Ordinanza ingiunzione nei confronti di Clearview AI - 10 febbraio 2022 [9751362]

VEDI ANCHE Comunicato stampa del 9 marzo 2022

[doc. web n. 9751362]

Ordinanza ingiunzione nei confronti di Clearview AI - 10 febbraio 2022

Registro dei provvedimenti
n. 50 del 10 febbraio 2022

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, l'avv. Guido Scorza, componente ed il cons. Fabio Mattei, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati, di seguito "Regolamento");

Scheda

Doc-Web
9751362

Data
10/02/22

Argomenti

Biometria
Particolari categorie di dati
Internet e social media
Intelligenza artificiale
Riconoscimento facciale

Tipologie

Ordinanza ingiunzione o revoca

Documenti citati

- Riconoscimento facciale: il Garante privacy sanziona Clearview per 20 milioni di euro Vietato l'uso dei dati biometrici e il monitoraggio degli italiani

VISTO il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196), come modificato dal d.lgs. 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento dell'ordinamento nazionale al citato Regolamento (di seguito "Codice");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione n. 98 del 4 aprile 2019, pubblicato in G.U. n. 106 dell'8 maggio 2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE l'avv. Guido Scorza;

PREMESSO

1. INTRODUZIONE

Il procedimento trae origine da una complessa attività istruttoria avviata d'ufficio a seguito di notizie stampa che hanno rivelato l'esistenza di diverse problematiche relative ai prodotti di riconoscimento facciale della società statunitense Clearview AI Inc. (di seguito "Clearview" o "Società").

Nel corso del 2021 l'Ufficio ha ricevuto quattro reclami presentati nei confronti di Clearview. Nello specifico:

- il 24 febbraio 2021 da parte del sig. XX (fascicolo n. XX);

- il 22 marzo 2021 da parte del sig. XX (fascicolo n. XX);

- il 1° giugno 2021 da parte del sig. XX (fascicolo n. XX);

- il 22 luglio 2021 da parte del sig. XX, che ha lamentato il mancato riscontro alle richieste di accesso ai dati ex art. 15 del GDPR, anche a seguito di due solleciti avvenuti il 25 maggio e il 18 giugno 2021 (fascicolo n XX).

I reclamanti XX, XX e XX hanno segnalato la circostanza che il trattamento dei loro dati sia avvenuto senza consenso ed hanno riferito della richiesta di Clearview di inviare copia di un documento di identità personale per dare seguito alle istanze di accesso presentate.

Dalla documentazione allegata ai reclami l'Ufficio ha rilevato che Clearview ha dato riscontro alle istanze di accesso dei reclamanti XX, XX e XX tramite appositi report contenenti i risultati della ricerca

Vedi anche (1)

- Riconoscimento facciale: il Garante privacy sanziona Clearview per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani

generata dal software. In particolare è emerso che:

- con riferimento al sig. XX, la Società dispone nei propri database di tre immagini indicizzate tramite i seguenti Url:

  https://...;

  https://...;

  https://...

- con riferimento al sig. XX, la Società dispone nei propri database di 13 immagini indicizzate tramite i seguenti Url:

  https://...

  https://...

  https://...

  https://...

  http://...

  https://...

  https://...

  https://...

  https://...

  https://...

  https://...

  https://...

  https://...

- con riferimento al sig. XX, la Società dispone nei propri database di 9 immagini indicizzate tramite i seguenti Url:

  http://...

  https://...

  https://...

  https://...

  https://...

  https://...

  https://...

  https://...

http://...

L'Autorità ha ricevuto anche due segnalazioni da parte di due organizzazioni impegnate nella difesa della privacy e dei diritti fondamentali delle persone.

Con nota del 19 febbraio 2021, l'associazione XX, oltre a segnalare i precedenti delle Autorità svedese e tedesca, ha posto all'attenzione dell'Autorità rilevanti criticità riguardo alla base giuridica del trattamento posto in essere da Clearview, nonché relativamente alle procedure adottate dalla società in materia di diritto di accesso (fascicolo n. XX).

Il 7 settembre 2021 la stessa associazione ha inviato un'ulteriore segnalazione con cui ha chiesto all'Ufficio di accertare la fruizione dei servizi offerti da Clearview da parte della Polizia di Stato.

Il 25 maggio 2021 l'organizzazione XX ha segnalato all'Ufficio criticità riguardo al trattamento posto in essere da Clearview, in particolare con riferimento alla base giuridica, al rispetto dei principi generali in materia di data protection ed ai rischi per i diritti e le libertà fondamentali degli interessati, derivanti dall'impiego del prodotto di Clearview da parte delle autorità preposte all'applicazione della legge (fascicolo n. XX).

2. ATTIVITÀ ISTRUTTORIA

Con nota del 25 marzo 2021 (prot. del Garante n. 16155/2021), in risposta alla richiesta d'informazioni dell'Autorità del 9 marzo 2021, la Società ha sostenuto la non applicabilità del Regolamento e quindi la carenza di giurisdizione del Garante italiano. In particolare, ha dichiarato i) di non offrire prodotti e servizi in Italia in quanto ha adottato misure tecniche volte a bloccare ogni tentativo di accesso alla piattaforma da parte di indirizzi IP italiani e ii) di non effettuare alcun monitoraggio ai sensi dell'art. 3, par. 2, lett. b) del Regolamento in quanto il concetto di monitoraggio implica un'osservazione continua e perdurante laddove l'unico prodotto di Clearview AI è un'applicazione per la ricerca di immagini che fornisce risultati di ricerca con collegamenti a siti web di terze parti. Tale tecnologia, dunque, secondo la Società, non traccerebbe né monitorerebbe le persone nel tempo, ma si risolverebbe in un'istantanea dei risultati della ricerca al momento del compimento della stessa, paragonabile alle operazioni di ricerca effettuate da Google Search. La Società ha riferito di non detenere alcun elenco di clienti italiani, di non aver inserito nella privacy policy alcun riferimento al Regolamento e di non aver nominato un rappresentante ai sensi dell'art. 27, in quanto anche tale norma, come il resto del Regolamento, non troverebbe applicazione alla attività dalla stessa svolta.

Con nota del 22 aprile 2021 (prot. n. 22235/2021), l'Ufficio, sulla base degli elementi acquisiti, ha notificato a Clearview, ai sensi dell'art. 166, comma 5, del Codice, l'avvio del procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento, avente ad oggetto le presunte violazioni di cui agli artt. 5, par. 1 lett. a), b ed e), 6, 9, 12, 13, 14 e 15 e 22 del Regolamento.

Con la medesima nota, la Società è stata invitata a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentita dall'Autorità (art. 166, commi 6 e 7, del Codice).

Con nota del 22 giugno (prot. n. 33759/2021), a seguito di una richiesta di proroga del termine in data 2 giugno (prot. 30734/2021), cui l'Ufficio ha dato riscontro in data 4 giugno (prot. 30787/2021), Clearview ha presentato la propria memoria difensiva, dichiarando che:

- sin dalla fine del 2019 le forze dell'ordine americane hanno promosso l'utilizzo dei prodotti Clearview, specie nell'ambito delle indagini sulla pornografia infantile. Ciò ha fatto sorgere un interesse internazionale per i prodotti Clearview che ha portato alla sottoscrizione di account di prova da parte di agenzie governative europee per un breve periodo di tempo;

- a marzo 2020, a seguito dei reclami ricevuti per il tramite di Autorità di controllo europee, tali account di prova, peraltro di numero esiguo, sono stati tutti chiusi e disattivati;

- attualmente Clearview non ha più alcun utente di prova europeo, né clienti stabiliti in Unione europea: ciò è assicurato da una precisa impostazione che impedisce l'accesso al software tramite indirizzi IP europei;

- la tecnologia sottesa al servizio è finalizzata a migliorare la sicurezza pubblica, riducendo i tempi delle indagini e adiuvando le forze dell'ordine nell'identificazione dei criminali (compresi criminali violenti, pedofili e narcotrafficanti). La Società mette in evidenza come queste attività siano svolte e sottoposte al diretto controllo delle autorità pubbliche che, sotto la loro responsabilità, decidono di utilizzare il software Clearview; l'utilizzo del software è soggetto alle condizioni d'uso, le quali prevedono che sia responsabilità del cliente verificare che l'utilizzo di tale prodotto sia legittimo alla luce delle normative locali ad esso applicabili. Pertanto, come per qualsiasi fornitore di tecnologia, non spetta alla Società occuparsi dell'uso della tecnologia o dei dispositivi da parte dei clienti;

- la valutazione della base giuridica per l'utilizzo del software da parte dei clienti o potenziali clienti non può essere una mission o responsabilità di Clearview;

- la Società richiede contrattualmente ai suoi clienti di condurre ulteriori indagini al fine di corroborare, in modo indipendente, tutte le informazioni raccolte utilizzando la tecnologia Clearview, in primis l'identificazione del soggetto avvenuta attraverso il suo software; nessuna decisione, per quanto a conoscenza della Società, viene presa solamente sulla base dei dati forniti dal software Clearview;

- per quanto concerne la giurisdizione, la Società, dopo aver ricordato di aver sede negli U.S.A. e di non avere alcuna filiale nell'Unione Europea, sostiene l'inapplicabilità dell'art. 3, par. 1, del Regolamento in quanto non è stabilita nell'Unione o in Italia e l'inapplicabilità dell'art. 3, par. 2, del Regolamento (targeting criterion) sia sotto il profilo dell'offerta di beni e servizi ad interessati che si trovano nell'Unione che del monitoraggio del loro comportamento nella misura in cui il monitoraggio avviene nell'Unione;

- con riferimento al criterio dell'offerta di beni e servizi, indipendentemente dall'obbligatorietà di un pagamento da parte dell'interessato (art. 3, par. 2, lett. a) del Regolamento), la Società ribadisce di non offrire beni e di non prestare servizi a clienti europei. La Società sostiene, sulla base di quanto stabilito dal Comitato per la protezione dei dati personali nelle linee guida n. 3/2018 e dal Considerando 23 del Regolamento, che l'analisi della sussistenza del criterio de quo debba essere svolta nel senso di accertare se l'attività di vendita di Clearview sia intenzionalmente, e non inavvertitamente o accidentalmente, rivolta a soggetti che si trovano nell'Unione.

La Società ritiene che gli argomenti addotti dal Garante nella contestazione ex art. 166 del Codice non siano idonei a provare la sussistenza del criterio per i seguenti motivi:

- è vero che, in passato, Clearview ha offerto i suoi prodotti in Canada in quanto si tratta di un mercato in cui, per ragioni di prossimità al mercato statunitense, l'espansione è abbastanza naturale; tuttavia, a seguito dei procedimenti avviati dai Privacy Commissioner canadesi, la Società ha cessato ogni attività di trattamento in quel Paese e questo non può essere un elemento che dimostri la sua intenzione di entrare nel mercato italiano;

- le fonti giornalistiche secondo cui Clearview intenderebbe espandere le proprie attività in diversi paesi tra cui, in particolare, l'Italia, non sono utilizzabili: si tratta di speculazioni basate sul fatto che la Società, in precedenza, aveva utenti di prova nell'Unione europea e non possono essere utilizzate per dedurre l'intenzione della stessa di offrire prodotti o servizi in Italia;

- Clearview ha ricevuto richieste di accesso ad account di prova, non sollecitate, da parte di utenti europei, ma tali accessi non sono più disponibili in quanto la Società ha deciso di non offrire più il suo prodotto nel contesto dell'Unione europea, prima ancora che il Garante avviasse la presente indagine; inoltre, il concetto di "intenzione" (a fornire servizi agli interessati in uno o più Stati membri dell'Unione) citato nel Considerando 23, deve essere interpretato, conformemente alle linee guida 3/2018, come una intenzione deliberata ed esistente e non ipotetica e futura;

- il provvedimento adottato dall'Autorità di protezione dei dati svedese riguarda uno degli account di prova sopra menzionati ed ora non più disponibili. Tali account, inoltre, non sono stati mai messi a disposizione di persone fisiche ed infatti, nella decisione svedese, risulta che il software era stato utilizzato dalle forze dell'ordine svedesi;

- con riferimento al criterio del monitoraggio del comportamento degli interessati che si trovano nell'Unione europea, nella misura in cui tale comportamento abbia luogo all'interno dell'Unione (art. 3, par. 2, lett. b), del Regolamento), la Società osserva come, dal Considerando 24, il criterio in questione afferisca ad attività di trattamento che consentono un monitoraggio del comportamento degli interessati, compreso il potenziale successivo utilizzo di tecniche di trattamento di dati personali. Tali tecniche consistono nella profilazione di una persona fisica, in particolare, al fine di prendere decisioni che la riguardano o di analizzarne o prevederne le preferenze, comportamenti e atteggiamenti personali; da tale definizione, emerge che non qualsiasi monitoraggio assume rilievo, ma solo quelli che concernono o si riferiscono al comportamento degli interessati, da intendere come specifiche azioni da questi poste in essere (ad esempio, cosa acquistano, dove vanno, come vivono);

