UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA

***European Digital Law of the Person, of the Contract and of the Technological Marketplace* - EUDILA**
Cattedra Jean Monnet del Progetto ERASMUS +

LA SANZIONE DEL GARANTE DELLA PRIVACY CONTRO CLEARVIEW AI

Un caso emblematico sulla violazione dei dati biometrici

Giorgia Meconi

0342647

Anno accademico 2023/2024

INDICE

ABSTRACT

Lo sviluppo informatico ha condotto alla creazione ed implementazione di algoritmi di intelligenza artificiale sempre più sofisticati e tra le molte funzioni che possono fornire vi entra anche l'identificazione biometrica. Contemporaneamente a questo scenario, si è sviluppata la potenza e la pervasività di sfruttare queste tecnologie da parte di autorità competenti e no, sfociando nella sorveglianza di massa. Assistiamo ad una crescita prepotente dell'utilizzo di questi dati, per mezzo della raccolta, del trattamento e della loro conservazione. A tale rischio, inoltre, si aggiungono i problemi legati al funzionamento e alla logica connessa a questi algoritmi, i quali fanno emergere la lampante necessità che il violento sviluppo tecnologico sia seguito da una rapida evoluzione giuridica. Infatti, si può facilmente intuire che regolare questi movimenti di dati, costituisce a livello legale un'ardua impresa. È richiesto al legislatore continui aggiornamenti per rimanere al passo con le innovazioni tecnologiche e allo stesso tempo una legislazione organica e quanto più completa possibile, favorendo un trattamento coerente di tutte le informazioni che riguardano i cittadini. L'unione Europea ha risposto attraverso l'ormai famoso Regolamento UE 2016/679 del 27 aprile del 2016, relativo alla protezione delle persone fisiche con un riguardo al trattamento dei dati personali, più noto come GDPR (General Data Protection Regulation), ma anche attraverso il recentissimo regolamento sull'Intelligenza Artificiale, ovvero l'AI Act, approvato il 21 maggio 2024.

L'intento di questa tesi è quello di esaminare il caso di Clearview AI, società statunitense, posta sotto accusa dal Garante della Privacy italiano a causa dei suoi algoritmi di raccolta e conservazione dei dati biometrici delle persone. In particolare, il percorso esaminato pone come punto di partenza il congruo rapporto tra il dato biometrico e le diverse normative in materia di privacy, per poi spostare la lente di ingrandimento su alcuni articoli del GDPR e AI Act di notevole importanza per esaminare il caso della startup americana. Quindi, come ultimo passo, ci si propone di focalizzarsi sul territorio internazionale per capire come gli altri Stati abbiano agito circa le azioni di Clearview AI.

1. INTRODUZIONE AL DATO BIOMETRICO

Per determinare il concetto di dato biometrico, è utile analizzare l'etimologia di tali termini: dato, dal latino *datum*, ossia la manifestazione formalizzata e concreta di informazioni attraverso processi di codifica; biometrico, suddivisibile in due parole greche, ovvero *bios* (vita) e *metron* (misura) [1]. Il dato biometrico è una caratteristica fisica e/o comportamentale di un soggetto, atta a identificare ed autenticare una persona in maniera univoca. Fa riferimento al riconoscimento automatico di un individuo, le cui caratteristiche possono essere divise in due classi principali:

- Fisiologica, quali impronte digitali, geometria della mano, l'iride e la retina;
- Comportamentale, come la firma, la camminata e i modelli vocali.

Tali fattori sono distintivi per ciascuna persona e non possono essere facilmente replicati, né tantomeno falsificati. Viene, così, sottolineato che ogni soggetto ha caratteristiche uniche, collezionabili, permanenti ed universali. Non a caso, i sistemi biometrici vengono utilizzati come parte di una configurazione AMF, ossia l'autenticazione multifattoriale, meccanismo di sicurezza che utilizza diversi fattori di autenticazione per la verifica dell'identità di un utente. Essi funzionano andando a confrontare le informazioni biometriche di una persona con dei modelli (approccio "one to one" [2]) o database (approccio "one to many" [3]) per determinare se la persona corrisponde a quella che dichiara di essere. Degli esempi sono il Face ID e il Touch ID, sviluppati dalla Apple.

Nell'iperuranio tecnologico odierno, l'utilizzo dei dati biometrici sta diventando sempre più calzante. Tuttavia, l'idea per l'identificazione e l'autenticazione di un soggetto risale a molti anni fa. Nel XIX secolo, il riconoscimento biometrico iniziò ad assumere una forma più scientifica. Infatti, nel 1982 Sir Francis Galton, pubblicò "Finger Prints", un'opera letteraria in cui venivano affrontate le basi per la classificazione e l'uso delle impronte digitali forense. Nel 1901, Sir Edward Henry, sviluppò un sistema per classificare le impronte digitali, che fu adottano da Scotland Yard e

[1] Fonte Wikipedia.
[2] Approccio basato sulla verifica dell'identità dell'interessato attraverso una comparazione tra un determinato modello biometrico associato all'identità dichiarata dall'utente nella fase decisiva ed il modello biometrico generato durante il momento della richiesta di identificazione.
[3] È un sistema di identificazione che presuppone l'esistenza di un database contenente numerosi dati biometrici appartenenti ad un cospicuo numero di soggetti, per il quale avviene un match, ossia controllando l'affinità del dato biometrico prelevato durante la fase di identificazione, con tutti quelli contenuti nella banca dati.

divenne uno standard in molti paesi. Il punto di svolta ci fu nel 1960, con il progresso tecnologico, quando alcuni ricercatori iniziarono ad esplorare dei metodi con l'ausilio del computer. Nel 2001, a seguito degli attacchi terroristici dell'11 settembre, l'adozione di tecnologie biometriche aumentò significativamente, fino ad arrivare ad oggi. Infatti, l'uso dell'intelligenza artificiale e del machine learning, ha migliorato notevolmente l'affidabilità circa questi dati.

