SEGNALAZIONE AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

–

RICHIESTA DI VALUTAZIONE DEL TRATTAMENTO DI DATI SVOLTO DA CLEARVIEW AI, INC.

I. Introduzione e scopo della presente segnalazione

1. Con la presente, l'Associazione Hermes ("**Centro Hermes**") fornisce prove e analisi al Garante per la protezione dei dati personali ("**Autorità**") al fine di assisterlo nelle indagini in corso sulla conformità di Clearview AI, Inc. ("**Clearview**") alla normativa in materia di protezione dei dati, in particolare il Regolamento Generale per la protezione dei dati personali (EU) 2016/679 ("**GDPR**"), il Codice in materia di protezione dei dati personali ("**Codice**"), la direttiva UE 2016/680 e il d.lgs. 18 maggio 2018, n. 51 ("**Decreto**").

2. Le pratiche di Clearview e le modalità di utilizzo dei dati della sua piattaforma danno luogo a continue violazioni sostanziali del GDPR, del Codice e del Decreto. Dopo le sezioni introduttive, la presente segnalazione si concentra sulle due fasi principali che caratterizzano l'impatto di Clearview sugli interessati in Italia: (1) il trattamento iniziale dei dati personali da parte di Clearview mediante la raccolta, la conservazione e l'identificazione (sezione V), e (2) l'utilizzo dei servizi di Clearview da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (sezione VI).

II. Associazione Hermes

3. Il Centro Hermes per la trasparenza e i diritti umani digitali è un'associazione senza scopo di lucro con base in Italia. Dal 2012 l'associazione promuove e sviluppa conoscenza sulle tematiche del whistleblowing, della trasparenza, dei diritti umani digitali e della privacy. La visione di Hermes è fortemente legata alla cultura dell'open source e dei software liberi. I diritti digitali sono diritti umani e per questo Hermes ha come missione la loro difesa e promozione, attraverso attività di divulgazione e azioni concrete e mirate. La protezione dei dati personali è uno dei pilastri di una società libera e democratica, per questo motivo è al centro di diverse iniziative dell'associazione.

III. Il Titolare del trattamento - Clearview AI, Inc.

4. Clearview AI, Inc. è una società con sede legale negli Stati Uniti, costituita nel 2017. Il suo unico prodotto è una piattaforma di riconoscimento facciale che permette agli utenti di abbinare foto di persone a loro immagini reperite online. La piattaforma "include un database di oltre 3 miliardi di immagini facciali estratte da fonti web pubbliche, inclusi mezzi di informazione, siti web di foto segnaletiche, social media pubblici e altre fonti di pubblico accesso."[1]

5. Nel 2020, Clearview aveva circa 2.900 utenti attivi. Nonostante tutti i suoi materiali di marketing pubblicamente disponibili fossero destinati alle forze di polizia, i clienti di Clearview, a quanto riferito, variavano dagli "uffici per la sicurezza dei college agli uffici dei Procuratori Generali" e includevano "un numero notevole di società private in settori quali l'intrattenimento (Madison Square Garden e Eventbrite), giochi d'azzardo (Las Vegas Sands e Pechanga Resort Casino), sport (NBA), fitness (Equinox) e persino criptovalute (Coinbase)."[2] Secondo alcune fonti, la piattaforma Clearview sarebbe stata utilizzata anche da privati cittadini, che a quanto riferito avrebbero utilizzato "l'applicazione ad appuntamenti e feste – e per spiare il pubblico".[3]

Descrizione tecnica del database di immagini e del prodotto di Clearview

6. Secondo la nostra indagine e analisi delle fonti pubblicamente disponibili[4], e le nostre competenze tecniche, risulta che il database di immagini creato da Clearview per la sua piattaforma di riconoscimento facciale viene popolato in quattro fasi:

    1) ***Web scraping* automatico delle immagini** – uno strumento automatizzato cerca nelle pagine web pubblicamente accessibili e raccoglie qualsiasi immagine contenente volti umani. Insieme alle immagini, lo strumento di *web scraping* raccoglie anche i metadati ad esse associati, ad esempio il titolo dell'immagine o della pagina web, il link alla fonte, e la geolocalizzazione[5].

---

[1] 'Overview' (Clearview AI). Disponibile al seguente link https://clearview.ai/overview.

[2] BuzzFeed News, 'Clearview's Facial Recognition App Has Been Used by The Justice Department, ICE, Macy's, Walmart, And the NBA' (27 February 2020). Disponibile al seguente link https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

[3] Kashmir Hill, 'Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich' (The New York Times, 5 March 2020). Disponibile al seguente link https://www.nytimes.com/2020/03/05/technology/clearview-investors.html.

[4] Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001 (2 February 2021). Disponibile al seguente link: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/; Clearview AI, 'Law Enforcement' (Clearview AI Website). Disponibile al seguente link https://clearview.ai/law-enforcement; Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Letter to Clearview AI Inc. - Consultation prior to an order pursuant to Article 58(2)(g) GDPR (27 January 2021). Disponibile al seguente link https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.PDF.

[5] Clearview AI, Inc. Privacy Policy (versione 1, ultimo aggiornamento 20 marzo 2021). Disponibile al seguente link https://clearview.ai/privacy-policy

2) **Conservazione dell'immagine e dei metadati** - le immagini e i relativi metadati raccolti mediante il processo di *web scraping* vengono conservati sui server di Clearview. La conservazione è a tempo indeterminato, cioè permane anche dopo che la foto precedentemente raccolta o la pagina web su cui si trovava è stata rimossa o resa privata.

3) **Estrazione delle caratteristiche facciali mediante reti neurali di elaborazione delle immagini** – ogni volto contenuto in ciascuna immagine raccolta viene scansionato ed elaborato per estrarne le caratteristiche identificative. I volti vengono tradotti in rappresentazioni numeriche qui denominate "vettori". Questi vettori sono costituiti da 512 punti dati che rappresentano le diverse linee uniche che formano un volto. A questo punto, i volti vengono convertiti da immagini riconoscibili all'occhio umano a identificatori numerici biometrici unici leggibili elettronicamente dalle macchine.

4) **Conservazione e indicizzazione/*hashing* delle caratteristiche facciali** - Clearview conserva i vettori in un database sui propri server, lì sono associati alle immagini e alle altre informazioni raccolte tramite *web scraping*. Questi vettori vengono quindi sottoposti ad *hashing* (tecnica che consiste nella trasformazione, mediante una funzione matematica, di un vettore in un valore di lunghezza fissa più breve o in una chiave che rappresenta il vettore originale), per due finalità correlate: l'indicizzazione del database e l'identificazione futura dei volti. Ciascuna foto di un volto nel database ha un diverso vettore e un valore *hash* a esso associato per permetterne l'identificazione e il *matching*.

7. La quinta e ultima fase nel ciclo del prodotto Clearview è il ***matching***. Viene eseguito quando un utente di Clearview desidera identificare una persona e a tale scopo carica un'immagine del soggetto stesso e avvia una ricerca. A questo punto la piattaforma di Clearview analizza l'immagine, estrae un vettore dal volto del soggetto, lo sottopone quindi ad *hashing* e lo confronta con tutti i vettori *hash* precedentemente salvati nel database. Infine, lo strumento Clearview estrae dal database dei vettori tutte le immagini che presentano una stretta corrispondenza e le mostra all'utente come risultato della ricerca insieme a tutti i metadati associati, permettendo all'utente di vedere la pagina sorgente originale da cui sono state estratte le immagini risultanti dal *matching*.

IV. Contesto

A. Le "rivelazioni" su Clearview e il conseguente interesse delle autorità preposte alla regolamentazione

8. Il 18 gennaio 2020, l'esistenza di Clearview è stata rivelata al mondo da un articolo apparso sul New York Times intitolato *"The Secretive Company That Might End Privacy as We Know It"* ("L'azienda segreta che potrebbe porre fine

alla privacy per come la conosciamo").[6] Prima di questo articolo, Clearview aveva mantenuto intenzionalmente riserbo sulla propria attività, offrendo il suo prodotto a "più di 600 forze di polizia" e "almeno una manciata di aziende per motivi di sicurezza".[7] A seguito di queste "rivelazioni", diverse organizzazioni e autorità preposte negli Stati Uniti (USA) e altrove hanno iniziato a esaminare la condotta di Clearview.

9. Negli Stati Uniti, "otto iniziative legali putative sono state presentate nei giorni successivi alla pubblicazione dell'articolo del Times e altre sono seguite".[8] A causa della mancanza di una legge federale sulla privacy negli Stati Uniti, queste azioni sono state intraprese a livello statale e secondo le normative dei singoli Stati. Una di queste iniziative è stata presentata nel maggio 2020 dalla ACLU (American Civil Liberties Union) in Illinois[9] ai sensi del Biometric Information Privacy Act (trad. Legge sulla privacy delle informazioni biometriche) (BIPA) di tale Stato, che regola la raccolta e l'utilizzo delle informazioni biometriche. Un'altra iniziativa è stata presentata a febbraio 2021 in California da attivisti per le libertà civili e gruppi per i diritti degli immigrati, che sostengono che le la condotta di Clearview violi i vari divieti locali sull'uso della tecnologia di riconoscimento facciale da parte del governo.[10]

10. In Canada, a febbraio 2020 l'Ufficio del Commissario in materia di protezione dei dati (Office of the Privacy Commissioner of Canada - "**OPCC**"), insieme alle autorità preposte alla regolamentazione sulla privacy a livello provinciale, ha avviato un'indagine sulla condotta di Clearview. Il rapporto sui risultati di tale indagine è stato pubblicato il 2 febbraio 2021 con la raccomandazione che Clearview (i) cessi di offrire i suoi servizi in Canada, (ii) "interrompa la raccolta, l'utilizzo e la divulgazione di immagini e matrici biometriche facciali di soggetti in Canada", e (iii) "cancelli le immagini e le matrici biometriche facciali raccolte dagli individui canadesi in suo possesso".[11]

11. Nel Regno Unito e in Australia, a luglio 2020 le autorità preposte alla regolamentazione in materia di protezione dei dati hanno avviato un'indagine

---

[6] Kashmir Hill, 'The Secretive Company That Might End Privacy as We Know It' (The New York Times, 18 January 2020). Disponibile al seguente link https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[7] Ibid.

[8] Sam Jungyun Choi et al, 'Clearview AI revelations spark action on use of facial recognition', Privacy Laws & Business International Report (August 2020). Disponibile al seguente link https://www.cov.com/-/media/files/corporate/publications/2020/08/clearview-ai-revelations-spark-action-on-use-of-facial-recognition.pdf.

[9] ACLU, 'ACLU sues Clearview AI' (28 May 2020). Disponibile al seguente link https://www.aclu.org/press-releases/aclu-sues-clearview-ai.

[10] CNN Business, 'Clearview AI sued in California by immigrant rights groups, activists' (10 March 2021). Disponibile al seguente link https://edition.cnn.com/2021/03/09/tech/clearview-ai-mijente-lawsuit/index.html.

[11] OPCC (n 4).

congiunta sulle “pratiche di gestione delle informazioni personali” di Clearview.[12]

12. Nella UE, diverse azioni sono state intraprese in vari Paesi. In Germania, un cittadino ha ottenuto dall'Autorità di protezione dei dati di Amburgo una notifica preventiva di intenti richiedendo a Clearview di cancellare il valore *hash* associato alle sue immagini facciali.[13] La decisione si limitava al singolo caso in questione e non richiedeva la cessazione delle attività di Clearview nel territorio di competenza. In Svezia, a febbraio 2021 l'Autorità statale per la protezione della privacy ha rilevato che l'autorità di polizia svedese aveva utilizzato illegalmente i servizi di Clearview e trattato i dati personali in violazione della Legge svedese sui dati penali, la direttiva sull'applicazione della direttiva Europea 2016/680 (Law Enforcement Directive -“**LED**”).[14] La vostra stessa Autorità ha inviato una richiesta di chiarimenti in merito al trattamento di dati biometrici e sulla condotta di Clearview.[15]

13. A seguito delle interrogazioni da parte dei Membri del Parlamento europeo che sollevavano timori riguardo a Clearview, il Comitato europeo per la protezione dei dati (European Data Protection Board - “**EDPB**”) ha emesso una valutazione preliminare il 10 giugno 2020.[16] Tale valutazione si incentrava sulla “conformità e la liceità del trattamento derivante dall'eventuale uso da parte delle autorità preposte all’applicazione della legge dell'UE di un servizio come quello offerto dalla Clearview AI” ed esprimeva seri dubbi al riguardo.

14. La quantità di casi diversi sollevati in Europa e altrove dimostra che le singole persone e le autorità preposte alla regolamentazione nutrono una viva e diffusa preoccupazione con riferimento alla condotta di Clearview. Tuttavia, ad oggi non sono stati profusi sforzi per adottare un approccio coordinato a questo problema prettamente globale. Un approccio coordinato è atteso da tempo in Europa, dove si vanta uno dei quadri normativi sulla privacy e la protezione dei dati più stringente al mondo. Un approccio frammentario sminuirebbe il valore e la forza del GDPR e della LED nell'assicurare a tutti i cittadini europei il medesimo livello di protezione della privacy.

---

[12] Information Commissioner’s Office, ‘The Office of the Australian Information Commissioner and the UK’s Information Commissioner’s Office open joint investigation into Clearview AI Inc.’ (9 July 2020). Disponibile al seguente link https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc.

[13] noyb, ‘Clearview AI’s biometric photo database deemed illegal in the EU, but only partial deletion ordered’ (28 January 2021). Disponibile al seguente link https://noyb.eu/en/clearview-ai-deemed-illegal-eu.

[14] Integritetsskydds myndigheten, ‘Police unlawfully used facial recognition app’ (11 February 2021). Disponibile al seguente link https://www.imy.se/nyheter/police-unlawfully-used-facial-recognition-app/.

[15] Wired, ‘Il Garante italiano della privacy indaga sulla più controversa società di riconoscimento facciale al mondo’ (15 April 2021). Disponibile al seguente link https://www.wired.it/attualita/tech/2021/04/15/riconoscimento-facciale-garante-privacy-clearview-ai/.

[16] EDPB, Letter to Members of the European Parliament (Ref: OUT2020-0052, 10 June 2020). Disponibile al seguente link https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-meps-sophie-t-veld-moritz-korner-michal-simecka_en.

B. Il trattamento di Clearview è soggetto al GDPR e al Decreto

15. Il Centro Hermes sostiene che la condotta del titolare del trattamento rientra sotto il disposto dell'Art. 3 par. 2 del GDPR, dato che in più occasioni è stato riferito che Clearview ha offerto i propri servizi sia a soggetti privati che alle autorità preposte all'applicazione della legge nella UE e ha monitorato il comportamento di cittadini all'interno della Unione, raccogliendo i loro dati personali. Inoltre, precedenti versioni del sito web e la condotta passata della società rispetto all'esercizio dei diritti da parte degli interessati confermano che Clearview ha agito in passato come se fosse soggetta agli obblighi imposti dal GDPR.

Il targeting dei clienti di Clearview ricade sotto l'Art. 3.2.a del GDPR

16. Innanzitutto, a febbraio 2020, secondo quanto riportato da BuzzFeed News sulla base di documenti visionati dalla stessa, il titolare del trattamento ha coinvolto "le forze dell'ordine, enti governativi e forze di polizia in Belgio, Danimarca, Finlandia, Francia, Irlanda, Italia, Lettonia, Lituania, Malta, Paesi Bassi, Portogallo, Slovenia, Spagna e Svezia".[17]

17. Nel caso dell'Italia, in un'interrogazione parlamentare a risposta scritta di gennaio 2020[18], il Ministero dell'Interno non ha fornito dettagli e chiarimenti sull'uso degli strumenti offerti da Clearview.[19]

18. Secondo quanto riportato da VICE Italia[20], la Direzione Centrale dei servizi tecnico-logistici e della Gestione patrimoniale del Ministero dell'Interno ha dichiarato che non esistono atti negoziali né evidenze di rapporti di interlocuzione con Clearview. Non è dato sapere però se le altre Direzioni del Ministero dell'Interno o singoli ufficiali abbiano testato gli strumenti di Clearview.

