issn 1591-9544 vol. 24 n. 73 (1 - 2023) Estratto

Ciberspazio e Diritto

Rivista Internazionale di Informatica Giuridica

Periodico quadrimestrale

STEM Mucchi Editore

Ciberspazio e Diritto

Rivista Internazionale di Informatica Giuridica

Informatica Giuridica
Diritti di Libertà e Dissidenza Digitale
Investigazioni Digitali

Rivista quadrimestrale

Vol. 24, n. 73 (1 - 2023)

STEM Mucchi Editore

Rivista pubblicata con il contributo dell'Università degli Studi di Milano

Direzione e Redazione: Prof. Avv. Giovanni Ziccardi c/o
STEM Mucchi Editore - Via Jugoslavia, 14 - 41122 Modena

Autorizzazione del Tribunale di Modena, n. 1507 del 10/12/1999

issn 1591-9544

info@mucchieditore.it
www.mucchieditore.it
facebook.com/mucchieditore
twitter.com/mucchieditore
instagram.com/mucchi_editore

Vol. 24 n. 73 (1 - 2023)
Impaginazione STEM Mucchi (MO), stampa Legodigit (TN)

Finito di stampare nel mese di aprile del 2023

Ciberspazio e Diritto

Informazioni per gli abbonati

L'abbonamento decorre dal 1 gennaio di ogni anno e dà diritto a tutti i numeri dell'annata, compresi quelli già pubblicati. Il pagamento può essere effettuato direttamente all'editore tramite bonifico intestato a STEM Mucchi Editore (IT92E0760112900000011051414 - SWIFT/BIC:BPPIITRRXX), a ricevimento fattura (valido solo per enti e società), mediante carta di credito (sottoscrivendo l'abbonamento on line all'indirizzo www.mucchieditore.it, oppure precisando numero, scadenza e data di nascita). Al fine di assicurare la continuità nell'invio dei fascicoli, gli abbonamenti si intendono rinnovati per l'anno successivo. La disdetta dell'abbonamento va effettuata tramite raccomandata a/r alla sede della Casa editrice entro il 31 dicembre dell'annata in corso. I fascicoli non pervenuti all'abbonato devono essere reclamati al ricevimento del fascicolo successivo. Decorso tale termine si spediscono, se disponibili, dietro rimessa dell'importo (prezzo di copertina del fascicolo in oggetto). Le annate arretrate sono in vendita al prezzo della quota di abbonamento dell'anno in corso. Si accordano speciali agevolazioni per l'acquisto di più annate arretrate, anche non consecutive, della stessa rivista. Per l'acquisto di singoli fascicoli della rivista consultare il catalogo online all'indirizzo www.mucchieditore.it. Il cliente ha la facoltà di recedere da eventuali ordini unicamente mediante l'invio di una lettera raccomandata a/r alla sede della Casa editrice, o e-mail (seguita da una raccomandata a/r) entro le successive 48 ore atte a consentire l'identificazione del cliente e dell'ordine revocato (merce, data, luogo, etc.). La revoca dell'ordine deve essere spedita entro e non oltre il 10° giorno successivo alla data di sottoscrizione.

Abbonamento annuo **(3 numeri, iva inclusa)**
Italia € 80,00 - Cartaceo + Digitale € 91,00 - Cartaceo + Digitale IP € 100,00
Estero € 94,00 - Cartaceo + Digitale € 105,00 - Cartaceo + Digitale IP € 114,00
Versione digitale € 56,00 - Digitale IP € 65,00

Ogni fascicolo cartaceo € 27,00 + spese di spedizione
Ogni fascicolo digitale € 20,00

La fruizione dei contenuti digitali avviene tramite la piattaforma www.torrossa.it

Per maggiori informazioni si rimanda alla Sezione Riviste di www.mucchieditore.it

Rivista soggetta a doppia peer-review

Codice etico della Rivista e procedura di Review

La qualità scientifica dei lavori pubblicati è assicurata da una procedura di revisione (c.d. peer review), attuata secondo principi di trasparenza, autonomia e indiscusso prestigio scientifico dei revisori.

