T4F Series
PAPER N. 4
a.a. 2022/2023

Trento BioLaw Selected Student Papers

L'uso di *Clearview* in Europa: come evitare il fenomeno del *Big Brother*?

ELISA DABERGAMO, YASMINE HEGAZ

Jean Monnet EUROPEAN CENTRE UNIVERSITY OF TRENTO
Co-funded by the Erasmus+ Programme of the European Union
UNIVERSITÀ DI TRENTO Facoltà di Giurisprudenza

I paper sono stati selezionati a conclusione del corso *Diritto e Intelligenza Artificiale* a.a. 2022-2023, organizzato all'interno della Cattedra Jean Monnet "T4F – TrAIning 4 Future. Artificial Intelligence and EU Law", coordinato presso l'Università di Trento dal docente Carlo Casonato.

L'uso di *Clearview* in Europa: come evitare il fenomeno del *Big Brother*?

Elisa Dabergamo e Yasmine Hegaz[*]

ABSTRACT: Artificial intelligence has become an important part of our society, an extremely precious resource, giving rise to numerous benefits for individuals, but also to significant risks that could negatively affect fundamental rights, revealing itself as a real threat to our community. This paper aims at analysing the controversial aspects connected to the employment of biometric data and its use for public interests. In particular, the authors analyse an interesting case study concerning *Clearview AI*, an innovative facial recognition system from the USA, which quickly spread worldwide and can identify anyone in the world real – time. After a brief description of its mechanism, the authors consider whether this system could possibly be applied in Europe too, according to the current regulation.

KEYWORDS: Artificial intelligence; biometric data; facial recognition system; fundamental rights; AI Act.

SOMMARIO: 1. Premessa: i rischi connessi all'uso dei dati biometrici – 2. *Clearview AI* – 3. È possibile l'applicazione di *Clearview* in Europa?

1. Premessa: i rischi connessi all'uso dei dati biometrici

Le nuove tecnologie sono ormai divenute parte integrante della società odierna e hanno un impatto significativo anche nelle nostre vite.

Uno dei profili ad oggi maggiormente controversi riguarda l'utilizzo della biometria e, in particolare, il trattamento del dato biometrico per finalità di pubblico interesse.

La biometria è tradizionalmente definita come la «*disciplina che studia le grandezze biofisiche allo scopo di identificarne i meccanismi di funzionamento, di misurarne il valore e di indurre un comportamento desiderato in specifici sistemi tecnologici*».

Oggigiorno, la disciplina biometrica viene spesso utilizzata per le attività di identificazione e riconoscimento delle persone.

Più in generale, sarebbe più appropriato parlare di «autenticazione biometrica»[1], per tale intendendosi quel processo di identificazione avente ad oggetto l'osservazione di caratteristiche sia «anatomiche o

[*] *Studentesse dell'Università degli Studi di Trento, Facoltà di Giurisprudenza.* elisa.dabergamo@studenti.unitn.it; yasmine.hegaz@studenti.unitn.it.

[1] Si puntualizza che nell'elaborato in oggetto le autrici utilizzano le espressioni "autenticazione biometrica" e "riconoscimento biometrico" come sinonimi.

fisiologiche», come nel caso del riconoscimento facciale, sia comportamentali o diverse, ad esempio il riconoscimento vocale[2].

La biometria, quindi, si serve dei cd. dati biometrici, definiti dall'art. 4 par. 1 n. 14 regolamento n. 679/2016 (d'ora in avanti GDPR) come «i dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici»[3].

Vengono annoverati in questa categoria, ad esempio, l'impronta digitale utilizzata per sbloccare gli smartphone di ultima generazione; la conformazione fisica della mano, del volto, dell'iride o della retina; il timbro e la tonalità della voce.

La raccolta di questi dati avviene tramite componenti hardware e software, che ottengono le informazioni e le analizzano, mettendole a confronto con dati acquisiti in precedenza e conservati in un database: così facendo, è possibile identificare la persona interessata[4].

Gli ambiti in cui la scienza biometrica viene frequentemente impiegata sono la sicurezza e la prevenzione dell'attività illecita, ove il riconoscimento facciale trova maggiore applicazione. Sempre più spesso, le autorità di prevenzione e repressione del crimine si servono di software capaci di associare le immagini di soggetti sconosciuti con quelle delle persone segnalate, già note alle forze dell'ordine e accuratamente custodite in appositi database (cd. *matching*). Tuttavia, questi sistemi non vengono impiegati soltanto in quest'ambito, poiché trovano diffusa applicazione anche tra privati, i quali, ad esempio, si servono di innovativi sistemi di videosorveglianza, capaci di effettuare operazioni di riconoscimento e autenticazione, sia in contesti privati, che negli spazi pubblici[5].

I sistemi di *facial recognition* possono operare sia in modalità *real time*, ad esempio nel corso di manifestazioni pubbliche, che in differita: nel primo caso, lo strumento analizza in diretta i video provenienti dalle telecamere[6]; nel secondo caso, invece, i dati vengono collezionati ed esaminati in un momento successivo.

---

[2] E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?,* in *Diritto Penale e Uomo* (DPU) – *Criminal Law and Human Condition*, 5, 2021, p. 3.

[3] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche in materia di trattamento dei dati personali e alla libera circolazione di tali dati e abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), 27 aprile 2016. È opportuno evidenziare che l'Italia ha adeguato la normativa vigente al Regolamento con l'adozione del d. lgs. 10 agosto 2018, n. 101.

[4] B. SAETTA, *Dati biometrici*, 2 marzo 2020, disponibile al link https://protezionedatipersonali.it/dati-biometrici (ultima consultazione 5/10/2023).

[5] B. SAETTA, *op. cit.*

[6] Questa tecnica è particolarmente utile nel caso in cui si voglia localizzare una persona specifica.

Questa tecnologia rende incredibilmente agevole la raccolta e la memorizzazione dei dati: l'immagine riesce ad essere catturata anche a distanza e in ambienti particolarmente affollati.

Malgrado gli innumerevoli vantaggi, detti strumenti hanno scaturito animati dibattiti legati alla pervasività degli stessi e al forte timore che questi possano essere utilizzati per finalità di sorveglianza di massa. Come se non bastasse, queste tecnologie sono spesso oggetto di applicazioni contrastanti con i diritti fondamentali. Tale criticità è particolarmente evidente nel riconoscimento facciale *real tim*e, ove il sistema è in grado di immagazzinare immagini di volti e dati biometrici di un numero indeterminato di soggetti, salvo poi operare una selezione delle immagini acquisite o, in alcuni casi, conservarle comunque per futuri eventuali *matching*. Anche la modalità in differita non è esente da critiche: in questo caso si pone il problema di definire e limitare il tempo di memorizzazione e raccolta delle immagini, per evitare che possano essere conservate per un lasso temporale indeterminato[7].