19. In secondo luogo, indipendentemente dal fatto che il software del titolare del trattamento fosse utilizzato da uno qualsiasi o tutti gli enti sopra menzionati in detti territori, è chiara l'intenzione del titolare del trattamento di rendere disponibili i propri servizi e promuoverli in Europa, rivolgendosi sia a soggetti privati che ad autorità preposte all'applicazione della legge come potenziali clienti. Per esempio, un documento ottenuto da BuzzFeed News mediante una richiesta di documenti pubblici ha rivelato che Clearview prospettava ai potenziali clienti una "rapida espansione internazionale" utilizzando una mappa

---

[17] BuzzFeed News (27 February 2020) (n 2).

[18] Testo interrogazione dell'On. Sensi https://aic.camera.it/aic/scheda.html?numero=4/04528&ramo=CAMERA&leg=18.

[19] Commento dell'On. Sensi alla risposta del Ministero https://twitter.com/nomfup/status/1225051423148253185.

[20] Vice Italia, 'Questa azienda 'segreta' di riconoscimento facciale ha delle mie foto e non so perché' (25 marzo 2020). Disponibile al link https://www.vice.com/it/article/4ag83j/clearview-ai-riconoscimento-facciale.

che mostrava come si era espansa o aveva intenzione di espandersi.[21] Il documento indica come target potenziali una serie di paesi dell'UE, inclusa l'Italia.

20. Questi rapporti e documenti evidenziano la "condotta del titolare del trattamento", dimostrando la sua "intenzione di offrire beni o servizi agli interessati nell'Unione", un elemento chiave per determinare se il criterio di *targeting* stabilito nell'Art. 3.2.a è stato soddisfatto.[22]

Il trattamento dei dati personali da parte di Clearview ricade sotto l'art. 3.2.b del GDPR

21. In terzo luogo, le risposte ricevute alle richieste di accesso ai dati personali ("DSAR") inviate secondo l'articolo 15 del GDPR mostrano che Clearview ha raccolto dati personali di interessati presenti in Europa e ha effettuato un trattamento che ricade nell'Articolo 3.2.b del GDPR. Come riportato da diversi giornali e associazioni, quali WIRED Italia[23], VICE Italia[24], e Privacy Network[25], le risposte ricevute contengono un file PDF con le foto dei soggetti accompagnate da link alle fonti dei siti web da cui sono state prese, e una breve descrizione dei siti web originali. Nella risposta, la società rinvia anche a una pagina web chiamata "Clearview Data Policy"[26] che dovrebbe fornire risposta alle varie domande inviate dagli interessati ma che, in pratica, offre informazioni generiche. In un caso, una delle foto inserite nel PDF è stata presa dalla foto profilo di una terza persona includendo anche parte del suo volto.[27]

22. La risposta di Clearview dimostra che, mediante il suo algoritmo di riconoscimento facciale, la società raccoglie e tratta sistematicamente i dati personali degli interessati che si trovano nella UE. Questa pratica equivale a monitorare il comportamento degli interessati nell'Unione e rientra precisamente nel requisito del Considerando 24 del GDPR, che stabilisce che "per determinare se un'attività di trattamento sia assimilabile al controllo del

---

[21] BuzzFeed News, 'Clearview AI Wants To Sell Its Facial Recognition Software To Authoritarian Regimes Around The World' (5 February 2020). Disponibile al seguente link https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-authoritarian-regimes-22.

[22] EDPB, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1' (12 November 2019). Disponibile al seguente link https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.

[23] Wired Italia, 'Ho scoperto che la più discussa società di riconoscimento facciale al mondo ha le mie foto' (23 marzo 2021). Disponibile al link https://www.wired.it/attualita/tech/2021/03/23/clearview-ai-riconoscimento-facciale-foto/.

[24] Vice Italia (25 marzo 2020) (n 20)

[25] Privacy Network, 'Come verificare se sei nel database di Clearview AI' (31 marzo 2021). Disponibile al link https://www.privacy-network.it/come-verificare-se-sei-nel-database-di-clearview-ai/

[26] Clearview AI, Inc. Clearview Data Policy. Disponibile al link https://staticfiles.clearview.ai/clearview_data_policy.html

[27] Vice Italia (25 marzo 2020) (n 20)

comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica".

23. In quarto luogo, il trattamento dei dati personali degli interessati dell'UE da parte del titolare del trattamento è indicato dai seguenti elementi rintracciabili sul sito web/piattaforma online dello stesso titolare: (a) un riferimento ai trasferimenti internazionali presente in una versione recente della *Privacy Policy* di Clearview - "Nel caso in cui i dati personali vengano trasferiti al di fuori dello SEE, verranno attuate idonee misure di protezione per assicurare che tale trasferimento sia conforme alle normative applicabili in materia di protezione dei dati"[28] - e (b) riferimenti espliciti al "General Data Protection Regulation" nelle Condizioni di servizio e nella *Privacy Policy* del titolare del trattamento.[29]

24. In quinto luogo, a seguito di un reclamo presentato da un interessato risiedente ad Amburgo, il Commissario per la protezione dei dati e la libertà d'informazione di Amburgo ("**HmbBfDI**"), in data 27 gennaio 2021, ha comunicato la sua intenzione di ordinare a Clearview di intraprendere alcune azioni per cancellare i dati dell'interessato. L'HmbBfDI ha riaffermato la propria competenza e l'applicazione del GDPR dopo aver concluso che Clearview effettua il monitoraggio del comportamento degli interessati nell'Unione, in particolare osservando che "la finalità della società è essere in grado di identificare i soggetti. Tale identificazione è resa possibile mediante la conservazione di pubblicazioni/profili/account degli utenti collegati ad una fotografia, in particolare ad esempio sui social network, forum o blog, su un profilo, o mediante la possibilità di creare un profilo di una persona in qualsiasi momento. Questo successivo ricorso a tecniche di trattamento dei dati personali tese alla profilazione è un indicatore determinante".[30] Non vediamo alcuna ragione per cui l'Autorità debba giungere a una conclusione diversa da quella dell'HmbBfDI riguardo all'applicabilità del GDPR.

25. Infine, una precedente versione della *Privacy Policy* di Clearview mostrava che la società si sottoponeva apertamente alla giurisdizione delle Autorità di protezione dei dati (DPA) dello SEE: "I soggetti residenti nello Spazio Economico Europeo o in Svizzera che vogliano presentare reclamo o cercare di dirimere una controversia in relazione al trattamento dei dati personali da parte di Clearview AI possono presentare ricorso gratuitamente contattando la competente Autorità di protezione dei dati (DPA) nel proprio Paese."[31] Questa versione della *Privacy Policy* è stata sostituita nel marzo 2021 con una versione in cui non si fa riferimento ai residenti dello SEE o alla normativa

---

[28] Clearview AI, Inc. Privacy Policy (versione 2, ultimo aggiornamento del 29 gennaio 2020). Disponibile al seguente link https://clearview.ai/privacy/privacy_policy.

[29] Clearview AI, Inc. Terms of Service. Disponibile al seguente link https://web.archive.org/web/20210411225644/https://clearview.ai/help/tos.

[30] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (n 4).

[31] Clearview AI, Inc. Privacy Policy (version 2) (n 28).

europea,[32] apparentemente per eludere questo tipo di segnalazione. Al momento della stesura di questa nostra segnalazione, sia la versione della privacy policy antecedente al marzo 2021 che i moduli "EU/UK/Switzerland Data Access Form" e "EU/UK/Switzerland/Australia Opt-Out" sono ancora disponibili online, seppur senza riferimenti diretti nel sito web di Clearview.[33] Questi due moduli erano precedentemente disponibili in una pagina chiamata "Privacy Requests Form" del sito di Clearview.[34] Ma dato che non ci sono prove che Clearview abbia modificato le sue pratiche e interrotto il trattamento dei dati personali dei residenti dell'UE, non vi è motivo di ritenere che la giurisdizione riguardo alle pratiche sia in qualche modo cambiata. Anche se lo avessero fatto, i dati raccolti mentre era in vigore la precedente privacy policy sono soggetti a quella giurisdizione.

26. In aggiunta, pur avendo rimosso i link dal proprio sito per i moduli di richiesta di esercizio dei diritti degli interessati, dietro le quintet Clearview ancora sa di essere, e si comporta come tale, soggetta agli obblighi di rispondere a tali richieste. Infatti, un'interessata ha inviato una richiesta di accesso ai dati attraverso quei moduli il 24 marzo, dopo che i link erano stati rimossi. Dopo un mese ha scritto nuovamente a Clearview sottolineando come i 30 giorni di tempo per la risposta fossero scaduti, a quel punto ha ricevuto una email da privacy@clearview-ai.zendesk.com che le richiedeva di inviare una nuova foto del proprio volto e del documento di identità, e promettendo che la sua richiesta sarebbe stata prioritaria. Al momento dell'invio di questa segnalazione, l'interessata non ha ancora ricevuto i dati da lei richiesti. I dettagli di questa corrispondenza sono disponibile nel reclamo presentato all'Autorità di protezione dei dati personali greca da parte di Homo Digitalis.

27. Per le motivazioni sopra addotte, il Centro Hermes ritiene che l'Autorità debba considerare la condotta del titolare del trattamento come rientrante nel campo di applicazione dell'Art. 3.2 del GDPR.

28. Inoltre, alla luce degli attuali dibattiti e proposte di regolamentazione della sorveglianza biometrica di massa,[35] il Centro Hermes ritiene che le leggi sulla privacy e le norme in materia di protezione dei dati esistenti siano del tutto sufficienti per ritenere illegali le pratiche di Clearview. Ma un trattamento di massa dei dati biometrici da parte di una società privata rientra a tutti gli effetti nella normativa esistente, che è stata pensata per proteggere i cittadini europei proprio da questo tipo di pratiche.

C. Perché il Garante per la protezione dei dati personali dovrebbe prendere in considerazione questa segnalazione

[32] Clearview AI, Inc. Privacy Policy (version 1) (n 5).

[33] 'EU/UK/Switzerland Data Access Form', disponibile al link https://clearviewai.typeform.com/to/ePcsEp e 'EU/UK/Switzerland/Australia Opt-Out' disponibile al link https://clearviewai.typeform.com/to/zqMFnt.

[34] Clearview AI, "Privacy Request Forms", disponibile in versione archiviata sul sito Wayback Machine Internet Archive, https://web.archive.org/web/20210303033642/https://clearview.ai/privacy/requests.

[35] European Commission, 'Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)', COM(2021) 206 final (21 April 2021).

28. Secondo quanto riportato da Wired Italia, a inizio marzo 2021 l'Autorità ha aperto un'istruttoria e inviato richieste formali a Clearview sul trattamento di dati biometrici[36]. Il Centro Hermes accoglie con favore l'apertura di questa istruttoria e spera che le dettagliate analisi tecniche e legali delle pratiche di Clearview, presenti in questa nostra segnalazione, possano essere di aiuto per l'istruttoria in corso.

29. L'impiego della tecnologia di Clearview solleva timori significativi per quanto riguarda l'impiego delle tecnologie per il riconoscimento facciale ("**RF**") sia da parte di privati che di enti pubblici. In Italia, come accennato sopra, il Ministero dell'Interno non ha ancora chiarito se abbia utilizzato Clearview, un'interrogazione parlamentare proprio su questo tema ha visto il Ministero dell'Interno eludere la risposta. Inoltre, viste le pratiche di marketing aggressive messe in pratica da Clearview, non si può escludere che singoli funzionari abbiano effettuato dei test, o che altre forze dell'ordine italiane, non facenti capo al Ministero dell'Interno, abbiano usato Clearview. L'incertezza e la mancanza di trasparenza intorno all'uso della tecnologia di RF negli spazi privati e pubblici in Italia è inaccettabile, considerando la grave interferenza, senza precedenti, che questa tecnologia presenta nei confronti della privacy.

30. Il Centro Hermes nutre il timore che permettere a società come Clearview di distribuire, vendere o offrire software di riconoscimento facciale a clienti privati e ad autorità preposte all'applicazione della legge possa andare a detrimento dei diritti delle persone alla protezione dei dati, non rispettando i principi di protezione dei dati e le norme rigorose per il loro trattamento imposte dal GDPR e dal Codice privacy. La modalità di funzionamento e impiego attuale di queste tecnologie favoriscono i medesimi danni a cui la normativa intende porre rimedio. Se non sanzionate, queste pratiche potrebbero avere gravi ripercussioni sulla nostra società. Nell'era digitale, tra tali ripercussioni possiamo includere: un effetto deterrente sulla partecipazione delle persone ai processi democratici mediante Internet, limitazioni allo sviluppo delle identità socio-politiche dei cittadini e danni nella "vita reale" come ad esempio la vulnerabilità allo "stalking" e l'impossibilità di svolgere le attività quotidiane senza la paura di essere sorvegliati.

31. È quindi di fondamentale importanza che l'Autorità faccia chiarezza sull'interpretazione di importanti disposizioni del GDPR, come quelle relative alle basi giuridiche di cui agli articoli 6 e 9, in modo da evitare il proliferare di aziende il cui modello di business cerca di distorcere i valori fondamentali della privacy e della protezione dei dati.

32. Inoltre, il Centro Hermes ritiene che sarebbe di grande importanza per l'Autorità considerare questa segnalazione in coordinamento con le altre Autorità per la protezione dei dati personali in UE utilizzando i meccanismi di cooperazione e coerenza previsti dal GDPR, altri partner del Centro Hermes hanno infatti

---

[36] Wired Italia, 'Il Garante italiano della privacy indaga sulla più controversa società di riconoscimento facciale al mondo' (15 aprile 2021). Disponibile al link https://www.wired.it/attualita/tech/2021/04/15/riconoscimento-facciale-garante-privacy-clearview-ai/.

inviato segnalazioni simili in altri Stati.[37] La più recente valutazione del GDPR[38] da parte della Commissione Europea sottolinea che "le autorità di protezione dei dati non hanno ancora utilizzato appieno gli strumenti forniti dal GDPR, quali ad esempio le operazioni congiunte che potrebbero portare a indagini congiunte". Il Centro Hermes sostiene che le indagini su Clearview trarrebbero grande beneficio dalla cooperazione transfrontaliera e che un'applicazione efficace della normativa richiede un approccio transfrontaliero coerente. Come spiegato più avanti nella sezione V.D, la condotta di Clearview minaccia il carattere aperto di Internet e le numerose libertà che garantisce. Data la natura globale di Internet, la conservazione di queste sue caratteristiche essenziali richiede un approccio globale che abbia effetti su una scala più ampia possibile.

V. Quadro giuridico e preoccupazioni: il trattamento da parte di Clearview AI, Inc. (GDPR)

33. Questa sezione riporta i timori del Centro Hermes riguardo alla prima fase dell'interazione di Clearview con gli interessati nella UE, nello specifico il trattamento iniziale dei dati personali effettuato dalla società mediante la raccolta, conservazione e estrazione delle caratteristiche facciali. La nostra analisi legale e i nostri timori poggiano su indagini condotte dal Centro Hermes su fonti pubblicamente disponibili riguardo alla tecnologia Clearview, sulla base della competenza tecnica e legale del Centro Hermes. I principali timori sono relativi al fatto che (i) Clearview tratta sia dati personali non sensibili che categorie speciali di dati personali, senza una valida base giuridica e (ii) tale trattamento costituisce una violazione di diversi princìpi di protezione dei dati.

34. Dopo aver dimostrato che Clearview tratta dati personali e dati personali sensibili (sezione A), in questa sezione verranno illustrate le diverse violazioni del GDPR nelle pratiche di raccolta, conservazione e identificazione dei dati personali da parte di Clearview, che non rispettano i seguenti principi di protezione dei dati previsti all'Art. 5 del GDPR:

    (a) Principio 1 – Liceità, correttezza e trasparenza
        i. Trasparenza (sezione B)
        ii. Correttezza (sezione C)
        iii. Liceità e base giuridica ai sensi degli Artt. 6 e 9 del GDPR (legittimi interessi e categorie particolari di dati personali) (sezione D)
    (b) Principio 2 – Limitazione della finalità (sezione E)

A. La società Clearview tratta dati personali e categorie particolari di dati

Clearview tratta dati personali come definiti nell'Art. 4 paragrafo 1 del GDPR

[37] [UK, Grecia, Austria e Francia.]