- alla luce della suddetta definizione di monitoraggio, Clearview ritiene di non porre in essere attività di trattamento finalizzate ad analizzare il comportamento degli interessati, né crea alcun "profilo" riconducibile (related to) ad una persona

fisica: il Considerando 24 del Regolamento afferma che un'attività di trattamento può potenzialmente essere considerata un monitoraggio, se "le persone fisiche sono tracciate su Internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione di una persona fisica". Il termine "tracciare" (tracking) non è definito, ma il significato del verbo deve essere inteso nel senso che una persona è seguita nel tempo. Il termine "profilazione" (profiling) è definito all'art. 4, par. 1, n. 4, del Regolamento ed indica "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di dati personali per valutare determinati aspetti personali relativi a una persona fisica". Inoltre, il Comitato spiega che il termine "monitoraggio" implica che il responsabile del trattamento abbia una finalità specifica per la raccolta e il successivo riutilizzo dei dati concernenti il comportamento di un individuo all'interno dell'Unione;

- l'unica finalità di Clearview è quella di offrire un motore di ricerca per consentire la ricerca di immagini in Internet da parte dei suoi clienti. I vettori facciali che la Società utilizza per cercare le immagini non possono essere utilizzati per dedurre o ricavare matematicamente informazioni su una persona, perché non sono collegati al nome e/o alla posizione e/o ad altri identificatori. Anche se si ottiene un vettore facciale, non lo si potrebbe analizzare per rivelare informazioni intelligibili sulle caratteristiche facciali di una persona. Un tracciamento nel tempo (tracking over time) non è possibile perché una ricerca produce sempre solo i risultati disponibili al momento della ricerca stessa. Pertanto, anche un confronto tra ricerche effettuate in momenti diversi non consente di tracciare una persona; ciò che può accadere è che un agente di polizia trovi un indizio investigativo e poi conduca indagini specifiche che, tuttavia, non vengono effettuate dal software di Clearview. Certamente, conclude la Società, non si tratta di un tracciamento con mezzi automatizzati. Lo stesso vale per la profilazione in quanto, secondo la ricostruzione della Società, un agente di polizia può trarre conclusioni su una persona, ad esempio perché la ricerca di immagini produce una corrispondenza con il sospettato, ma queste conclusioni non vengono tratte in base al software di Clearview, in quanto le informazioni provengono da siti di terze parti;

- per essere considerato un monitoraggio ai sensi del criterio in questione, il trattamento dei dati effettuato dal titolare del trattamento deve essere finalizzato all'esecuzione di qualsiasi successiva analisi comportamentale o all'utilizzo di tecniche di

profilazione. Clearview non persegue né sarebbe potenzialmente in grado di raggiungere dal punto di vista tecnico tali obiettivi;

- il Garante stesso non pare in grado di indicare in maniera inequivocabile se l'attività svolta da Clearview costituisca un monitoraggio (solo monitoraggio comportamentale) o un'attività di profilazione nonostante, come già rappresentato, non vengano creati profili degli interessati, né venga eseguita un'analisi del loro comportamento;

- asserisce Clearview che la mera raccolta di dati, anche di un volume rilevante, non costituisce automaticamente un monitoraggio;

- il Gruppo di lavoro Articolo 29 in materia di processo decisionale automatizzato relativo alle persone fisiche e profilazione (Linee guida WP251), a pagina 7, afferma che l'uso del verbo "valutare" suggerisce che "la profilazione implichi una qualche forma di valutazione o giudizio in merito a una persona. La semplice classificazione di persone basata su caratteristiche note quali età, sesso e altezza non determina necessariamente una profilazione. Quest'ultima dipende infatti dalla finalità della classificazione". L'esempio fornito nelle linee guida alla stessa pagina chiarisce ancora meglio il punto laddove afferma che "un'azienda potrebbe voler classificare i propri clienti in base all'età o al sesso per finalità statistiche e per acquisire una panoramica aggregata dei propri clienti senza effettuare previsioni o trarre conclusioni in merito a una persona specifica. In questo caso, la finalità non è la valutazione delle caratteristiche individuali e quindi non si tratta di profilazione". Da ciò risulta evidente che la finalità è l'elemento decisivo per valutare se il trattamento rientri nella definizione di profilazione;

- le linee guida WP251, nella stessa pagina, facendo riferimento alla raccomandazione CM/Rec. (2010)13 del Consiglio d'Europa, specificano che l'attività di profilazione si articola in tre fasi: i) raccolta di dati; ii) analisi automatizzata per individuare le correlazioni; iii) applicazione della correlazione a una persona fisica per individuarne le caratteristiche di comportamento presenti o future. Si aggiunge l'indicazione secondo cui "il titolare del trattamento che effettua la profilazione dovrà assicurarsi di soddisfare le prescrizioni del regolamento in relazione a tutte le fasi di cui sopra". Anche supponendo che il sistema di Clearview sia coinvolto nelle prime due fasi, dai fatti risulta chiaramente che la terza fase è pacificamente al di fuori di ciò che il software

Clearview può fare e della posizione commerciale della Società. Se vengono individuate caratteristiche di comportamento presenti o future di una persona fisica attraverso l'utilizzo dei risultati di ricerca forniti dal software, il titolare del trattamento non è Clearview, ma il cliente che acquista il servizio. L'autorità svedese ha sottolineato nella sua decisione che la polizia svedese (e solo la polizia), in quanto cliente del software, era titolare del trattamento e che la stessa fosse indipendente rispetto a Clearview, fornitore dello strumento di ricerca;

- Clearview raccoglie immagini e tag relativi alle fonti Internet da cui esse vengono raccolte. Solo quando un cliente interroga il database, sottoponendo allo stesso un'immagine da ricercare, questa viene confrontata con quelle raccolte da Cleraview. Verificata la corrispondenza tra le immagini, il cliente riceve l'esito e Clearview raggiunge il suo scopo commerciale offrendo la corrispondenza tra immagini previamente sottoposte ad un processo di hashing; tutte le successive attività ed il relativo trattamento dei dati effettuato dal cliente non rientrano nell'ambito dell'attività di Clearview ma afferiscono ad una decisione commerciale distinta e basata sulle finalità perseguite dal cliente stesso in qualità di titolare autonomo del trattamento;

- inoltre, l'art. 3, par. 2, lett. b) non si applica genericamente alla profilazione, ma si riferisce al monitoraggio del comportamento e richiede, pertanto, che le attività di trattamento del titolare siano svolte per ottenere un'analisi delle abitudini comportamentali degli individui, finalità che Clearview chiaramente non persegue e non realizza. La Società non classifica in alcun modo le persone fisiche. Inoltre, il software non è in grado di valutare, giudicare, o prevedere un comportamento; i dati forniti al cliente sono semplicemente costituiti da immagini, metadati (se presenti) e la loro fonte (URL) su Internet al momento della ricerca;

- per quanto concerne i dati di geolocalizzazione cui fa riferimento la privacy policy di Clearview, con il termine geolocalizzazione si intendono solo i metadati di localizzazione incorporati nella foto, i quali indicano dove la stessa è stata scattata. Clearview non fornisce tali metadati di localizzazione ai clienti, ma se una foto online ha metadati di posizione incorporati, il cliente può vederli della foto quando i utilizza il link URL della stessa, come chiunque altro visualizzi la foto su Internet;

- con riferimento, infine, alla richiesta del reclamante XX di fornire una copia del suo documento d'identità, contestata in quanto ritenuta ingiustificata, la Società richiede alle persone, che avanzano una richiesta di accesso ai dati, di fornire una foto identificativa ufficiale. Clearview non ha alcun mezzo per verificare l'identità delle persone che appaiono nelle immagini che raccoglie e non conserva alcuna informazione sui nomi, sugli indirizzi e-mail, sulla residenza o sull'identità delle persone, come emerge chiaramente anche dai risultati della ricerca facciale (Face Search Results) che Clearview fornisce in risposta alle richieste di accesso ai dati. Dalla semplice indicazione del nome è impossibile per la Società sapere se la persona che formula una richiesta di accesso ai dati è presente nel database; per attivare la ricerca, dunque, il software Clearview ha bisogno di una foto per il relativo riscontro e, al fine di evitare richieste fraudolente, la Società ha deciso che tale foto debba essere quella presente su un documento ufficiale, come la carta d'identità. La Società non conserva le immagini della carta d'identità, né le utilizza per altri scopi. Tale richiesta non pare eccessiva atteso che l'art. 12, par. 6, del Regolamento prevede espressamente che "[...] se il titolare del trattamento nutre ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 15 a 21, può richiedere la fornitura di ulteriori informazioni necessarie per confermare l'identità dell'interessato";

- con riferimento ai reclami XX e XX, la Società ribadisce di non essere soggetta al Regolamento e che la privacy policy è conseguentemente conforme agli standard statunitensi. Tuttavia, la Società è disposta ad agire spontaneamente per risolvere le doglianze dei reclamanti e dunque a cancellare tutte le immagini ed i link prodotti dalla ricerca di immagini per le foto fornite dai due reclamanti. La Società ha spontaneamente esteso i diritti degli interessati ai residenti europei come gesto di buona volontà e trasparenza ed è con lo stesso spirito che offre la cancellazione delle immagini e dei collegamenti relativi ai reclamanti, tuttavia ciò non può essere inteso come accettazione della giurisdizione italiana e/o applicabilità del GDPR, che vengono contestati e fortemente negati.

Con nota del 12 ottobre 2021 (prot. n. 50926/2021), l'Ufficio, a seguito della ricezione dei reclami XX e XX, ha notificato a Clearview, ai sensi dell'art. 166, comma 5, del Codice, una contestazione suppletiva con contestuale avvio del procedimento

per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento, avente ad oggetto le presunte violazioni di cui agli artt. 5, par. 1 lett. a) e b), 6, 9, 12, 13, 15 e 27 del Regolamento.

Con la medesima nota, la Società è stata nuovamente resa edotta della possibilità di produrre scritti difensivi o documenti ed eventualmente di chiedere di essere sentita dall'Autorità (art. 166, commi 6 e 7, del Codice).

Con nota dell'11 novembre 2021 (prot. n. 56766/2021), Clearview ha presentato la propria memoria difensiva, dichiarando che:

- la Società non opera in alcuno Stato membro dell'Unione Europea, non monitora i comportamenti di interessati che si trovano in essa e quindi nessuna Autorità europea ha giurisdizione sulla sua attività, salvo violare il principio internazionale di territorialità;

- non esiste alcuna base giuridica che giustifichi procedimenti amministrativi nei confronti di società non stabilite in Italia e che non fanno affari in Italia; un procedimento di tal genere violerebbe l'ordine pubblico degli U.S.A.;

- con specifico riferimento al Regolamento, la Società ribadisce la non applicabilità dell'art. 3, par. 2, lett. a) e b), che stabilisce i criteri per l'applicazione del Regolamento alle società non stabilite nell'Unione europea;

- in particolare, l'art. 3, par. 2, lett. a) del Regolamento non sarebbe applicabile perché Clearview non offre prodotti e servizi nell'Unione, come già sottolineato nella precedente corrispondenza. La Società ribadisce di fornire un motore di ricerca per immagini per le forze dell'ordine al di fuori dell'Unione;

- inoltre, l'art. 3, par. 2, lett. b) si applica ai "monitoraggi dei comportamenti" degli interessati nell'Unione. Sebbene non vi sia una definizione di monitoraggio, la parola stessa e la ratio dell'art. 3 chiariscono che occorre l'osservazione di una persona fisica per un certo periodo di tempo;

- il Considerando 24 precisa che per determinare se un trattamento consiste nel monitoraggio di un comportamento deve essere verificato se la persona fisica è tracciata (tracked) in Internet. Al riguardo viene citato il contributo di Thaomas Zerdick, membro del drafting team della Commissione europea sul Regolamento, il quale sostiene che il tracciamento sotteso all'art. 3, par. 2, lett. b) deve equivalere alla

sorveglianza di una persona (citando come esempio sistemi che scattano delle istantanee fotografiche rispetto a sistemi di monitoraggio in tempo reale);

- il motore di ricerca di Clearview fornisce solo delle istantanee di foto disponibili in Internet al momento in cui il cliente effettua la ricerca. La Società non raccoglie né fornisce alcuna informazione sulla localizzazione, sulla cronologia browser, sull'attività commerciale o sul comportamento della persona fisica che appare come risultato della ricerca e non implica alcun modello comportamentale, predittivo o di analisi. Le informazioni che possono essere ricavate su di una persona, utilizzando il motore di ricerca di Clearview, sono meno significative di quelle che si possono ottenere da una ricerca su Google Search basata sul nome di quella stessa persona e nessuno sostiene che una ricerca sul browser di Google costituisca un monitoraggio comportamentale;