Come anticipato, questi dati, proprio per la loro elevata capacità identificativa, sono sottoposti ad un regime speciale: il GDPR, all'art. 9, par. 1, ne vieta il trattamento, nel caso in cui questi siano intesi ad identificare in modo univoco una persona fisica, fatte salve alcune eccezioni, che ammettono il trattamento dei dati biometrici soltanto a determinate condizioni.

In particolare, esso è autorizzato qualora sia giustificato, ai sensi dell'art. 9, par. 2, lett. g), GDPR, da «motivi di particolare interesse pubblico» previsti dalla legge. Tale trattamento deve, in ogni caso, risultare proporzionato alla finalità perseguita e dev'essere accompagnato dall'adozione di misure di sicurezza appropriate per tutelare i diritti fondamentali e gli interessi del soggetto cui questi dati si riferiscono[8].

In base all'art. 10 della Direttiva UE 2016/680[9], il trattamento di dati biometrici «intesi a identificare in modo univoco una persona fisica è autorizzato solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e soltanto: a) se autorizzato dal diritto dell'Unione o dello Stato membro; b) se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; c) se riguarda dati resi manifestamente pubblici dall'interessato»[10].

Orbene, se, da un lato, l'uso di questa particolare categoria di dati si rivela incoraggiante, poiché eleva sicuramente il livello di sicurezza dei servizi a seguito di autenticazione biometrica; dall'altro, è necessario adottare determinate cautele per non configurare rischi o pregiudizi per i soggetti interessati al trattamento, conseguenti all'utilizzazione non autorizzata dei dati al di fuori degli scopi originari.

---

[7] E. CURRAO, *op. cit*., pp. 5-6.

[8] Art. 9, par. 2, lett. g) Regolamento (UE) 679/2016 (GDPR).

[9] Direttiva (UE) 2016/680 del Parlamento Europeo e del Consiglio, Relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, 27 aprile 2016 (recepita nel nostro ordinamento mediante l'approvazione del d.lgs. n. 51/2018).

[10] E. CURRAO, *op. cit*., p. 7.

Infatti, come precisato dalla Commissione Europea nel Libro Bianco sull'intelligenza artificiale[11] e dal Consiglio d'Europa nella recente elaborazione delle Linee guida in merito all'attività di riconoscimento facciale[12], l'uso dell'AI potrebbe pregiudicare i valori su cui si fonda l'Unione, causare gravi violazioni dei diritti fondamentali, tra cui quelli alla riservatezza e alla protezione dei dati, e avere un effetto dissuasivo sulle libertà fondamentali, come quella di espressione e di riunione[13].

Il problema che si pone è inevitabilmente quello di capire se, effettivamente, l'impiego di questa tipologia di intelligenza artificiale sia proporzionato rispetto ai diritti che vengono in gioco. Il riconoscimento facciale può, infatti, implicare taluni rischi per la tutela della dignità umana, dal momento che la tecnologia utilizzata è per sua natura destinata a incidere nella sfera più intima dei soggetti coinvolti, com'è particolarmente evidente nella modalità *real time*.

Questo sistema è, appunto, in grado di catturare milioni di immagini e coinvolgere un numero indeterminato di soggetti, anche del tutto estranei rispetto alla finalità dell'attività di identificazione, col rischio che costoro possano avvertire una lesione della loro dimensione personale, in quanto vittime di un'acquisizione illegittima di propri dati.

L'individuo potrebbe sentirsi controllato e, pertanto, limitato nelle sue più elementari attività quotidiane.

In secondo luogo, è possibile individuare una lesione del diritto alla riservatezza e alla protezione dei dati personali, specialmente quando, considerate talune modalità di acquisizione delle informazioni, il loro trattamento avviene in totale assenza di un previo consenso del titolare, il quale è così spogliato di qualsiasi potere sul controllo della circolazione dei propri dati personali[14].

Le modalità di acquisizione dei dati biometrici si scontrano anche con il diritto alla tutela della propria identità e immagine personale. È indubbio, infatti, che il dato biometrico rappresenti un attributo della persona, in quanto rivela elementi che ne consentono l'identificazione inequivoca. É proprio per questa ragione che, oggigiorno, la necessità di regolamentare le attività di raccolta di questi dati e il modo in cui gli stessi vengono trattati diventa essenziale per l'effettiva tutela della persona umana.

Come se non bastasse, l'attività di processazione dei dati biometrici rischia di entrare in contrasto anche con il diritto all'autodeterminazione del titolare dei dati, nella misura in cui il trattamento, eseguito senza che il soggetto possa esserne al corrente, non gli consenta di conoscere e decidere, in modo del tutto autonomo e

---

[11] COMMISSIONE EUROPEA, *Libro Bianco sull'Intelligenza Artificiale*, 19 febbraio 2020, disponibile al link https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf (ultima consultazione 5/10/2023).

[12] COMITATO CONSULTIVO DELLA CONVENZIONE 108 (CONSIGLIO D'EUROPA), *Linee guida sul riconoscimento facciale*, 28 gennaio 2021, disponibile al link https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 (ultima consultazione 5/10/2023).

[13] E. CURRAO, *op. cit.,* p. 10.

[14] E. CURRAO, *op. cit.,* p. 11.

consapevole, le modalità con cui le informazioni che lo riguardano vengano acquisite e conservate. Del resto, ciò contrasterebbe con la progressiva valorizzazione di tale diritto nel contesto del GDPR, specialmente nella parte in cui si precisa che il soggetto debba essere sempre messo al corrente di tutte le «informazioni significative sulla logica utilizzata nel trattamento, sull'importanza e le conseguenze previste per la persona» (art. 14, par. 2, lett. g).

Il trattamento dei dati in assenza del consenso del titolare, come avviene spesso nei casi di riconoscimento facciale in aree pubbliche, sacrifica irrimediabilmente la libera scelta dell'individuo[15].

Il trattamento dei dati biometrici, specialmente se acquisiti ai fini della prevenzione del crimine e in un'ottica di successivo utilizzo in un processo penale, può compromettere significativamente anche il diritto alla tutela giurisdizionale e all'equo processo. Difatti, il rischio è che tali informazioni possano essere utilizzate per avviare un'indagine, un procedimento penale o, addirittura, nei casi più gravi, per sottoporre il soggetto a misure preventive limitative della libertà personale. Ciò pone numerosi problemi, anche perché, come dimostrato da numerosi studi, tali sistemi presentano tuttora margini di errore, inaccettabili se incidenti sulla libertà personale[16].

Questo bilanciamento di interessi ha assunto particolare rilevanza al momento della presentazione del sistema di riconoscimento facciale *Clearview AI*, diffusamente applicato negli Stati Uniti.

Tuttavia, non possiamo escludere che, in un futuro, anche in Europa ci si troverà (e in alcuni casi ci si è già trovati) davanti a sistemi che potrebbero costituire una minaccia per la tutela dei diritti fondamentali dei cittadini europei.