Lo scopo della creazione dei sistemi biometrici e dunque di tali dati, può essere ricercata nell'esigenza di migliorare la sicurezza nell'identificazione di una persona. Tale sfida sta diventando sempre più ambiziosa, poiché la disarmante sensazione di vulnerabilità generata da eventi catastrofici, come ad esempio deepfake [4], spinge verso l'adozione di misure di sicurezza. In questa ottica, ciò che assume rilevanza è senz'altro il concetto di tutela della privacy. Sicuramente l'adozione di un riconoscimento biometrico offre molte più garanzie rispetto ai sistemi tradizionali, ma necessita di un uso responsabile e rispettoso, al fine di evitare abusi e violazioni. Nonostante, risulti essere pacifico il bisogno di identificare ciascun cittadino all'interno di una società evoluta, altrettanto pacifico è la partecipazione dalla biometria. Tuttavia, di fronte all'utilizzo di tecnologie avanzate, il rischio di tramutare le azioni di riconoscimento è elevato. Dinanzi a questa prospettiva, la persona si sente minacciata, poiché l'unione degli elementi di rilevazione dei dispositivi, può consentire, oltre a decifrare il nome e cognome, anche carte di credito, passaporto, password, … Infatti, tali dati vengono decifrati sotto forma di stringhe matematiche e conservati nei server o banca dati in maniera permanente. È così, che il diritto all'identità personale [5] viene meno, introducendo un concetto più ampio, ovvero il chilling effect o effetto inibitore. [6]

Il timore per la violazione dei diritti fondamentali degli interessati è un caposaldo su cui si muove la Commissione Europea. Il primo diritto sensibile all'utilizzo di questi sistemi avanzati di AI e il diritto al rispetto della vita privata nonché alla protezione dei dati personali. "*Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a*

[4] Tecnica di sintetizzazione di immagini umane basate sull'Intelligenza Artificiale.
[5] "*La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale*". art. 2 delle Costituzione Italiana.
[6] Il chilling effect è un fenomeno sociale e giuridico che si verifica quando le sanzioni o le minacce di sanzioni contro un individuo o un'organizzazione hanno un impatto negativo sulla sua libertà di espressione e di informazione.

meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui" (Carta di Nizza, 7 dicembre 2000) [7].

[7] Articolo 7 della Carta dei diritti fondamentali dell'Unione Europea.

2. IL RUOLO DELLA PRIVACY NELL' AMBITO BIOMETRICO

La principale violazione al diritto alla privacy è determinata da leggi che disciplinano in maniera specifica queste tipologie di strumentazioni. Infatti, si può pensare alla tipologia di dati di cui gli algoritmi si servono. Si tratta di dati in grado di consentire l'identificazione di una persona fisica. Eppure, nonostante il carattere di estrema delicatezza, la maggior parte delle operazioni di identificazione avviene in modo occulto, ossia senza il previo consenso del diretto interessato [8]. Dunque, il soggetto perde il controllo sulla circolazione dei dati che lo riguardano, subendo altresì una lesione del suo diritto all'autodeterminazione. In tale contesto, risulta necessario dover definire il consenso come *"qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento"* (GDPR, 2016) [9]

È utile tenere presente l'articolato rapporto tra la sicurezza e libertà e in questo ambito sicuramente trova ampio margine il diritto alla privacy. *"Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni*." (Costituzione Italiana , 1947) [10] . Di conseguenza, nella sfera del digitale, il diritto alla privacy si qualifica nel diritto alla protezione dei dati personali, rappresentando il diritto più toccato dal riconoscimento facciale e dall'analisi biometrica.

[8] È la persona fisica cui si riferiscono i dati personali, identificata o identificabile.
[9] Articolo 4 del GDPR
[10] Articolo 2 della Costituzione italiana: diritto alla privacy

3. IL DATO BIOMETRICO ALLA LUCE DEL GDPR

Il quadro normativo vigente, fa comprendere la necessità di delineare a pieno la tipologia di dati che le tecnologie odierne sfruttano. Fornire una definizione di dato biometrico rappresenta un'operazione complessa, quanto precaria. L'articolo 4, paragrafo 1, n.14 del GDPR chiarisce che il dato biometrico è un *"dato personale ottenuto da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quale immagine facciale o i dati dattiloscopici"* (GDPR, 2016).

In base a questa definizione, il dato biometrico costituisce una classe particolare di informazioni personali e come tale il Garante europeo per la Protezione dei dati stabilisce che il loro trattamento [11] deve essere subordinato al perseguimento di un interesse pubblico rilevante. Ovviamente, il perseguimento di un interesse pubblico non riproduce una ragione sufficiente, in quanto deve essere considerato un congruo rapporto del processo e l'adozione di relative misure di sicurezza in grado di salvaguardare i diritti fondamentali dell'interessato. Infatti, il dato biometrico è soggetto alla stringente disciplina della Direttiva UE 2016/680, meglio conosciuta come GDPR. Analizzando l'articolo 10 della suddetta direttiva, viene stabilito che il trattamento dei dati biometrici viene autorizzato solo se risulta necessario, ma è sottoposto a delle garanzie adeguate e sotto particolari condizioni: sia stato autorizzato dal diritto dell'UE oppure da uno Stato Membro; sia idoneo a preservare l'interesse della persona fisica oppure riguardi dati resi espressamente pubblici dall'interessato. Così come è descritto, il dato biometrico risulta essere un elemento fortemente lesivo dei diritti fondamentali. Sicuramente tra tutti i rischi, primeggia il diritto all'identità d'immagine e all'immagine personale, poiché il dato biometrico rileva elementi che consentono di caratterizzare in maniera univoca un soggetto. Dunque, la necessità di preservare e tutelare a tutti i costi la propria identità, trova il suo nucleo nella sua stessa funzione: l'identità è il principio *"che genericamente indica l'uguaglianza di un soggetto rispetto a sé stesso"* [12].

In questo scenario, la sfera biofisica dell'individuo risulta essere il fulcro predominante e per questo la trattazione dei dati biometrici diviene estremamente delicata. Nonostante il

[11] *"Trattamento è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali"* (Articolo 4, co.1, n.2, GDPR).
[12] https://it.wikipedia.org/wiki/Identit%C3%A0

regolamento GDPR pone le basi per una protezione dei dati personali, pone anche delle eccezioni. Se si considera l'articolo 9, la prima eccezione prevede che l'interessato abbia autorizzato il trattamento. Seguono: l'utilizzo di dati biometrici solo se necessari in ambito lavorativo, della sicurezza sociale e collettiva; l'uso necessario per la protezione di un interesse vitale dell'interessato; se necessario in un procedimento giudiziario; per motivi di interesse sanitario, come il controllo di malattie trasmissibili e per motivi di tutela di gravi minacce per la salute delle persone.