- se, ad esempio, si facesse una ricerca su Google Search con i nomi dei reclamanti, limitandola alle immagini, la risposta fornirebbe le foto, verosimilmente dei reclamanti, in quanto liberamente disponibili in Internet. Inoltre, clickando sui risultati, l'URL indirizzerebbe ai siti web ove compaiono le foto e da cui si potrebbero trarre ulteriori informazioni (la Società fornisce gli screenshot di una simile ricerca effettuata su Google search coi nomi dei reclamanti XX e XX);

- come noto, il motore di ricerca di Google non monitora le persone trattandosi, piuttosto, di un algoritmo che rende accessibili le informazioni pubblicate in Internet. Google fornisce una istantanea dei più rilevanti pezzi su una specifica ricerca al momento dell'esecuzione della stessa. Lo stesso accade con i risultati ottenuti a seguito di una ricerca fatta con il prodotto di Clearview. Potrebbero esserci elementi (leads) per ulteriori ricerche, ma nulla di più;

- dal testo del Considerando 24 del Regolamento emerge chiaramente come il legislatore abbia inteso far riferimento ad un uso successivo delle informazioni derivanti dal tracciamento della persona per cui un monitoraggio costante è il presupposto di qualsiasi "uso successivo"; la tecnologia di Clearview non produce tali informazioni, ma solo gli esiti di una ricerca che poi il cliente può utilizzare per farne di ulteriori, anche sulla base di altre fonti di informazioni. Clearview è solo un motore di ricerca;

- la Società fornisce solo uno strumento (tool), non è il titolare della ricerca condotta dall'utilizzatore dello strumento e di qualsiasi conseguente uso degli esiti della ricerca. È il cliente di Clearview che decide di usare il motore di ricerca per la ricerca delle sue immagini, caricando una immagine per ottenere i risultati ad essa corrispondenti È il cliente che decide cosa fare con gli esiti della ricerca. Dunque, è il cliente che decide se lo strumento possa essere usato nell'ambito di una specifica cornice normativa e Clearview è pagato per lo strumento, non per i risultati della ricerca o per ciò che il cliente farà con i risultati della ricerca;

- tale interpretazione è confermata dall'art. 25, par. 1, del Regolamento, il quale stabilisce che il titolare, al momento di determinare i mezzi del trattamento, deve assicurare che i parametri del Regolamento siano rispettati. Di conseguenza, è onere del cliente, che è il titolare del trattamento, stabilire se e come utilizzare il motore di ricerca di Clearview. Questa impostazione spiega anche perché le Autorità svedese e finlandese di protezione dei dati personali hanno avviato dei procedimenti nei confronti delle forze dell'ordine nazionali e non nei confronti di Clearview;

- il Garante dovrà anche tenere in considerazione il fatto che la Società ha implementato misure tecniche per assicurare che le ricerche non possano essere effettuate dall'Unione europea o dall'Italia. Tali misure sono state adottate al fine di allontanare ogni dubbio ai sensi della legge europea, atteso che il prodotto non è offerto a o all'interno del mercato europeo;

- la Società chiede quindi che il Garante chiuda il procedimento per carenza di giurisdizione;

- in un mondo globalizzato è impossibile tenere in considerazione tutte le leggi esistenti quando si progetta un prodotto; Clearview rispetta la legislazione statunitense e, poiché il Regolamento non si applica ai suoi servizi, non è necessario esaminarlo ulteriormente. Peraltro, dato che si presume che il motore di ricerca di Google rispetti le leggi europee in quanto Google è stabilito nell'Unione e offre i suoi servizi ad utenti nell'Unione, se anche il Regolamento venisse ritenuto applicabile a Clearview, il trattamento dei dati del reclamante dovrebbe essere considerato lecito;

- sebbene la Società non offra i propri prodotti nell'Unione europea e il Regolamento non si applichi, Clearview spontaneamente ottempera alle richieste di accesso dei residenti europei;

- la Società ha adempiuto alla richiesta del reclamante XX in data 29 aprile 2021 e ha risposto alla richiesta del reclamante XX il 29 settembre 2021, prima della notifica della contestazione suppletiva del Garante;

- la Società prende seriamente in considerazione le doglianze dei reclamanti e si offre di implementare misure atte ad assicurare che le due persone interessate non siano più oggetto di ricerca sul motore di ricerca di Clearview. Dato che si tratta di misure che implicano costi e risorse, la Società chiede se l'intervento potrebbe contribuire a definire i casi.

3. ESITO DELL'ATTIVITÀ ISTRUTTORIA

3.1 CARATTERISTICHE DEL SERVIZIO OFFERTO

Clearview è una società, con sede legale negli Stati Uniti, costituita nel 2017 che ha creato un motore di ricerca per il riconoscimento facciale (facial recognition search engine). Sulla scorta delle informazioni emerse in sede di assistenza reciproca con altre autorità di controllo europee, dalle informazioni rese note dalla Società stessa e dai reclami e dalle segnalazioni ricevuti dal Garante, risulta che la piattaforma di riconoscimento facciale sviluppata da Clearview permette la ricerca di immagini all'interno di un proprio database. La Società, infatti, raccoglie, attraverso tecniche di web scraping, immagini da social network (es. Twitter o Facebook), blog e, in genere, da siti web in cui sono presenti foto pubblicamente accessibili, ma anche dai video disponibili online (es. su Youtube). Le immagini così raccolte vengono elaborate con tecniche biometriche al fine di estrarre le caratteristiche identificative di ognuna di esse e, successivamente, trasformate in "rappresentazioni vettoriali". Tali rappresentazioni, costituite da 512 vettori che ricalcano le diverse linee uniche di un volto, vengono successivamente sottoposte ad hashing per finalità di indicizzazione del database e di successiva ricerca. La Società crea, dunque, dei modelli (template) biometrici che, nella fase della ricerca vengono sottoposti a comparazione con il campione oggetto della ricerca generando un processo di verifica 1 a N (one to many). L'image hash, l'identificativo univoco di ogni immagine (una sorta di impronta digitale facciale), agevola, come detto, l'indicizzazione e la successiva ricerca. La piattaforma è dichiaratamente stata creata al fine di generare degli investigation lead di alta qualità.

Ogni immagine può essere arricchita con i metadati associati (ad esempio, il titolo dell'immagine o della pagina web, il link della fonte, la geolocalizzazione, il genere, la data di nascita, la nazionalità, la lingua) cosicché quando il software identifica una corrispondenza, estrae dal database tutte le relative immagini e le

presenta al cliente del servizio come risultato della ricerca unitamente ai metadati e ai link associati, permettendo così di risalire ad ogni singola pagina sorgente.

Un'immagine così raccolta rimane nel database anche nell'ipotesi in cui la foto originaria o la pagina web di riferimento sia successivamente rimossa o resa privata.

Come si evince dal sito web della società (https://...) la piattaforma "include un database di oltre 10 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".

La tecnologia di machine learning alla base della piattaforma Clearview è stata oggetto di una richiesta di brevetto depositata nel febbraio 2021 al US Patent & Trademark Office l'11 febbraio 2021 e al World Intellectual Property Organization.

Da tale richiesta emerge che la tecnologia, denominata "Metodo per fornire informazioni su una persona sulla base di riconoscimento facciale", comprende vari metodi per fornire informazioni su una persona in base al riconoscimento facciale e varie applicazioni dello stesso, inclusi il face-based check-in, l'identificazione personale basata sul volto, la verifica dell'identità basata sul volto, i controlli dei precedenti basati sul volto, il facial data collaborative network, la ricerca di volti correlati e l'identificazione personale basata sul volto. Tali metodi vengono rappresentati come idonei a fornire informazioni accurate su di una persona in tempo reale.

La richiesta di brevetto presentata dalla stessa Società offre precisi dettagli sul funzionamento della tecnologia. Il sistema si snoda attraverso i seguenti passaggi: i) ricezione dei dati di immagine facciale che comprendano almeno un'immagine facciale del soggetto dal dispositivo di un utente; ii) trasformazione dei dati dell'immagine facciale in dati di riconoscimento facciale; iii) comparazione, via server, dei dati di riconoscimento facciale di riferimento con i dati di riconoscimento facciale associati a una pluralità di immagini facciali memorizzate al fine di identificare almeno un probabile candidato corrispondente all'immagine catturata; iv) sulla base della identificazione del candidato corrispondente all'immagine facciale acquisita, recupero dal database delle informazioni personali associate al candidato; v) restituzione delle informazioni personali al dispositivo dell'utente con assicurazione che tale dispositivo visualizzi le informazioni personali.

Clearview, dunque, non raccoglie solamente immagini per renderle accessibili ai propri clienti, ma tratta le immagini raccolte mediante web scraping, attraverso un algoritmo proprietario di matching facciale, al fine di fornire un servizio di ricerca biometrica altamente qualificata.

Inoltre, secondo le informazioni disponibili nel sito di Clearview, il servizio gratuito offerto non è liberamente accessibile al pubblico, ma è destinato a determinate categorie di clienti (i.e. forze di polizia).

I profili appena descritti portano a ritenere che la piattaforma offerta da Clearview assuma caratteri peculiari che la differenziano da un comune motore di ricerca che non elabora né arricchisce le immagini presenti in rete. In particolare, Clearview non lavora su memoria cache, ma crea un database di istantanee di immagini che vengono memorizzate come presenti all'atto della raccolta e non aggiornate. Inoltre, come detto, Clearview elabora tali immagini con tecniche biometriche, le sottopone ad hashing e le associa ai metadati eventualmente disponibili.

Le affermazioni addotte dalla Società secondo cui il servizio da essa offerto è sovrapponibile a quello offerto da Google Search paiono, pertanto, del tutto destituite di fondamento.

3.2. SUSSISTENZA DELLA GIURISDIZIONE EUROUNITARIA

L'art. 3 del Regolamento europeo n. 2016/679 disciplina il proprio "Ambito di applicazione territoriale" individuando presupposti differenziati a seconda che il titolare del trattamento risulti o meno stabilito nel territorio dell'Unione europea.

Nel caso in esame, Clearview non ha individuato uno stabilimento in Europa e pertanto, al fine di condurre una valutazione in ordine all'applicabilità al trattamento posto in essere dalla Società della normativa europea in materia di protezione dei dati personali, occorre verificare la sussistenza dei criteri di cui all'art. 3, par. 2, del Regolamento (cd. targeting). Tali criteri sono individuati nell'offerta di beni o servizi ad interessati che si trovano nell'Unione oppure nello svolgimento, rispetto a questi ultimi, di un'attività correlata al monitoraggio del comportamento di essi, nella misura in cui quest'ultimo ha luogo nell'Unione.

Preliminarmente occorre dire che, ai fini dell'applicazione del criterio di targeting, i dati oggetto del trattamento devono riguardare interessati nell'Unione. Nel caso di specie, il fatto che Clearview effettui un trattamento di dati personali di soggetti che si trovano nell'Unione europea e, in particolare in Italia, si evince dai riscontri che la Società ha fornito ai reclamanti, da cui risulta

pacificamente che sono state raccolte immagini degli stessi, che tali immagini sono state associate a metadati e sottoposte ad elaborazione biometrica (tali immagini sono, infatti, l'esito dell'identificazione risultante dal confronto dei dati memorizzati nel database con il campione fornito dai reclamanti), ma anche, indirettamente, dalle evidenze emerse nell'ambito dei procedimenti avviati dalle Autorità di controllo europee (cfr. decisione dell'Autorità di controllo tedesca del Land di Amburgo (decisione 545/2020; 32.02-102) e della Commission Nationale de l'Informatique et des Liberté (CNIL, Decision n° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI).

ART. 3, PAR. 2, LETT. A), DEL REGOLAMENTO

Quanto al primo dei profili considerati (cfr. art. 3, par. 2, lett. a) del Regolamento), Clearview, nel corso del procedimento, ha dichiarato di non offrire servizi in Europa e di non avere clienti europei che utilizzino il sistema di riconoscimento facciale prodotto dalla Società.

Le considerazioni svolte dal titolare del trattamento risultano tuttavia smentite, con riferimento a quanto avvenuto finora, dal provvedimento di recente adottato dall'Autorità di controllo svedese (DI-2020-2719:A126.614/2020 del 10 febbraio 2021) relativamente all'avvenuto utilizzo del sistema di riconoscimento facciale offerto da Clearview da parte di soggetti appartenenti alle forze dell'ordine nazionali, circostanza quest'ultima che presuppone, ab origine, un impiego del relativo servizio in capo ad utenti europei.