La tecnologia di riconoscimento facciale è sempre stata controversa. La stessa crea frustrazione nelle persone che si sentono costantemente controllate, alimentando, così, il fenomeno del cd. *Big Brother*, di cui George Orwell già trattò nella sua opera "1984".

Inoltre, questa tecnologia spesso presenta alcuni *bias*, andando, di conseguenza, a fornire false corrispondenze per determinati gruppi, come avviene per certi gruppi etnici.

Per di più alcuni prodotti di riconoscimento facciale non seguono le indicazioni di supervisione e controllo richiesti per il loro utilizzo, come avvenuto con alcuni sistemi adottati dalla polizia, fra cui lo stesso *Clearview AI*, i quali non sono mai stati sottoposti al controllo di esperti indipendenti[17].

In questo breve elaborato andremo, prima di tutto, ad analizzare, senza alcuna pretesa di esaustività, la vicenda che ha coinvolto la società *Clearview AI* e successivamente cercheremo di comprendere e rilevare le

[15] E. CURRAO, *op. cit.*, p.12.
[16] E. CURRAO, *op. cit.*, p. 12.
[17] K. HILL, *The Secretive Company That Might End Privacy as We Know It*, in *The New York Times*, 18 gennaio 2020, disponibile al link https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (ultima consultazione 5/10/2023).

principali questioni problematiche che si potrebbero porre nel caso di applicazione in Europa di sistemi come quello appena richiamato, soprattutto in presenza della proposta di regolamento europeo, l'*AI Act*, che si prefigge di disciplinare l'intelligenza artificiale.

2. Clearview AI

Uno dei più famosi casi di utilizzo del sistema di riconoscimento facciale si è avuto con lo sviluppo, da parte della società statunitense *Clearview AI*, dell'omonimo software di riconoscimento facciale basato sull'intelligenza artificiale[18].

Prima di entrare nel merito della questione, però, è utile fare una precisazione in materia di riconoscimento facciale: è fondamentale distinguere tra mera "identificazione biometrica" e "autenticazione". Mentre il primo è un sistema che riconosce i dati "uno a uno" ed è in grado di catturare volti di individui; il secondo esegue un confronto "uno a molti" ed è capace di autenticare il volto identificato, abbinandolo alla foto di una specifica persona contenuta all'interno di un database. Il sistema sceglie uno o più volti e ne misura rapidamente i tratti somatici, utilizzando algoritmi per codificare i dati nei cd. *faceprint* o modelli[19].

L'attività dell'azienda sopra menzionata può essere, quindi, inquadrata proprio in quest'ultima categoria.

Clearview AI è una società statunitense con sede a Manhattan, New York, nata nel 2017 dall'incontro tra i due co-fondatori, Hoan Ton-That e Richard Schwartz, ma che, nell'arco di pochissimo tempo, a gennaio 2020, è stata oggetto di un'inchiesta del New York Times quando, a causa di un *data breach* (ovverosia una violazione dei dati personali) sono state diffuse informazioni sui clienti, che l'hanno fatta conoscere al grande pubblico[20].

La stessa si descrive come "la più grande rete facciale del mondo", perché possiede oltre 20 miliardi di immagini di volti, provenienti da fonti web, quali social media, media, e siti web, acquisite tramite il cd. *web scraping* [21].

[18] J. CONDEMI, *Clearview AI: cos'è e come funziona il riconoscimento facciale*, 2 maggio 2022, disponibile al link https://www.ai4business.it/sicurezza/clearview-ai-cose-e-come-funziona-il-riconoscimento-facciale/ (ultima consultazione 5/10/2023).

[19] C. O'CONNOR, *Biometrics: challenges of facial recognition and the normative frameworks of the European Union and the USA*, 2019, in https://www.biodiritto.org/Pubblicazioni/Student-Papers/Student-papers-Modulo-Jean-Monnet-Biotell/30.-Biometrics-challenges-of-facial-recognition-and-the-normative-frameworks-of-the-European-Union-and-the-USA (ultima consultazione 5/10/2023).

[20] J. CONDEMI, *op. cit.*

[21] Il *web scraping*, dall'inglese "grattare" o "raschiare", è una tecnica consistente nell'estrazione di informazioni specifiche da pagine web, utili ad allenare l'algoritmo di *matching* facciale.

Su 650 algoritmi da tutto il mondo testati dal NIST [22] si è rilevato come *Clearview AI* sia seconda solo alla società cinese *SenseTime,* sia per portata che per accuratezza del *database*.

L'azienda vende il software principalmente alle forze dell'ordine (il primo cliente fu la Polizia di Stato dell'Indiana), e risulta abbia contratti con l'FBI, il Dipartimento della Sicurezza Nazionale, l'esercito e più di 3100 agenzie di polizia degli Stati Uniti.

Tuttavia, in seguito a un'inchiesta, a febbraio 2020, *BuzzFeed* ha rivelato che nella lista di account *Clearview* comparivano anche società private in settori come l'intrattenimento (Madison Square Garden e Eventbrite), il gioco (Las Vegas Sands e Pechanga Resort Casino), lo sport (NBA), il fitness (Equinox), le criptovalute (Coinbase), la distribuzione commerciale (Kohl's, Walmart), e il settore bancario (Wells Fargo, Bank of America)[23].

Più nel dettaglio, *Clearview* raccoglie tutte le foto reperite sul web, come riportato dalla *ONG Privacy International*, e le archivia nel suo *database*. Successivamente, vende l'accesso al sistema a vari clienti, che potranno eseguire ricerche nel database semplicemente caricando la foto di un soggetto per individuare i volti corrispondenti.

Questa raccolta indiscriminata di foto e altre informazioni personali costituisce, quindi, una minaccia ai diritti e alle libertà delle persone, sia online che offline.

Di conseguenza, è lapalissiano il fatto che l'uso del database di *Clearview* da parte delle autorità rappresenti una notevole espansione del regno della sorveglianza, con un potenziale rischio di abuso[24].

È proprio in questa sua caratteristica che è insito il principale problema di tutta la vicenda *Clearview*: la società ha raccolto inestimabili quantità di immagini ritraenti moltissime persone che, di conseguenza, si sono ritrovate nei database della suddetta, senza aver mai previamente espresso il consenso al trattamento dei propri dati personali[25].

Ancor più sconcertante è il fatto che la società si sia appropriata di foto ritraenti non soltanto criminali, bensì anche persone comuni, indiscriminatamente trasferite all'interno di un archivio finalizzato all'identificazione dei sospettati, dal momento che l'applicazione era originariamente finalizzata all'aumento della sicurezza nazionale.

---

[22] NATIONAL INSTITUTE STANDARDS OF TECHNOLOGY (NIST), *FRVT 1:1 Verification*, 28 October 2021, disponibile al link https://www.clearview.ai/press-room/clearview-ais-facial-recognition-platform-achieves-superior-accuracy-and-reliability-across-all-demographics-in-nist-testing (ultima consultazione 5/10/2023).