[38] European Commission, 'Communication From the Commission to the European Parliament and the Council – Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation' (COM(2020)0264) (24 giugno 2020). Disponibile al link https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264.

35. Sulla base della descrizione tecnica del prodotto Clearview nella sezione III di cui sopra, il Centro Hermes sostiene che Clearview effettua il "trattamento interamente o parzialmente automatizzato di dati personali" come stabilito nell'Art. 2 paragrafo 1 del GDPR.

36. Innanzitutto, le immagini raccolte da Clearview da fonti pubblicamente disponibili su Internet sono a tutti gli effetti dati personali. Le fotografie rientrano appieno nella definizione di dato personale ai sensi dell'Art. 4 paragrafo 1 del GDPR, soprattutto se interpretato alla luce del Considerando 26 del GDPR: "È auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. […] Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'unicità, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente." Data l'unicità di qualsiasi volto, la fotografia di un viso permette necessariamente, mediante il riconoscimento "umano", di identificare una persona. Come dimostrato dalla tecnologia Clearview, ciò permette anche necessariamente l'identificazione mediante riconoscimento automatizzato.

37. Tale conclusione è in linea anche con la giurisprudenza della Corte di Giustizia dell'Unione Europea ("**CGUE**"). Quest'ultima ha stabilito che "l'immagine di una persona ripresa da una macchina fotografica costituisce un dato personale ai sensi dell'Art. 2.a della Direttiva 95/46 nella misura in cui rende possibile l'identificazione della persona in questione".[39] La definizione di dato personale ai sensi della Direttiva 95/46 è, in sostanza, la stessa contenuta nell'Art. 4 paragrafo 1 del GDPR.

38. In secondo luogo, anche i metadati che Clearview raccoglie, conserva e associa alle immagini contengono dati personali. Come evidenziato dai risultati di una richiesta di accesso ai dati descritti negli articoli pubblicati da Wired Italia[40] e Vice Italia[41], l'"Image Index" fornito relativamente ai risultati del volto contiene descrizioni dell'immagine e/o della pagina web su cui è stata trovata l'immagine e può contenere dati personali quali ad esempio i nomi dei soggetti – inclusi quelli di altri interessati. Ciò conferma ulteriormente che le foto raccolte da Clearview sono dati personali, considerato che possono "indirettamente" permettere l'identificazione dell'interessato – il titolare del trattamento ha quindi "i mezzi, di cui può ragionevolmente avvalersi per identificare l'interessato", cosa che rende quest'ultimo indirettamente identificabile, come stabilito dalla CGUE in *Breyer*.[42]

39. Infine, i dati personali vengono raccolti, conservati, strutturati mediante indicizzazione con vettori e recuperati quando un utente effettua una *ricerca*.

---

[39] Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014] ECLI:EU:C:2014:2428, para 22.

[40] Wired Italia (23 marzo 2021) (n 23)

[41] Vice Italia (25 marzo 2020) (n 20)

[42] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779, para 48.

Tutte queste operazioni rientrano nella definizione di "trattamento" ai sensi dell'Art. 4 par. 2 del GDPR.

Clearview tratta dati biometrici come definiti nell'Art. 4 par. 14 del GDPR

40. Ai sensi dell'Art. 4 par. 14 del GDPR, i "dati biometrici" sono definiti come "dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, **quali l'immagine facciale**".

41. Clearview, di conseguenza, tratta dati biometrici almeno sotto due punti di vista:

    (a) le immagini facciali che raccoglie da fonti online sono dei dati biometrici e
    (b) una volta creati i vettori, questi stessi diventano dati biometrici, dato che sono dati ottenuti da "un trattamento tecnico specifico relativo alle caratteristiche fisiche […] di una persona fisica che ne consentono o confermano l'identificazione univoca".

Clearview tratta categorie particolari di dati come definiti nell'Art. 9 par. 1 del GDPR

42. Clearview tratta sistematicamente categorie particolari di dati come definiti nell'Art. 9 par. 1 del GDPR. Ai sensi dell'Art. 9 par. 1, le categorie particolari di dati personali includono per definizione i “dati biometrici al fine di identificare in modo univoco una persona fisica”. Secondo il Considerando 51 del GDPR, “Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica.” Se da un lato questo significa che le fotografie raccolte dalla Clearview da fonti online non rientrano necessariamente nelle categorie particolari di dati personali, dall'altro chiarisce che queste fotografie diventano tali non appena vengono elaborate attraverso la fase 3 del sistema di costruzione del database Clearview. La scansione di tutti i volti, l'estrazione delle loro caratteristiche facciali identificative uniche e la trasformazione di tali caratteristiche in vettori rappresentano "un dispositivo tecnico specifico che consente l'identificazione univoca […] di una persona fisica."

43. Inoltre, i metadati raccolti, conservati e associati alle immagini facciali possono contenere dati personali che rivelano “l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale”, che sono anche categorie particolari di dati personali secondo l’art. 9 par. 1 del GDPR. Per esempio, le immagini facciali possono essere reperite su un sito web di un'associazione di fedeli o di membri di un sindacato, associando così persone identificabili in modo univoco a tali caratteristiche.

44. Occorre anche notare che Clearview tratta i dati personali di minori le cui immagini facciali sono disponibili online,[43] il cui trattamento è soggetto a limitazioni anche più stringenti in conformità al GDPR.[44]

B. Trasparenza e diritto all'informazione

48. La trasparenza è una componente fondamentale del primo principio di protezione dei dati stabilito nell'Art. 5.1.a del GDPR e sostenuto dal diritto all'informazione negli Artt. 13 e 14. Il Considerando 60 del GDPR stabilisce che "[i] principi di trattamento corretto e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento e delle sue finalità." Ai sensi dell'Art. 14.3.a, qualora i dati personali non siano stati ottenuti presso l'interessato, come nel caso del trattamento da parte della Clearview, il titolare del trattamento fornisce all'interessato le informazioni "entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese".

49. Sul suo sito web, Clearview riporta una *Privacy Policy* ("**Policy**")[45], aggiornata a marzo 2021 ed elaborata a partire da una precedente versione, indirizzata al pubblico di tutto il mondo.[46] Nella nuova versione è stato rimosso il riferimento ai residenti dello Spazio Economico Europeo o della Svizzera. Tuttavia, si applica espressamente alle "foto pubblicamente disponibili su Internet" e all'estrazione della "geo-localizzazione e delle misurazioni delle caratteristiche facciali delle persone nelle foto" – nel senso che si applica necessariamente a tutte le persone del mondo che, consapevolmente o meno, hanno le proprie immagini facciali su parti pubblicamente disponibili di Internet e di conseguenza ai residenti in Italia e UE.

50. Clearview non fornisce la trasparenza richiesta almeno sotto due punti di vista. Innanzitutto, non informa mai gli interessati che sta trattando i loro dati personali, di modo che gli interessati non leggono mai la privacy policy della Clearview prima o dopo il trattamento dei propri dati personali. Secondo le Linee guida sulla trasparenza del Gruppo di lavoro Articolo 29,[47] "una considerazione fondamentale del principio di trasparenza […] è che l'interessato sia in grado di stabilire in anticipo la portata e le conseguenze del trattamento e che non sia colto di sorpresa in un secondo momento circa i modi in cui i suoi dati personali sono stati utilizzati." La sorpresa, nel caso di Clearview, è totale: l'unico modo per l'interessato di sapere che i suoi dati

---

[43] Lettera da Edward J. Markey (United States Senator) a Mr. Hoan Ton-That (3 March 2020), p. 2, Disponibile al seguente link: https://www.markey.senate.gov/imo/media/doc/Markey%20Letter%20-%20Clearview%20II%203.3.20.pdf, che cita Kashmir Hill e Gabriel J.X. Dance, 'Clearview's Facial Recognition App Is Identifying Child Victims of Abuse', (New York Times, 7 February 2020), Disponibile al seguente link https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html.

[44] Ad esempio, Articoli 8, 12(1), e 17(1)(f), e Considerando 38.

[45] Clearview Privacy Policy (versione 1) (n 5).

[46] Clearview Privacy Policy (version 2) (n 28).

[47] Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' (17/EN WP260 rev.01, Adopted on 29 November 2017, Revised and Adopted on 11 April 2018). Disponibile al seguente link https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

personali sono stati oggetto di trattamento è leggere le notizie riportate dai media sulle pratiche della società e a quel punto contattare Clearview.

51. In secondo luogo, anche se un interessato fosse in grado di accedere alla Policy nel momento opportuno prima o subito dopo che i suoi dati sono stati trattati, Clearview fornisce informazioni incomplete e fuorvianti. Nella sezione "What Data Do We Collect?" ("Quali dati raccogliamo?", ndt), riferisce che "raccoglie foto pubblicamente disponibili su Internet" e "potrebbe estrarre informazioni da tali foto, incluse la geo-localizzazione e le misurazioni delle caratteristiche facciali delle persone nelle foto". L'affermazione è incompleta e fuorviante in due modi: (1) presenta l'estrazione delle informazioni e delle misurazioni delle caratteristiche facciali come una mera possibilità (utilizzando il termine "potrebbe", che dovrebbe essere evitata nelle *privacy policy*[48]), mentre in realtà si tratta di un processo automatico e (2) omette vari altri tipi di dati personali che Clearview raccoglie in automatico, nello specifico nomi e altri dati ottenuti dagli URL, dalle foto e dai titoli delle pagine web raccolti.

52. Inoltre, nella nuova versione della *Privacy Policy* di Clearview sono state rimosse le informazioni relative alle basi giuridiche a cui fa riferimento la Clearview per il trattamento dei dati personali. La versione precedente della *Privacy Policy* di Clearview menzionava basi giuridiche specifiche del GDPR quali gli interessi legittimi o il consenso esplicito.[49] Di nuovo, in ciò che può essere percepito come un tentativo di eludere la giurisdizione del GDPR, Clearview ha rimosso informazioni essenziali che devono essere fornite in caso di trattamento di dati personali di residenti dell'UE.

53. In varie dichiarazioni pubbliche,[50] Clearview sembra presumere che qualsiasi diritto all'informazione sia cancellato dal fatto che i dati personali ottenuti siano disponibili pubblicamente e che gli interessati abbiano quindi "rinunciato" a questo diritto accettando tranquillamente che le proprie immagini fossero pubblicamente disponibili online. Tuttavia, come verrà analizzato e spiegato più avanti nei paragrafi 91-99, sussistono molti motivi per cui un tale presupposto è da considerarsi falso. Di conseguenza, è inaccettabile che Clearview presuma che gli interessati siano pienamente informati e diano il consenso al trattamento delle proprie immagini in questo modo.

54. Questa mancanza di trasparenza è una violazione del GDPR stesso e implica anche che la stragrande maggioranza degli interessati non sono consapevoli del trattamento dei loro dati personali da parte di Clearview e, di conseguenza, non hanno la possibilità di esercitare nessuno dei propri diritti in relazione a tale trattamento.

C. Correttezza e ragionevoli aspettative nutrite dagli interessati

---

[48] Art 29 WP Guidelines on transparency (n 47), para 13.

[49] Clearview Privacy Policy (version 2) (n 28).

[50] Ad esempio CNN Business YouTube channel, 'Clearview AI's founder Hoan Ton-That speaks out [Extended interview]' (6 March 2020). Disponibile al seguente link https://www.youtube.com/watch?v=q-1bR3P9RAw.

55. La correttezza è un'altra componente del primo principio di protezione dei dati nell'Art. 5 par. 1 del GDPR. L'essenza della correttezza è che il trattamento dei dati in questione dovrebbe avvenire in linea con le ragionevoli aspettative degli interessati: "correttezza significa che i dati personali dovrebbero essere trattati secondo le ragionevoli aspettative delle persone e non utilizzati in modi che abbiano effetti negativi ingiustificati su di esse."[51]

56. Le ragionevoli aspettative di privacy sono un principio chiave anche nella giurisprudenza della Corte europea dei diritti dell'uomo ("**CEDU**"), utilizzato per valutare l'esistenza di un'eventuale interferenza nella vita privata di un interessato ai sensi dell'Art. 8 della Convenzione europea per i diritti umani ("**Cedu**"). La CEDU ha più volte indagato se gli interessati "avessero ragionevoli aspettative riguardo al fatto che la loro privacy sarebbe stata rispettata e protetta".[52] Nella sua giurisprudenza, la Corte ha sottolineato che nessuno potrebbe ragionevolmente aspettarsi che le immagini e i video raffiguranti aspetti sensibili della propria vita privata siano successivamente divulgati nei media, anche se le loro azioni sono "già di dominio pubblico"[53] e che l'utilizzo di attrezzature fotografiche per catturare ed elaborare i dati biometrici delle persone per finalità diverse da quelle che queste avevano originariamente previsto non possono rientrare nelle loro ragionevoli aspettative di privacy.[54]

57. Il Centro Hermes sostiene che le ragionevoli aspettative degli interessati sono palesemente calpestate dalle pratiche di Clearview. Nella sua recente decisione, l'OPCC ha ritenuto che "le persone che hanno postato le proprie immagini online, o le cui immagini sono state postate da terzi, non si aspettavano ragionevolmente che Clearview avrebbe raccolto, utilizzato e divulgato le loro immagini a fini identificativi".[55] Questa affermazione trova ulteriore conferma anche in un sondaggio condotto dalla Agenzia europea per i diritti fondamentali (European Agency for Fundamental Rights), che chiedeva ai cittadini europei se fossero disponibili a condividere diversi tipi di dati personali con agenzie governative e società private.[56] Nei 27 paesi della UE, il 94% degli intervistati ha affermato espressamente di non essere disponibile a condividere le proprie immagini facciali con società private a fini identificativi.

---

[51] ICO, 'Guide to the General Data Protection Regulation (GDPR) – Principle (a): Lawfulness, fairness and transparency'. Disponibile al seguente link https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/#fairness; Ehmann/Selmayr/Heberlein, 2. Ed. 2018, GDPR Art. 5 para. 9, 10).

[52] *Barbulescu v. Romania* [GC] App no 1496/08 (ECtHR, 5 September 2017), para 73.

[53] *Peck v. United Kingdom* App No 44647/98 (ECtHR, 28 January 2003), paras 61-62.

[54] *Perry v. United Kingdom* App No 63737/00 (ECtHR, 17 July 2003), para 41.

[55] OPCC (n 4), Overview.

[56] European Union Agency for Fundamental Rights, 'Your rights matter: Data protection and privacy - Fundamental Rights Survey' (18 June 2020). Disponibile al seguente link https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection#TabPubSharingdataonline1.

58. La pratica di raccogliere ed elaborare dati pubblicamente disponibili tratti da piattaforme social, nota come “social media intelligence” (“**SOCMINT**”) o “social media monitoring”, è stata apertamente criticata negli ultimi anni a causa dei timori riguardo alla sua compatibilità con le ragionevoli aspettative di privacy. Nell'ambito di una consultazione sull'utilizzo del *Social Media Monitoring* da parte dell'Ufficio europeo di sostegno per l'asilo, il Garante europeo della protezione dei dati (“**EDPS**”) ha ritenuto che il *Social Media Monitoring* “implichi un utilizzo dei dati personali che va contro o oltre le ragionevoli aspettative degli interessati. Tale utilizzo spesso comporta che i dati personali vengano usati al di là delle loro finalità iniziali, del contesto originale e in modi che l'interessato non poteva ragionevolmente prevedere.”[57]

59. Il trattamento operato da Clearview si profila come una forma particolarmente invasiva di *Social Media Monitoring*, che va ben oltre la consultazione e l'analisi di informazioni pubblicamente disponibili su una base *ad hoc*. La raccolta, conservazione ed elaborazione automatica ai fini dell'estrazione di identificatori biometrici operate da Clearview rendono tale pratica ancora più lontana da qualsiasi ragionevole aspettativa degli interessati e quindi in nessun modo compatibile con il principio di correttezza. L'applicazione del riconoscimento facciale alla raccolta di dati complica la questione: nella sua lettera al Parlamento Europeo in cui esprime un parere preliminare riguardo all'uso dello strumento Clearview ai fini di polizia e applicazione della legge, il Comitato europeo per la protezione dei dati (EDPB) ha sottolineato che le tecnologie di riconoscimento facciale (Facial Recognition Technology - FRT) potrebbero “influenzare le ragionevoli aspettative degli interessati riguardo all'anonimato nei luoghi pubblici”.[58] Unendo SOCMINT e tecnologie di RF, il servizio offerto da Clearview annulla di fatto l'aspettativa degli interessati sul fatto che le proprie vite e identità fisiche nella vita materiale non possano essere immediatamente ricollegate alle loro vite e identità su Internet.