Inoltre, come dichiarato da Clearview con la citata nota del 22 giugno (prot. n. 33759/2021), nel corso del 2020 la società ha deciso di chiudere gli account europei e di non offrire più il suo prodotto nel contesto dell'Unione europea, inibendo l'accesso agli IP europei. Pertanto, per stessa ammissione di Clearview, sino ad una certa data la Società indirizzava - e aveva l'intenzione di farlo - i propri servizio anche in Europa.

Ai fini dell'applicabilità del criterio del targeting di cui all'art. 3, par. 2, lett. a) del Regolamento, sulla base delle indicazioni contenute all'interno delle "Guidelines 3/2018 on territorial scope", adottate dal Comitato per la protezione dei dati personali il 12 novembre 2019, è richiesto che la condotta del "titolare del trattamento, che determina i mezzi e gli scopi del trattamento stesso, dimostr[i] la sua intenzione di offrire beni o servizi a un interessato che si trova nell'Unione" (cfr. par. 2.a delle Linee guida citate). In particolare il Considerando 23 del Regolamento stabilisce che «[m]entre la

semplice accessibilità del sito web del titolare del trattamento, del responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica o di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il titolare del trattamento è stabilito sono insufficienti per accertare tale intenzione, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione possono evidenziare l'intenzione del titolare o del responsabile del trattamento di offrire beni o servizi agli interessati nell'Unione».

La stessa Corte di Giustizia dell'Unione europea (sentenza Pammer/Reederei Karl Schlüter GmbH & Co e Hotel Alpenhof/Heller (cause riunite C-585/08 e C-144/09) ha indicato alcuni fattori in presenza dei quali possa ritenersi che un'attività commerciale svolta da un soggetto sia diretta nei confronti di uno Stato membro, citando, tra gli altri, la circostanza che l'Unione europea sia menzionata in riferimento al bene o servizio offerto, la natura internazionale dell'attività oppure l'avvio di campagne pubblicitarie e di marketing rivolte al pubblico di un paese dell'UE.

L'intenzione del titolare del trattamento di rivolgersi al mercato europeo, oltre che confermata dalla decisione adottata dall'Autorità svedese di protezione dati sopra menzionata e dalla nota del giugno 2021 citata, emerge in modo evidente anche dai termini in cui è stata formulata la privacy policy anteriormente alle modifiche apportate a partire dal 20 marzo 2021, ovvero in un tempo collocabile tra la prima richiesta di informazioni da parte del Garante, datata 9 marzo 2021, ed il successivo riscontro fornito dalla società il 25 marzo 2021.

Fino ad allora detta informativa conteneva, infatti, una serie di indicatori dai quali era possibile desumere la volontà del titolare del trattamento di rivolgere l'offerta del proprio servizio anche ad utenti dell'Unione europea, tra cui la base giuridica del trattamento, in linea con quanto previsto dall'art. 6 del Regolamento, l'impegno ad adottare garanzie adeguate per conformare alle norme in materia di protezione di dati personali l'eventuale trasferimento di dati al di fuori dello Spazio economico europeo e la previsione della possibilità per i residenti dello Spazio economico europeo o della Svizzera di presentare reclamo all'Autorità di protezione dati competente riguardo al trattamento effettuato nei loro confronti da parte di Clearview.

In particolare, due punti dell'informativa paiono rilevanti, quello su "Independent Recourse" e il successivo su "International Transfers". Nel primo si legge che "Residents of the European Economic Area

or of Switzerland who wish to submit a complaint or seek resolution of a dispute related to Clearview AI's processing of personal data may seek appropriate recourse free of charge by contacting the appropriate Data Protection Authority (DPA) in their respective country"[enfasi aggiunta], mentre nel secondo si precisa che "The personally identifiable information we receive in the computers and systems of our offices in the United States is processed by us in the United States, where laws regarding data protection may be less stringent than the laws in your country. When personal data is transferred outside the EEA, we will put in place suitable safeguards to ensure that such transfer is carried out in compliance with applicable data protection rules. Clearview deeply values user privacy and data security controls; our cybersecurity infrastructure includes technical and policy controls that are consistent with the requirements of General Data Protection Regulation" [enfasi aggiunta].

Inoltre, con specifico riguardo ai destinatari del servizio, i "Termini di utilizzo del servizio", applicabili a partire dal 17 gennaio 2020 prevedevano che per "Utente" dovesse intendersi "ciascuna organizzazione (…) e tutte le persone che accedono al Servizio come Utente esecutivo o Utenti consentiti" descrivendo pertanto delle categorie idonee a ricomprendere una platea più ampia di quella costituita dalle sole forze dell'ordine alle quali Clearview ha fatto invece riferimento nei propri riscontri, confermando peraltro di avere reso disponibili ad agenzie governative europee una serie di account di prova sino al mese di marzo del 2020.

Art. 3, par. 2, lett. b), del Regolamento

Il secondo dei criteri di targeting individuati, ovvero quello di cui all'art. 3, par. 2, lett. b), riconduce l'applicazione del Regolamento europeo di protezione dati alle attività di trattamento correlate al monitoraggio del comportamento di interessati nell'Unione europea che avvenga all'interno dell'Unione.

La natura dell'attività di trattamento che può essere considerata monitoraggio del comportamento viene specificata nel Considerando 24 del Regolamento, il quale prevede che per "stabilire se un'attività di trattamento sia assimilabile al controllo del 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, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali".

Le Linee guida 3/2018 sopra menzionate precisano che, ai fini dell'operatività della disposizione, non sia necessario indagare la sussistenza, in capo al titolare del trattamento, dell'intenzione di "indirizzarsi ad un soggetto", ma che, tuttavia, "l'uso della parola «monitoraggio» implica che il titolare del trattamento abbia in mente uno scopo specifico per la raccolta e il successivo riutilizzo dei dati pertinenti sul comportamento di una persona fisica all'interno dell'UE" (cfr. par. 2.c delle Linee guida citate) e che, a tale riguardo, risulti fondamentale valutare se vi sia un tracciamento delle persone fisiche su Internet, compreso l'eventuale successivo utilizzo di tecniche di profilazione.

Il trattamento posto in essere da Clearview consiste, come rappresentato, nella raccolta di immagini dal web (cd. web scraping) e nella loro elaborazione con strumenti automatizzati al fine di creare rappresentazioni vettoriali di volti e, successivamente, sottoporli ad hash per indicizzare i dati, operazione necessaria per stabilire una eventuale correlazione con le immagini oggetto di comparazione caricate dagli utenti. L'attività svolta non appare dunque sovrapponibile, come invece dichiarato dalla società, a quella posta in essere da un qualsiasi motore di ricerca, tenuto conto del fatto che il titolare compie una rielaborazione tecnica delle immagini raccolte, tanto da renderle "dati biometrici", alle quali sono peraltro associate informazioni certamente idonee ad identificare la persona ritratta.

L'informativa pubblicata nel sito di Clearview indica, infatti, tra i dati raccolti, oltre alle fotografie accessibili al pubblico e disponibili in Internet, anche le informazioni che possono essere estratte da tali fotografie, come i metadati di geolocalizzazione che queste ultime possono contenere, nonché quelle derivate dall'analisi dei volti delle persone raffigurate e che, in quanto tali, costituiscono, come detto, dati biometrici sulla base dei quali viene eseguito il processo di comparazione.

Ma è proprio quest'ultimo passaggio a costituire la chiave di lettura dell'intero processo di raccolta ed elaborazione posto in essere da Clearview che ha come finalità quella di costituire un data set al quale comparare le immagini caricate dall'utente ed estrarre poi, dal proprio archivio, le immagini associabili ad esse da un punto di vista biometrico, nonché le informazioni correlate. Il meccanismo di ricerca si rivela, dunque, un mezzo per attivare un processo di comparazione che qualifica lo scopo del trattamento effettuato dalla società fornitrice, oltreché di quello posto in essere dai clienti che si avvalgono del servizio. Esiste dunque una correlazione tra le due tipologie di trattamento che peraltro trova riconoscimento anche all'interno del Regolamento europeo nel momento in cui, ai

fini dell'applicazione del criterio di targeting, richiama le circostanze in cui "the processing activities are related to (…) b) the monitoring of their behaviour as far as their behaviour takes place within the Union".

Le informazioni in questione formano oggetto di archiviazione nel database di Clearview e vengono arricchite nel tempo con altre estratte da nuovi template idonei a riflettere anche i cambiamenti fisici avuti dallo stesso soggetto, come emerge dall'esame di alcuni dei reclami proposti all'Autorità (cfr. in particolare quello presentato dal sig. XX). Ne discende che Clearview non offre come risultato della ricerca una semplice corrispondenza, ma anche un archivio di risorse che si snoda attraverso il tempo. La valutazione di tale circostanza, unitamente alla finalità comparativa sopra evidenziata, è idonea ad integrare, come richiesto nel Considerando 24, un'attività assimilabile al controllo del comportamento dell'interessato in quanto posta in essere tramite il tracciamento in internet e la successiva profilazione.

A differenza di quanto eccepito da Clearview nelle proprie difese (cfr. nota n. 33759 del 22/06/2021), l'attività svolta dalla medesima non sembra riconducibile ad una mera classificazione di individui sulla base di caratteristiche note come l'età, il sesso e l'altezza, in quanto viene effettuata un'attività ulteriore consistente nell'estrazione di dati biometrici dalle immagini raccolte nel web utilizzandole a fini comparativi per poi recuperare anche le informazioni ad esse associate. La stessa Società, nella domanda di brevetto depositata al US Patent & Trademark Office l'11 febbraio 2021, nel descrivere le finalità del trattamento effettuato tramite l'utilizzo di strumenti di riconoscimento facciale, evidenzia la potenziale attitudine di un sistema di questo tipo ad essere impiegato allo scopo di acquisire informazioni accurate sulle persone e di valutarne specifiche caratteristiche. Ed occorre considerare che anche i motori di ricerca, ai quali Clearview tenta di assimilare la propria attività, pongono in essere un tipo di trattamento che, sia pure effettuato con strumenti diversi da quelli utilizzati dalla Società, può avere proprio l'effetto di costruire un profilo personale dell'interessato - al quale si riferisce la ricerca - in virtù dell'associazione creata tra le informazioni che risultano in esito ad essa. A tale riguardo occorre considerare che la Corte di Giustizia dell'Unione europea, con la sentenza del 13 maggio 2014 causa C/131-12 (cd. Google Spain), ha rilevato che il gestore di un motore di ricerca pone in essere un trattamento distinto da quello effettuato dagli editori dei siti web, al quale si aggiunge, in quanto consente di rendere i dati accessibili "a qualsiasi utente di Internet che effettui una ricerca a partire dal nome della persona interessata, anche a quegli utenti che non avrebbero altrimenti

trovato la pagina web su cui questi stessi dati sono pubblicati" (cfr. punto 36 della sentenza), precisando peraltro che "l'organizzazione e l'aggregazione delle informazioni pubblicate su Internet, realizzate dai motori di ricerca allo scopo di facilitare ai loro utenti l'accesso a dette informazioni, possono avere come effetto che tali utenti, quando la loro ricerca viene effettuata a partire dal nome di una persona fisica, ottengono attraverso l'elenco di risultati una visione complessiva strutturata delle informazioni relative a questa persona reperibili su Internet, che consente loro di stabilire un profilo più o meno dettagliato di quest'ultima" (cfr. punto 37 della stessa).

L'art. 4, par. 1, n. 4, del Regolamento descrive la "profilazione" come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di (…) dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

Sulla base di quanto previsto dalle "Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione", adottate dal Comitato per la protezione dei dati personali il 3 ottobre 2017 ed emendato il 6 febbraio 2018, "la diffusa disponibilità di dati personali su Internet e di quelli ricavabili dai dispositivi di Internet delle cose, associata alla capacità di trovare correlazioni e creare collegamenti, può consentire la determinazione, l'analisi e la previsione di aspetti della personalità, del comportamento, degli interessi e delle abitudini di una persona". Le Linee guida citate individuano tre fasi specifiche che caratterizzano l'attività di profilazione stabilendo che debba a) riguardare dati personali, b) essere una forma di trattamento automatizzato e c) essere finalizzata a valutare aspetti personali relativi a una persona fisica.

Queste fasi risultano senz'altro integrate nel trattamento posto in essere da Clearview, ivi incluso, contrariamente a quanto affermato dalla società, il momento valutativo che può dirsi coincidente con l'attività di comparazione biometrica - effettuata a seguito dell'esecuzione di una ricerca da parte dell'utente - e con la successiva estrazione dei profili associabili all'immagine caricata nel sistema. Questa parte del processo, che fa sempre capo a Clearview, resta ben distinta dalla eventuale ulteriore attività valutativa che può essere effettuata dall'utente finale sulla base degli esiti della consultazione e che, pur essendo correlata alla

prima nel senso richiesto dall'art. 3.2.b, non è ad essa sovrapponibile, come eccepito invece dalla società nelle proprie difese.