- Il lavoro è sottoposto a un esame preliminare da parte del Direttore, del Comitato di Redazione o di un loro componente delegato, per rilevare la sua attinenza alle caratteristiche e ai temi propri della rivista, nonché l'eventuale presenza di evidenti e grossolane carenze sotto il profilo scientifico.
- Il successivo referaggio consiste nella sottoposizione del lavoro alla valutazione di due professori esperti nella materia, italiani o stranieri, scelti dalla direzione nell'ambito di un comitato di *referees* o, in casi eccezionali, inerenti alla specificità dell'argomento trattato, all'esterno dello stesso.
- Il sistema di referaggio è quello c.d. doppio cieco (*double blind peer review*): lo scritto è inviato ai due revisori in forma anonima. All'autore non sono rivelati i nomi dei revisori. I revisori sono vincolati a tenere segreto il loro operato e si impegnano a non divulgare l'opera e le relative informazioni e valutazioni, che sono strettamente confidenziali: l'accettazione preventiva di questo vincolo e di questo impegno è precondizione per assumere il compito di referaggio.
- I nomi dei revisori consultati per la valutazione dei lavori pubblicati dalla rivista nel corso dell'anno sono pubblicati in apposito elenco nell'ultimo fascicolo dell'annata senza riferimento ai lavori valutati.
- I revisori invieranno alla direzione (o al componente delegato), la proposta finale, che può essere di: accettazione dello scritto per la pubblicazione (eventualmente con un lavoro di editing); accettazione subordinata a modifiche migliorative, sommariamente indicate dal revisore (in questi casi lo scritto è restituito all'autore per le modifiche da apportare); non accettazione dello scritto per la pubblicazione.
- I revisori, nel pieno rispetto delle opinioni degli autori e a prescindere dalla condivisione del merito delle tesi da essi sostenute, dovranno tenere in specifica considerazione l'originalità e l'utilità pratica delle idee espresse nel lavoro, nonché la conoscenza delle fonti pertinenti, la consapevolezza culturale, la consistenza critica del percorso argomentativo e la correttezza formale.
- La direzione della rivista ha la responsabilità ultima della decisione di pubblicazione o meno del contributo, ferma restando la esclusiva responsabilità dell'autore per il suo contenuto e le opinioni in esso manifestate.

Ciberspazio e Diritto n. 73 (1 - 2023), in questo numero:

Ciberspazio e diritto, vol. 24, n. 73 (1 - 2023), pp. 43-58

Il caso Clearview AI: uno *stress test* per il Regolamento generale per la protezione dei dati e la proposta di Regolamento sull'intelligenza artificiale in relazione alle nuove sfide poste dal riconoscimento facciale

Jacopo Piemonte[*], Vagelis Papakonstantinou[**]

1. *Introduzione*

I sistemi di riconoscimento biometrici sono quelle tecnologie che consentono di identificare una persona sulla base di caratteristiche fisiologiche o comportamentali, a partire da dati precedentemente acquisiti[1]. In questo Contributo si analizzerà una categoria particolarmente rile-

* Laureato in giurisprudenza presso l'Università degli Studi di Udine, ha conseguito un LLM presso l'Università VUB di Bruxelles con specializzazione in data law. Esercita la professione di avvocato presso lo studio legale De Berti Jacchia dividendosi tra le sedi di Milano e Bruxelles. Si occupa principalmente di tematiche legate alla data protection e di arbitrato domestico ed internazionale.

** Professore di *personal data protection law* presso l'Università VUB di Bruxelles, si occupa anche di cybersecurity, proprietà intellettuale e del più ampio tema della regolamentazione tecnologica. In seno all'Università VUB di Bruxelles, collabora con il Cyber and Data Security Lab (CDSL), di cui è coordinatore scientifico, nonché con il gruppo di ricerca su *Law Science Technology & Society* (LSTS) e con il Brussels Privacy Hub.

[1] Per un inquadramento dei sistemi di riconoscimento biometrico cfr. E. Sacchetto, "Spunti per una riflessione sul rapporto fra biometria e processo penale", «Diritto Penale Contemporaneo», n. 2, 2019, disponibile al link https://dpc-rivista-trimestra-

vante di sistema biometrico: il riconoscimento facciale. Attraverso tale sistema è possibile identificare un individuo avvalendosi dell'immagine del suo volto[2]. Questa tecnologia, un tempo confinata soprattutto alla repressione dei fenomeni criminali, è destinata a diventare sempre più rilevante. Sembra esservi infatti una tendenza in atto, per cui in futuro svolgeremo sempre più operazioni utilizzando la nostra faccia (si pensi, ad esempio, alla possibilità di accedere al proprio smartphone, alla possibilità di effettuare pagamenti o all'identificazione di soggetti per l'ingresso presso un edificio, ecc.)[3].