[23] J. CONDEMI, *op. cit.*

[24] S. PIERANNI, *Il nostro smartphone ci sorveglia. E siamo noi che glielo permettiamo*, in *L'Espresso*, 18 luglio 2022, disponibile al link https://lespresso.it/c/mondo/2022/7/17/il-nostro-smartphone-ci-sorveglia-e-siamo-noi-che-glielo-permettiamo/25075 (ultima consultazione 5/10/2023).

[25] J. CONDEMI, *op. cit.*

Il sistema è molto semplice da usare: è sufficiente scattare una foto a una persona e caricarla nel database; compariranno, così, tutte le foto pubbliche del soggetto in questione, allegate ai link delle fonti ove queste sono state reperite. L'algoritmo impiegato è, infatti, in grado di convertire il volto fornito dall'utente in un insieme di vettori geometrici, ovverosia segmenti orientati, successivamente ricercati nelle immagini già contenute nel *database*. Queste vengono, quindi, confrontate tra loro e attraverso la tecnica del cd. *matching* è possibile identificare la persona rappresentata nell'immagine fornita dall'utente.

In altre parole, il Garante della Privacy italiano spiega: «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 per indicizzarle e arricchite con metadati (come geolocalizzazione, link della fonte, genere, nazionalità o lingua della persona rappresentata)»[26].

All'interno di questo sistema viene impiegato il FRT, un algoritmo capace di riconoscere i visi umani attraverso l'uso della biometria e di raccogliere informazioni a partire da video o foto, prestando particolare attenzione ai dettagli dei volti, quali, ad esempio, la distanza degli occhi dalla fronte, per creare una *facial signature*, o più semplicemente una forma del nostro viso.

Infatti, è noto che il database di *Clearview AI* sia diviso in *neighbourhoods*: nonché un "raggruppamento" di foto con vettori simili. La scomposizione del volto in vettori geometrici rende, quindi, possibile il *clustering*, una forma di apprendimento automatico (cd. *machine learning*) non supervisionato, privo cioè di "etichette predefinite" che necessitano dello *human in the loop*. È, quindi, l'algoritmo stesso ad imparare autonomamente come suddividere grandi quantità di dati, in questo caso fotografie, in gruppi, anche noti come "*cluster*", in base a caratteristiche simili[27].

Per giunta, l'algoritmo riesce addirittura a identificare la persona anche se questa non guarda verso l'obiettivo o ha il viso parzialmente coperto, essendo «*progettato per tenere conto della progressione dell'età, delle variazioni di pose e posizioni, dei cambiamenti nella peluria del viso e di molte condizioni visive*», come descritto dalla società sul proprio sito internet.

Come se non bastasse, alla luce di quanto riportato dal New York Times, il codice informativo alla base di *Clearview AI* include un linguaggio di programmazione, che si serve della cd. realtà aumentata, in particolare degli *smart glasses*, capaci di identificare in tempo reale qualunque volto[28].

In ogni caso, proprio a causa di questa raccolta indiscriminata di immagini, Facebook, Twitter e YouTube hanno chiesto all'azienda di cessare la raccolta di foto dai loro siti e di cancellare quelle precedentemente

[26] Garante per la Protezione dei Dati Personali, Ordinanza 10 febbraio 2022, n. 50.
[27] J. CONDEMI, *op. cit.*
[28] J. CONDEMI, *op. cit.*

acquisite. Ciononostante, *Clearview* non vi ha ancora provveduto, giacché, come dichiarato al *Washington Post* dallo stesso Hoan Ton-That, «il modo in cui raccogliamo le immagini sia proprio come qualsiasi altro motore di ricerca. E questa è roba di dominio pubblico. Gli scopi per cui vengono usate penso possano essere di vero beneficio alla società»[29].

Orbene, in occasione di una presentazione finanziaria risalente a dicembre 2021, ottenuta dal *Washington Post*, si è giunti a una constatazione sconcertante riguardante le previsioni della società: nell'arco di un breve periodo, il database avrebbe contato più di 100 miliardi di foto e l'attività si sarebbe estesa oltre la mera scansione di volti per la polizia, operando anche l'identificazione tramite il movimento o la geolocalizzazione da una fotografia[30].

Le principali criticità di questo sistema possono essere riassunte come segue.

In primo luogo, l'applicazione si serve di dati biometrici, i quali, come anticipato, costituiscono informazioni distintive di un individuo che lo caratterizzano in maniera unica rispetto a qualunque altro essere vivente; perciò, è fondamentale prestare rilevante attenzione circa la necessità e la proporzionalità del loro trattamento.

In secondo luogo, l'attività condotta dalla società comprende un numero inestimabile di foto ritraenti numerose persone del tutto ignare dell'uso che potrebbe esserne fatto, senza avere alcun controllo sui loro dati personali.

Infine, risulta piuttosto sconcertante la scarsità di informazioni riguardanti la reale attività dell'azienda, che fa un uso illecito dei dati di cui dispone, senza una concreta base giuridica, non potendo questa coincidere con il solo legittimo interesse della società stessa.

Alla luce delle numerose infrazioni commesse, oggi *Clearview AI* sta affrontando diverse cause legali negli Stati Uniti, e ne è stato precluso l'utilizzo, in quanto ritenuto illegale, in Canada[31], Francia[32], Australia[33], Regno Unito[34] e Italia [35]. Come se non bastasse, questi ultimi due Paesi hanno anche applicato ingenti sanzioni; in particolare, in Italia, il Garante per la protezione dei dati personali ha sanzionato la società al pagamento di 20 milioni di euro «per aver messo in atto un vero e proprio monitoraggio biometrico anche di persone che si trovano nel territorio italiano»[36].

---

[29] J. CONDEMI, *op. cit.*

[30] J. CONDEMI, *op. cit.*

[31] Commission d'accès à l'information du Québec, Décision du 14 décembre 2021; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (OPC), *PIPEDA Findings #2021-001*, 2 febbraio 2021, disponibile al link https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/#toc9 (ultima consultazione 5/10/2023).

[32] Commission Nationale de l'Informatique et des Libertés (CNIL), Décision n° MED-2021-134 du 26 novembre 2021 mettant en demeure la société CLEARVIEW AI.

[33] Australian Information Commissioner and Privacy Commissioner, Decision of 14 October 2021.

[34] Information Commissioner's Office (ICO), Enforcement notice 18 may 2022.

[35] J. CONDEMI, *op. cit.*

[36] Garante per la Protezione dei Dati Personali, Ordinanza 10 febbraio 2022, n. 50.