Paragone con il motore di ricerca Google

60. Clearview, in vari rapporti pubblici, ha spesso paragonato il proprio servizio al motore di ricerca Google, sostenendo che il suo strumento è semplicemente un “motore di ricerca di volti” invece di un motore di ricerca di siti web, e usa volti invece che parole come termini di ricerca.[59] Questo paragone sembra teso a mostrare che lo strumento di Clearview rientrerebbe nella ragionevole aspettativa di privacy degli interessati, dato che ognuno è consapevole che i suoi dati vengono estratti dai motori di ricerca. Tuttavia, il Centro Hermes vorrebbe fornire alcuni chiarimenti riguardo ai processi tecnici eseguiti dalle piattaforme Google e Clearview, che dimostreranno che sono fondamentalmente diverse.

---

[57] EDPS, ‘Formal consultation on EASO’s social media monitoring reports (case 2018-1083)’ (Brussels, D(2019) 1961). Disponibile al seguente link https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf.

[58] EDPB letter to the European Parliament (n 16).

[59] Per esempio CNN Business, ‘Clearview AI’s founder Hoan Ton-That speaks out [Extended interview]’ (n 50).

61. I "motori di ricerca" Google e Clearview eseguono entrambi tre diverse operazioni:

(a) *Crawling* (Acquisizione) – il sistema accede in automatico a un sito web e ne estrae i dati;
(b) *Indexing* (Indicizzazione) – il sistema scarica il contenuto dal sito web sul server del motore di ricerca, aggiungendo quindi contenuti al suo "indice"; e
(c) *Listing* (Elencazione) – il sistema mostra i contenuti dei *match* nelle pagine dei risultati di ricerca.

62. Nella fase di *crawling*, il proprietario di un sito web può utilizzare il file robots.txt per istruire i robot web su come scansionare le pagine del proprio sito. Si tratta di un file di testo con cui i webmaster indicano al motore di ricerca, per esempio, che non vogliono che i contenuti della propria pagina siano indicizzati. Il rispetto del file robots.txt è facoltativo da un punto di vista tecnico, e può essere ignorato dai software di *crawling*. Piattaforme come LinkedIn o Facebook hanno incluso questi file nelle proprie pagine web e proibiscono specificamente i *crawler* nei loro Termini e condizioni di servizio.

63. Google dà ai webmaster la facoltà di controllare quali informazioni delle loro pagine vengono indicizzate ed elencate nella pagina dei risultati, inclusa l'opzione di revoca (c.d. *opt-out*) totale. Clearview ha affermato che il suo *crawler* per le analisi delle immagini è configurato per rispettare qualsiasi istruzione presente nei file robots.txt.[60] Tuttavia, Clearview ha indicizzato il contenuto estratto da YouTube, Facebook, Twitter e Instagram.[61] YouTube proibisce espressamente la raccolta automatica di qualsiasi informazione che potrebbe identificare una persona e il *web scraping* di qualsiasi dato, fatta eccezione per i "motori di ricerca pubblici", come ad esempio quello di Google.[62]

64. Clearview quindi non rispetta le istruzioni che vietano di effettuare il *crawling* e il *web scraping* del contenuto di certi siti web e per questa ragione è stata citata da diverse grandi piattaforme per aver violato le loro politiche.[63] Clearview è piombata nel settore oltre un decennio dopo il boom dei social media, rivendicando la legittimità dello *scraping* di qualsiasi dato messo online dagli utenti durante quel decennio ed elaborando tali dati mediante la tecnologia di RF, che non esisteva fino a qualche anno fa. Questo è fondamentalmente contrario ai principi di prevedibilità e ragionevole aspettativa di privacy.

65. Di conseguenza, la raccolta sistematica e indiscriminata delle immagini facciali degli interessati da Internet non rientra nelle ragionevoli aspettative degli

---

[60] OPCC (n 4), para 17.

[61] Hill (n 6).

[62] YouTube, 'Terms of Service'. Disponibile al link https://www.youtube.com/static?template=terms.

[63] Alfred Ng and Steven Musil, 'Clearview AI hit with cease-and-desist from Google, Facebook over facial recognition collection' (CNET, 5 February 2020). Disponibile al seguente link https://www.cnet.com/news/clearview-ai-hit-with-cease-and-desist-from-google-over-facial-recognition-collection/.

interessati e viola il principio di correttezza. La questione della correttezza è aggravata dall'assenza di trasparenza e dalla mancanza di rispetto per il diritto degli interessati all'informazione e da varie altre violazioni dei principi di protezione dei dati come più avanti esposto in questa segnalazione.

D. Liceità e base giuridica

66. La terza componente del primo principio di protezione dei dati nell'Art. 5.1.a del GDPR è la liceità, che impone che i dati personali siano trattati in conformità alla legge. L'Art. 6 riporta un elenco esaustivo di fondamenti giuridici in base ai quali i dati personali possono essere trattati.

67. Oltre a richiedere una base giuridica ai sensi dell'Art. 6, il trattamento di dati personali di "categorie particolari" è proibito a meno che non sia soddisfatta una delle condizioni dell'elenco esaustivo di cui all'Art. 9 par. 2 del GDPR. Dato che Clearview tratta dati biometrici identificati come dati di "categorie particolari", è tenuta ad avere una base giuridica valida sia ai sensi dell'Art 6 che ai sensi dell'Art. 9 e non ai sensi di uno o dell'altro.[64] Dalla precedente versione della *Privacy Policy* di Clearview[65] appare evidente che questo doppio requisito non è stato ben compreso: nella sezione "Base giuridica del trattamento", la società forniva le basi giuridiche per il trattamento dei dati personali (tratte dall'Art. 6) separatamente dalle basi giuridiche del trattamento di categorie particolari di dati (tratte dall'Art. 9). Inoltre, nei rapporti pubblici Clearview sembra credere che l'affermazione "estraiamo dati solo da fonti pubblicamente disponibili" di per sé fornisca la giustificazione per tutti i trattamenti da lei effettuati.

68. Questa segnalazione analizzerà ora l'applicabilità delle basi giuridiche più significative per il trattamento effettuato da Clearview ai sensi degli Artt. 6 e 9.

<u>Interessi legittimi - Art. 6.1.f del GDPR</u>

69. La principale base giuridica a cui Clearview può - e sembra - appoggiarsi, ai sensi dell'Art. 6 è l'"interesse legittimo" (Art. 6.1.f). Questo può essere visto dall'evidente inapplicabilità di altre basi giuridiche e dal fatto che, nella precedente versione della sua *Privacy Policy*,[66] Clearview faceva espresso affidamento su questa base: "il trattamento è necessario per gli interessi legittimi di Clearview e non pregiudica indebitamente i vostri interessi o diritti e libertà fondamentali". Le altre basi su cui ha cercato di appoggiarsi si applicavano solo ai dati relativi agli utenti dei suoi servizi. Per esempio, la base giuridica "necessaria per proteggere gli interessi vitali dell'interessato o di

---

[64] Per un supporto inequivocabile a questa visione "cumulativa", vedere Article 29 Data Protection Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (844/14/EN WP217 Adopted on 9 November 2014), p.14. Vedere anche Edward S Dove and Jiahong Chen, 'What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9(2)(e)' (2021) Vol. 00, No. 0, International Data Privacy Law, 1, 2.

[65] Clearview Privacy Policy (versione 2) (n 28).

[66] Ibid.

un'altra persona fisica" (Art. 6.1.d) potrebbe potenzialmente applicarsi solo all'ultima fase del trattamento nel ciclo dello strumento Clearview, cioè quando viene utilizzato da un'autorità preposta all'applicazione della legge nel contesto delle indagini su un reato ben identificato, ma non può giustificare tutto il trattamento precedente.

70. Il Considerando 47 del GDPR stabilisce che gli interessi legittimi di un titolare del trattamento:

> *possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato,* ***tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento****. Ad esempio, potrebbero sussistere tali legittimi interessi quando esista* ***una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento,*** *ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento. In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione* ***anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi*** *che abbia luogo un trattamento a tal fine.* (grassetto aggiunto)

71. Se da un lato la base giuridica del 'legittimo interesse' consente una certa flessibilità da parte dei titolari del trattamento, questo non implica che tale flessibilità sia illimitata o possa essere modellata esattamente per giustificare o adattarsi a qualsiasi trattamento.[67] Tuttavia, questa base giuridica continua ad essere abusata: una recente risoluzione del Parlamento Europeo avverte che la base degli interessi legittimi è "molto spesso citata in modo improprio come base giuridica del trattamento".[68] E continua:

> *Il Parlamento Europeo [...] fa notare che i titolari del trattamento continuano a basarsi sul legittimo interesse senza effettuare il necessario esame del bilanciamento degli interessi, che comprende una valutazione dei diritti fondamentali; esprime particolare preoccupazione per il fatto che alcuni Stati membri stanno adottando una legislazione nazionale per determinare le condizioni per il trattamento sulla base del legittimo interesse, prevedendo il bilanciamento dei rispettivi interessi del titolare del trattamento e delle persone interessate, mentre il GDPR obbliga ogni singolo titolare del trattamento a effettuare tale esame del bilanciamento a livello individuale e ad avvalersi di tale fondamento giuridico [...]*

Valutazione degli interessi legittimi

---

[67] ICO, 'Guide to the General Data Protection Regulation (GDPR) – Lawful basis for processing – Legitimate interests'. Disponibile al seguente link https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/.

[68] European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP)), para 7.

72. Un titolare del trattamento che voglia appoggiarsi alla base giuridica degli interessi legittimi deve effettuare una valutazione e renderla disponibile agli interessati.[69] Clearview non ha reso pubblicamente disponibile alcuna valutazione degli interessi legittimi.

73. La valutazione degli interessi legittimi deve essere effettuata sulle tre condizioni previste nell'Art. 6.1.f e ulteriormente spiegate nelle sentenze della CGUE *Rigas Satiksme*[70] e *Fashion ID*[71]:

(1) **Il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati ("finalità")** – nel caso di Clearview, si tratterebbe di un interesse commerciale, cioè di fornitura di un servizio a terzi a fronte di un pagamento. È palese che le società non possono trattare il mero perseguimento dei propri modelli di attività o di profitto come "interessi legittimi". L'interesse legittimo dei terzi a cui vengono divulgati i dati può essere considerato l'identificazione di persone reali. Prendendo in considerazione il cliente più comune di Clearview, ossia un organismo preposto all'applicazione della legge, l'Art. 6.1 del GDPR stabilisce esplicitamente che la base degli interessi legittimi "non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti". Prendendo in considerazione un altro cliente di Clearview, ossia le società private e singoli cittadini, la legittimità dei loro interessi è puramente ipotetica e nella migliore delle ipotesi di natura limitata e certamente inquietante. In ogni caso, l'interesse futuro di terzi non meglio definiti non può giustificare le operazioni di trattamento all'origine. In questo caso la raccolta, l'elaborazione biometrica e la conservazione delle immagini degli interessati vengono effettuati prima che un qualsiasi cliente utilizzi tali dati e che si possa anche solo immaginare quale uso specifico ne faranno i clienti di Clearview. Come descritto dall'Ufficio del Commissario in materia di protezione dei dati del Canada, le attività di Clearview consistono semplicemente nella "identificazione e sorveglianza di massa di persone da parte di un'entità privata nel corso di un'attività commerciale".[72]

(2) **La necessità del trattamento dei dati personali per il perseguimento dell'interesse legittimo ("necessità")** – se Clearview avesse un interesse legittimo rilevante per questa valutazione, tale condizione richiederebbe di valutare se il beneficio commerciale di Clearview possa essere ottenuto con mezzi meno invasivi dei diritti e delle libertà fondamentali degli interessati, in conformità al principio che le deroghe e limitazioni relative alla protezione dei dati personali debbano applicarsi solo quando strettamente

---

[69] ICO (n 67).

[70] Case 13/16 *Rigas Satiksme* [2017] ECLI:EU:C:2017:336, paras 28-31.

[71] Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 95.

[72] OPCC (n 4), para 72.

necessarie.[73] Avendo stabilito che gli interessi di un'autorità preposta all'applicazione della legge non possono essere considerati in questa particolare valutazione, non si può sostenere che i clienti privati di Clearview *necessitino* di utilizzare lo strumento per i propri interessi. L'esistenza di alternative meno invasive è di cruciale importanza, come il principio di minimizzazione dei dati, secondo cui i dati devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati".[74] Per esempio, Clearview riferisce che le banche possono utilizzare il suo strumento per controlli di sicurezza e verifica dei precedenti penali; tuttavia, le banche hanno effettuato tali controlli per decenni senza usare tale strumento. È inoltre difficile comprendere perché simili controlli possano essere effettuati solo in base a un'immagine facciale, piuttosto che mediante altri identificatori.

(3) **Il fatto che i diritti fondamentali e le libertà dell'interessato i cui dati richiedono tutela non prevalgano ("bilanciamento")** – questo richiede che venga trovato un bilanciamento tra gli interessi del titolare del trattamento e gli effetti del trattamento sull'interessato. Nel caso determinante di *Google Spagna*, la CGUE ha ritenuto che:

> *un trattamento di dati personali, quale quello in esame nel procedimento principale, effettuato dal gestore di un motore di ricerca, può incidere significativamente sui diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, nel caso in cui la ricerca con l'aiuto di tale motore venga effettuata a partire dal nome di una persona fisica, dal momento che detto trattamento consente a qualsiasi utente di Internet di ottenere, mediante l'elenco di risultati, una visione complessiva strutturata delle informazioni relative a questa persona reperibili su Internet, che toccano potenzialmente una moltitudine di aspetti della sua vita privata e che, senza il suddetto motore di ricerca, non avrebbero potuto – o solo difficilmente avrebbero potuto – essere connesse tra loro, e consente dunque di stabilire un profilo più o meno dettagliato di tale persona.[75]*

La CGUE ha anche concluso che "[v]ista la gravità potenziale di tale ingerenza, è giocoforza constatare che quest'ultima non può essere giustificata dal semplice interesse economico del gestore di un siffatto motore di ricerca in questo trattamento di dati".[76]

---

[73] Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] EU:C:2010:662, para 86; Case C-473/12 *IPI* [2013] EU:C:2013:715, para 39; Case C-212/13 *Ryneš* [2014] EU:C:2014:2428, para 28.

[74] C/Jorge Juan 6 28001 – Madrid. Disponibile al seguente link https://edpb.europa.eu/sites/edpb/files/article-60-final-decisions/es_2010_10_right_to_erasure_transparency_and_information_decisionpublic_redacted.pdf.

[75] Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 80.

[76] Ibid, para 81.

Ciò che la CGUE ha descritto in quella sede come una ingerenza significativa nei diritti fondamentali degli interessati è precisamente ciò che sta facendo Clearview, con fattori che possono solo rafforzare la gravità di questa interferenza: (a) con lo strumento Clearview, non è necessario il nome dell'interessato per ottenere risultati dalla ricerca, è sufficiente un'immagine del suo volto, che può essere acquisita anche semplicemente passando vicino all'interessato per strada e scattandogli una foto; e (b) nel caso di Clearview, un interessato non può, senza a sua volta utilizzare il prodotto Clearview, sapere quali informazioni su di sé sono disponibili in esso (mentre può eseguire una ricerca del proprio nome e di altri identificatori di testo attraverso Google).