La questione si è ora resa ancora più di attualità alla luce del recente caso che ha visto coinvolta la società statunitense Clearview AI ("Clearview"). Clearview ha infatti introdotto sul mercato un sistema di riconoscimento facciale del tutto innovativo, che alimenta il proprio database raccogliendo immagini facciali (oltre a tutte le altre informazioni a queste riferibili) sul web senza chiedere alcun consenso ai diretti interessati[4]. Obbiettivo di questo Contributo è verificare brevemente come le autorità di controllo di protezione dei dati europee ("Autorità di controllo") stiano affrontando tale fenomeno sulla base del «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» ("GDPR"). In misura più rilevante, si analizzerà cosa potrebbe cambiare in futuro con l'effettiva implementazione della proposta di Regolamento sull'intelligenza artificiale (definita anche "AI Act"), presentata dalla Commissione nell'aprile 2021[5].

le.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_sacchetto.pdf (ultimo accesso in data 20 marzo 2023), pp. 469-472.

[2] *Ivi,* pp. 470, 471.

[3] Cfr. T. Klosowski, "Facial Recognition Is Everywhere. Here's What We Can Do About It", «nytimes.com», 2020, disponibile al link https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/ (ultimo accesso in data 20 marzo 2023).

[4] Cfr. K. Hill, "The Secretive Company That Might End Privacy as We Know It", «nytimes.com», 2020, disponibile al link https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (ultimo accesso in data 20 marzo 2023).

[5] Cfr. proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, 21 aprile 2021, Commissione Europea, COM (2021) 206 *final*, disponibile al link https://eur-lex.europa.

2. *Il caso Clearview e la risposta delle Autorità di controllo europee sulla base del Regolamento generale per la protezione dei dati*

I sistemi di riconoscimento facciale sono costruiti partendo dall'analisi di svariate immagini. Per ogni volto umano ivi raffigurato, un algoritmo (utilizzando tecniche definite di "hashing") è in grado di tracciare una sorta di impronta digitale facciale, impostando un template biometrico unico. Ciò sul presupposto che la conformazione di ogni volto umano presenta caratteristiche proprie solo di quel viso. Viene dunque creato un database contenente i diversi template biometrici riconducibili alle facce delle singole persone presenti nelle immagini originariamente prese in considerazione. Successivamente, sottoponendo ad esempio al sistema un volto presente in una nuova fotografia, è possibile verificare se sia possibile trovare una corrispondenza nel database[6].

I sistemi di riconoscimento facciale trovano un vasto impiego, soprattutto per esigenze di pubblica sicurezza. In particolare, i software di riconoscimento facciale delle forze di polizia vengono tradizionalmente alimentati con immagini provenienti da foto segnaletiche o patenti. Il loro perimetro di azione è dunque ben definito. Si utilizzano, ad esempio, per verificare se soggetti ripresi da immagini di circuiti di sicurezza nell'atto di compiere crimini possano essere identificati dal sistema di riconoscimento facciale in quanto già noti ai corpi di polizia[7].

Clearview si è però ora affacciata in questo settore come un *game changer*. Ha infatti creato un sistema di riconoscimento facciale particolarmente invasivo e rivoluzionario che raccoglie, con procedimento denominato di "web scraping", tutte le immagini facciali che sono liberamente reperibili sul web e sui social network (in ipotesi, Twitter e Facebook) oppure su video presenti online (ad esempio, su YouTube). Attraverso le

eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0006.02/DOC_1&format=PDF (ultimo accesso in data 20 marzo 2023).

[6] Cfr. T. Madiega, H. Mildebrath, "Regulating facial recognition in the EU", 2021, disponibile al link https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf (ultimo accesso in data 20 marzo 2023), pp. 1, 2.