Il provvedimento di febbraio 2022, frutto di un'istruttoria avviata anche a seguito di diverse segnalazioni, comprende, inoltre, l'obbligo di cancellazione dei dati dei cittadini italiani, il divieto di ulteriori raccolte e trattamento dati attraverso il sistema di riconoscimento facciale, e l'obbligo di designazione di un rappresentante presente nel territorio dell'Unione Europea che funga da interlocutore, in aggiunta o sostituzione del titolare del trattamento dati con sede negli Stati Uniti, in modo da agevolare l'esercizio dei diritti degli interessati[37].

Ciononostante, il sistema di riconoscimento facciale *Clearview* è stato recentemente impiegato dall'Ucraina, come strumento di supporto al servizio delle forze militari durante i combattimenti che interessano il Paese da ormai un anno a questa parte. Il ministro della Difesa ucraino ha, infatti, dichiarato che la società avrebbe loro offerto gratuitamente i suoi servizi per individuare potenziali spie o infiltrati russi al posto di blocco, combattere la disinformazione e identificare i morti sul campo. Inoltre, le autorità di Kiev si sarebbero servite di questo strumento di riconoscimento facciale per verificare con una certa efficacia che i viaggiatori in Ucraina fossero esattamente chi dichiaravano[38]. Come reso noto dal New York Times, *Clearview AI* avrebbe anche tradotto l'applicazione in ucraino e creato più di 200 account per gli utenti di cinque agenzie governative ucraine, che hanno condotto più di 5000 ricerche[39].

Tuttavia, l'impiego di un software come questo, specialmente in un contesto di guerra, potrebbe rivelarsi a dir poco problematico e piuttosto invasivo, aprendo scenari drammatici, dal momento che i sistemi di AI forniscono, il più delle volte, indicazioni errate, nonché i cd. falsi positivi, costituendo, così, un rischio potenziale per la protezione dei diritti e delle libertà fondamentali. É, infatti, possibile che questo sistema di riconoscimento facciale identifichi erroneamente le persone ai posti di blocco o in battaglia, comportando l'uccisione di civili innocenti, così come arresti del tutto ingiustificati da parte delle forze armate ucraine[40].

La società *Clearview* avrebbe trovato nella guerra in Ucraina una via d'uscita dalla difficile situazione in cui versa attualmente, provando, così, a riscattarsi agli occhi dell'opinione pubblica.

Come dichiarato dallo stesso Evan Greer, vicedirettore del gruppo per i diritti digitali *Fight for the Future*, si teme che queste zone di guerra costituiscano un mero campo di prova per normalizzare l'uso di detti

[37] *Ibidem*.

[38] *Ucraina ha iniziato a usare il riconoscimento del volto di Clearview AI*, in *ANSA*, 25 marzo 2022, disponibile al link 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 (ultima consultazione 6/10/2023).

[39] K. HILL, *Facial Recognition Goes to War*, in *The New York Times*, 07 aprile 2022, disponibile al link https://www.nytimes.com/2022/04/07/technology/facial-recognition-ukraine-clearview.html (ultima consultazione 6/10/2023).

[40] L. MISCHITELLI, *Il riconoscimento facciale di Clearview aiuta l'Ucraina? Ecco i rischi*, in *Agenda Digitale*, 30 marzo 2022, disponibile al link https://www.agendadigitale.eu/sicurezza/privacy/il-riconoscimento-facciale-di-clearview-aiuta-lucraina-ecco-i-rischi/ (ultima consultazione 30/03/2022).

strumenti di sorveglianza a dir poco cruenti e dannosi, i quali verrebbero, così, successivamente dispiegati sulla popolazione civile o utilizzati per scopi di applicazione della legge o di controllo di massa[41].

3. È possibile l'applicazione di "Clearview" in Europa?

Ai sensi della normativa europea in materia di protezione dei dati, i dati biometrici sono considerati particolarmente sensibili e il loro trattamento è vietato, salvo per motivi di "interesse pubblico rilevante" e nel pieno rispetto di rigorosi requisiti di necessità e proporzionalità.

Secondo un'indagine condotta dall'Agenzia per i diritti fondamentali, l'83% degli europei si oppone alla condivisione dei dati relativi al proprio volto con enti pubblici, mentre il 94% è contrario a condividerli con soggetti privati[42].

Eppure, i dati biometrici vengono sempre più spesso utilizzati dalle autorità di contrasto e dagli enti pubblici, nazionali ed europei, nonché da soggetti privati, per identificare o profilare le persone negli spazi pubblici.

Invero, le limitate tutele previste dalla vigente normativa dell'UE non garantiscono la trasparenza del trattamento dei dati biometrici, tantomeno ne impediscono usi che costituiscono intrinsecamente una sorveglianza di massa sproporzionata.

Come se non bastasse, i principi generali della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie rimettono agli Stati membri la facoltà di consentire, nel diritto nazionale, usi della biometria che potrebbero sconfinare in attività di sorveglianza di massa. Ciò contrasta in maniera evidente con gli obblighi che incombono sugli Stati membri, ai sensi della normativa dell'UE in materia di protezione dei dati e delle tutele costituzionali nazionali per i diritti fondamentali[43].

Tutta questa crescente preoccupazione per la lesione dei diritti personali ha portato ad includere, all'interno dell'AI Act, i sistemi che utilizzano dati biometrici all'interno dei cd. sistemi ad alto rischio, collocandosi sulla scia già tracciata dall'art. 9 GDPR.

L'AI Act è il primo a evidenziare come l'Intelligenza Artificiale, date le sue caratteristiche specifiche, quali opacità, complessità, dipendenza dai dati, e comportamento autonomo, possa incidere negativamente su una serie di diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, meglio nota come Carta di Nizza.

---

[41] C. ROSSI, *Ecco come l'Ucraina utilizza il software Clearview AI in guerra*, 14 aprile 2022, disponibile al link https://www.startmag.it/innovazione/ucraina-utilizza-il-software-per-riconoscimento-volto-di-clearview-ai/ (ultima consultazione 14/04/2022).

[42] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Fundamental Rights Report 2020*, 11 Giugno 2020, disponibile al link https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-report-2020-opinions_it.pdf (ultima consultazione 6/10/2023).

[43] D. J. NARANJO BARROSO, *Iniziativa della società civile per il divieto delle pratiche di sorveglianza biometrica di massa*, 07 gennaio 2021, disponibile al link https://europa.eu/citizens-initiative/initiatives/details/2021/000001_it (ultima consultazione 6/10/2023).

La presente proposta si pone l'obiettivo di assicurare un livello elevato di protezione dei diritti fondamentali e affrontare varie fonti di rischio, attraverso un approccio basato sul rischio chiaramente definito[44].

Quindi, definendo una serie di requisiti per un'IA affidabile e di obblighi proporzionati per tutti i partecipanti alla catena del valore, questa proposta migliorerà e promuoverà la protezione dei diritti tutelati dalla Carta, nonché: il diritto alla dignità umana (articolo 1), al rispetto della vita privata e alla protezione dei dati di carattere personale (articoli 7 e 8), alla non discriminazione (articolo 21) e alla parità tra donne e uomini (articolo 23).