Tuttavia, laddove il trattamento dei dati abbia avuto un previo consenso, l'interessato deve essere sempre correttamente informato circa le modalità e finalità dell'utilizzo dei dati biometrici che lo riguardano. Nell'articolo 12 viene ribadito quanto sotteso nell'intero testo del GDPR: quando non vi è un'attività di trattamento dei dati personali, questa deve avvenire seguendo un principio di trasparenza, il quale coinvolge anche l'informativa circa l'esistenza della profilazione e delle conseguenze sulla stessa. Tale articolo pone le basi per i successivi articoli 13 e 14, riguardanti l'informativa.

L'informativa è un documento o comunicazione rivolta ad un soggetto, il cui scopo è di rendere conscio il cittadino, sulle finalità e le modalità dei trattamenti operati dal titolare del trattamento [13]. In tal modo si scindono due concetti calibro, che prevedono il rispetto del diritto individuale ad essere informato ed il dovere del titolare del trattamento ad assicurare trasparenza e correttezza nell'esercizio che va fin dalla fase di progettazione, richiamando il principio di accountability.[14] Inoltre, laddove il trattamento richieda una base giuridica, l'informativa aggiunge l'ulteriore condizione di legittimità del trattamento. Dunque, occorre suddividere due categorie di dati, ossia quelli acquisiti da terzi e quelli raccolti direttamente dall'interessato. In entrambi i casi l'informativa è dovuta ogni qual volta sia presente un trattamento dei dati nell'istante immediatamente precedente o nel momento in cui si avvia la raccolta dati. Tuttavia, il Garante della Privacy italiano ha rammentato che nei casi seguenti non è previsto l'obbligo dell'informativa:

[13] *"è la persona fisica o giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le scelte di fondo sulle finalità e sulle modalità del trattamento dei dati, anche per ciò che riguarda la sicurezza."* (Legge n 675/1996).

[14] *"L'accountability è il processo con cui (a livello sociale, politico, aziendale, contabile o comunque collettivo) si è chiamati a rendere conto delle conseguenze delle proprie azioni."* (Wikipedia).

- il caso in cui il trattamento riguarda dati anonimi;
- il caso in cui il trattamento del dato sia connesso allo svolgimento di investigazioni in materia penale.

Nell'articolo 14 del GDPR, viene chiarito che l'informativa deve essere fornita entro un termine ragionevole, non oltre un mese dalla raccolta dei dati. In questo modo, si evidenzia la facoltà del cittadino di poter decidere in autonomia e consapevolmente, il modo in cui le sue informazioni siano acquisite e conservate. A causa dell'inaccessibilità del metodo algoritmico dei sistemi di intelligenza artificiale, viene reso difficile l'esercizio del diritto di accesso, di cui se ne parla nell'articolo 15 del Regolamento europeo 2016/679. Infatti, è garantito al titolare del trattamento dei dati di poter accedere a questi ultimi e di essere informato circa le finalità del trattamento, i destinatari, il periodo di conservazione e l'esistenza di un processo decisionale automatizzato dei dati. Nello scenario del dato biometrico, il problema degli algoritmi sembra che possa essere affievolito dall'obbligo di un intervento umano. Infatti, spetterebbe all'operatore umano di dare conferma o meno del risultato ottenuto, poiché l'ammissibilità di una decisione sul trattamento automatizzato deve ravvivarsi oltre che sulla predisposizione normativa anche sulla possibilità di un intervento umano.

Analizzando in maniera più dettagliata la natura opaca dei sistemi di intelligenza artificiale, questa sembra contraria alla legge in ragione dell'impossibilità di poter verificare il procedimento seguito dagli algoritmi durante la fase di esecuzione, poiché nemmeno gli operatori hanno pieno controllo. Conseguenza lecita è che il soggetto risulta privo di difendersi nel processo dinanzi all'utilizzo di taluni algoritmi, non essendo possibile contestare le procedure che hanno condotto ad un esito negativo per le garanzie di cui egli è titolare. Tuttavia, grazie alla Direttiva, si ritiene necessario che l'operatore umano mantenga un ruolo attivo nel processo decisionale. Inoltre, non essendo ancora entrato in vigore l'AI Act (paragrafo successivo), è bene focalizzarsi sul GDPR, al fine di andare a valutare quale sia il corretto comportamento da tenere per minimizzare i rischi. Il principio che viene richiamato è quello descritto nell'articolo 5, lettera a, il quale esplicita il principio della Trasparenza. È previsto un trattamento dei dati e nel caso in questione anche quelli biometrici, che sia interamente o parzialmente automatizzato. La rilevazione dei dati biometrici sfrutta algoritmi di Machine e Deep learning, i quali operano in maniera autonoma e di conseguenza sembra venir meno la trasparenza. Quest'ultima apre numerose questioni circa la forma che deve assumere. Per questo motivo se non possono essere individuate apposite

soluzioni, volte ad eliminare l'opacità degli algoritmi, allora devono essere fornite adeguate tutele e garanzie nei confronti dell'interessato. Questa forma di garanzia è fornita dal principio di trasparenza sancito nel GDPR, 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.*" (GDPR articolo 5, 2016) [15]. Dunque, in questa ottica, non è sufficiente riportare all'interessato le informazioni di cui gli articoli 13 e 14 del GDPR dispongono. È fondamentale che il titolare del trattamento permetta al destinatario di comprendere le conseguenze del trattamento stesso.

In virtù della Direttiva, ogni trattamento di dati biometrici ai fini dell'identificazione di un soggetto, è considerato altamente invasivo e come tale deve essere trattato e classificato nella categoria dei "particolari dati personali", la cui elaborazione è proibita, salvo eccezioni che richiedono valutazioni di liceità.

[15] Considerando 39 del GDPR.