La valutazione complessiva delle circostanze sopra dedotte porta a ritenere integrati i presupposti di applicabilità dell'art. 3.2 del Regolamento e della disciplina ivi contenuta alla luce della quale dovrà pertanto essere valutato il trattamento di dati personali di interessati italiani posto in essere da Clearview (cfr. sul punto anche decisione dell'Autorità di controllo tedesca del Land di Amburgo (decisione 545/2020; 32.02-102) e della Commission nationale de l'informatique et des liberté (CNIL, Decision n° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI).

3.3. SUSSISTENZA DELLA COMPETENZA DEL GARANTE

Il trattamento posto in essere da Clearview risulta qualificabile come trattamento transfrontaliero di dati personali ai sensi dell'art. 4, par. 1, n. 23 del Regolamento in quanto idoneo ad incidere su interessati in più di uno Stato membro.

Per questa tipologia di trattamenti, laddove il titolare abbia individuato uno stabilimento, unico o principale, nell'Unione europea, trova applicazione il meccanismo di cooperazione descritto negli artt. 60 ss. del Regolamento la cui direzione viene affidata alla cd. Autorità di controllo capofila che coincide con l'Autorità di controllo dello Stato membro in cui si trova il predetto stabilimento.

Tuttavia, nei casi nei quali manchi il presupposto di operatività di tale meccanismo, ossia la presenza in territorio europeo di uno stabilimento del titolare del trattamento, quest'ultimo dovrà "interfacciarsi con le autorità di controllo di ciascuno Stato membro in cui opera per il tramite del rappresentante designato" (cfr. par. 3.3. delle "Guidelines on the Lead Supervisory Authority" adottate dal Gruppo di Lavoro Articolo 29 il 13 dicembre 2016, revisionate il 5 aprile 2017 e fatte proprie dal Comitato per la protezione dei dati personali in data 25 maggio 2018).

Nel caso in esame Clearview è una società con sede negli Stati Uniti d'America che non ha stabilimenti nel territorio dell'Unione europea e, pertanto, sulla base di quanto previsto dall'art. 55, par. 1, del Regolamento, "ogni Autorità di controllo è compente ad eseguire i compiti assegnati e a esercitare i poteri ad essa conferiti a norma del (…) regolamento nel territorio del rispettivo Stato membro".

Tale disposizione è dunque idonea a fondare la competenza dell'Autorità di protezione dati italiana in ordine alla valutazione, con riguardo al proprio territorio, della conformità al Regolamento europeo del trattamento di dati personali posto in essere da Clearview e ad esercitare i poteri ad essa riconosciuti dall'art. 58 (cfr. analoga conclusione contenuta nel par. IV della decisione della Commission nationale de l'informatique et des liberté - CNIL, Decision n° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI).

3.4 SUSSISTENZA DI UN TRATTAMENTO DI DATI PERSONALI E CONSIDERAZIONI GENERALI SULLA LICEITÀ DELLO STESSO

Si osserva innanzitutto che un'immagine fotografica costituisce, ai sensi dell'art. 4, par. 1, n. 1), del Regolamento, "dato personale" nella misura in cui consenta l'identificazione di una persona fisica (interessato). La stessa disposizione precisa che si considera identificabile "la persona che può essere identificata, direttamente o indirettamente, con particolare riferimento a […] uno o più elementi caratteristici della sua identità fisica". In materia di immagini fotografiche è intervenuta specificamente la Corte di Giustizia dell'Unione Europea sancendo che "l'immagine di una persona registrata da una telecamera costituisce un dato personale ai sensi della disposizione menzionata nel punto precedente [Art. 2.a della Direttiva 95/46, n.d.r.] se e in quanto essa consente di identificare la persona interessata" (cfr. sentenza 11 dicembre 2014, causa C-212/13, par. 22).

I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale, sono definiti "dati biometrici", ai sensi dell'art. 4, par. 1, n. 14), del Regolamento e, come tali, sottoposti al regime di maggior tutela previsto dall'art. 9 del Regolamento.

La differenza tra le due tipologie di dati è ben delineata dal considerando 51 del Regolamento, secondo cui "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".

Per quanto concerne il concetto di "trattamento", si rileva che esso è definito dall'art. 4, par. 1, n. 2), del Regolamento "qualsiasi operazione o insieme di operazioni […] applicate a dati personali i

insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

Come esposto al paragrafo 3.1, dall'istruttoria condotta è emerso che Clearview ha creato un database di oltre 10 miliardi di immagini facciali che, raccolte in Internet attraverso tecniche di web scraping, vengono sottoposte ad un processo di elaborazione biometrica con successivo hashing per finalità di indicizzazione e ricerca, mediante messa a disposizione del database a soggetti terzi.
Posto che i dati in questione sono classificabili come dati comuni e biometrici, occorre analizzare se l'attività posta in essere dalla Società possa essere qualificata come trattamento ai sensi e per gli effetti del Regolamento.

A tal proposito, pare innanzitutto doveroso ricordare come la pubblica disponibilità di dati in Internet non implica, per il solo fatto del loro pubblico stato, la legittimità della loro raccolta da parte di soggetti terzi. Infatti, ogni dato che viene pubblicato on-line subisce tale operazione di trattamento (segnatamente, la diffusione), sulla scorta di una base giuridica e per finalità determinate e legittime stabilite e perseguite dal titolare del trattamento che ne ha disposto la pubblicazione.

Anche le cd. tecniche di OSINT (open-source intelligence) che consistono nella raccolta ed elaborazione di informazioni, inclusi dati personali, da fonti liberamente disponibili, come Internet e dati pubblici, possono essere svolte solo a fronte di una adeguata base giuridica, come recentemente precisato dal Garante europeo per la protezione dei dati personali con riferimento alla suddetta attività posta in essere dall'Europol (cfr. EDPS Opinion on the possibility to use Clearview AI and similar services at Europol (Case 2020-0372)).

Parimenti, si osserva come anche la pubblicazione in Internet di dati personali da parte del soggetto cui si riferiscono, ad esempio nell'ambito di un social media network, non comporta, di per sé, una condizione sufficiente per legittimarne il libero riutilizzo da parte di soggetti terzi. Se, infatti, è vero che il Regolamento (e, quindi, nella fattispecie, il principio di finalità di cui all'art. 5, par. 1, lett. b), del Regolamento) non si applica ai trattamenti di dati personali effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico (cd. household exemption, di cui all'art. 2, par. 2, lett. c), del Regolamento), anche con riferimento ad attività on-line, è altresì vero che la deroga va interpretata in senso restrittivo. Come sancito dalla Corte di

giustizia dell'Unione europea, la deroga "comprende unicamente le attività che rientrano nell'ambito della vita privata o familiare dei singoli, il che manifestamente non avviene nel caso del trattamento di dati personali consistente nella loro pubblicazione su Internet in modo da rendere tali dati accessibili ad un numero indefinito di persone" (cfr. sentenza 6 novembre 2003, causa C-101/01, par. 47). Deve, pertanto, ritenersi che anche la pubblicazione di dati personali da parte dell'interessato sui social network sia vincolata al mero scopo per cui l'interessato ha inteso renderli pubblici (ad esempio, la visibilità nell'ambito di un particolare social network per i soli fini sottesi all'utilizzo di tale SNS).

La correttezza della tesi è suffragata dal Gruppo di Lavoro Articolo 29, il quale ha chiarito "che, anche se sono stati resi accessibili al pubblico, i dati personali continuano a essere considerati tali e, di conseguenza, per il loro trattamento continuano a essere necessarie adeguate garanzie" (cfr. Parere 6/2014 - WP217) e, più di recente, dal Comitato per la protezione dei dati personali, il quale ha stabilito che "qualsiasi comunicazione di dati personali costituisce uno specifico trattamento per il quale il titolare deve avere una base giuridica fra quelle di cui all'articolo 6", che "la trasmissione di filmati a terzi per scopi diversi da quelli per i quali i dati sono stati raccolti è possibile a norma dell'articolo 6, paragrafo 4" e, infine, che "il terzo destinatario dovrà effettuare una propria analisi giuridica, in particolare individuando la base giuridica del suo trattamento ai sensi dell'articolo 6" (cfr. Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, versione 2.0, 29 gennaio 2020).

Quanto, in particolare al data scraping, trattasi di una modalità particolare di raccolta che avviene a completa insaputa degli interessati.

Come detto, l'eventuale natura pubblica delle immagini non è sufficiente a far ritenere che gli interessati possano ragionevolmente attendersi un utilizzo per finalità di riconoscimento facciale, per giunta da parte di una piattaforma privata, non stabilita nell'Unione e della cui esistenza ed attività la maggior parte degli interessati è ignaro.

A ciò si aggiunga che le attività di web scraping sono quasi sempre vietate dai gestori di servizi di social networking, attraverso esplicite clausole contenute nei termini di servizio, tant'è che, nel caso di specie, da informazioni di stampa, è emerso che alcuni dei maggiori fornitori di tali servizi (Twitter, Youtube, LinkedIn) hanno

inviato a Clearview una diffida affinché cessi la raccolta di dati che possono essere usati per identificare una persona (cease and desist letter).

Sulla scorta di quanto sopra, si può ragionevolmente concludere che la raccolta di dati personali liberamente disponibili in Internet mediante tecniche di web scraping costituisce un trattamento di dati personali, che deve trovare legittimazione in una delle basi giuridiche previste dall'art. 6 del Regolamento.

Volendo trasporre tale principio al caso di specie, si ritiene che l'attività di web scraping di immagini posta in essere dalla Società integri un'operazione di raccolta di dati personali, la quale costituisce trattamento di dati personali.

Nel caso di specie, tuttavia, la Società non si limita a raccogliere immagini da Internet atteso che, su tali dati, vengono effettuate ulteriori operazioni di trattamento, nella fattispecie, elaborazioni biometriche ed indicizzazioni mediante hashing. Più nel dettaglio, le immagini raffiguranti volti di persone vengono sottoposte ad ulteriori operazioni di trattamento (rappresentazione vettoriale) che trasformano l'immagine comune (dato personale) in immagine facciale (dato biometrico).

Si aggiunga, infine, l'operazione di interconnessione dei dati immagine (comuni e biometriche) di cui sopra con metadati raccolti, conservati e associati alle immagini facciali, i quali, a loro volta, possono contenere dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale (le immagini potrebbero, infatti, essere reperite da siti web di associazioni di fedeli ad un determinato culto o di membri di un sindacato o partito politico), circostanze che confermano la peculiarità dei trattamenti posti in essere da Clearview.

L'analisi sull'insussistenza delle condizioni di liceità per il trattamento di dati sopra delineato sulla base dell'impianto del Regolamento e quindi sotto un profilo di protezione dei dati personali, sarà analizzata nei prossimi paragrafi.

In questa sede pare, tuttavia, doveroso anticipare alcune brevi considerazioni, di più ampio respiro, in ordine ai profili di legittima dell'attività posta in essere da Clearview. Come noto, infatti, nell'Unione europea il dibattito sulla legittimità dell'utilizzo di tecniche che consentono il riconoscimento facciale è molto vivace e la soglia di attenzione si è innalzata a seguito dell'approvazione, in data 6 ottobre 2021, da parte del Parlamento europeo di una risoluzione in tema di intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito

penale. Con tale risoluzione è stato proposto (alla Commissione europea) un divieto permanente dell'utilizzo dei sistemi di analisi e/o riconoscimento automatici negli spazi pubblici non solo del volto, ma anche di altre caratteristiche umane quali l'andatura, le impronte digitali, il DNA, la voce e altri segnali biometrici e comportamentali. Inoltre, preso atto dei diversi tipi di utilizzo del riconoscimento facciale, come, ma non solo, la verifica/autenticazione (abbinamento di un volto dal vivo a una foto in un documento di identità, per es. i bordi intelligenti), l'identificazione (ricerca della corrispondenza tra una fotografia e un database di immagini) e la rilevazione (individuazione di volti in tempo reale da fonti quali la televisione a circuito chiuso e ricerca di una corrispondenza con i database, per es. sorveglianza in tempo reale), ciascuna delle quali ha diverse implicazioni per la protezione dei diritti fondamentali, il Parlamento europeo chiede che "la diffusione dei sistemi di riconoscimento facciale da parte delle autorità di contrasto venga limitata a finalità chiaramente giustificate nel pieno rispetto dei principi di proporzionalità e di necessità e della legge vigente". Il Parlamento europeo ribadisce, inoltre, che l'utilizzo di tecnologie di riconoscimento facciale debba essere conforme ai principi di minimizzazione, esattezza, limitazione della finalità e della conservazione, integrità e sicurezza.