Suddetta proposta di regolamento mira a prevenire un effetto dissuasivo sui diritti alla libertà di espressione (articolo 11) e alla libertà di riunione (articolo 12), nonché ad assicurare la tutela del diritto a un ricorso effettivo e a un giudice imparziale, della presunzione di innocenza e dei diritti della difesa (articoli 47 e 48), così come il principio generale di buona amministrazione.

Inoltre, ai sensi dell'articolo 52, paragrafo 1, della Carta di Nizza, qualsiasi limitazione all'esercizio dei diritti ivi garantiti dev'essere prevista dalla legge, proporzionata e rispondente a obiettivi d'interesse generale o alla necessità di tutelare i diritti e la libertà altrui: di conseguenza, la proporzionalità nell'uso di sistemi che, come quello di *Clearview,* vanno inevitabilmente a ledere e comprimere i diritti fondamentali qui considerati è essenziale.

Proprio per evitare sbilanciamenti di interessi, la proposta di regolamento dell'Intelligenza Artificiale dedica il Titolo III all'individuazione di regole specifiche per i sistemi di IA che creano un rischio alto per la salute e la sicurezza, o per i diritti fondamentali delle persone fisiche.

In linea con un approccio basato sul rischio, questa particolare categoria di sistemi di IA è consentita sul mercato europeo subordinatamente al rispetto di determinati requisiti obbligatori e ad una valutazione della conformità *ex ante*. In altre parole, il loro utilizzo non è proibito, ma soggetto a una serie di condizioni vincolanti che includono, tra l'altro, l'attuazione di un sistema di gestione del rischio e pratiche adeguate di *governance* e gestione dei dati, nonché la garanzia di trasparenza, e un'adeguata supervisione umana.

In ogni caso, la classificazione di un sistema di IA come ad alto rischio non dipende soltanto dalla funzione svolta, ma anche dalle finalità e modalità specifiche di utilizzo dello stesso[45].

Posta questa premessa, è facile rilevare che l'applicazione in Europa di un sistema come quello di *Clearview* potrebbe risultare decisamente problematica e le criticità emergono, in prima battuta, come già accennato,

[44] Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione (COM (2021) 206 final.
[45] *Ibidem*.

dai contrasti che sorgerebbero con il GDPR, il quale già all'articolo 9, pone come regola generale il divieto di trattamento di questi dati biometrici, essendo fortemente identificativi.

Ciò si osserva specialmente nell'ipotesi in cui *Clearview* e simili sistemi siano utilizzati in tempo reale[46], nel qual caso, sul territorio comunitario, ne sarebbe tendenzialmente proibito l'utilizzo per finalità di contrasto in luoghi aperti al pubblico, salve le dovute eccezioni in seguito riportate, in quanto qualificabile come sistema a rischio inaccettabile.

Non si potrebbe giungere alla medesima conclusione nel caso in cui, al contrario, il sistema sia utilizzato a posteriori[47], in quanto inquadrabile nella diversa disciplina prevista per quelli ad alto rischio.

Partendo dall'analisi della prima possibilità, si può notare come l'AI Act, condividendo il potenziale rischio nascente dall'uso di suddetti dati, qualifichi i sistemi di identificazione biometrica remota come a rischio inaccettabile e, in questo caso, ne escluda l'applicazione. Infatti, l'articolo 5 par. 1 lett. d) afferma espressamente come siano: «vietate le pratiche di intelligenza artificiale seguenti: (...) l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto»[48].

L'espressione "sistemi di identificazione biometrica remota" indica, infatti, quel sistema di intelligenza artificiale volto all'identificazione dei soggetti attraverso il mero confronto dei loro dati biometrici, tratti dalle loro caratteristiche fisiologiche o comportamentali, con le informazioni contenute in una banca dati di riferimento[49], e «senza che l'utente del sistema di IA sappia in anticipo se la persona sarà presente e può essere identificata»[50].

Il software *Clearview* rientrerebbe, quindi, in questa categoria e, perciò, quando utilizzato in questo modo, subirebbe una prima battuta d'arresto all'ingresso in Europa.

In ogni caso, la regola generale di divieto di utilizzo dell'intelligenza artificiale per sistemi di identificazione biometrica remota "in tempo reale" in luoghi accessibili al pubblico a fini di contrasto, non va esente da eccezioni.

---

[46] Art. 3, par. 1, n. 37, proposta di Regolamento (UE) in materia di intelligenza artificiale: «*sistema di identificazione biometrica remota "in tempo reale"": un sistema 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*».

[47] Art. 3, par. 1, n. 38, proposta di Regolamento (UE) in materia di intelligenza artificiale: «*sistema di identificazione biometrica remota "a posteriori"": un sistema di identificazione biometrica remota diverso da un sistema di identificazione biometrica remota "in tempo reale*».

[48] Art. 5, par.1, lett. d), proposta di Regolamento (UE) in materia di intelligenza artificiale.

[49] G. RAMINA, *Riconoscimento facciale e intelligenza artificiale nella proposta di regolamento europeo sull'IA*, 10 maggio 2021, disponibile al link https://www.smartius.it/data-it-law/riconoscimento-facciale-intelligenza-artificiale-proposta-regolamento-europeo/ (ultima consultazione 10/05/2023).

[50] Art. 3, par. 1, n. 36, proposta di Regolamento (UE) in materia di intelligenza artificiale.

L'AI Act cerca, infatti, di condensare la necessità di tutelare i diritti delle persone che si troverebbero fortemente lesi dall'impiego dei suddetti sistemi, con la consapevolezza che l'apporto degli stessi potrebbe essere molto utile in ambiti come quello della sicurezza nazionale.

Per questo motivo, l'articolo 5 par. 1 lett. d) prosegue affermando come questi sistemi di Intelligenza Artificiale siano vietati «a meno che e nella misura in cui tale uso sia strettamente necessario per uno dei seguenti obiettivi:

1. La ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi;
2. La prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico;
3. Il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni, come stabilito dalla legge di tale Stato membro»[51].

Queste eccezioni, però, richiedono anche il rispetto di altri due requisiti indicati al par. 2:

1. «La natura della situazione che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del danno causato dal mancato uso del sistema;
2. Le conseguenze dell'uso del sistema per i diritti e le libertà di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze».

Devono, inoltre, essere rispettate «le tutele e le condizioni necessarie e proporzionate in relazione all'uso, in particolare per quanto riguarda le limitazioni temporali, geografiche e personali»[52].