Il Parere sul concetto di interesse legittimo del Gruppo di lavoro Articolo 29[77] stabilisce alcuni ulteriori fattori da considerare quando si effettua tale test di bilanciamento:

i. **La natura e l'origine dell'interesse legittimo** – come spiegato nel paragrafo (1), l'interesse di Clearview nel trattamento è puramente commerciale.

ii. **L'impatto sugli interessati**, incluso:

- la natura dei dati ossia se il trattamento riguarda dati che possono essere considerati sensibili o ottenuti da fonti pubblicamente disponibili – Clearview tratta dati biometrici, che sono dati particolarmente sensibili e, come verrà spiegato nei paragrafi 93-101, il fatto che i dati siano stati ottenuti da fonti pubblicamente disponibili non sminuisce la loro qualità di dati sensibili né la necessità di protezione della privacy. Il Gruppo di lavoro Articolo 29 ha sottolineato che:

> *è innanzitutto importante sottolineare che, anche se sono stati resi accessibili al pubblico, i dati personali continuano ad essere considerati tali e, di conseguenza, per il loro trattamento continuano ad essere necessarie garanzie adeguate. Non esiste un'autorizzazione generalizzata a riutilizzare e a sottoporre ad ulteriore trattamento dati personali resi accessibili al pubblico ai sensi dell'articolo 7.f.*[78]

Pur riconoscendo che il fatto che i dati personali siano accessibili al pubblico potrebbe essere un fattore rilevante a favore dell'individuazione di interessi legittimi, il Gruppo di lavoro ha però segnalato che questo sarebbe il caso solo "se la pubblicazione

[77] Art 29 WP Opinion on Legitimate Interests (n 64), pp. 36-43. **Il Centro Hermes rileva che l'EDPB sta aggiornando questo parere al fine di affrontare le questioni evidenziate nella relazione della Commissione adottata dalla risoluzione del Parlamento europeo di cui sopra (n 68), e che ci si può aspettare che il parere aggiornato richiederà una valutazione più rigorosa, anziché più blanda, di quella esposta nella presente comunicazione.**

[78] Ibid, p. 39.

[fosse] stata effettuata con una ragionevole aspettativa in merito all'ulteriore utilizzo dei dati per determinate finalità (per esempio, a scopi di ricerca o a fini di trasparenza e responsabilità)." Come già spiegato nella sezione C, il trattamento effettuato da Clearview non può rientrare nelle ragionevoli aspettative di ulteriore utilizzo nemmeno con uno sforzo di immaginazione.

- le modalità di trattamento dei dati (tra cui l'eventualità che i dati siano resi pubblici o altrimenti resi accessibili ad un ampio numero di persone o che grandi quantità di dati personali siano trattate o combinate con altri dati, per esempio nel caso dell'elaborazione di profili a fini commerciali, a fini di contrasto o per altri scopi) – i dati trattati da Clearview possono essere sottoposti al loro algoritmo di riconoscimento facciale, che è un tipo di trattamento particolarmente invasivo. Dato che qualsiasi cliente di Clearview può accedere ai dati trattati dalla società, si tratta in questo caso di un numero ampio, indefinito e illimitato di persone. Inoltre, unendo pezzi di informazioni sulla vita privata degli interessati, divulgate in modo intenzionale o meno su Internet, si può ottenere una panoramica molto invasiva e intima delle vite degli interessati, che non avrebbe mai potuto essere ottenuta con una ricerca manuale online o tramite l'uso di motori di ricerca per parole chiave. Considerando che tali informazioni possono essere utilizzate per decidere se arrestare o condannare un individuo, l'impatto è da considerarsi di altissimo livello.

- le ragionevoli aspettative degli interessati relative in particolar modo all'uso e alla divulgazione dei dati nel contesto pertinente – come spiegato nella sezione C, il trattamento effettuato da Clearview non può rientrare nelle ragionevoli aspettative degli interessati relativamente all'uso e divulgazione dei dati.

- lo status del titolare del trattamento e dell'interessato, tra cui il bilanciamento dei poteri tra l'interessato e il titolare del trattamento o l'eventualità che l'interessato sia un minore o altrimenti appartenga a una categoria più vulnerabile della popolazione – le circostanze in cui avviene il trattamento da parte di Clearview rendono l'impatto sugli interessati particolarmente intenso. Come chiarito nel Considerando 47 del GDPR, la legittimità di un interesse dovrebbe dipendere almeno in parte dal fatto che tale interesse legittimo derivi dalla relazione tra l'interessato e il titolare del trattamento. Clearview non solo non ha alcuna relazione con gli interessati, ma la sua esistenza e le sue attività sono totalmente sconosciute alla maggioranza di questi. Tali circostanze, unite all'imprevedibilità dell'utilizzo del suo strumento da parte di autorità preposte all'applicazione della legge ed entità private in tutto il mondo, rendono il bilanciamento dei poteri particolarmente sfavorevole agli interessati. Inoltre, a causa delle sue pratiche indiscriminate, Clearview tratta necessariamente dati personali di

minori e categorie più vulnerabili della popolazione. Tale vulnerabilità è spesso aggravata dalla perdita del controllo di queste categorie sulle proprie identità online.

Il Parere del Gruppo di lavoro Articolo 29 sugli interessi legittimi specifica che, ove la previsione o l'individuazione del danno o pregiudizio agli interessati sia particolarmente difficile, "è ancora più importante concentrarsi sulla prevenzione e garantire che le attività di trattamento dei dati possano essere svolte solo a patto che non comportino rischi o prevedano un rischio molto basso di indebito impatto negativo sull'interesse o sui diritti e sulle libertà fondamentali degli interessati".[79] Tenuto conto dell'impatto significativo che il trattamento effettuato da Clearview può avere sui diritti e le libertà fondamentali degli interessati, il Centro Hermes sostiene che l'Autorità dovrebbe adottare un approccio particolarmente prudente e prevenire un trattamento così rischioso.

iii. **Garanzie supplementari volte ad evitare un indebito impatto sugli interessati**, tra cui:

- minimizzazione dei dati – il modello operativo di Clearview poggia su principi opposti alla minimizzazione dei dati. La raccolta e il trattamento indiscriminati dei dati mediante i suoi algoritmi di riconoscimento facciale sono molto simili alla raccolta in blocco di dati e alla sorveglianza di massa.

- misure tecniche e organizzative volte a garantire che i dati non possano essere utilizzati per adottare decisioni o intraprendere altre azioni riguardo alle persone ("separazione funzionale") – la finalità ultima del prodotto Clearview è relativa a decisioni e azioni da intraprendere nei confronti degli interessati, con un sostanziale impatto negativo sulle loro vite, come spiegato più avanti nella sezione VI.A.

- utilizzo estensivo di tecniche di anonimizzazione, aggregazione dei dati, tecnologie di rafforzamento della tutela della privacy, tutela della privacy fin dalla progettazione, valutazioni di impatto sulla tutela della privacy e sulla protezione dei dati – Per quanto sappiamo, il prodotto non integra tecnologie o elementi progettuali di rafforzamento della tutela della privacy. In ogni caso, la finalità del prodotto Clearview è quella di spogliare tutti i soggetti presenti (volontariamente o meno) online delle tutele che possono ragionevolmente aspettarsi per la propria identità.

- maggiore trasparenza, diritto generale e incondizionato di revoca (c.d. *opt-out*), portabilità dei dati e misure correlate volte a responsabilizzare gli interessati (questioni che ricoprono "un ruolo

[79] Ibid, p.51.

cruciale nel contesto dell'Art. 6.f"[80]) – questo punto richiede che il titolare del trattamento debba "preventivamente eseguire un test meticoloso ed effettivo, basato sulle specifiche circostanze del caso, anziché operare in maniera astratta, tenendo altresì conto delle ragionevoli aspettative degli interessati". Nonostante le molteplici opportunità, quali la *Privacy Policy* della società o le numerose richieste di accesso ai dati da parte degli interessati, per quanto a conoscenza del Centro Hermes, la Clearview non ha mai effettuato o mostrato di aver effettuato un test di bilanciamento. Come già spiegato nella sezione B, le attività di Clearview mostrano una completa mancanza di trasparenza e responsabilità nei confronti degli interessati. Clearview dà un diritto limitato di revoca del trattamento, sebbene non sia chiaro cosa comporterebbe tale revoca. A causa della natura della tecnologia Clearview, è probabile che la revoca influirebbe solo sulla restituzione dei risultati che deriverebbero da una *ricerca* e non limiterebbe l'ulteriore raccolta di dati personali e l'ulteriore trattamento mediante gli algoritmi di riconoscimento facciale.

74. Utilizzando il quadro di cui sopra per analizzare l'applicabilità della base giuridica dei legittimi interessi alle attività di trattamento di Clearview, è evidente che su ogni singolo fattore la società rientra nella categoria ad alto rischio e ad alto impatto negativo. Inoltre, i vari fattori "di riscatto" a loro disposizione che attenuerebbero questo impatto sono semplicemente assenti nelle attività di Clearview. E dato che qualsiasi interesse legittimo si concretizza tuttalpiù in un interesse commerciale, la bilancia pende a sfavore dell'accettabilità del loro trattamento e della concessione di una base giuridica ai sensi dell'Art. 6.1.f.

75. Alcune valutazioni degli interessi legittimi sono state effettuate dalle autorità di protezione dei dati in Europa e indicano un'interpretazione molto ristretta degli interessi legittimi che certamente non può estendersi al tipo di trattamento sistematico e indiscriminato effettuato da Clearview. Per esempio, nella sua decisione No. 35/2020,[81] l'Ufficio Contenziosi dell'Autorità di protezione dei dati belga ha valutato se il riutilizzo dell'immagine del profilo Facebook di un interessato pubblicamente disponibile da parte di un'autorità giudiziaria belga per far rispettare un Daspo (Divieto di accedere alle manifestazioni sportive, ndt) rientrasse nei legittimi interessi dell'autorità. L'Ufficio ha sottolineato che:

> *Il GDPR limita in modo significativo la libertà di riutilizzo di dati personali pubblicamente disponibili. L'Ufficio Contenziosi sottolinea che il principio applicabile è il seguente: il fatto che l'immagine del profilo di un interessato sia liberamente accessibile al pubblico non significa che altri possano*

[80] Ibid, p.43.

[81] Autorité de Protection des Données, Chambre Contentieuse, 'Décision quant au fond 35/2020 du 30 juin 2020' (Numéro de dossier : DOS-2019-01240). Disponibile al seguente link https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-35-2020.pdf.

utilizzarla liberamente. L'utilizzo di tale fotografia è possibile solo se esiste una valida base giuridica.

L'Ufficio ha ritenuto che il riutilizzo della fotografia di un interessato rientrava nella base giuridica degli interessi legittimi, perché l'autorità aveva un interesse legittimo (l'applicazione della sua decisione), per la cui realizzazione il trattamento si era reso necessario (non poteva essere raggiunto con altri mezzi e l'autorità ha avuto cura di offuscare i volti degli altri interessati presenti nella fotografia). Tale base giuridica era specifica per quel singolo reclamo e non poteva essere estesa in modo indiscriminato. L'attenzione avuta dall'Autorità di protezione dei dati belga nell'autorizzare il riutilizzo specifico e limitato dell'immagine del profilo del denunciante dimostra la totale sproporzione e inaccettabilità di permettere a Clearview la raccolta sistematica e indiscriminata e il riutilizzo di ogni singola immagine facciale disponibile su Internet.

76. Allo stesso modo, l'Ufficio del commissario in materia di protezione dei dati del Canada ha condotto la stessa valutazione degli interessi legittimi nel contesto della giurisdizione canadese e ha concluso che:

> *A nostro avviso, in queste circostanze, Clearview non ha una finalità adeguata per:*
> *i. il* web scraping *di massa e indiscriminato di immagini di milioni di persone in tutto il Canada, inclusi minori, tra più di 3 miliardi di immagini sottoposte a* web scraping *a livello mondiale;*
> *ii. lo sviluppo di vettori di riconoscimento facciale biometrici sulla base di queste immagini e la conservazione di tali informazioni anche dopo che l'immagine o il link sorgente sono stati rimossi da Internet; o*
> *iii. il conseguente utilizzo e divulgazione di tali informazioni per le proprie finalità commerciali;*
>
> *dove tali finalità:*
>
> *iv. non sono connesse allo scopo per cui le immagini sono state originariamente postate (per esempio, fare* networking *sui* social media *o* networking *professionale);*
> *v. vanno spesso a scapito dell'interessato (per esempio, indagine, potenziale persecuzione, fonte di imbarazzo, ecc.); e*
> *vi. creano il rischio di danni significativi alle persone le cui immagini vengono catturate da Clearview (inclusi danni associati a errori di identificazione o esposizione a potenziali* data breach*), quando la grande maggioranza degli interessati non è mai stata e mai sarà implicata in un reato o identificata per aiutare nella risoluzione di un grave crimine.*[82]

77. Per completare ed arricchire la suddetta valutazione di impatto sugli interessati, le sezioni seguenti metteranno in luce i tre aspetti chiave del danno causato agli interessati dallo strumento di Clearview: (a) i rischi conosciuti del

[82] OPCC (n 4), para 76.

trattamento dei dati biometrici, (b) un inevitabile effetto dissuasivo sui diritti fondamentali e (c) i danni specifici da prevedere per le categorie vulnerabili.

(a) Rischi legati al trattamento dei dati biometrici

78. I dati biometrici sono considerati di categoria particolare perché sono dati unici e generati dalle caratteristiche fisiche delle persone, come ad esempio le impronte digitali, la voce, il volto, i modelli di retina e di iride, la topografia della mano, l'andatura o i profili di DNA. Indipendentemente dalla provenienza e da come vengono raccolti, questi dati sono di per sé sensibili.[83] Come rilevato dall'ufficio del Commissario per la Privacy del Canada:

> *Le informazioni biometriche sono distintive, variano difficilmente nel tempo, sono difficili da modificare e in gran parte sono uniche per ogni persona. Particolarmente sensibili sono i dati biometrici facciali, perché costituiscono una chiave di accesso all'identità della persona, fornendo supporto nella capacità di identificare e sorvegliare i cittadini.*[84]

79. La CEDU ha inoltre sottolineato che:

> *L'immagine di una persona costituisce uno dei principali attributi della sua personalità, poiché rivela le caratteristiche uniche della persona e la distingue dai suoi simili. Il diritto alla protezione della propria immagine è quindi una delle componenti essenziali dello sviluppo personale e presuppone il diritto di controllare l'uso di tale immagine.*[85]

80. Se adottate in assenza di solidi quadri giuridici e rigorose tutele, le tecnologie biometriche costituiscono una grave minaccia per la privacy e la sicurezza personale, poiché la loro applicazione può essere estesa per facilitare la discriminazione, la profilazione e la sorveglianza di massa[86]. Allo stato attuale, con uno strumento come Clearview, l'impronta facciale di una persona può essere utilizzata per trovare il suo nome e i suoi *account* sui *social media* e si possono incrociare queste informazioni con la sua presenza fisica per strada, i negozi che visita e le foto che questa persona o i suoi amici pubblicano online: si tratta quindi di un massiccio ampliamento dell'utilizzo della biometria rispetto alle limitate applicazioni pratiche alle quali era circoscritta fino ad ora. Secondo il Commissario delle Nazioni Unite per i diritti umani, "[r]egistrare, analizzare e conservare le immagini del volto di una persona senza il suo consenso costituisce un'interferenza con il diritto alla privacy di una persona."[87]

---

[83] *S. and Marper v. UK* [GC], App nos 30562/04 and 30566/0 (ECtHR, 12 April 2008).

[84] OPCC (n 4), para 74.

[85] *Reklos and Davourlis v. Greece*, App No 1234/05 (ECtHR, 15 April 2009), para 40.

[86] Privacy International, 'Biometrics'. Disponibile al seguente link: https://privacyinternational.org/learn/biometrics.

[87] Office of the United Nations High Commissioner for Human Rights ("OHCHR"), 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests' (UN Doc A/HRC/44/24, 24 June 2020), para 33. Disponibile al link https://undocs.org/A/HRC/44/24.