4. L'AI ACT E LA REGOLAMENTAZIONE DEL RICONOSCIMENTO BIOMETRICO NELL'ERA DEL MACHINE LEARNING E DELL'INTELLIGENZA ARTIFICIALE

Come già evidenziato in gran parte nelle pagine precedenti, l'ascesa dell'intelligenza artificiale ha rivoluzionato il modo in cui le tecnologie influenzano la società. L'unione europea ha riconosciuto la necessità di garantire un quadro normativo adeguato all'uso di codeste tecnologie e di conseguenza ad una regolamentazione del dato biometrico. L'AI Act introduce delle specifiche per le regolamentazioni dei sistemi di intelligenza artificiale, specialmente in merito a quelle degenerative. Lo scopo di suddette normative è accentuare la trasparenza, la sicurezza e la responsabilità degli algoritmi utilizzati. Infatti, il legislatore europeo mira ad instaurare un rapporto tra l'odierna tecnologia e i diritti fondamentali dell'individuo. L'idea alla base è quella di aumentare la rigidità delle regole al crescere del rischio di violazione dei diritti fondamentali da parte dell'AI. I quattro livelli di rischio, ovvero inaccettabile, alto, limitato e basso, vengono normati e classificati. In particolar modo, l'articolo 6 dell'AI ACT fornisce un ordinamento delle intelligenze artificiali considerate pericolose, identificando come alto rischio quelli che vanno ad intaccare la sfera della sicurezza dei diritti fondamentali. Tale categorizzazione è utilizzata in otto tematiche, tra cui l'identificazione biometrica. Inoltre, saranno classificati a rischio limitato quei sistemi interattivi con gli esseri umani, dunque dedicati al riconoscimento delle emozioni, alle operazioni di categorizzazione biometrica, nonché le intelligenze artificiali coinvolte nella generazione o manipolazione di immagini. Tali sistemi, pur non essendo soggetti a requisiti in maniera di trasparenza, dovranno obbligatoriamente informare chi interagisce con essi, se le persone desiderino proseguire l'iterazione con una macchina oppure con un soggetto umano. In tale ottica traspare il timore per la violazione dei diritti fondamentali degli interessati. Infatti, le tecnologie di riconoscimento facciale sono ad oggi in grado di analizzare una quantità smisurata di dati riferiti in maniera diretta a persone fisiche identificabili e no, soprattutto quando operano in modalità real time. Per garantire una maggiore sicurezza pubblica, il cittadino accetta la presenza di telecamere di videosorveglianza e conseguentemente la pretesa di restare anonimi in luoghi pubblici. Ragion per cui si aprono le porte ad una sorveglianza di massa, che può degenerare fino ad arrivare alla profilazione. Per questo servono dei limiti specifici che vengono posti alla base dell'AI Act.

L'AI Act introduce un divieto generale sull'utilizzo dei sistemi di riconoscimento biometrico in tempo reale per la sorveglianza di massa negli spazi pubblici. È applicato a qualunque sistema che abbia come fine l'identificazione di individui a distanza. Ovviamente sono previste eccezioni al riguardo, le quali sono oggetto dell'articolo 5, comma 2. L'utilizzo per la ricerca di persone scomparse, le prevenzioni di reati gravi o l'identificazione di persone in situazione di vulnerabilità sono esenti da suddette leggi. La proibizione dei sistemi biometrici si applica, dunque, all'identificazione di persone fisiche. Ecco che si apre un nuovo tema su ciò che viene inteso con il termine identificazione. Infatti, è noto che molti sistemi biometrici che utilizzano dati biometrici, come il movimento degli occhi o la frequenza cardiaca, non hanno come obiettivo quello di indentificare un soggetto specifico, ovvero associare un nome e cognome. Tuttavia, nella cornice normativa dell'AI Act, è consentito l'utilizzo dei sistemi real time biometric identification, ossia quei particolari sistemi utilizzati senza una latenza tra l'istante di acquisizione del dato e il momento in cui avviene il riconoscimento della persona.

5. ACCENNO AL DATA ACT E ALLA STRATEGIA DELL'UNIONE EUROPEA PER LA GESTIONE DEI DATI BIOMETRICI

In tale scenario normativo, c'è senz'altro da aggiungere ed annoverare il Regolamento che completa la strategia dell'Unione Europea in merito ai dati. A differenza dell'AI Act è entrato in vigore già a partire dall'11 gennaio 2024. Il Data Act è volto a favorire l'accesso e la circolazione dei dati nell' Internet of Things [16], con lo scopo di mirare a creare un ambiente legale che promuova la condivisione sicura dei dati. Ponendo un focus sulla relazione tra i dati biometrici e le leggi del Data Act, vengono incrementati ulteriori questioni. Infatti, le regole principali sono:

- trasparenza e controllo, includendo la possibilità di sapere chi ha accesso ai loro dati biometrici e a quale scopo, nonché il diritto di revoca del consenso del trattamento dei propri dati.
- sicurezza e protezione, imponendo degli standard rigorosi per la sicurezza. Le aziende e le organizzazioni devono implementare delle misure adeguate a proteggere i dati da accessi privi di autorizzazione e violazioni.
- Interoperabilità e condivisione dei dati, promuovendo la facilitazione della condivisione dei dati tra entità differenti. Ciò comporta sicuramente degli incentivi, specialmente nel campo della biometria, per produrre applicazioni sanitarie o di sicurezza pubblica, pur mantenendo la privacy dei cittadini.
- Diritto degli utenti, rafforzando il diritto degli individui ad accedere o cancellare i propri dati, al fine di garantire un maggior controllo sulla loro identità digitale.

[16] Rappresenta un neologismo con lo scopo di delineare l'evoluzione dell'estensione del mondo di Internet agli oggetti e ai luoghi concreti, i quali acquisiscono una vera identità digitale, in modo tale da comunicare con altri oggetti e generare dei servizi utili agli utenti.

6. CLERVIEW AI TRA INNOVAZIONE E CONTROVERSIE NEL RICONOSCIMENTO FACCIALE

6.1 LA SOCIETÀ

Clearview AI è un'azienda statunitense, operante nel settore IT che fornisce software di riconoscimento facciale. Fu fondata nel 2017 da Hoan Ton-That e Richard Schwartz. Clearview AI utilizza un sistema di algoritmi di machine learning atti ad analizzare le immagini scaricate da vari siti web e piattaforme online, tra cui i social media, acquisite tramite web scraping. Nel dettaglio i suoi software vanno a identificare le persone presenti in immagini e associarle a profili di utenti online, anche se le immagini sono state modificate o manipolate. L'idea della società era quella di fornire i suoi servizi a clienti governativi e privati, al fine di aiutare le autorità a identificare e prevenire crimini, senza alcuno scopo commerciale o di marketing. L'azienda ha contratti con l'FBI, il Dipartimento della Sicurezza Nazionale, l'esercito e 3100 agenzie di polizia negli Stati Uniti. La popolarità dell'azienda è da ricercare nell'efficacia dell'algoritmo, il quale è considerato tra i primi dieci migliori per il riconoscimento tra due immagini della stessa persona. Infatti, il sistema avrebbe una precisione che oscilla tra il 98,6% e il 100%, dunque un livello di confidenza molto elevato. Non a caso ha ottenuto il primo brevetto dallo US Patent and Trademark Office.
L'algoritmo funziona nel seguente modo: un utente carica una foto, Clearview lo riconosce e mostra tutte le altre immagini in cui la persona compare nel web o, meglio, da una banca dati che Clearview ha archiviato, creando un database che vanta circa trenta miliardi di immagini.