Notiamo, quindi, come il sistema di *Clearview* esuli da quest'applicazione circoscritta. Infatti, il suo impiego è indipendente dalle circostanze concrete e non fa seguito ad una valutazione degli interessi in gioco, bensì effettua un controllo indiscriminato sulla popolazione: raccoglie immagini senza il consenso delle persone rappresentate, vendendole ai clienti che potranno, quindi, utilizzarle per qualsiasi fine. Ciò comporta che, inevitabilmente, il sistema di cui trattasi non abbia alcuna ragion d'essere, in quanto lo sbilanciamento che ne deriverebbe nei confronti dei diritti fondamentali sarebbe eccessivo e del tutto ingiustificato rispetto alle prevalenti necessità che ne consentirebbero l'applicazione e che l'AI Act identifica nelle eccezioni sopra riportate.

[51] Art. 5, par. 1, lett. d), proposta di Regolamento (UE) in materia di intelligenza artificiale.
[52] Art. 5, par. 1, lett. d), proposta di Regolamento (UE) in materia di intelligenza artificiale.

Il paragrafo 3 aggiunge anche un requisito formale: l'utilizzo di questi sistemi necessita, pur rispettando quanto indicato dai paragrafi 1 lett. d) e 2, di «un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e in conformità alle regole dettagliate del diritto nazionale di cui al paragrafo 4».

Tuttavia, se per situazioni d'urgenza, che dovranno comunque essere debitamente giustificate, non è possibile ottenere preventivamente suddetta autorizzazione, è consentito iniziare ad utilizzare il sistema di rilevazione biometrica e richiederne il rilascio durante o dopo il suo impiego.

É interessante osservare come l'AI Act cerchi di bilanciare le potenzialità di questi strumenti, specialmente nell'ambito della sicurezza nazionale, ma, al contempo, conscio dei problemi che l'IA potrebbe produrre, provi a tutelare i diritti fondamentali delle persone[53].

In realtà, non tutte le tecniche biometriche sono annoverate tra quelle ad alto rischio ex Titolo III; da queste dobbiamo, infatti, distinguere quelle diverse dall'identificazione biometrica, come il riconoscimento delle emozioni e la categorizzazione biometrica, che, presentando un particolare rischio di trasparenza, sono sottoposte alla disciplina del Titolo IV.

Ai sensi dell'art. 52, co. 2, della proposta di AI Act, i sistemi di riconoscimento delle emozioni e di categorizzazione biometrica richiedono particolari misure di trasparenza, ragion per cui l'utilizzatore di tali sistemi deve fornire informazioni sul loro funzionamento a coloro che ne sono esposti.

Tuttavia, è importante precisare che i livelli di rischio non si escludono a vicenda. Ciò significa che i sistemi di riconoscimento delle emozioni e quelli di categorizzazione biometrica sono normalmente soggetti solo al Titolo IV, ma, laddove si qualifichino come sistemi ad alto rischio alla luce del loro scopo concreto, devono soddisfare anche i requisiti elencati all'interno del Titolo III[54], in cui, oltre alla più rigida disciplina a cui è già stato cenno, sono contenute molteplici disposizioni applicabili specificamente alle tecniche biometriche.

L'art. 12, par. 4 prevede che, per i sistemi di identificazione biometrica e di categorizzazione, le capacità di registrazione comprendano, come minimo, la registrazione del periodo di ciascun utilizzo del sistema (data e ora di inizio e data e ora di fine di ciascun utilizzo), il *database* di riferimento rispetto al quale i dati di input sono stati verificati dal sistema, i dati di input per i quali la ricerca ha portato a una corrispondenza, e l'identificazione delle persone fisiche coinvolte nella verifica dei risultati.

[53] Art. 5, par. 1, lett. d), proposta di Regolamento (UE) in materia di intelligenza artificiale.

[54] Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, *Biometric Recognition and Behavioural Detection*, *Policy Department for Citizens' Rights and Constitutional Affairs*, agosto 2021, disponibile al link https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2021)696968 (ultima consultazione 6/10/2023).

L'art. 14, par. 5 sancisce che, per tali sistemi, le misure di controllo umano siano tali da garantire che, inoltre, l'utente non adotti alcuna azione o decisione sulla base dell'identificazione risultante dal sistema, a meno che ciò non sia stato verificato e confermato da almeno due persone fisiche. Non sarebbe, quindi, possibile utilizzare l'identificazione derivante dal sistema come base per avviare un'indagine, un procedimento penale, o per sottoporre il soggetto a misure preventive limitative della libertà personale.

La scelta effettuata nell'AI Act trova una propria ragion d'essere nel rischio di errore da parte del sistema che, come già detto in apertura, diventa inaccettabile se incidente sulla libertà personale.

Per giunta, è importante notare che, mentre i sistemi di IA autonomi ad alto rischio sono normalmente soggetti a una valutazione di conformità attuata tramite verifiche di controllo interno da parte dei fornitori; i sistemi di identificazione biometrica remota sono per lo più soggetti a valutazione di conformità da parte di terzi[55].

Si constata che la proposta AI Act non tratta in modo esaustivo questi sistemi. Per questa ragione è comunque necessaria la combinazione della disciplina prevista dal GDPR e quella contenuta nell'AI Act. La prima si applicherà al trattamento dei dati biometrici, mentre la seconda verrà attuata in riferimento all'utilizzo di questi dati ai fini di formazione, convalida e test dei sistemi di intelligenza artificiale[56].

Come accennato in apertura, *Clearview* e simili sistemi di rilevazione biometrica potrebbero essere utilizzati non soltanto ai fini di rilevazione biometrica in tempo reale, ma anche a posteriori.

La disciplina fissata dall'AI Act per i sistemi di identificazione biometrica remota a posteriori è differente rispetto a quella appena analizzata, applicabile a quelli che operano in tempo reale.

La principale differenza è data dalla diversa qualificazione che ne viene data: i sistemi di identificazione biometrica in tempo reale sono definiti a rischio inaccettabile dall'articolo 5 par. 1 lett. d) con le dovute eccezioni già analizzate; invece, i sistemi che operano a posteriori sono definiti ad alto rischio, in quanto lesivi dei diritti fondamentali delle persone[57], e vengono disciplinati dalle disposizioni del Titolo III.

L'applicazione di suddetti sistemi non viene, quindi, proibita di *default*, bensì è consentita solo ed esclusivamente se si rispettano tutti gli obblighi ivi indicati, come quelli di: i) conformità ai requisiti; ii) gestione dei rischi; iii) governance dei dati; iv) documentazione tecnica; v) conservazione delle registrazioni; vi) trasparenza; vii) sorveglianza umana; viii) accuratezza, robustezza, cybersicurezza.

[55] Art. 43, par. 1, proposta di Regolamento (UE) in materia di intelligenza artificiale.
[56] *Ibidem*.
[57] Ad esempio, il diritto alla riservatezza, all'immagine, alla dignità umana, alla vita privata, e molti altri ancora.

Rispettando questi requisiti e gli obblighi previsti per i fornitori (come quelli di redazione di documentazione tecnica o quelli di qualità), sistemi che effettuano un'autenticazione biometrica remota a posteriori potrebbero, in potenza, essere utilizzati.

