembre 2007.

Corte Europea dei diritti dell'uomo, Chamber Judgment in the case of Peck v. The United Kingdom (28.1.2003), https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22003-687182-694690%22]}.

Decreto Legislativo, 29 Luglio 2003, n.196, *Codice in materia di protezione dei dati personali*

Corte Costituzionale, sentenza n. 290 del 2001.

Corte Europea dei diritti dell'uomo, caso *Rotaru v. Romania*, 2000.

Corte Europea dei diritti dell'uomo, caso *Amann v. Svizzera*, 2000

Carta dei diritti fondamentali dell'Unione Europea, 18 Dicembre 2000.

Corte Costituzionale, sentenza del 22 Luglio 1999 n. 341

Direttiva (CE) del Paramento Europeo e del Consiglio, 24 Ottobre 1995, n.46 *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*

Convenzione del Consiglio d'Europa, 28 Gennaio 1981, n.108, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*

Corte Costituzionale, sentenza del 26 Luglio 1988 n. 27

Corte Europea dei diritti dell'uomo, sentenza *Herbecq v. Belgio*, 1988

Convenzione Europea dei diritti dell'uomo, 4 Novembre 1950, *Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali*

Costituzione della Repubblica Italiana, 27 Dicembre 1947.