Le attività di Clearview AI hanno suscitato diverse controversie e critiche. Infatti, molte persone hanno espresso preoccupazione per la raccolta e l'analisi dei dati personali senza il consenso degli utenti, nonché la possibilità che questi dati siano utilizzati per scopi commerciali o di videosorveglianza.

6.2 LA SANZIONE DEL GARANTE DELLA PRIVACY CONTRO CLEARVIEW AI

Il 9 marzo 2022, il Garante della Privacy ha imposto una sanzione di 20 milioni di euro a Clearview AI, per aver violato i diritti dei cittadini europei e italiani. La società era accusata di aver raccolto e trattato illegalmente i dati biometrici di milioni di persone, inclusi quelli di cittadini italiani, senza il loro consenso e senza una base giuridica adeguata. Secondo quanto detto dal Garante della Privacy: *"le fotografie vengono elaborate con tecniche biometriche per estrarre i caratteri identificativi e associare 512 vettori che ricalcano le fattezze del volto, sottoposte a hashing [17] per indicizzarle e arricchite con metadati (come geolocalizzazione, link della fonte, genere, nazionalità o lingua della persona rappresentata)"* (Garante della Privacy, 2022). La sanzione è stata comminata a seguito di segnalazioni da parte di Privacy Network e di altre autorità nazionali.

Dunque, il Garante ha condannato Clearview AI per aver messo in atto un vero e proprio monitoraggio biometrico anche di persone che si trovano nel territorio italiano, violando i principi fondamentali del GDPR. La società americana aveva creato un database contenente più di 20 miliardi di immagini di volti di persone, estratte da fonti web pubbliche tramite web scraping. Queste immagini venivano elaborate con tecniche biometriche per estrarre le caratteristiche identificative di ogni immagine. Tuttavia, Clearview AI non aveva mai chiesto il consenso delle persone per poter utilizzare i loro dati biometrici e non aveva alcuna base legale per motivare la loro raccolta e il loro utilizzo per "legittimo interesse".

La sanzione del Garante della Privacy è stata vista come un importante passo per proteggere i diritti dei cittadini europei e italiani e per contrastare l'utilizzo illegale dei dati biometrici. Inoltre, il Garante ha ordinato a Clearview AI di cancellare i dati relativi a persone che si trovano in Italia e di non ulteriormente raccogliere e trattare i dati attraverso il suo sistema di riconoscimento facciale.

Le segnalazioni presentate nei confronti dell'azienda statunitense, mettono in luce l'adozione di rimedi a garanzia dei cittadini, sottolineando l'efficienza funzionale di un sistema di tutela dei dati personali presente nell'Unione Europea. L'obiettivo è quello di stabilire un equilibrio del diritto alla

[17] È una tecnica di mappatura dati che consente di convertire dati da un formato testuale ad un codice numerico univoco (hash code). Tale codice è generato da una funzione hash che prende in input i dati e li trasforma in un valore numerico di una certa lunghezza. La funzione hash è progettata per essere rapida ed efficiente, permettendo di accedere rapidamente ai dati utilizzando il codice hash come chiave di ricerca. Viene utilizzata in ambiti quali la sicurezza sui dati, la gestione dei database e la crittografia.

privacy e temperando l'asimmetria di conoscenza e di potere tra gli attori nel processo della datification [18].

6.3 LE CRITICITÀ RILEVATE

Sulla base delle informazioni raccolte dai reclamanti, il Garante della Privacy ha avviato un procedimento per violazione di diversi articoli del GDPR. In particolar modo, ha osservato che la società Clearview non rispettava le seguenti leggi:

- articolo 5, il quale stabilisce i principi fondamentali per il trattamento dei dati personali. Sulla base dell'interpretazione del par. 1, lett. a), difatti il trattamento è lecito se è conforme al diritto. Inoltre, i dati personali devono essere trattati in modo corretto e trasparente nei confronti dell'interessato. Un ulteriore principio del trattamento deriva dal par. 1, lett. b), ossia quello concernente la finalità. Viene previsto che i dati personali debbano essere *"raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; …"* (GDPR articolo 5, 2016) [19]. Infine, l'ultimo punto dell'art. 5 violato dalla società riguarda il par. 1, lett. e), il quale va a disporre delle limitazioni concernenti la conservazione dei dati. Quest'ultimi devono essere "*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, …"* (GDPR articolo 5, 2016) [20].
- Articolo 6, in aggiunta all'articolo 5, va a delineare le condizioni che rendono lecito il trattamento dei dati. È richiesto che il consenso espresso dall'interessato sia definito per delle finalità specifiche. Se questo viene effettuato per finalità differenti da quelle riportate, il titolare del trattamento deve accertare la compatibilità tra le finalità secondarie e quelle

[18] È il processo tecnologico che trasforma vari aspetti della vita quotidiana, sociale e individuale in dati digitali. Ad esempio, Facebook ha datificato la rete delle conoscenze e amicizie degli utenti.
[19] https://gdpr-text.com/it/read/article-5/#comment_gdpr-a-05_1b
[20] https://gdpr-text.com/it/read/article-5/#comment_gdpr-a-05_1b

originarie, tenendo conto delle ragionevoli aspettative dell'interessato e di eventuali misure di sicurezza. In aggiunta, il titolare del trattamento deve necessariamente permettere la revoca del consenso in qualsiasi momento, senza pregiudicare la liceità del trattamento basato sul consenso prima della revoca. [21]

- Articolo 9, in cui viene affermato il divieto di trattare dati personali *"che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona"* (articolo 6 GDPR , 2016) [22]. La disposizione mira a tutelare e rafforzare tali modelli di dati personali, la cui natura particolare e debole richiede una specifica disciplina. Infatti, il divieto di trattamento non implica un'applicazione dove sussista almeno una fattispecie sopracitata. Sicuramente tra queste tipologie si segnala il caso in cui l'interessato abbia prestato il proprio consenso al trattamento di tali dati, salvo possibili revoche.
- Articolo 12, il quale delinea le modalità di comunicazione e la trasparenza delle informazioni fornite agli interessati in relazione al trattamento dei loro dati personali. È richiesto che la forma della comunicazione risulti *"concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato."* (Articolo 12 GDPR , 2016) [23].
- Articoli 13 e 14, riguardanti le informazioni da fornire qualora i dati personali siano raccolti presso l'interessato (art. 13), oppure qualora i dati personali non siano stati ottenuti presso l'interessato (art. 14). *"In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni: l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; i dati di contatto del responsabile della*

[21] https://gdpr-text.com/it/read/article-6/#:~:text=L'interessato%20ha%20il%20diritto,interessato%20%C3%A8%20informato%20di%20ci%C3%B2.
[22] https://gdpr-text.com/it/read/article-9/
[23] https://gdpr-text.com/it/read/article-12/

protezione dei dati, ove applicabile; le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; …" (Articolo 13 GDPR, 2016) [24].