Sulla scorta di tale raccomandazione, in Italia, è stata disposta, col d.l. 139/2021, convertito con modificazioni nella l. 205/2021 (cd. "decreto capienze"), una moratoria dei sistemi biometrici di riconoscimento facciale in luoghi pubblici o aperti al pubblico fino al 31 dicembre 2023, ad eccezione, tuttavia, dei trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali di cui al d.lgs. 51/2018 (attuativo della direttiva 2016/680, cd. Law Enforcement Directive).

3.5 SUSSISTENZA DELLA TITOLARITÀ

Come esposto al paragrafo 2, la Società ha negato di essere titolare del trattamento, riconducendo l'esistenza di tale ruolo solo in capo ai clienti utilizzatori della piattaforma. In particolare, Clearview ritiene di non poter essere qualificata come titolare del trattamento ai sensi e per gli effetti del Regolamento in quanto si limita a fornire uno strumento (tool), di ricerca, le cui finalità d'uso, connesse all'identificazione di persone mediante riconoscimento facciale, sarebbero appannaggio dei clienti, ai quali spetterebbe agire nel rispetto della normativa applicabile nell'ambito di riferimento in cui operano. Tale assunto sarebbe suffragato dal disposto di cui all'art. 25, par. 1, del Regolamento, nella parte in cui prevede che il titolare, al momento di determinare i mezzi del trattamento, deve assicurare che i parametri del Regolamento siano rispettati. Di

conseguenza, sarebbe onere del cliente - e non di Clearview - stabilire se e come utilizzare il motore di ricerca e dunque assumere in relazione ad esso la veste di titolare del trattamento.

Il Garante considera tale linea difensiva infondata in fatto ed in diritto.

La definizione di "titolare del trattamento" enunciata dall'art. 4, par. 1, n. 7), del Regolamento stabilisce che debba essere considerato tale chi determina le finalità e i mezzi del trattamento e ciò può essere fatto "singolarmente o insieme ad altri".

Nell'attività di raccolta ed elaborazione delle immagini Clearview definisce le modalità e le fonti della raccolta, realizza l'algoritmo da utilizzare per la creazione delle rappresentazioni vettoriali e stabilisce con quale funzione di hash archiviare le immagini in tal modo determinando anche i parametri necessari per l'indicizzazione delle informazioni e il relativo arricchimento con metadati utili per una maggiore efficacia dei risultati delle ricerche.

La società utilizza pertanto mezzi propri per realizzare la raccolta di immagini e la successiva trasformazione di esse in dati biometrici, disponendo altresì di un database proprietario all'interno del quale le informazioni sono conservate ed estratte in esito alla ricerca eseguita dall'utente. La finalità perseguita da Clearview è dunque quella di rendere disponibili, a fronte di un corrispettivo, informazioni, quali immagini e metadati, utili ai clienti per il perseguimento di finalità diverse ed ulteriori. Alla stessa conclusione giunge, peraltro, anche il Garante europeo per la protezione dei dati personali nel parere sopra citato nella misura in cui esclude che Clearview possa qualificarsi come un responsabile del trattamento che agisce per conto di Europol (ed Europol non potrebbe, pertanto, avvalersi dei suoi servizi ai sensi dell'art. 17, par. 2, del Regolamento UE 2016/7943) in quanto Clearview vende un servizio di riconoscimento facciale completamente ospitato e gestito sulla propria piattaforma, decidendo autonomamente le finalità e gli elementi essenziali dei mezzi dei servizi che offre (cfr. EDPS Opinion on the possibility to use Clearview AI and similar services at Europol (Case 2020-0372), pag. 3).

Le caratteristiche dell'attività svolta da Clearview sono già di per sé sufficienti per sostenere che la medesima sia un titolare del trattamento. Ma tali considerazioni appaiono altresì supportate dal fatto che, sino al marzo 2021, la privacy policy pubblicata nel sito web della Società conteneva una serie di elementi indiscutibilmente riferibili alla figura del titolare del trattamento, quali l'indicazione della base legale del trattamento, dei diritti esercitabili dagli interessati, nonché di uno specifico indirizzo di

posta elettronica utilizzabile per le richieste di informazioni e l'esercizio dei diritti da parte degli interessati ai sensi del Regolamento. Tale indirizzo peraltro veniva espressamente ricondotto alla funzione del responsabile per la protezione dati la cui nomina spetta al titolare del trattamento secondo quanto previsto dalle norme del Regolamento che ne disciplinano la designazione e le attribuzioni.

La circostanza che il cliente utilizzatore della piattaforma persegua finalità proprie non rileva per i profili che qui interessano. Come chiarito dal Comitato per la protezione dei dati personali, se un soggetto decide da solo le finalità e le modalità delle operazioni che precedono o sono successive nella catena del trattamento, tale soggetto deve considerarsi unico titolare dell'operazione precedente o successiva (cfr. Linee Guida del Comitato europeo per la protezione dei dati persoali 07/2020 on the concepts of controller and processor in the GDPR, par. 57). Pertanto, la circostanza che i clienti di Clearview possano perseguire finalità ulteriori rispetto a quelle connesse all'attività di Clearview non infinge, né risulta incompatibile con il ruolo di titolare del trattamento di quest'ultimo soggetto.

3.6 LE VIOLAZIONI ACCERTATE

3.6.1 ART. 5, PAR. 1 LETT. A), B) ED E), DEL REGOLAMENTO

In prima battuta l'Ufficio ha contestato la violazione dell'art. 5, par. 1, lett. a), del Regolamento, il quale prevede il rispetto dei principi di liceità, correttezza e trasparenza nel trattamento dei dati nei confronti dell'interessato.

Sul punto, il Considerando 39 del Regolamento espressamente prevede, tra l'altro, che "dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che le riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro […]".

Come sopra rappresentato, nel caso di specie, gli interessati non hanno alcun contatto con la Società, non sono direttamente informati dell'attività svolta dalla stessa, né sono destinatari di alcuna informazione neanche consultando il sito di Clearview.

In secondo luogo, l'Ufficio ha contestato la violazione dell'art. 5, par. 1, lett. b), del Regolamento, il quale prevede il rispetto del principio di limitazione della finalità che, anche nell'ambito del test

comparativo (balancing test) tra interesse legittimo del titolare e diritti e libertà dell'interessato (v. infra), rappresenta uno dei fattori chiave da considerare e che si sostanzia nelle ragionevoli aspettative degli interessati (cfr. Parere 6/2014 – WP 217, pag. 47) a che le proprie immagini possano essere sottoposte ad ulteriori trattamenti.

Nel caso di specie, tale principio non pare possa dirsi integrato, anche considerata l'assenza di qualsivoglia relazione tra gli interessati e la Società. Infatti, l'eventuale natura pubblica delle immagini non è sufficiente a far ritenere che gli interessati possano ragionevolmente attendersi un utilizzo per finalità di riconoscimento facciale, per giunta da parte di una piattaforma privata, non stabilita nell'Unione e della cui esistenza ed attività la maggior parte degli interessati è ignaro. Dall'altro lato, e come già rappresentato, la stessa circostanza della natura pubblica delle immagini non autorizza automaticamente Clearview a poter riutilizzare legittimamente le stesse in modo libero, come invece vorrebbe lasciar intendere la Società.

Infine, l'Ufficio ha contestato la violazione dell'art. 5, par. 1, lett. e), del Regolamento, il quale prevede il prevede il rispetto del principio di conservazione.

Non si evince l'indicazione di alcun periodo di conservazione né dall'analisi della privacy policy di Clearview, né dai riscontri ricevuti dalla Società, risultati incompleti sul punto, né dalle informazioni contenute nei reclami presentati dagli interessati.

La Società ha rappresentato che le immagini vengono raccolte e conservate con tutti i riferimenti (metadati) relativi alla fonte ed al momento in cui è avvenuta la raccolta, in tal modo creando un database, stratificato ed alimentato in modo progressivo e costante, costituito da una serie di informazioni legate ad una certa immagine attraverso il tempo. Tale aspetto induce a ritenere che tali informazioni vengano conservate a tempo indeterminato e vengano cancellate solo su espressa richiesta degli interessati. Tra l'altro, tale circostanza denota anche una contraddizione rispetto a quanto dichiarato da Clearview in quanto le immagini oggetto di trattamento non sono sempre pubblicamente disponibili in quanto permangono nel database anche immagini rese private o cancellate nella loro fonte originaria successivamente alla raccolta effettuata dalla Società.

Per quanto sopra rappresentato, si ritiene che Clearview abbia espressamente violato l'art. 5, par. 1 lett. a), b) ed e) del Regolamento. In particolare, con riferimento agli obblighi di trasparenza e di liceità, si ritiene violato l'art. 5, par. 1, lett. a) del

Regolamento alla luce della gravità, della natura e dell'impatto delle singole specifiche violazioni degli artt. 6, 9 e da 12 a 14 del Regolamento (cfr. EDPB decisione vincolante 1/2021).

3.6.2. ART. 6 DEL REGOLAMENTO

Secondo l'art. 6 del Regolamento, il trattamento di dati personali è lecito se, e nella misura in cui, ricorra almeno uno delle condizioni elencate nello stesso articolo.

Nel caso di specie, essendo pacifico che non è stato acquisito il consenso degli interessati ed escludendo la sussistenza delle circostanze di cui alle lettere b), c), d) ed e), occorre analizzare se possa ritenersi sussistente il legittimo interesse del titolare, base giuridica implicitamente invocata dalla Società nella misura in cui equipara la sua attività al trattamento effettuato da Google Search nella sua attività di indicizzazione.

Sotto tale profilo, pare innanzitutto doveroso richiamare la posizione generale assunta sul punto dal Comitato europeo per la protezione dei dati personali il quale ha escluso che ci possa essere "un'autorizzazione generalizzata a riutilizzare e a sottoporre a ulteriore trattamento dati personali resi accessibili al pubblico ai sensi dell'articolo 7, lettera f) [ovvero, il legittimo interesse dell'attuale art. 6, lett. f]", concedendo, al più, che tale circostanza possa assurgere ad eventuale elemento valutativo nel bilanciamento di interessi (cfr. Parere 6/2014 - WP217).

Nel caso di specie, il legittimo interesse della società è costituito da un fine di lucro a fronte di un trattamento che presenta una particolare intrusività nella sfera privata degli individui, dal momento che si sostanza in una raccolta di dati fotografici, associati ad ulteriori link che sono idonei a rilevare diversi aspetti della vita privata degli individui. Tali dati vengono, inoltre, sottoposti ad elaborazione biometrica e, infine, per stessa dichiarazione della società, sono relativi ad un numero particolarmente elevato di soggetti, a cui va affiancato un ulteriore elemento di delicatezza, quello relativo alla reperibilità in Internet di immagini di minori, anch'esse oggetto di trattamento.

Considerati gli elementi appena rappresentati, si ritiene che l'interesse legittimo della Società alla libera iniziativa economica non possa che flettere rispetto ai diritti e alle libertà degli interessati, in particolare alla grave messa in pericolo del diritto alla riservatezza, al divieto di essere sottoposti a trattamenti automatizzati e al principio di non-discriminazione insiti in un trattamento di dati personali come quello effettuato dalla Società.

In conclusione, si ritiene che Clearview non possa vantare alcuna valida base giuridica su cui fondare la liceità del trattamento di dati personali posto in essere.

3.6.3 ART. 9 DEL REGOLAMENTO

Nei paragrafi precedenti è stato evidenziato come il trattamento posto in essere da Clearview non si limiti ad una semplice raccolta di dati, ma si sostanzi anche in un ulteriore trattamento che rende le immagini raccolte "dati biometrici" e, perciò, soggetti alle tutele più stringenti dell'art. 9 del Regolamento.

Tale articolo contempla il regime giuridico riguardante le categorie di dati particolari, prevedendo un generale divieto di trattamento, fatte salve alcune eccezioni. Appare evidente che la ratio della disposizione sia quella di prevedere una protezione rafforzata per talune categorie di dati richiedendo, sotto il profilo applicativo, un cumulo tra le garanzie dell'art. 6 e la disciplina dell'art. 9 del Regolamento. Questo significa anche che, per legittimare un'attività di trattamento, un titolare che tratta categorie particolari di dati non può mai invocare soltanto un fondamento giuridico ai sensi dell'art. 6, ma dovrà applicare, in maniera cumulativa, anche le previsioni dell'art. 9 citato al fine di garantirne il livello di tutela pertinente. In tal senso si è espresso, nelle Linee guida n. 8/2020 "on the targeting of social media users", il Comitato per la Protezione dei dati personali, il quale ha ribadito che "oltre alle condizioni dell'articolo 9 GDPR, il trattamento di categorie particolari di dati deve fondarsi su una base giuridica stabilita nell'articolo 6 GDPR ed essere effettuato in conformità con i principi fondamentali di cui all'articolo 5 GDPR". L'applicazione cumulativa delle tutele previste dagli articoli citati risulta dirimente anche per escludere interpretazioni che portino a sostenere la possibilità di trattare categorie particolari di dati, senza rispettare l'art. 6, in presenza delle eccezioni di cui all'art. 9. Come ribadito, ancora una volta, dal Comitato per la protezione dei dati personali "sarebbe inappropriato concludere per esempio che il fatto che qualcuno abbia reso alcune categorie particolari di dati manifestamente pubbliche ai sensi dell'articolo 8 [oggi art. 9 del GDPR], paragrafo 2, lettera e), sia (sempre in sé e per sé) una condizione sufficiente a consentire qualunque tipo di trattamento dei dati, senza effettuare un test comparativo degli interessi e dei diritti in gioco in conformità dell'articolo 7 [oggi art. 6 del GDPR], lettera f" (cfr. Parere 6/2014 - WP217).