81. Essendo intrinsecamente difficili o impossibili da modificare, i dati biometrici possono identificare una persona per tutta la sua vita. Ciò rende problematica la creazione di banche dati biometriche, poiché i rischi dovrebbero essere previsti molto in là nel tempo: un cambiamento a livello politico, un futuro *data breach*, o ancora lo sviluppo delle tecnologie darebbe luogo a possibili nuovi utilizzi della biometria, con una conseguente divulgazione delle informazioni personali più ampia di quanto non sia attualmente possibile. In quanto tale, la raccolta e la conservazione dei dati biometrici potrebbe essere soggetta a gravi abusi.[88]

82. Alcuni anni fa, il Gruppo di lavoro Articolo 29 della direttiva 95/46 aveva già riconosciuto l'importanza del trattamento dei dati biometrici: "I dati biometrici cambiano irrevocabilmente la relazione tra corpo e identità, perché rendono le caratteristiche fisiche 'leggibili dalle macchine' e soggette a un ulteriore utilizzo"[89]; inoltre, aveva già previsto il danno che sarebbe stato causato dall'estrazione di caratteristiche biometriche da informazioni pubblicamente disponibili, anticipando con precisione le attività di trattamento dati di Clearview:

> *In assenza di una base legale specifica (ad esempio, il consenso) per questo nuovo scopo, le fotografie su internet, sui* social media*, nelle applicazioni di gestione o condivisione delle foto online non possono essere ulteriormente elaborate per estrarne modelli biometrici o per essere inserite in un sistema biometrico per riconoscere in automatico le persone fotografate (riconoscimento facciale).*[90]

83. I danni derivanti dal trattamento dei dati biometrici sono persino maggiori e motivo di seria preoccupazione in relazione ai diritti fondamentali, se considerati nel contesto del loro utilizzo da parte delle forze dell'ordine. Questo punto sarà trattato in modo più esteso nella sezione VI.A a seguire. Per il momento, il Centro Hermes sostiene che i rischi siano troppo alti per consentire a un'entità privata di trattare dati biometrici in modo indiscriminato e su larga scala.

(b) Effetto dissuasivo sui diritti fondamentali

84. Il Gruppo di lavoro Articolo 29 raccomanda che nel valutare l'impatto del trattamento dei dati, "occorr[a] tenere nella debita considerazione anche l'effetto dissuasivo sui comportamenti protetti, quali la libertà di ricerca o la libertà di espressione, che potrebbe derivare da continue attività di

---

[88] UN High Commissioner for Human Rights, 'The right to privacy in the digital age' (UN Doc.A/HRC/39/29, 3 August 2018). Disponibile al seguente link https://undocs.org/A/HRC/39/29.

[89] Article 29 Data Protection Working Party, 'Opinion 03/2012 on developments in biometric technologies'. Disponibile al seguente link https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

[90] Ibid.

monitoraggio/tracciamento".[91] Il Centro Hermes desidera richiamare l'attenzione sulla giurisprudenza dei tribunali e delle autorità tedesche, che hanno condotto ampie valutazioni sull'impatto della videosorveglianza sui diritti fondamentali nel contesto della valutazione degli interessi legittimi. In particolare, l'Autorità per la Protezione dei Dati della regione Baden-Württemberg ha sottolineato l'importanza del diritto al libero sviluppo della personalità per valutare l'intensità del monitoraggio attraverso la videosorveglianza: ha rilevato che nei ristoranti, nei parchi avventura e in generale nei luoghi in cui le persone si riuniscono per mangiare, bere, discutere e rilassarsi, il diritto al libero sviluppo della personalità prevale sugli interessi legittimi del Titolare del trattamento.[92] Lo stesso principio dovrebbe essere applicato anche all'Internet, essendo questo diventato un luogo di socializzazione al pari di tali spazi pubblici. Inoltre, i rischi della video-sorveglianza identificati risultano di ulteriore gravità quando l'identificazione di massa nel mondo reale è abilitata dalla tecnologia Clearview.

85. Il Garante europeo della protezione dei dati (GEPD) considera esplicitamente che la Social Media Intelligence (SOCMINT), che è proprio la pratica consentita e facilitata dalla tecnologia Clearview, ha notevoli effetti dissuasivi su vari diritti e libertà:

> *Il monitoraggio degli utenti dei social media è un'attività di trattamento dei dati personali che crea un rischio elevato per i diritti e le libertà della persona. Una nuova finalità del trattamento dei dati potrebbe influenzare l'autodeterminazione delle informazioni della persona, ridurre ulteriormente il controllo degli interessati sui propri dati... Infatti, la diminuzione della sfera di intimità delle persone, come risultato di un'inevitabile attività di sorveglianza da parte delle società e dei governi, sortisce un effetto dissuasivo sulla capacità e sulla volontà di esprimersi e di stringere relazioni liberamente, ivi inclusi i rapporti civici così essenziali per la salute della democrazia. [93]*

86. Inoltre, il Consiglio per i diritti umani delle Nazioni Unite ha esortato alla prudenza nei confronti della SOCMINT. Il Commento generale n. 37 sull'articolo 21 del Patto internazionale sui diritti civili e politici (diritto di riunione pacifica), adottato dal Comitato dei diritti umani delle Nazioni Unite, ha stabilito che:

> *Il semplice fatto che una particolare assemblea si svolga in pubblico non significa che la privacy dei partecipanti non possa essere violata. [...] Lo stesso vale per il monitoraggio dei social media al fine di ottenere informazioni sulla partecipazione alle assemblee pacifiche. È necessario che siano esercitati un controllo e una supervisione indipendenti e trasparenti sulla decisione di raccogliere le informazioni e i dati personali di*

---

[91] Art 29 WP Opinion on Legitimate Interests (n 77).

[92] Der Landesbeauftragte für den Datenschutz Baden-Württemberg, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen', p. 9.

[93] EDPS (n 57).

coloro che partecipano alle assemblee pacifiche e sulla loro condivisione o conservazione[94]

87. Internet e le piattaforme di *social media* sono giunti a rivestire un ruolo vitale per lo sviluppo non solo dell'identità online delle persone, ma anche della loro vita sociale, politica e privata. Costituiscono lo scenario di vita digitale degli spazi civici dei nostri giorni, dove le persone accedono alle informazioni, formulano e discutono le proprie idee, sollevano opinioni dissenzienti, considerano possibili riforme, mettono a nudo pregiudizi e corruzione, e si organizzano per sostenere il cambiamento politico, economico, sociale, ambientale e culturale della società.[95]

88. Per un Internet sano, stimolante e aperto, è essenziale che le persone si sentano libere di condividere foto e informazioni personali come meglio credono, senza il timore che queste siano immediatamente intercettate e conservate per scopi non dichiarati. La libertà di definire se stessi come più si ritiene opportuno in vari spazi su Internet, controllando la distribuzione di specifiche informazioni in vari luoghi, viene sottratta dalla minaccia incombente che tutte queste diverse informazioni possano essere rintracciate e riunificate con un semplice click.

(c) Danni per le comunità vulnerabili

89. Lo strumento di Clearview può anche arrecare particolare danno alle persone in posizioni vulnerabili. Per questa sezione abbiamo attinto molte informazioni dal lavoro di documentazione dell'American Civil Liberties Union (ACLU) - sul quale vorremmo attirare l'attenzione - relativo ai reclami da loro presentati contro Clearview nello stato dell'Illinois, dove vige il Biometric Information Privacy Act (BIPA).[96]

90. Gli individui in posizioni vulnerabili corrono un rischio maggiore laddove vengano identificati nella loro vita e abitudini di tutti i giorni. Ad esempio, i migranti e le vittime di violenza sessuale o di sfruttamento sessuale a scopo commerciale, hanno ripetutamente subìto molestie o discriminazioni sia da parte di privati cittadini che da agenti di polizia. "Privando queste persone del controllo e della sicurezza dei propri identificatori biometrici sensibili e minacciando di rendere estremamente semplice la loro identificazione e il loro tracciamento sia online che nel mondo fisico, il sistema Clearview li espone ad atti persecutori, a molestie e a violenze."[97] La paura di essere identificati può inoltre dissuadere queste persone dal frequentare luoghi e riunioni che permetterebbero loro di accedere ai servizi di supporto di cui hanno bisogno.

---

[94] Disponibile al seguente link https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx.

[95] Privacy International, 'Protecting civic spaces' (May 2019). Disponibile al seguente link https://privacyinternational.org/sites/ default/files/2019-07/Protectin%20civic%20spaces%20PI%20May%202019.pdf.

[96] Complaint, ACLU and others v. Clearview AI, Inc., Circuit Court of Cook County, Illinois, Case No.: 2020 CH 04353. Disponibile al seguente link https://www.aclu.org/legal-document/aclu-v-clearview-ai-complaint.

[97] Plaintiff's response to defendant's motion to dismiss, ACLU and others v. Clearview AI, Inc., Circuit Court of Cook County, Illinois, Case No.: 2020 CH 04353.

91. Inoltre, l'*hashing* dei vettori, che viene eseguito nel momento in cui Clearview estrae le caratteristiche biometriche dalle immagini facciali, rende possibile la categorizzazione dei volti delle persone in base ai gradi di somiglianza. Ciò dà la possibilità ai clienti di Clearview di eseguire raggruppamenti automatici di persone in base alla loro etnia, al colore della pelle, o altre categorizzazioni e apre la porta al tracciamento e al monitoraggio discriminatorio, o a pratiche come la polizia predittiva.

92. Dopo aver esposto i gravi e molteplici rischi e danni per i diritti e le libertà delle persone legati alle attività di Clearview, il Centro Hermes ritiene che la valutazione del bilanciamento dei legittimi interessi in gioco debba fondarsi su una base giuridica valida ai sensi dell'art. 6.1.f del GDPR. L'assenza di una base giuridica ai sensi dell'art. 6 è sufficiente per riscontrare un trattamento illegittimo; tuttavia, laddove l'Autorità non convenisse su questo punto, la prossima sezione valuta l'applicabilità di una base giuridica per il trattamento dei dati di categoria particolare.

Dati personali resi manifestamente pubblici - Articolo 9.2.e del GDPR

93. Dal momento che Clearview tratta dati di categorie particolari, oltre ad una base giuridica valida ai sensi dell'articolo 6 del GDPR (al momento assente, come dimostrato nella sezione precedente), Clearview deve anche soddisfare almeno una delle condizioni di cui all'art. 9.2 del GDPR. L'unica condizione riferibile alle circostanze in cui Clearview opera è che "il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato", ai sensi dell'articolo 9.2.e del GDPR. Anche considerando valida tale condizione, il Centro Hermes osserva che si applicherebbe solo alle immagini facciali (che sono di per sé dati biometrici, vd. sez. V.A di cui sopra) che Clearview raccoglie online; i dati biometrici che Clearview crea attraverso l'estrazione vettoriale non possono assolutamente soddisfare questa condizione.

94. Il fatto che le informazioni siano pubblicamente disponibili online non costituisce automaticamente una base giuridica per il loro trattamento ai sensi dell'art. 9. Come autorevolmente riconosciuto da diverse linee guida delle autorità di protezione dei dati e dai relativi commenti del mondo accademico, l'eccezione di cui all'articolo 9.2.e deve essere interpretata in modo restrittivo.[98] In particolare, i termini "manifestamente" e "dall'interessato" richiedono circostanze molto specifiche in cui i dati personali siano stati resi pubblici.

95. In primo luogo, le informazioni pubblicamente disponibili online devono comunque essere adeguatamente tutelate tramite una significativa protezione della privacy. Trattasi, questo, di un presupposto essenziale per un Internet sano e aperto, dove le persone possano esercitare i propri diritti e libertà fondamentali, e deriva dal principio di limitazione delle finalità perché ogni

[98] Per ulteriori informazioni e riferimenti sulle linee guida delle Autorità, vedere Edward S Dove and Jiahong Chen, 'What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9(2)(e)' (2021) Vol. 00, No. 0, International Data Privacy Law, 1, 2. Disponibile al seguente link https://doi.org/10.1093/idpl/ipab005.

azione di "rendere pubblico" qualcosa avviene per uno scopo specifico. La pubblicazione di un CV con dati di contatto sul proprio sito web è fatta allo scopo di trovare un lavoro. Un titolare del trattamento violerebbe chiaramente lo scopo originale se usasse quei dati a fini pubblicitari o se un'agenzia di rating del credito usasse i dati per valutare l'affidabilità creditizia dell'individuo. Lo strumento di riconoscimento facciale di Clearview è l'archetipo di una nuova tecnologia apparentemente innocua che, laddove ne siano concessi la distribuzione e l'utilizzo su vasta scala, rischia di alterare profondamente Internet come lo conosciamo oggi e il comportamento delle persone online. Ad oggi, Clearview opera sul presupposto errato che ciò che è pubblicamente disponibile su Internet appartiene immediatamente ad una sfera completamente pubblica e che è stato benevolmente offerto al mondo intero per essere visto all'istante e riutilizzato a piacimento. Tuttavia, nelle società moderne in cui la maggior parte delle nostre vite economiche, sociali e democratiche sono condotte online, una netta divisione tra la sfera pubblica e quella privata è poco rilevante. È scorretto considerare Internet, difatti, come uno spazio omogeneo, interamente pubblico e completamente accessibile, in cui tutti gli utenti acconsentono a lasciare le proprie informazioni personali "alla mercé" di chiunque non appena queste entrano in una parte tecnicamente pubblica di Internet.[99]

96. I pericoli di una contrapposizione così netta sono molto reali anche nel mondo offline, come già riconosciuto dalla Corte europea dei diritti dell'uomo. Come la Corte ha dichiarato nella causa *Peck c. Regno Unito*[100], la divulgazione ai media per la relativa trasmissione di filmati che ritraevano il ricorrente, provenienti da telecamere a circuito chiuso che avevano filmato il suo tentativo di suicidio, ha costituito una grave ingerenza nella vita privata del ricorrente, nonostante questo si trovasse in quel momento in un luogo pubblico. In quel caso, il ragionamento della CEDU si basava sul presupposto che nessuna persona può ragionevolmente aspettarsi che i filmati che ritraggono aspetti sensibili della propria vita privata siano poi diffusi dai media, anche se le sue azioni sono "già di dominio pubblico".[101]

97. In secondo luogo, qualunque utente di Internet e dei social media, seppur non prettamente esperto nel loro utilizzo, sa bene che molte foto online che ritraggono persone non sono state rese pubbliche *dal soggetto interessato*. I social media permettono agli utenti di caricare foto non solo di se stessi, ma di qualsiasi altra persona. Queste ultime (siano esse degli amici di chi ha caricato le immagini o semplici passanti in uno spazio pubblico) non hanno caricato in prima persona le proprie immagini facciali online, e potrebbero ignorare il fatto che foto che ritraggono il loro volto sono state caricate e sono presenti su Internet.

---

[99] Vedere la citazione del GEPD al paragrafo 85, e quella del UNHRC al paragrafo 86.

[100] App no 44647/98 (ECtHR, 28 January 2003), paras 53, 61-62.

[101] Ibid.

98. L'OPCC è giunto alla stessa conclusione nel valutare se i dati personali che Clearview raccoglie rientrano o meno nell'eccezione canadese delle "pubblicazioni", eccezione che si applica solo "laddove la persona abbia fornito le informazioni" o dove "è ragionevole supporre che l'interessato abbia fornito tali informazioni". Secondo l'OPCC: "Dato che Clearview effettua la raccolta massiva di immagini col supporto di strumenti automatizzati, in molti casi, è inevitabile che le immagini siano invece state caricate da una terza parte".[102] Come avvenuto nel caso riportato da Vice Italia.[103]

99. In terzo luogo - come spiegato nella sezione III del presente documento - una volta raccolte, le foto vengono conservate nel *database* di Clearview a tempo indeterminato, senza alcun riguardo del fatto che queste foto siano ancora pubblicamente disponibili o meno. Come giustamente osservato in un articolo del New York Times su Clearview, "se il vostro profilo è già stato sottoposto a *web scraping*, ormai è troppo tardi. La società conserva tutte le immagini che ha raccolto, anche se queste vengono poi cancellate o rimosse dal web" e aggiunge: "il Sig. Ton-That ha comunque dichiarato che la società stava lavorando a uno strumento che avrebbe permesso agli interessati di richiedere che le immagini fossero rimosse, qualora queste fossero state cancellate dal sito internet di origine". In riferimento a quest'ultima "scusa", è innanzitutto inaccettabile che Clearview abbia implementato la propria tecnologia senza l'esistenza di tale strumento e, in secondo luogo, questo strumento costituirebbe comunque una possibilità di ricorso estremamente limitata; implicherebbe infatti che gli interessati: (1) sappiano in primo luogo che Clearview raccoglie le loro immagini facciali, (2) presentino sistematicamente richieste di accesso ai dati per sapere quali foto sono state raccolte da Clearview, (3) confrontino i risultati di queste richieste con ciò che hanno reso disponibile online, e (4) presentino richieste individuali di rimozione.[104] Ciò è del tutto irragionevole e un affronto lampante al diritto delle persone di detenere il controllo sulla propria identità online, impedendo qualsiasi esercizio effettivo dei diritti degli interessati previsti dal GDPR.