Tuttavia, in riferimento al caso di specie, non si potrebbe affermare altrettanto: *Clearview* non rispetta molti dei requisiti indicati al Capo II del Titolo III dell'*AI Act*, soprattutto con riguardo al criterio della trasparenza.

Per comprendere le problematicità connesse all'applicazione di un sistema come questo, seppur a posteriori, seguirà un breve *excursus*.

Come anticipato al § 2, la società statunitense è stata centro di un'inchiesta a causa di *data breach*, nonché una violazione di dati personali, raccolti indiscriminatamente, senza alcun tipo di consenso delle persone coinvolte.

L'attività condotta prevede un uso (poi rilevatosi un "abuso") improprio di una quantità inestimabile di immagini (raccolte nel *database* del sistema il cui accesso veniva venduto ai clienti abbonatisi) ritraenti innumerevoli persone del tutto ignare dell'utilizzo che ne sarebbe stato fatto. Più in generale, potremmo dire che non avevano alcun controllo sui loro dati personali, non essendovi informazioni riguardanti la reale attività dell'azienda, la quale aveva omesso di fornire gran parte della documentazione tecnica, invece, richiesta dalla normativa vigente sul territorio europeo[58].

È evidente vi sia una vera e propria violazione del principio di trasparenza, connessa alla necessarietà, espressa dall'art. 13, par. 2 dell'AI Act, che i sistemi di IA "ad alto rischio" siano «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»[59]. Nella vicenda *Clearview* non avevamo alcuna di queste indicazioni, poiché gli usi derivanti dall'applicazione di questo sistema erano dei più disparati e, soprattutto, non circoscritti, potendo essere adoperato sia in tempo reale (utilizzo per eccellenza) sia a posteriori, e per qualsivoglia finalità, comportando, così, la rilevazione di numerosi profili problematici a livello costituzionale.

Tuttavia, quello della trasparenza non è l'unico requisito che, a detta di chi scrive, non è stato rispettato; infatti, l'art. 14, par. 1 dell'AI Act afferma che: «i sistemi di IA ad alto rischio sono progettati e sviluppati, anche con 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»[60].

[58] Art. 11, proposta di Regolamento (UE) in materia di intelligenza artificiale.
[59] Art. 13 par. 2, proposta di Regolamento (UE) in materia di intelligenza artificiale.
[60] Art. 14 par. 1, proposta di Regolamento (UE) in materia di intelligenza artificiale.

Nel caso di cui trattasi, la sorveglianza umana non era presente, anzi, il software operava autonomamente, effettuando un'attività di *matching* senza che vi fosse alcun controllo da parte di un soggetto preposto a questa mansione o dell'utilizzatore stesso.

La disposizione prosegue indicando come «la sorveglianza umana miri a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile […]»[61]. Nella fattispecie in oggetto, il problema sorge già a monte, data la mancata indicazione delle finalità perseguite dal sistema.

Alla luce di ciò, anche se potrebbero essere analizzati molti altri requisiti per i quali sarebbe necessaria un'approfondita trattazione a sé stante, si intuisce come, pur non potendo escludere a priori l'applicazione di un sistema di rilevazione biometrica operante a posteriori, sia necessario verificare se, in concreto, siano rispettate tutte le necessarie prescrizioni contenute nel Titolo III, volte ad effettuare un'opera di bilanciamento tra l'impiego di simili strumenti d'indubbia utilità, ma potenzialmente lesivi di taluni diritti fondamentali, e la protezione di questi ultimi.

Il mancato adeguamento a suddetti requisiti comporta l'inevitabile esclusione dell'applicazione del sistema, in quanto, altrimenti, comprimerebbe in maniera significativa la tutela dei diritti fondamentali, garantiti *in primis* dalla cd. Carta di Nizza e dalle Costituzioni dei singoli Stati membri.

L'analisi fin qui svolta si rivela utile per rispondere al principale quesito posto in questo elaborato: allo stato attuale della legislazione, tenuto conto della proposta di regolamento *AI Act*, potrebbe essere legittimamente applicato un sistema di intelligenza artificiale basato sulla rilevazione biometrica, così come effettuata da *Clearview AI*?

Dal nostro punto di vista, la risposta non può che essere negativa, almeno con riguardo al suo utilizzo in tempo reale. Le eccezioni di cui all'art. 5 par. 1 lett. d) non sono applicabili al caso in esame, non essendoci il supporto dei requisiti previsti dal paragrafo 2.

Infatti, il software *Clearview* effettua un controllo continuo e indiscriminato, non certo limitato a singole situazioni concretamente considerate, quali una specifica notizia di reato, o la ricerca di una determinata vittima, senza, quindi, nemmeno cercare di comprendere se suddetto intervento, rispetto al risultato finale, sia proporzionato o si tratti di un'inaccettabile limitazione dei diritti fondamentali delle persone.

Un sistema come questo rischierebbe di alimentare una vera e propria sorveglianza di massa, incrementando il già citato fenomeno del *Big Brother*, che provocherebbe costante frustrazione nelle persone, oltre a una

[61] Art. 14 par. 2, proposta di Regolamento (UE) in materia di intelligenza artificiale.

persistente violazione di diritti, che verrebbero, a questo punto, rispettati soltanto in astratto, senza riuscire a garantirne un'applicazione concreta. Infatti, «La sorveglianza produce effetti non solo individuali, ma anche profondamente sociali. La stessa ci rende visibili ad altri sconosciuti in modi che non hanno precedenti, e attraverso l'analisi dei dati da parte degli algoritmi», coloro che riescono ad entrare in possesso di suddetti dati acquisiscono un enorme potere di controllo[62].

Sarebbe, quindi, auspicabile individuare un punto di equilibrio, che consenta di sfruttare al meglio le grandi potenzialità intrinseche di questi software, previa valutazione delle circostanze e soltanto in caso di proporzionalità dell'intervento, tali da giustificare la limitazione di taluni importanti diritti fondamentali.

In realtà, anche qualificando il sistema di *Clearview AI* come sistema ad alto rischio, quindi impiegato ai soli fini dello svolgimento di un'autenticazione biometrica a posteriori, non potrebbe, quantomeno allo stato attuale del sistema, trovare cittadinanza all'interno dell'ordinamento dell'Unione europea, non presentando la maggior parte dei requisiti richiesti dal Titolo III dell'AI Act, idonei a garantire una riduzione della lesione dei diritti fondamentali, a cui purtroppo assistiamo.

Concludendo, si evince come la possibilità di applicare questi sistemi sia molto complessa, specialmente in un contesto, come quello europeo, ove vigono condizioni stringenti, finalizzate alla salvaguardia degli interessi dei cittadini e dei loro diritti.

Da questo punto di vista, l'AI Act potrebbe sicuramente essere visto come un primo importante tentativo di bilanciamento di dette esigenze.

[62] S. PIERANNI, *op. cit.*