- Articolo 15, che assicura agli interessati di verificare l'uso che viene fatto dei loro dati personali, promuovendo la trasparenza e la responsabilità nel trattamento. Infatti, il diritto dell'interessato si concreta nell'ottenere la conferma e successivamente di conseguire l'accesso dei dati che vengono trattati. Dunque, il titolare è obbligato a fornire una copia dei dati personali oggetto di trattamento.[25]
- Articolo 22, il quale disciplina il diritto dell'interessato a non *"essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona."* (Articolo 22 GDPR, 2016) [26]. In tal modo si configura il diritto di poter ottenere l'intervento umano da parte del titolare del trattamento, cosicché si possa contestare la decisione.
- Articolo 27, in cui è richiesto che i titolari e i responsabili del trattamento non stabili dall'Unione Europea, designino un rappresentante dell'UE, al fine di facilitarne la comunicazione e le conformità con il Regolamento.[27]

6.4 LA RISPOSTA DI CLEARVIEW AI ALLA SANZIONE DEL GARANTE

Come risposta alla sanzione ricevuta, Clearview AI ha affermato la non applicabilità del Regolamento GDPR e, perciò, l'assenza di giurisdizione del Garante. Secondo quanto riportato dalla società, questa non offre servizi o prodotti in Italia, poiché ha implementato qualsiasi tentativo di accesso alla piattaforma da indirizzi IP italiani. In aggiunta, non viene effettuato alcun tipo di monitoraggio, poiché secondo Clearview il monitoraggio richiede ed implica un'analisi continua e prolungata, mentre il loro fine ultimo è un'applicazione per la ricerca di immagini con link a siti terzi. Dunque, non verrebbero monitorate né tracciate le persone nel tempo, ma

[24] https://gdpr-text.com/it/read/article-13/ . https://gdpr-text.com/it/read/article-14/
[25] https://gdpr-text.com/it/read/article-15/
[26] https://gdpr-text.com/it/read/article-22/
[27] https://gdpr-text.com/it/read/article-27/

verrebbero forniti esclusivamente dei risultati istantanei, come quelli di Google Search. La società ha, di seguito, dichiarato che non ha nessun cliente italiano.

Nonostante la risposta del Garante della Privacy circa la violazione degli articoli 5,6,9,12,13,14,15,22 e 27 del GDPR, Clearview ha sostenuto che la società non offre intenzionalmente beni e servizi ai clienti europei. Inoltre, vengono: trattati solo i metadati di localizzazione delle foto, perciò il luogo dove l'immagine è stata scattata; le attività consentite dal loro software sono svolte e monitorate da autorità pubbliche e sotto la loro responsabilità; le condizioni d'uso del programma prevedono che sia responsabilità del cliente di verificare la legittimità dell'uso del prodotto in base alle normative locali; le loro attività non sono finalizzate ad analizzare il comportamento degli interessati né creano profili riconducibili a persone fisiche. Infatti, le attività non rilevano informazioni legittime che tracciano i soggetti nel tempo.

La risposta di Clearview AI alle sanzioni del Garante della Privacy evidenzia un aspetto fondamentale: la complessità della regolamentazione internazionale in un mondo tecnologicamente avanzato e interconnesso. Infatti, da un lato le argomentazioni sopracitate rappresentano una strategia comune tra le aziende che si occupano dell'IT nel mercato globale, poiché cercano di delimitare la giurisdizione e l'applicabilità di suddette norme. Dall'altro lato, le autorità cercano di proteggere i diritti dei cittadini nell'era digitale.

Non a caso, la vicenda ha sollevato una serie di questioni legate alla privacy, sull'uso dei dati biometrici e la capacità delle normative esistenti di essere al passo con l'innovazione tecnologica, il cui andamento è risultato esponenziale. Dunque, è necessario un dialogo continuo tra i regolatori e gli innovatori, poiché bisogna garantire un congruo equilibrio tra la tecnologia e la salvaguardia dei diritti fondamentali degli individui, garantendo giuste e robuste normative in grado di affrontare le sfide emergenti.

6.5 LA REAZIONE DELL'UNIONE EUROPEA

A seguito della condanna da parte del Garante della Privacy italiana alla società, l'autorità francese per la protezione dei dati, la CNIL, ha imposto la medesima sanzione alla società statunitense, adducendo a motivazioni simili a quelle italiane. In particolar modo, il Garante della Privacy francese ha osservato due violazioni del Regolamento del GDPR. Restando in linea con quanto affermato dal Garante italiano, ha aggiunto che *''Queste persone, le cui fotografie o video sono accessibili su vari siti web e social network non si aspettano, in maniera ragionevole, di vedere le loro immagini elaborate da Clearview Ai per fornire un sistema di riconoscimento facciale che può essere usato dagli stati per scopi di controllo e polizia''* (Wired, 2016). Il Garante ha verificato il modo in cui la società ha permesso ai soggetti di accedere ai propri dati solo per due volte all'anno, a seguito di un numero eccessivo di richieste da parte degli interessati. Come in Italia, il Garante ha imposto a Clearview di cessare tutte le operazioni di raccolta dei dati di persone francesi, di facilitare l'accesso e soddisfare le richieste di cancellazione.

Muovendosi sulla stessa linea d'onda, anche il Garante della Privacy greco e quello austriaco hanno mosso denunce con conseguenti sanzioni alla startup statunitense.