100. Infine, le impostazioni di privacy sono notoriamente difficili da modulare e regolare per fare in modo che le informazioni che si desiderano circoscrivere a gruppi privati online siano effettivamente condivise e rimangano accessibili solo all'interno di tali cerchie. Le ricerche svolte dal Centro Hermes e da altre associazioni, come Privacy International, hanno ripetutamente dimostrato quanto sia complesso per gli utenti regolare le proprie impostazioni secondo il livello di privacy desiderato e che spesso i requisiti di validità legale del consenso non sono soddisfatti.[105] Questi “dark patterns", come definiti dal

---

[102] OPCC (n 4), para 66.

[103] Vice Italia (25 marzo 2020) (n 20)

[104] Hill (n 6).

[105] Privacy International, ‘Most cookie banners are annoying and deceptive. This is not consent.’ (21 May 2019). Disponibile al seguente link https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent. Privacy International, ‘Facebook - Profile Settings’ (7 January 2021). Disponibile al seguente link https://privacyinternational.org/guide-step/3959/facebook-profile-settings.

Consiglio norvegese dei consumatori, implicano l'impossibilità per gli interessati di detenere sempre il controllo sui propri dati personali online.[106]

101. Pertanto, il Centro Hermes sostiene che Clearview non può soddisfare alcuna condizione per il trattamento di dati di categoria particolare ai sensi dell'articolo 9.2.e del GDPR.

E. Limitazione della finalità

100. Un altro principio fondamentale della protezione dei dati palesemente calpestato dal trattamento di Clearview è quello della limitazione della finalità, ai sensi dell'articolo 5.1.b del GDPR, e come menzionato sopra in relazione all'articolo 9.2.e GDPR. L'applicazione del principio dovrebbe considerare i fattori elencati nell'articolo 6.4, che in questo caso indicano chiaramente che il trattamento di Clearview non è compatibile con lo scopo per cui i dati personali sono stati inizialmente divulgati.

101. La questione della limitazione delle finalità è intrinsecamente legata a come l'utente si può aspettare che vengano utilizzati i propri dati personali disponibili al pubblico, come già illustrato nei paragrafi da 55 a 65 di cui copra. Il Centro Hermes ha dimostrato che il loro riutilizzo per il trattamento all'interno di una banca dati biometrica non rientra chiaramente in tali aspettative. Come affermato dal GEPD, i vari utilizzi dei dati personali nel contesto del *Social Media Monitoring* "comportano spesso l'utilizzo dei dati personali al di là della loro finalità e del loro contesto iniziali e in modi che l'interessato non poteva ragionevolmente prevedere".[107]

102. La seguente dichiarazione sulla biometria, contenuta nel parere del Gruppo di lavoro Articolo 29, è particolarmente eloquente:

> *In assenza di una base legale specifica (ad esempio, il consenso) per questo nuovo scopo, le fotografie su internet, sui* social media*, nelle applicazioni di gestione o condivisione delle foto online non possono essere ulteriormente elaborate per estrarne modelli biometrici o per essere inserite in un sistema biometrico per riconoscere in automatico le persone fotografate (riconoscimento facciale). Se esiste una base giuridica per questo secondo scopo, il trattamento deve comunque essere adeguato, pertinente e non sproporzionato in relazione a tale scopo. Se il soggetto interessato ha acconsentito al trattamento delle fotografie che lo ritraggono per essere taggato in automatico in un album fotografico online tramite un algoritmo di riconoscimento facciale, questo trattamento deve essere realizzato in modo rispettoso della protezione dei dati: i dati biometrici non più necessari dopo l'etichettatura delle immagini con il nome, il* nickname *o qualsiasi altro testo specificato dall'interessato devono essere cancellati. La*

[106] Norwegian Consumer Council, 'Deceived by Design – How tech companies use dark patterns to discourage us from exercising our rights to privacy' (27 June 2018). Disponibile al seguente link https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[107] EDPS (n 57).

creazione di una banca dati biometrica permanente non è a priori necessaria a tale scopo.[108]

103. Alla luce di questa dichiarazione, il trattamento di Clearview costituisce uno scopo completamente nuovo rispetto a quello dell'originale pubblicazione dei dati, e in quanto tale deve avere una base giuridica valida separata. Come dimostrato precedentemente nella sezione V.D, tale base risulta inesistente, risultando in una violazione del principio di limitazione della finalità da parte di Clearview.

104. Si conclude che le pratiche di Clearview costituiscono una violazione dei principi di trasparenza, equità e limitazione della finalità, così come del requisito di un fondamento giuridico. Il Centro Hermes non cercherà di valutare la conformità al GDPR dell'uso dello strumento da parte dei clienti di Clearview che non siano le autorità preposte all'applicazione della legge, essendo queste autorità gli unici clienti coi quali Clearview commercializza apertamente. Vorremmo tuttavia attirare l'attenzione dell'Autorità sulle previsioni di alcuni "ufficiali di polizia e investitori di Clearview", che sostengono che lo strumento "finirà per essere disponibile al pubblico".[109]

VI. Quadro giuridico e preoccupazioni: Trattamento da parte delle autorità preposte all'applicazione della legge (LED / Decreto)

105. Le limitazioni dei diritti fondamentali delle persone devono essere stabilite da misure legislative in relazione a questioni di estrema importanza quali ad esempio la sicurezza dello Stato, la difesa, la prevenzione, le indagini di polizia, l'accertamento o il perseguimento di reati, ecc. Se, tramite il d.lgs. 18 maggio 2018, n. 51, tali ristrette limitazioni possono applicarsi al trattamento da parte delle autorità preposte all'applicazione della legge, queste non potranno in alcun modo applicarsi ad un soggetto commerciale che raccoglie dati personali in modo indiscriminato, con il potenziale fine ultimo di vendere l'uso di tale *database* ad autorità soggette a una rigida regolamentazione. Come più volte osservato nel lavoro dell'associazione Privacy International,[110] l'utilizzo di strumenti privati per l'applicazione della legge porta spesso ad eludere le estese garanzie stabilite nei confronti delle autorità pubbliche a tutela dei diritti fondamentali.

106. Sebbene il Centro Hermes ritenga che le violazioni del GDPR individuate nella sezione V siano di per sé sufficienti all'emissione di un'ordinanza contro la raccolta dei dati personali degli utenti in Italia da parte di Clearview, si sottolinea che tali violazioni risultano ancora più evidenti se considerate in

---

[108] Art 29 WP (n 89), p.7.

[109] Hill (n 6).

[110] See for example: Privacy International, 'Public-Private surveillance partnerships'. Disponibile al seguente link https://privacyinternational.org/campaigns/unmasking-policing-inc; Privacy International, 'One Ring to watch them all' (25 June 2020). Disponibile al seguente link https://privacyinternational.org/long-read/3971/one-ring-watch-them-all.

relazione all'utilizzo finale previsto dei dati personali raccolti e trattati da Clearview. Se l'Autorità intende permettere le pratiche di raccolta dati da parte di Clearview in Italia, il Centro Hermes sostiene che, al fine di limitare il danno causato agli interessati, si debba vietare l'uso dei dati personali così raccolti da parte delle autorità preposte all'applicazione della legge. Tale utilizzo è infatti motivo di grave preoccupazione e viola il d.lgs. 18 maggio 2018, n. 51.

107. La presente sezione del reclamo espone in primo luogo le preoccupazioni del Centro Hermes riguardo all'uso delle tecnologie di riconoscimento facciale e di SOCMINT da parte delle forze dell'ordine, preoccupazioni ancora maggiori quando queste tecnologie vengono usate insieme, come nel caso di Clearview. In secondo luogo, si analizzerà come tali preoccupazioni si traducono in varie violazioni del d.lgs. 18 maggio 2018, n. 51 e del GDPR, in particolare del principio di protezione dei dati e del requisito di liceità.

A. Preoccupazioni sull'uso di tecnologie di RF e SOCMINT da parte della polizia

108. L'uso delle tecnologie di RF da parte della polizia ha un profondo impatto sul modo in cui la nostra società viene monitorata e sorvegliata. L'introduzione di tecnologie così invadenti non solo pone importanti questioni legate alla privacy e alla protezione dei dati, ma anche problematiche etiche relative all'autorizzazione da parte delle democrazie moderne dell'utilizzo di tali tecnologie. Con lo strumento di Clearview in mano, la polizia può di fatto identificare ogni singola persona ripresa dalle telecamere (o almeno associare la loro identità fisica alla loro presenza online). Una forza di polizia potrebbe molto realisticamente decidere di identificare ogni singolo individuo in una folla di manifestanti e costruire su di questi dei profili sulla base delle informazioni reperite online. Questa è una possibilità completamente distopica che può realisticamente concretizzarsi grazie allo strumento di Clearview.

109. Nel parere dell'Autorità sul sistema SARI Real-Time, si sottolinea infatti come i dati biometrici processati nel riconoscimento facciale siano dei sistemi ontologicamente diversi da quelli dei sistemi di videosorveglianza e di ripresa fotografica, audio e video. E inoltre che:

> *Il trattamento di immagini volte ad identificare le persone nel contesto pubblico è quindi di estrema delicatezza ed è perciò necessaria una valutazione d'insieme, per evitare che singole iniziative, sommate tra loro, definendo un nuovo modello di sorveglianza introducano, di fatto, un cambiamento non reversibile nel rapporto tra individuo ed autorità.*[111]

Nel caso di Clearview, il sistema in argomento realizza un trattamento automatizzato su larga scala che può riguardare, tra l'altro, anche coloro che siano presenti a manifestazioni politiche e sociali. Questo avviene tramite la raccolta di immagini da fonti disponibili pubblicamente e di cui le persone

[111] Garante per la protezione dei dati personali, 'Parere sul sistema SARI Real Time' (25 marzo 2021). Disponibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877.

presenti nelle foto potrebbero non essere a conoscenza (come nel caso in cui le foto siano state caricate su internet da soggetti terzi).

110. Le tecnologie di riconoscimento facciale impiegate negli spazi pubblici per controlli di polizia non solo costituiscono un'ingerenza nel diritto alla vita privata e alla protezione dei dati degli interessati, ma possono altresì minare seriamente l'esercizio di diritti quali la libertà di pensiero, di coscienza e di religione, la libertà di espressione e la libertà di riunione e di associazione. Il GEPD ha evidenziato che l'uso delle tecnologie di RF "è principalmente una questione etica, per una società democratica", poiché può "ovviamente inibire le libertà personali di espressione e di associazione".[112]

111. Nella sua relazione sull'articolo 21 della Convenzione internazionale sui diritti civili e politici indirizzata al Comitato per i Diritti Umani delle Nazioni Unite, Privacy International ha evidenziato come le nuove tecnologie di sorveglianza possano influenzare l'esercizio del diritto di riunione pacifica, sortendo *"un effetto dissuasivo sulle persone"*[113]. Ciò è stata confermato dal Commento generale n. 37: "Sebbene le tecnologie di sorveglianza possono essere utilizzate per rilevare minacce di violenza e quindi per proteggere il pubblico, possono anche violare il diritto alla privacy e altri diritti dei partecipanti e degli astanti e avere un effetto dissuasivo."[114] A causa di tale effetto, per le autorità che desiderano fare uso di queste tecnologie è estremamente difficile, se non impossibile, misurarne con precisione gli effetti negativi sull'esercizio dei suddetti diritti, e di conseguenza giustificarne l'utilizzo.[115] Al riguardo, l'Alto Commissario delle Nazioni Unite per i diritti umani ha invitato gli stati a non utilizzare mai tecnologie di RF "per identificare coloro i quali partecipano pacificamente a una adunata".[116]

112. In aggiunta al RF, lo strumento di Clearview permette anche di condurre operazioni di SOCMINT in piena luce, senza impiegare profili social sotto copertura o raccolta di informazioni mirate su singoli soggetti.

113. In Italia il tema della SOCMINT è già oggetto dell'attenzione della vostra Autorità. Come riportato da Vice Italia, il Ministero dell'Interno ha acquistato all'interno del progetto CRAIM un sistema per la trascrizione e il riconoscimento delle impronte vocali a partire da audio/video trovati sui social network. Nel 2017 la vostra Autorità aveva comunicato che avrebbe fatto richiesta al

---

[112] EDPS, 'Facial Recognition: A solution in search of a problem?' (28 October 2019). Disponibile al seguente link https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en.

[113] Privacy International, 'Submission on Article 21 of the International Covenant on Civil and Political Rights' (February 2019), p. 10. Disponibile al seguente link https://privacyinternational.org/sites/default/files/2019-03/Submission%20on%20Article%2021%20of%20ICCPR_0.pdf.

[114] UN Human Rights Committee (n 94), para 10.

[115] Privacy International, 'Protecting Civic Spaces' (1 May 2019). Disponibile al seguente link https://privacyinternational.org/long-read/2852/protecting-civic-spaces.

[116] OHCHR (n 87), para 54(h).

Ministero dell'Interno per ottenere informazioni ed elementi utili per valutare il progetto CRAIM.[117]

114. Il Centro Hermes teme che non vi siano sufficienti garanzie per gestire l'impiego della SOCMINT. Le forze dell'ordine (e le agenzie di intelligence) potrebbero ritenere che qualsiasi dato che un social network imposta come pubblicamente disponibile sul proprio sito sia, pertanto, un bersaglio legittimo da raccogliere e trattare senza sufficienti regole, supervisione, e tutele.

115. Il *Social Media Monitoring* pone rischi significativi per i diritti fondamentali delle persone. Le autorità preposte alla regolamentazione e gli organismi delle Nazioni Unite hanno evidenziato la necessità che tale condotta si attenga a misure di garanzia ben precise. Nella sua giurisprudenza, la Corte europea dei diritti dell'uomo ha sottolineato che "[l]a legislazione interna deve prevedere pertanto, le garanzie necessarie per impedire qualsiasi utilizzo di dati personali che non sia conforme con le garanzie sancite [nell']" articolo 8 della Convenzione. Tali garanzie devono disciplinare tutte le operazioni di trattamento dei dati personali da parte delle autorità pubbliche, ivi comprese la raccolta, conservazione o stoccaggio, analisi, diffusione o divulgazione, o qualsiasi altra forma di trattamento di tali dati personali.[118] Come la Corte ha evidenziato in *Marper*:

> *La necessità di tali garanzie risulta essere ancora maggiore allorché sia in gioco la protezione di dati personali sottoposti a trattamenti automatizzati e ancora di più quando tali dati siano utilizzati a fini di indagini di polizia. Il diritto interno dovrebbe assicurare non solo che siffatti dati siano rilevanti e non eccessivi in relazione alle finalità per le quali essi sono conservati, ma anche che essi siano conservati in una forma che consenta l'identificazione del titolare degli stessi per un periodo non eccedente a quello che è strettamente necessario in base alle finalità per le quali essi sono registrati […]. Il diritto interno deve altresì prevedere una serie di garanzie in grado di assicurare che i dati personali conservati siano efficacemente protetti da utilizzazioni improprie ed abusive […]. Le considerazioni che precedono valgono soprattutto in relazione alla protezione delle categorie speciali di dati particolarmente sensibili.*[119]

116. Nel complesso, il monitoraggio su larga scala può interferire con i diritti delle persone di esprimersi in modo anonimo, di formulare e condividere i propri pensieri, di partecipare a discussioni controverse o a raduni pubblici e di presentare richieste di risarcimento o reclami nei confronti del governo. Sul lungo periodo, ciò potrebbe sfociare nell'autocensura: gli utenti potrebbero infatti evitare di visitare certi profili sui *social media*, di mettere "mi piace", condividere o ritwittare *post* controversi, di unirsi a certi gruppi di discussione o persino di usare certe parole. In ultima istanza, questa autocensura è passibile

---

[117] Vice Italia, 'Ora la polizia può analizzare le voci nei video sui social' (7 settembre 2017). Disponibile al link https://www.vice.com/it/article/evv3xp/i-video-che-metti-online-vengono-spiati-dalla-polizia-italiana.