Concludendo, per le ragioni sopra esposte, con riferimento al trattamento di dati posto in essere da Clearview, non solo deve ritenersi insussistente alcuna valida base giuridica di cui all'art. 6

del Regolamento, ma risulta violato anche il divieto generale di trattamento di categorie particolari di dati (con riferimento ai dati biometrici).

3.6.4. ARTT. 12, 13, 14 E 15 DEL REGOLAMENTO

I reclami proposti all'Autorità sono stati preceduti dall'inoltro al titolare del trattamento di richieste preventive finalizzate a conoscere quali dati personali riguardanti gli interessati fossero detenuti dalla Società, nonché, in alcuni casi, le ulteriori informazioni indicate dall'art. 15 del Regolamento.

I reclamanti hanno lamentato, nella maggior parte dei casi, la mancanza, il ritardo o l'inidoneità del riscontro ricevuto e, dunque, una violazione dell'art. 12 del Regolamento che disciplina le modalità che il titolare deve osservare, tra l'altro, per le comunicazioni conseguenti all'esercizio dei diritti previsti dagli artt. 15-22 da parte dell'interessato.

Tali circostanze hanno poi formato oggetto di comunicazione di avvio di procedimento ai sensi dell'art. 166, comma 5, del Codice da parte dell'Autorità in esito alla quale è risultato quanto segue:

- con riguardo ai sig.ri XX e XX non sono state fornite in maniera chiara ed esplicita tutte le informazioni richieste ai sensi dell'art. 15 del Regolamento, ma è stato inviato esclusivamente un file contenente le immagini estratte dal sistema ed associabili alla fotografia trasmessa dagli interessati unitamente al documento di identità, rinviando, quanto alle restanti richieste, ad un link generico alla privacy policy della Società. Il riscontro è stato inoltre reso in un termine superiore a quello di trenta giorni indicato dall'art. 12, par. 3, del Regolamento e solo a seguito di diversi solleciti inviati dagli interessati;

- con riguardo al reclamo proposto dal sig. XX è stata invece rilevata la richiesta di dati eccedenti, quali il documento di riconoscimento, al fine di evadere l'istanza di accesso formulata dal medesimo.

I rapporti tra il titolare del trattamento e gli interessati, secondo le indicazioni fornite dal Regolamento, devono essere improntati al rispetto della trasparenza con riguardo alle informazioni relative al trattamento effettuato, nonché con riferimento alle comunicazioni fornite a seguito dell'esercizio dei diritti. In particolare, in base a quanto previsto dall'art. 12, par. 2, il titolare del trattamento deve agevolare l'esercizio dei diritti dell'interessato ai sensi degli articoli 15 a 22 e ciò sia con riguardo alle modalità utilizzate per fornire il riscontro che con riguardo ai tempi di esso il quale, sulla base di

quanto previsto dal par. 3 del medesimo articolo, deve essere fornito "senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa", salvo eccezioni specificamente disciplinate.

In alcuni dei casi esaminati dall'Autorità - nello specifico XX e XX - gli interessati hanno dovuto reiterare le loro istanze di accesso più volte prima di ottenere un riscontro da parte di Clearview e ciò nonostante siano stati utilizzati i canali di contatto indicati nel sito della Società (form on-line ed indirizzo e-mail dedicato alle richieste in materia di privacy).

Le modalità rese disponibili dalla Società per l'esercizio dei diritti non si sono pertanto rivelate né agevoli, né chiare, anche in virtù della sovrapposizione dei canali indicati per prendere contatto con essa, e non risultano essere stati rispettati i termini previsti dal Regolamento per fornire riscontro agli interessati, né sono state altrimenti comunicate le specifiche ragioni richieste dall'art. 12, par. 4, del Regolamento per l'eventuale proroga di tale termine. A ciò si aggiunga che Clearview, con lo scopo di evadere le istanze di accesso, ha chiesto agli interessati elementi identificativi, quali il documento di identità, che risultano eccedenti rispetto alla finalità perseguita posto che, unitamente ad esso, è stato altresì chiesto ai medesimi di produrre un'immagine alla quale comparare i dati presenti nell'archivio del titolare.

È vero, come eccepito da Clearview, che l'art. 12, par. 6, del Regolamento prevede che "qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli 15 a 21, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato", ma la disposizione richiede appunto che tali dubbi siano "ragionevoli" nei termini precisati anche dal Considerando 64. Nei casi esaminati le immagini richieste agli interessati, unitamente alle altre informazioni fornite, potevano ritenersi elementi sufficienti e, in ogni caso, eventuali ulteriori dubbi potevano comunque essere superati senza dover necessariamente richiedere l'allegazione della copia del documento di identità.

Il riscontro alle richieste di accesso, con particolare riguardo ai reclami proposti dai sig.ri XX e XX, è stato, inoltre, parziale non essendo stata fornita una comunicazione puntuale e trasparente con riferimento alle categorie di informazioni previste dall'art. 15, par. 1, del Regolamento che in ragione di ciò appare violato.

Il titolare del trattamento, nell'ottica di un rapporto con gli interessati improntato alla correttezza ed alla trasparenza, è tenuto inoltre a fornire alcune informazioni generali sul trattamento

effettuato, individuate dagli artt. 13 e 14 del Regolamento, le quali devono peraltro essere, oltreché complete, anche aggiornate al fine di tenere conto di tutte le variazioni che intervengono nel tempo.

Come precisato nel paragrafo 3.2, Clearview ha apportato sostanziali modifiche all'informativa pubblicata nel proprio sito a partire dal 20 marzo 2021, ovvero in un momento intermedio tra la presentazione dei primi due reclami (XX e XX) e dei successivi due (XX e XX).

La privacy policy presente nel sito fino a quella data conteneva una serie di indicazioni relative al trattamento di dati eseguito da Clearview che risultavano rispondenti ai contenuti informativi indicati dagli artt. 13 e 14 del Regolamento che, peraltro, veniva espressamente citato.

Già all'epoca l'informativa, benché in essa risultassero esplicitati diversi aspetti relativi al trattamento effettuato, appariva parziale in quanto carente di elementi nevralgici, quali la specifica indicazione del legittimo interesse perseguito dal titolare del trattamento o la precisazione del termine stabilito per la conservazione dei dati delle persone le cui immagini sono detenute nel database di Clearview

E ciò sia con riguardo all'informativa da rendere con riferimento ai dati personali raccolti direttamente presso l'interessato (cfr. art. 13 del Regolamento), quali ad esempio quelli degli utenti che richiedono il servizio e quelli di coloro che esercitano i diritti di cui agli artt, 15-22, che con riferimento ai dati personali raccolti tramite altre fonti e poi rielaborati dalla società (cfr. art. 14 del Regolamento).

A seguito poi degli interventi posti in essere da varie Autorità di controllo europee la Società ha, per sua stessa affermazione resa nel corso del procedimento, modificato l'informativa presente nel sito espungendo dalla stessa ogni riferimento al Regolamento europeo in materia di protezione dati ed eliminando altresì intere sezioni che integravano, nella sostanza, l'attuazione di quanto nello stesso previsto (ad esempio l'indicazione esplicita delle basi giuridiche del trattamento ovvero l'indicazione dei diritti esercitabili dagli interessati e che ricalcavano quelli di cui agli artt. 15-22 del Regolamento).

L'attuale privacy policy continua a prevedere la possibilità per gli interessati di conoscere le informazioni che li riguardano o di ottenerne la cancellazione, ma nell'ambito di quanto previsto dalla disciplina applicabile in California (cfr. California Consumer Privacy

Act (CCPA) e codice civile della California del 1798 citati nell'informativa) e dunque in termini diversi da quanto invece previsto dal Regolamento europeo.

È stata inserita, ad esempio, una limitazione – non prevista nella normativa europea o almeno non secondo le modalità indicate dal titolare – al numero delle richieste di accesso che l'interessato può effettuare nell'arco di dodici mesi e che vengono stabilite nel numero di due.

Sono inoltre riportati termini di riscontro alle richieste diversi e più lunghi rispetto a quelli contemplati nell'art. 12, par. 3, del Regolamento, prevedendo che l'impossibilità per il titolare di rispettarli debba essere semplicemente comunicata all'interessato senza indicare le specifiche condizioni in presenza delle quali lo slittamento possa reputarsi legittimo.

Infine, l'esercizio del diritto di accesso è subordinato alla trasmissione da parte dell'interessato di un documento di identità, mentre in caso di esercizio del diritto di cancellazione è prevista la possibilità per il titolare di non soddisfarla qualora ricorra, nel caso concreto, una delle eccezioni indicate dalle disposizioni del CCPA le quali non vengono tuttavia menzionate.

Sulla base di quanto emerso, deve pertanto ritenersi integrata la violazione degli artt. 12, 15, 13 e 14 del Regolamento.

3.6.5. ART. 27 DEL REGOLAMENTO

L'art. 27 del Regolamento prevede che, ove si applichi l'art. 3, par. 2, il titolare è tenuto a designare per iscritto un rappresentante nell'Unione europea, il quale deve essere stabilito in uno degli Stati membri in cui si trovano gli interessati i cui dati sono trattati nell'ambito dell'offerta di beni e servizi o il cui comportamento è monitorato e che funge da interlocutore, in particolare delle autorità di controllo e degli interessati, per tutte le questioni riguardanti il trattamento.

Nel caso di specie, la valutazione complessiva delle circostanze sopra dedotte porta a ritenere integrati i presupposti di applicabilità dell'art. 3.2 del Regolamento; Clearview tratta dati personali di interessati che si trovano nell'Unione e le sue attività di trattamento sono connesse alla prestazione di servizi ad utenti europei, nonché al controllo del comportamento di individui che si trovano nel territorio dell'Unione.

La Società ha quindi l'obbligo di designare, mediante mandato scritto, un rappresentante nel territorio dell'Unione europea incaricandolo ad interagire per suo conto con riguardo agli obblighi

che derivano dal Regolamento, anche per quanto riguarda la cooperazione con l'Autorità di controllo.

L'omissione integra la violazione dell'art. 27 del Regolamento.

3.6.6. ART. 22 DEL REGOLAMENTO

Nell'atto di avvio del procedimento ai sensi dell'art. 166 del Codice notificato in data 22 aprile 2021 l'Ufficio contestava anche la presunta violazione dell'art. 22 del Regolamento ritenendo che il trattamento posto in essere dalla Società potesse implicare la possibilità di assunzione di decisioni anche solo parzialmente automatizzate, idonee a produrre effetti rilevanti con riguardo ai diritti dei soggetti interessati. Dall'istruttoria non è emerso alcun elemento idoneo a comprovare tale violazione. La Società non ha, infatti, fornito alcun riscontro specifico in merito a tale profilo e non sono, allo stato, disponibili elementi tecnici di sistema che possano corroborare la tesi della sussistenza di un trattamento automatizzato. Si rileva ancora che l'art. 22 prevede il diritto a non subire una decisione basata unicamente su di un trattamento automatizzato ma, da quanto emerso in fase istruttoria, tale decisione pare al più poter essere assunta dei clienti del servizio offerto da Clearview e non dalla Società, la quale ha implementato e reso disponibile a terzi il suo sistema di riconoscimento facciale.

Sotto tale profilo, si ritiene dunque che non sussistano gli estremi per ritenere integrata la violazione dell'art. 22 del Regolamento.

CONCLUSIONI

Alla luce delle valutazioni sopra espresse, si conferma, pertanto, la maggior parte delle contestazioni dell'Ufficio notificate con l'atto di avvio del procedimento e si rileva l'illiceità del trattamento di dati personali effettuato dalla Società, in violazione degli artt. 5, par. 1, lett. a), b) ed e), 6, 9, 12, 13, 14, 15 e 27 del Regolamento.

La violazione delle predette disposizioni rende, altresì, applicabile la sanzione amministrativa prevista dall'art. 83, par. 5, del Regolamento, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 3, del Regolamento medesimo e art. 166, comma 2, del Codice.