6.6 CLEARVIEW AI SOTTO ACCUSA GLOBALE: FOCUS SU AUSTRALIA, REGNO UNITO, STATI UNITI E UCRAINA

Dopo la condanna da parte del Garante della Privacy italiano per la violazione di diversi articoli del GDPR, la startup è sotto accusa nel territorio inglese. Infatti, a seguito dell'indagine attuata dall' OAIC (Ufficio del Commissario Australiano per l'Informazione) per la violazione di numerose regole del Regolamento Privacy Act australiano, l'Information Commissioner's Office inglese (ICO) ha comminato alla società una multa di circa 7,5 milioni di sterline, l'equivalente di 9 milioni di euro, per la violazione di alcune leggi in materia di privacy del Data Protection Act.

Per quanto concerne la sanzione australiana, di circa 17 milioni di sterline, la denuncia verteva attorno all'uso illegittimo e non trasparente dei dati e delle informazioni biometriche delle persone, senza alcun permesso e tantomeno senza alcuna predisposizione di processi per

impedire la conservazione dei dati a tempo indeterminato. Come è stato sostenuto dal Commissario australiano, Angelene Falk, *"la raccolta segreta di questo tipo di informazioni sensibili è irragionevolmente invadente e ingiusta, … Per loro natura, queste informazioni sull'identità biometrica non possono essere riemesse o cancellate e possono anche essere replicate e utilizzate per il furto di identità. Anche gli individui presenti nel database potrebbero essere a rischio di identificazione errata. Queste pratiche sono ben al di sotto delle aspettative degli australiani per la protezione delle loro informazioni personali... Quando gli australiani utilizzano i social media o i siti di networking professionale non si aspettano che le loro immagini facciali vengano raccolte senza il loro consenso da un'entità commerciale per creare modelli biometrici per persone completamente estranee a scopi identificativi... L'eliminazione indiscriminata delle immagini facciali di persone, solo una frazione delle quali sarebbe collegata alle indagini delle forze dell'ordine, potrebbe avere un impatto negativo sulle libertà personali di tutti gli australiani che si sentono sotto sorveglianza… Le attività di intelligenza artificiale di Clearview in Australia comportano la raccolta automatizzata e ripetuta di informazioni biometriche sensibili dagli australiani su larga scala, a scopo di lucro."* (Grinbergs, 8 November 2021) [28].

L'autorità australiana, insieme a quelle europee, hanno inviato un chiaro messaggio. Per questo anche l'ICO ha intimidato alla società di cancellare dai suoi sistemi tutti i dati biometrici appartenenti ai cittadini anglosassoni. Dunque, se da una parte l'Unione Europea sta valutando se vietare quasi completamente l'utilizzo di forme di riconoscimento facciale basate su dati di scarto, dall'altra parte John Edwards, Commissario per l'Informazione del Regno Unito, ha evidenziato la necessità di una cooperazione internazionale tra tutte le amministrazioni per bloccare le violazioni della privacy. Tale convinzione è stata rafforzata anche dai risultati positivi ottenuti mediante la collaborazione con le autorità canadesi, ovvero: l'Office of the Privacy Commissioner of Canada, la Commission d'accès à l'information du Québec, l'Office of the Information and Privacy for British Columbia e all'Office of the Information and Privacy of Alberta.

Negli Stati Uniti, numerosi attivisti hanno intentato una causa contro la società, al fine di interrompere l'utilizzo dell'algoritmo in California. A presentare la denuncia sono stati due gruppi di advocacy della contea di Slameda. Secondo quest'ultimi il software di riconoscimento facciale di

[28] https://www.holmanwebb.com.au/blog/625/office-of-the-australian-information-commissioner-clearview-ai-breached-australians-privacy

Clearview AI, verrebbe ancora utilizzato dalle forze dell'ordine, nonostante le amministrazioni abbiano vietato l'utilizzo di suddetta tecnologia. Sejel Zota, avvocato che si sta occupando del caso, ha affermato che: *"la privacy è sancita dalla costituzione della California, garantisce che tutti i californiani possano condurre la propria vita senza il timore della sorveglianza e del monitoraggio. Clearview Ai capovolge questa dinamica, rendendo impossibile camminare per strada senza temere che la propria faccia possa essere catturata, archiviata a tempo indeterminato dalla società e utilizzata contro di te in qualsiasi momento in futuro."* (Zota, 2021) [29].

Caso totalmente opposto è quello ucraino, in quanto dal 17 marzo 2022, il Ministero della Difesa ucraino, ha avuto l'accesso e il permesso ad utilizzare il software di Clearview AI e in particolar modo il database dell'azienda. La società ha inviato una lettera al Ministro della Difesa ucraino Oleksii Reznikov, con lo scopo di "donare" la loro banca dati per *"scoprire assassini russi, combattere la disinformazione e identificare i morti"* (ANSA, 2022) [30]. Il direttore generale di Clearview, Hoan Ton- That, ha affermato che all'interno del loro database sono contenute circa due miliardi di immagini provenienti da Vkontakte [31] e il software è in grado di identificare le persone morte anche in caso di menomazioni fisiche. Sempre secondo il direttore generale, l'algoritmo potrebbe essere decisivo ed utile nel far ricongiungere i rifugiati con le loro famiglie, identificare gli agenti infiltrati russi e contrastare le fake news.

[29] https://thenextweb.com/news/clearview-ai-sued-californian-activists-seek-facial-recognition-operations-end
[30] https://www.ansa.it/osservatorio_intelligenza_artificiale/notizie/societa/2022/03/14/ucraina-ha-iniziato-a-usare-riconoscimento-volto-di-clearview-ai_5318453d-c836-4dcf-b323-cd24ba360010.html
[31] Social network russo, equivalente di Facebook.

7. CONCLUSIONI

Malgrado la drammaticità della situazione ucraina, è quanto mai imperativo andare a sottolineare il carattere profondamente diverso nel contesto dell'Unione Europea e dunque quello italiano. Infatti, considerando l'ambito europeo il legislatore ha adottato un'impostazione normativa largamente rispettosa dei diritti umani in materia dei dati personali, come appunto testimonia il Regolamento 2016/679, ovvero il GDPR, il Data Act e l'AI Act.

Le tecnologie di riconoscimento facciale nella società odierna devono essere introdotte con cautela, prestando attenzione alla regolamentazione. A pesare è proprio il timore di un impiego di dati personali, soprattutto quelli biometrici, il quale rende l'individuo altamente vulnerabile. Il rischio è che l'utilizzo indiscriminato e privo di una tecnologia, come nel caso di Clearview AI, porti alla diffusione di una costante sensazione di controllo. La sfida verterà anche attorno al piano etico nello sviluppo dei sistemi di intelligenza artificiale. In tal modo codeste tecnologie verranno intese anche come alleate agli strumenti e al servizio dell'essere umano.