[118] *S. and Marper v. UK* [GC], App nos 30562/04 and 30566/0 (ECtHR, 12 April 2008), para 103.

[119] Ibid.

di cambiare il modo in cui si reperiscono le informazioni, si sviluppano e discutono le proprie idee e ci si organizza di conseguenza.[120]

117. Inoltre, la raccolta e la prassi di raccogliere ed elaborare informazioni pubblicamente accessibili per la raccolta di dati di *intelligence* può portare al tipo di abusi che osserviamo in altre forme di sorveglianza discreta o in altre operazioni di polizia. Questo può comportare la presa di mira sistematica di certi gruppi etnici e religiosi da parte delle forze dell'ordine. In assenza di preavviso, trasparenza e supervisione, è impossibile garantire l'assenza di pregiudizi razziali o religiosi nel monitoraggio online e, dato che le forze dell'ordine rimangono spesso riservate sul ricorso al *Social Media Monitoring* e sulle proprie fonti di informazione, può essere estremamente difficile per un cittadino contestare un qualsiasi potenziale utilizzo illecito di tali dati.[121]

118. Qualsiasi trattamento di dati personali pubblicati sui *social media* effettuato da parte delle autorità, per scopi che vanno al di là di ciò che le persone potrebbero aspettarsi o prevedere, è da considerarsi una grave ingerenza nel diritto al rispetto della vita privata degli interessati, in particolare quando tale trattamento comporta l'uso di tecnologie di riconoscimento facciale per collegare e accostare fonti di informazione. Sostenere il contrario significherebbe negare la necessaria protezione offerta dalla Convenzione europea per i diritti dell'uomo alla vita privata delle persone nell'ambiente digitale, contesto "in cui in determinati casi si può essere facilmente vittime di abusi e si può andare incontro a conseguenze estremamente dannose per la società democratica nel suo complesso".[122]

B. Violazione del primo principio in materia di protezione dei dati: Liceità

119. Ai sensi dell'art. 5 del Decreto, in attuazione dell'art. 3 della Direttiva UE 2016/680, i trattamenti di dati personali da parte degli organi di Polizia devono basarsi su disposizioni di legge o, ove da questa previsto, di regolamento. I dati personali oggetto del trattamento in argomento rientrano nelle categorie particolari di dati di cui all'art. 9 del GDPR, "dati biometrici intesi a identificare in modo univoco una persona fisica". Inoltre, per le circostanze di funzionamento della piattaforma di Clearview descritte in precedenza, in relazione alla raccolta di immagini scattate durante manifestazioni pubbliche, il trattamento in argomento determina il possibile coinvolgimento di ulteriori dati personali di cui all'art. 9 del GDPR, quali quelli idonei a rivelare le opinioni politiche, religiose o l'appartenenza sindacale.

120. L'Autorità ha pubblicato a marzo 2021 un parere sul sistema SARI Real-Time del Ministero dell'Interno, evidenziando come le tecnologie per il

---

[120] Privacy International, 'Protecting Civic Spaces' (n 115).

[121] Privacy International, 'Is your Local Authority looking at your Facebook likes?' (May 2020), p. 7. Disponibile al seguente link https://privacyinternational.org/sites/default/files/2020-05/Is%20Your%20Local%20Authority%20Looking%20at%20your%20Facebook%20Likes_%20May2020.pdf.

[122] *Klass v. Germany*, App no 5029/71 (ECtHR, 6 September 1978), para 56.

riconoscimento facciale in tempo reale determinino “una forte interferenza con la vita privata delle persone interessate che deve trovare giustificazione in una adeguata base normativa.” E che al momento in Italia “non si rinviene alcuna disposizione specifica che consenta tale tipo di trattamento.” L’impiego dello strumento per il riconoscimento facciale offerto da Clearview è l’equivalente online del riconoscimento facciale in tempo reale—lasciare un’immagine di sé su parti di internet pubblicamente accessibili è molto simile, nel processo, all’esporsi negli spazi pubblici fisici. Ed è un’esposizione addirittura molto più involontaria, in quanto i soggetti potrebbero non essere nemmeno a conoscenza del fatto che vi siano loro immagini pubblicate online, e molto spesso quelle stesse immagini sono collegate ad altre informazioni quali nome, professione, rete sociale, etc.

121. La tecnologia di Clearview è quindi uno strumento per la sorveglianza di massa poiché chiunque potrebbe essere incluso nel database di Clearview e essere quindi aggiunto, indiscriminatamente, a una watchlist.

122. Questa parte espone le ragioni per cui un qualsiasi utilizzo dello strumento di Clearview da parte delle forze dell’ordine non può soddisfare i requisiti di cui all’art. 5 e 7 del Decreto, essendo il suddetto uso:

    (a) Non basato sulla legge - art. 5; e
    (b) Non strettamente necessario - art. 7;

Non basato sulla legge

123. L’assenza di una base legale per l’impiego di tecnologie per il riconoscimento facciale in tempo reale è stata sottolineata dall’Autorità nella vostra opinione sul sistema SARI Real-Time.

124. Inoltre, mentre nel caso del sistema SARI Enterprise sembra riscontrasi una base legale per il trattamento[123] — infatti, i soggetti inclusi nel database AFIS dovrebbero sapere di essere stati fotosegnalati e vi è una base legale per quel fotosegnalamento — nel caso di Clearview la situazione è completamente differente: con la raccolta ed estrazione dei vettori dei volti si effettua un trattamento di dati biometrici ontologicamente diverso da quello effettuato dai sistemi di videosorveglianza o fotografia, e chiaramente diverso da quello svolto nelle attività di fotosegnalamento. Per di più, oggetto di questo trattamento è qualunque persone che ha almeno una foto del proprio volto caricata online.

125. Infine, come spiegato nella sezione VI.A, Clearview pone dei rischi anche per quanto riguarda l’impiego di strumenti di SOCMINT, tema tutt’ora all’attenzione della vostra Autorità. Per tutti questi motivi, l'utilizzo dello strumento Clearview da parte delle autorità preposte all’applicazione della legge non può essere

[123] Garante per la protezione dei dati personali, ‘Sistema automatico di ricerca dell’identità di un volto’ (26 luglio 2018). Disponibile al link https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9040256.

considerato legittimo, né tanto meno basato su disposizioni di legge chiare, precise e prevedibili nella loro applicazione.

Non strettamente necessario

126. Il principio di necessità richiede che la polizia provi l'esistenza di una minaccia concreta, specifica e immediata alla sicurezza nazionale o alla sicurezza pubblica, che giustifichi la necessità di impiegare questo tipo di tecnologia. La Corte europea dei diritti dell'uomo applica una valutazione di stretta necessità alle ingerenze nel diritto alla privacy nel contesto della sorveglianza. In *Szabó e Vissy c. Ungheria*, la CEDU ha indicato che, visto "il potenziale delle tecnologie di sorveglianza all'avanguardia di invadere la privacy dei cittadini",

> *[una] misura di sorveglianza segreta può essere considerata conforme alla Convenzione solo se valutata strettamente necessaria, in termini generali, per la salvaguardia delle istituzioni democratiche e al contempo ritenuta imprescindibile, nello specifico, per ottenere informazioni vitali relative a una singola operazione. Secondo la Corte, qualsiasi misura di sorveglianza segreta che non corrisponda a questi criteri sarà propensa ad abusi da parte delle autorità che dispongono delle tecnologie più altamente evolute. La Corte nota che sia la Corte di giustizia dell'Unione Europea che il Relatore speciale delle Nazioni Unite richiedono che le misure di sorveglianza segreta rispondano ad un criterio di assoluta necessità; approccio considerato opportuno dalla stessa Corte dei diritti.*[124]

127. Il Centro Hermes ritiene che lo strumento di Clearview non sia mai da considerarsi strettamente necessario, perché il suo utilizzo costituisce un salto nel buio; difatti, la polizia non potrà mai essere sicura che il suo utilizzo possa produrre una corrispondenza positiva, contrariamente a ciò che accade quando si attinge alle watchlist "tradizionali", contenenti esclusivamente fotografie di persone sospettate.

128. La CGUE ha affermato inoltre che le misure di conservazione dei dati - per essere limitate ai casi di assoluta necessità - devono essere soggette a restrizioni che "circoscrivono, nella pratica, la portata della misura e, di conseguenza, il pubblico interessato".[125] Nel caso di Clearview, tale pubblico corrisponde di fatto all'intera popolazione, posto che chiunque viene inserito nella watchlist. Nel caso di Clearview, anche se la conservazione dei dati avviene da parte di una società privata piuttosto che della polizia, dovrebbe applicarsi lo stesso principio: i danni già identificati da più tribunali e autorità, dovuti alla conservazione di dati personali in modo indiscriminato e per un tempo indefinito, rimangono di fatto gli stessi quando le autorità di contrasto hanno accesso incondizionato al *database* di Clearview. Il Centro Hermes sollecita l'Autorità a intervenire per prevenire che le autorità pubbliche eludano i propri obblighi in materia di diritti umani e di protezione dei dati, impedendo a

---

[124] App no 37138/14 (ECtHR, 13 October 2015), para 73.

[125] Joined Cases C–203/15 and C–698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson* [2016] ECR I–970, para 110.

queste di affidarsi ad uno strumento privato per le proprie operazioni di sorveglianza senza che tale strumento sia sottoposto alle stesse obbligazioni.

129. Inoltre, l'attività indiscriminata da parte di Clearview di raccolta, archiviazione ed elaborazione di immagini fotografiche può essere facilmente paragonata a qualsiasi altra attività di raccolta su larga scala, già considerata illegittima.[126] Nel caso di banche dati così ampie, esiste un notevole rischio di incorrere in abusi, motivo per cui la CGUE ha ritenuto che "l'accesso generalizzato a tutti i dati conservati non può considerarsi strettamente necessario, indipendentemente dall'esistenza di un legame - diretto o indiretto - con lo scopo perseguito". [127]

130. Per valutare la necessità di tale pratica, dovrebbe essere considerato il principio di proporzionalità: come da *Necessity toolkit* del GEPD sulla valutazione della necessità, quest'ultima è di fatto soggetta alla proporzionalità, di modo che anche una misura strettamente necessaria deve essere soggetta alla verifica di proporzionalità.[128] In *S. e Marper c. Regno Unito,* la Corte europea dei diritti dell'uomo si è occupata di un'altra misura inerente alla conservazione indiscriminata di dati biometrici - nello specifico. impronte digitali e campioni cellulari e di DNA - per l'accertamento e il perseguimento dei reati.[129] In tale occasione ha osservato come:

> *la protezione offerta dall'articolo 8 della Convezione sarebbe indebolita in modo inaccettabile qualora si consentisse nel settore della giustizia penale l'utilizzo ad ogni costo di moderne tecniche scientifiche e ciò senza operare un attento bilanciamento tra i vantaggi che possono derivare da un ricorso generalizzato a tali tecniche e i fondamentali interessi che sono collegati al rispetto della vita privata. Secondo il punto di vista della Corte, il forte consenso esistente in proposito in seno agli Stati contraenti riveste una importanza considerevole e riduce il margine di apprezzamento di cui dispone uno Stato convenuto per determinare fino a che punto sono consentite in tale materia ingerenze nella vita privata. La Corte ritiene che qualsiasi Stato che pretenda di svolgere un ruolo pionieristico nello sviluppo di nuove tecnologie deve farsi carico anche della speciale responsabilità di individuare il corretto bilanciamento da applicare nella materia.*[130]

131. Le preoccupazioni espresse nella sezione VI.A di cui sopra dimostrano che lo strumento Clearview rappresenta una grave ingerenza nella vita privata, nella protezione dei dati e in altri diritti fondamentali. Questa grave ingerenza fa propendere fortemente per l'inesistenza di un qualsiasi potenziale beneficio

---

[126] Case C-623/17 *Privacy International v SSFCA and Ors* [2020] ECLI:EU:C:2020:790.

[127] Ibid, para 78.

[128] EDPS, 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit" (11 April 2017), p. 5. Disponibile al seguente link https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

[129] App nos 30562/04 and 30566/04 (ECtHR, 12 April 2008).

[130] Ibid, para 112.

delle tecnologie in questione. Inoltre, nel contesto delle tecnologie di riconoscimento facciale, sarà molto complesso effettuare un qualsiasi bilanciamento tra i benefici di tali tecnologie di sorveglianza ed i relativi danni ai diritti umani, data la difficoltà di apprezzare adeguatamente l'entità di questi ultimi a causa degli effetti inibitori delle tecnologie di RF. Per esempio, le autorità non sarebbero probabilmente in grado di valutare il numero esatto di persone che hanno scelto di non partecipare ad un evento pubblico, sacrificando la propria libertà di espressione e il proprio diritto di assemblea, a causa di legittime preoccupazioni relative all'uso improprio dei loro dati biometrici da parte della polizia. Considerati il volume e la natura indiscriminata dei dati raccolti e trattati da Clearview, insieme alle serie preoccupazioni in materia di diritti umani in relazione ad un loro utilizzo che possa facilitare l'apertura alle tecnologie di RF, il Centro Hermes sostiene che l'uso di Clearview da parte delle forze dell'ordine non potrà mai essere proporzionato.

VII. Istanze / Rimedi

135. Per i motivi fino a qui esposti, il Centro Hermes accoglie con favore la decisione di aprire un'istruttoria da parte dell'Autorità, e chiede con rispetto che l'Autorità tenga in considerazioni le preoccupazioni espresse in questa segnalazione e possa considerarle all'interno dell'istruttoria preliminare avviata nei confronti di Clearview.

136. Riassumendo, il Centro Hermes invita l'Autorità a considerare:

(a) La raccolta iniziale di immagini e il trattamento di dati biometrici da parte di Clearview, con riguardo a:

i. I principi di trasparenza e correttezza, in particolare rispetto alla ragionevole aspettativa di riservatezza da parte degli interessati;
ii. Il requisito di una base legale secondo quanto previsto dagli artt. 6 e 9 del GDPR, in particolare se il ricorso agli "interessi legittimi" e al "resi manifestamente pubblici" sia giustificato;
iii. Il principio di limitazione della finalità;

(b) L'impiego degli strumenti di Clearview da parte delle autorità preposte all'applicazione della legge, per quanto riguarda la liceità di tale trattamento, con particolare riguardo ai rischi per i diritti e le libertà fondamentali degli interessati.

137. Il Centro Hermes chiede che l'Autorità imponga a Clearview di cessare la raccolta e le attività di trattamento dei dati personali degli interessati in Europa, secondo quanto previsto dall'Art. 58.2.f del GDPR.

138. Inoltre, il Centro Hermes chiede che l'Autorità svolga un'indagine sull'impiego dello strumento di Clearview da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali italiane, secondo quanto previsto dall'Art. 37.3.a del Decreto.

139. Come indicato in questa segnalazione, le attività di raccolta e trattamento dei dati svolte da Clearview non conoscono confini, coinvolgendo potenzialmente individui che si trovano in qualsiasi paese del mondo. Per questo motivo, in conformità con le disposizioni di cooperazione e assistenza reciproca del Capo VII del GDPR, il Centro Hermes invita l'Autorità a collaborare con le altre autorità europee per la protezione dei dati personali che hanno ricevuto segnalazioni e reclami simili a questo del Centro Hermes e di altre associazioni della società civile.

Associazione Hermes

27 maggio 2021