4. MISURE CORRETTIVE

L'art. 58, par. 2, prevede in capo al Garante una serie di poteri correttivi, di natura prescrittiva e sanzionatoria, da esercitare nel caso in cui venga accertato un trattamento illecito di dati personali.

Tra questi poteri, l'art. 58, par. 2, lett. f), del Regolamento prevede il potere di "imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento".

Sulla scorta di quanto sopra esposto, considerato che il trattamento di dati personali posto in essere da Clearview è effettuato in violazione dei principi del Regolamento, delle norme che tali principi specificano, in particolare quelle sulla base giuridica, e delle norme relative ai diritti degli interessati che rappresentano il cardine del Regolamento, si rende necessario, ai sensi dell'art. 58, par. 2, lett. f), del Regolamento, disporre un divieto del trattamento, consistente nel i) divieto di ulteriore raccolta, mediante tecniche di web scraping, di immagini e relativi metadati concernenti persone che si trovano nel territorio italiano; ii) divieto di ogni ulteriore operazione di trattamento dei dati, comuni e biometrici, elaborati dalla Società attraverso il suo sistema di riconoscimento facciale relativi a persone che si trovano nel territorio italiano.

Ai sensi dell'art. 58, par. 2, lett. g), del Regolamento, è altresì necessario, al fine di rendere effettiva la tutela dei numerosi interessati al trattamento posto in essere dalla Società, disporre un ordine generale di cancellazione dei sopramenzionati dati, fermo restando l'obbligo di fornire puntuale riscontro alle richieste di esercizio dei diritti di cui agli artt. 15-22 del Regolamento che fossero nel frattempo eventualmente pervenute da parte di soggetti interessati. In tali ultime ipotesi, al fine di agevolare l'esercizio di diritti da parte degli interessati, il riscontro dovrà essere fornito nel rispetto dei tempi e delle modalità di cui all'art. 12, par. 3 del Regolamento.

Ai sensi dell'art. 58, par. 2, lett. d), del Regolamento si ingiunge altresì alla Società di designare, entro trenta giorni dalla notifica del provvedimento, un rappresentante nel territorio italiano che funga da interlocutore, in aggiunta o in sostituzione del titolare, con gli interessati al fine di agevolarne l'esercizio dei diritti.

Ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, la Società dovrà comunicare a questa Autorità, fornendo un riscontro adeguatamente documentato, entro trenta giorni dalla notifica del presente provvedimento, le iniziative intraprese al fine di dare attuazione a quanto sopra ordinato ai sensi del citato art. 58, par. 2, lett. f), nonché le eventuali misure poste in essere per agevolare l'esercizio dei diritti degli interessati.

5. ORDINANZA INGIUNZIONE PER L'APPLICAZIONE DELLA SANZIONE AMMINISTRATIVA PECUNIARIA E DELLE SANZIONI ACCESSORIE

Il Garante, ai sensi degli artt. 58, par. 2, lett. i), e 83 del Regolamento nonché dell'art. 166 del Codice, ha il potere di infliggere una sanzione amministrativa pecuniaria ai sensi

dell'articolo 83, in aggiunta o in luogo delle altre misure correttive previste nel medesimo paragrafo.

In tale ipotesi, il Garante adotta l'ordinanza ingiunzione con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice" (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

Nel caso di specie, tenuto conto del disposto di cui all'art. 83, par. 3, del Regolamento, si stabilisce innanzitutto che la violazione più grave deve essere ravvisata nella sanzione prevista dall'art. 83, par. 5, la quale fissa il massimo edittale nella somma di 20 milioni di euro ovvero, per le imprese, nel 4% del fatturato mondiale annuo dell'esercizio precedente ove superiore.

Ai sensi dell'art. 83, par. 1 del Regolamento, la sanzione amministrativa deve essere effettiva, proporzionata e dissuasiva in relazione al singolo caso.

Ai sensi dell'art. 83, par. 2, del Regolamento, la decisione sulla determinazione e sulla quantificazione dell'ammontare della sanzione, affinché la stessa risponda ai caratteri di effettività, proporzionalità e dissuasività, deve essere presa tenuto conto di una serie di elementi elencati al par. 2, lett. a)-k).

Per la determinazione dell'ammontare della sanzione nella fattispecie concreta occorre tenere conto degli elementi indicati nell'art. 83, par. 2, del Regolamento, che, nella presente fattispecie, possono considerarsi nei termini seguenti:

1. natura dei dati trattati;
2. gravità e durata della violazione;
3. numero soggetti coinvolti;
4. grado di responsabilità del titolare del trattamento;
5. misure adottate dal titolare del trattamento;
6. grado di cooperazione con l'autorità di controllo.

In relazione alla natura dei dati, si deve tenere in considerazione il fatto che il trattamento ha ad oggetto categorie particolari di dati, segnatamente dati biometrici, - verosimilmente anche di soggetti minori - rispetto ai quali il quadro normativo in materia di protezione dei dati personali prevede un livello più alto di tutela.

In merito alla gravità delle violazioni, si osserva che Clearview ha violato gli artt. 6 e 9 del Regolamento, che rappresentano le condizioni di liceità e dunque i requisiti fondamentali per il trattamento ai sensi del Regolamento. Un trattamento illecito di dati biometrici per finalità di riconoscimento facciale deve, inoltre, ritenersi una violazione molto grave attesa la posizione assunta dai legislatori europeo ed italiano a proposito dell'illegittimità di tale tipo di attività che concreta una sorveglianza di massa. Le violazioni, inoltre, non costituiscono un evento isolato in quanto il trattamento posto in essere dalla Società avviene in modo sistematico e si è protratto anche dopo che il servizio non è più stato offerto a clienti stabiliti nell'Unione europea.

Quanto al numero di soggetti coinvolti, il dato non è quantificabile con precisione, ma considerato che la raccolta di immagini è avvenuta "a strascico" con tecniche di web scraping, è ragionevole ipotizzare che coinvolga un elevatissimo numero di interessati, potenzialmente tutte le persone fisiche che si trovano in Italia e sono presenti in Internet, tramite account su servizi di social network o altre fonti pubblicamente accessibili che li ritraggono per motivi personali o professionali.

Il grado di responsabilità del titolare è molto alto in quanto l'attività di trattamento illecito non solo è continuata nonostante l'intervento di numerose autorità di protezione dei dati personali (europee ed extra europee), ma anche perché ne viene fortemente rivendicata la legittimità attraverso la negazione della giurisdizione europea, e segnatamente italiana.

Nonostante i sopramenzionati interventi di altre autorità e le contestazioni mosse dal Garante con i due atti di avvio del procedimento ai sensi dell'art. 166 del Codice, la Società non ha adottato alcuna misura per conformare la propria attività al Regolamento ed anzi ha ritenuto di modificare, a partire dal mese di marzo 2021, la propria privacy policy eliminando qualunque riferimento ad esso.

Da ultimo, con riferimento al grado di cooperazione, si rileva che la Società, pur avendo formalmente dato riscontro sia alla richiesta di informazioni che alle due contestazioni ex art. 166 del Codice, nel merito ha sostenuto e ribadito l'inapplicabilità del Regolamento all'attività di trattamento posta in essere e non ha fornito puntuali riscontri alle singole richieste.

L'unico fattore attenuante che si rileva è la mancanza di precedenti violazioni commesse dal titolare del trattamento o precedenti provvedimenti di cui all'art. 58 del Regolamento.

In ragione dei suddetti elementi, valutati nel loro complesso, in assenza di dati relativi al fatturato mondiale totale annuo dell'esercizio precedente della Società, si ritiene di determinare, ai sensi dell'art. 83, par. 3, del Regolamento, l'ammontare della sanzione pecuniaria per la violazione degli artt. 5, par. 1, lett. a), b) ed e), 6, 9, 12, 13, 14, 15 e 27, in misura pari al massimo edittale previsto dall'art. 83, par. 5, del Regolamento, ritenuta violazione più grave, ovverosia complessivi 20 milioni di euro (nel dettaglio, 3,8 milioni di euro per ciascuna violazione degli artt. 5, 6 e 9 del Regolamento; 2 milioni di euro per ciascuna violazione degli artt. 12, 13, 14 e 15 del Regolamento; 600.000 mila euro per la violazione dell'art. 27 del Regolamento).

Tale sanzione amministrativa pecuniaria viene ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Tenuto conto della particolare delicatezza dei dati trattati, si ritiene altresì che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del presente provvedimento, prevista dall'art. 166, comma 7 del Codice e art. 16 del Regolamento del Garante n. 1/2019.

Si ricorda che ai sensi dell'art. 170 del Codice, chiunque, essendovi tenuto, non osserva il presente provvedimento di divieto del trattamento è punito con la reclusione da tre mesi a due anni e che, in caso di inosservanza del medesimo provvedimento, è altresì applicata in sede amministrativa la sanzione di cui all'art. 83, par. 5, lett. e), del Regolamento.

Si ritiene, infine, che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante, per l'annotazione delle violazioni qui rilevate nel registro interno dell'Autorità, previsto dall'art. 57, par. 1, lett. u) del Regolamento.

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, dichiara illecito il trattamento descritto nei termini di cui in motivazione da parte di Clearview AI, con sede in 214 W 29th St, 2nd floor, New York City, NY, 10001, U.S.A. e conseguentemente:

a) ai sensi dell'art. 58, par. 2, lett. f), del Regolamento, dispone il divieto di prosecuzione del trattamento e di ulteriore raccolta, mediante tecniche di web scraping, di immagini e relativi metadati concernenti persone che si trovino nel territorio italiano ed il divieto di ogni ulteriore operazione di

trattamento dei dati, comuni e biometrici, elaborati dalla Società attraverso il proprio sistema di riconoscimento facciale, relativamente a persone che si trovino nel territorio italiano;

b) ai sensi dell'art. 58, par. 2, lett. g), del Regolamento, ordina la cancellazione dei dati, comuni e biometrici, elaborati dalla Società attraverso il suo sistema di riconoscimento facciale relativi a persone che si trovano nel territorio italiano, fermo l'obbligo di fornire puntuale riscontro alle richieste di esercizio dei diritti di cui agli artt. 15-22 del Regolamento che fossero eventualmente pervenute da parte di soggetti interessati nel rispetto dell'art. 12, par. 3, del Regolamento.

c) ai sensi dell'art. 58, par. 2, lett. d), del Regolamento ingiunge alla Società, entro trenta giorni dalla notifica del provvedimento, di designare un rappresentante nel territorio dell'Unione europea che funga da interlocutore, in aggiunta o in sostituzione del titolare, con gli interessati al fine di agevolarne l'esercizio dei diritti.

ORDINA

a Clearview AI, con sede in 214 W 29th St, 2nd floor, New York City, NY, 10001, U.S.A. di pagare la somma di euro venti milioni a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione, rappresentando che il contravventore, ai sensi dell'art. 166, comma 8, del Codice ha facoltà di definire la controversia, con l'adempimento alle prescrizioni impartite e il pagamento, entro il termine di sessanta giorni, di un importo pari alla metà della sanzione irrogata.

INGIUNGE

alla predetta Società, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro venti milioni, secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della legge n. 689/1981.

DISPONE

a) ai sensi dell'art. 17 del Regolamento del Garante n. 1/2019, l'annotazione nel registro interno dell'Autorità, previsto dall'art. 57, par. 1, lett. u) del Regolamento, delle violazioni e delle misure adottate;

b) ai sensi dell'art. 166, comma 7, del Codice, la pubblicazione per intero del presente provvedimento nel sito web del Garante.

Il Garante, ai sensi dell'art. 58, par. 1, lett. a) del Regolamento invita il titolare del trattamento a comunicare entro 30 giorni dalla data di ricezione del presente provvedimento, quali iniziative siano state intraprese al fine di dare attuazione a quanto prescritto nel presente provvedimento, fornendo riscontro adeguatamente documentato. Si ricorda che il mancato riscontro alla richiesta ai sensi dell'art. 58 è punito con la sanzione amministrativa di cui all'art. 83, par. 5, lett. e), del Regolamento.

Ai sensi dell'art. 78 del Regolamento, nonché degli artt. 152 del Codice e 10 del d.lgs. 1° settembre 2011, n. 150, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati personali, o, in alternativa, al tribunale del luogo di residenza dell'interessato, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 10 febbraio 2022

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei

SEDE
Piazza Venezia 11
00187 - Roma

CENTRALINO TELEFONICO
+39 06.696771

EMAIL protocollo@gpdp.it

PEC protocollo@pec.gpdp.it

> URP
> FAQ
> RSS
> Informativa protezione dati
> Dichiarazione di accessibilità
> Regole del sito
> Mappa del sito
> Link utili

Seguici su

Iscriviti alla Newsletter