SITOGRAFIA

https://www.keepersecurity.com/it_IT/resources/glossary/what-is-multi-factor-authentication/

https://www.europarl.europa.eu/charter/pdf/text_it.pdf

https://protezionedatipersonali.it/dati-biometrici

https://it.wikipedia.org/wiki/Biometria

https://focus.namirial.it/riconoscimento-biometrico/

https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Arricchito+con+riferimenti+ai+Considerando+Aggiornato+alle+rettifiche+pubblicate+sulla+Gazzetta+Ufficiale++dell%27Unione+europea+127+del+23+maggio+2018.pdf/1bd9bde0-d074-4ca8-b37d-82a3478fd5d3?version=1.9

https://www.senato.it/istituzione/la-costituzione

https://www.it-impresa.it/blog/dati-biometrici/

https://legalfordigital.it/gdpr/regolamento-gdpr-e-dati-biometrici/#:~:text=Garante%20della%20Privacy-,Dati%20biometrici%3A%20cosa%20sono%3F,o%20comportamentali%20di%20un%20soggetto.

https://www.cybersecurity360.it/legal/privacy-dati-personali/dati-biometrici-e-privacy-ecco-come-vanno-trattati-in-ambito-lavorativo/

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1835792

https://lumi4security.it/dati-biometrici-cosa-prevede-il-gdpr/

https://www.miur.gov.it/documents/20182/615845/Informativa++artt.+13+e+14+GDPR.pdf/f49d383f-8b2b-4bea-bd3e-a461c2209bc0?version=1.0&t=1539863373156

https://protezionedatipersonali.it/informativa

https://it.wikipedia.org/wiki/Accountability#:~:text=L'accountability%20%C3%A8%20il%20processo,delle%20conseguenze%20delle%20proprie%20azioni

https://www.lentepubblica.it/pa-digitale/utilizzo-dati-biometrici-ai-act/#:~:text=L'AI%20Act%20introduce%20un,di%20massa%20in%20spazi%20pubblici

https://www.cybersecurity360.it/legal/privacy-dati-personali/ai-act-accordo-europarlamento-sullo-stop-al-riconoscimento-facciale-nei-luoghi-pubblici/

https://www.bugnion.eu/it/ai-act-ce-il-si-del-parlamento-europeo-stretta-sui-sistemi-di-riconoscimento-biometrico/

https://www.ilsole24ore.com/art/ai-act-ecco-testo-cosi-l-europa-regola-chatgpt-c-l-ia-generativa-AFR5aRdC

https://www.clearview.ai/

https://en.wikipedia.org/wiki/Clearview_AI

https://www.ai4business.it/sicurezza/clearview-ai-cose-e-come-funziona-il-riconoscimento-facciale/

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A52021PC0206

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=COM%3A2022%3A68%3AFIN

https://gdpr-text.com/it/read/article-5/#comment_gdpr-a-05_1b

https://thenextweb.com/news/clearview-ai-sued-californian-activists-seek-facial-recognition-operations-end

https://www.ansa.it/osservatorio_intelligenza_artificiale/notizie/societa/2022/03/14/ucraina-ha-iniziato-a-usare-riconoscimento-volto-di-clearview-ai_5318453d-c836-4dcf-b323-cd24ba360010.html

https://www.schmidtconsulting.it/2022/03/23/clearview-ai-inc-la-storia-tra-presunta-legalita-e-illeciti-conclamati/

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751323#:~:text=Il%20Garante%20per%20la%20protezione,si%20trovano%20nel%20territorio%20italiano

https://dirittoaldigitale.com/2022/03/31/clearview-ai-sanzione-garante/

https://www.altalex.com/documents/news/2022/05/11/trattamento-dati-biometrici-caso-clearview-ai

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679

https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

https://www.holmanwebb.com.au/blog/625/office-of-the-australian-information-commissioner-clearview-ai-breached-australians-privacy

https://gdpr-text.com/it/read/article-13/ . https://gdpr-text.com/it/read/article-14/

https://gdpr-text.com/it/read/article-15/

https://gdpr-text.com/it/read/article-22/

https://gdpr-text.com/it/read/article-27/

https://gdpr-text.com/it/read/article-5/#comment_gdpr-a-05_1b

https://gdpr-text.com/it/read/article-6/#:~:text=L'interessato%20ha%20il%20diritto,interessato%20%C3%A8%20informato%20di%20ci%C3%B2.

https://gdpr-text.com/it/read/article-9/

https://gdpr-text.com/it/read/article-12/

https://www.wired.it/attualita/tech/2021/05/27/clearview-ai-europa-gdpr-ricorsi/

https://www.hdblog.it/sicurezza/articoli/n548643/clearview-ai-riconoscimento-ingiunzione-gdpr/

https://www.politico.com/news/2022/09/30/rcmps-facial-recognition-clearview-ai-00059639#:~:text=Clearview%20AI%20stopped%20offering%20its,%2C%20and%20it%20is%20illegal.%E2%80%9D

https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211214/

https://www.wired.it/internet/regole/2021/03/11/clearview-riconoscimento-facciale-usa-privacy/

https://appmaster.io/it/news/controverse-perquisizioni-della-polizia-clearview-ai

https://www.agendadigitale.eu/sicurezza/privacy/il-riconoscimento-facciale-di-clearview-aiuta-lucraina-ecco-i-rischi/

https://www.ansa.it/osservatorio_intelligenza_artificiale/notizie/societa/2022/03/14/ucraina-ha-iniziato-a-usare-riconoscimento-volto-di-clearview-ai_5318453d-c836-4dcf-b323-cd24ba360010.html

BIBLIOGRAFIA

ANSA. (2022).

Carta di Nizza. (7 dicembre 2000). *Carta Fondamentale dei Diritti dell'Unione Europea.* Nizza.

Costituzione Italiana . (1947).

Garante della Privacy. (2022).

Grinbergs, T. W. (8 November 2021).

Wikipedia. (s.d.).

Wired. (2016).

Zota, S. (2021).

Finger Prints, Sir Francis Galton (1892)

Regolamento Generale sulla Protezione dei Dati (27 aprile 2016)

Costituzione della Repubblica Italiana (27 dicembre 1947)

AI ACT (aprile 2021)

Data Act (11 gennaio 2024)