[7] Cfr. M. Lo Monaco, J. Scipione, "Anatomia legale del riconoscimento facciale", «civiltàdellemacchine.it», 2022, disponibile al link https://www.civiltadellemacchine.it/it/news-and-stories-detail/-/detail/lo-monaco-scipione-riconoscimento-facciale (ultimo accesso in data 20 marzo 2023), p. 4.

citate tecniche di "hashing", Clearview ha dunque potuto creare, in relazione ad ogni volto presente nelle immagini o video raccolti su Internet, un template biometrico unico, associandolo alle pagine web scandagliate (e da cui possono, ad esempio, emergere il nome e cognome delle facce categorizzate). Clearview propone quindi ai suoi clienti un servizio per cui, caricando sul suo software un supporto fotografico contenente un volto, vengono poi presentate all'utente: *i)* le immagini reperite su Internet (inclusive della stessa impronta digitale facciale di quella caricata a sistema) e *ii)* le pagine web che le contenevano, con annessi eventuali elementi identificativi come nome e cognome[8]. L'utilizzatore del sistema di Clearview è posto dunque nella maggiore parte dei casi (chi non ha un proprio profilo su Internet oggi giorno?) nella posizione di prendere piena contezza di chi sia rappresentato nell'immagine che è stata sottoposta al vaglio del software. Ci si muove, dunque, su un terreno sdrucciolevole, in quanto, potenzialmente, tutti coloro che hanno una propria immagine sul web rischiano di essere inseriti in database come quelli alimentati da Clearview, senza aver fornito alcun consenso.

Tale sistema di riconoscimento facciale risulta abbia avuto un successo portentoso e sia stato presto adottato da diversi corpi di polizia ma anche da agenzie governative[9], nonché proposto a diversi clienti privati per le finalità più varie (come, ad esempio, per controlli di sicurezza nelle scuole, in edifici privati, ecc.)[10]. Non sono però tardate le critiche. Il software ideato dalla società statunitense è stato infatti messo all'indice in svariate giurisdizioni del globo per la sua idoneità a determinare una sorta di sorveglianza di massa[11].

Anche a livello europeo si sta assistendo ad una risposta compatta nei confronti di Clearview (e del sistema di riconoscimento facciale da questa elaborato); dopo specifico intervento di censura da parte dell'EDPS (European Data Protection Supervisor), sul tema si stanno infatti pro-

[8] Per una spiegazione sul funzionamento del software utilizzato da Clearview si consulti il suo sito Internet disponibile al link https://www.clearview.ai (ultimo accesso in data 20 marzo 2023).

[9] Cfr. https://www.clearview.ai/blog/categories/success-stories (ultimo accesso in data 20 marzo 2023).

[10] Cfr. https://www.clearview.ai/commercial (ultimo accesso in data 20 marzo 2023).

[11] Cfr. K. Hill, op. cit.

nunciando a cascata diverse Autorità di controllo[12]. La prima a esprimersi è stata l'Autorità italiana[13]. Hanno poi fatto seguito gli interventi dell'Autorità greca[14] e francese[15]. I *driver* di fondo delle decisioni sono stati i medesimi e l'*iter* argomentativo dei pronunciamenti è molto simile (pur con i dovuti distinguo).

In primo luogo, sembra che, nei distinti procedimenti, Clearview abbia sostenuto di non dover essere sottoposta alla giurisdizione delle Autorità europee poiché non opererebbe in alcun Stato membro[16]. Tutte le Autorità di controllo sono invece arrivate alla conclusione opposta, sulla base, *inter alia*, del principio esposto all'articolo 3, par. 2, lett. b) del GDPR, per cui tale formante legislativo troverebbe applicazione «al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare […] che non è stabilito nell'Unione, quando le attività di trattamento riguardano: […] il monitoraggio del loro comportamento». Si è infatti rilevato che i presupposti di tale articolo sarebbero pienamente concretati, poiché l'indiscriminata raccolta di dati personali di cittadini europei sul web operata da Clearview (società pur non stabilita nell'Unione) costituirebbe un trattamento assimilabile in tutto e per tutto ad un'attività di *targeting*[17].

[12] Cfr. European Data Protection Supervisor, "EDPS opinion on the possibility to use Clearview AI and similar services at Europol (Case 202-0372)", 2020, disponibile al link https://edps.europa.eu/system/files/2022-01/21-03-29_edps_opinion_2020-0372.pdf (ultimo accesso in data 20 marzo 2023).

[13] Cfr. Autorità Garante Per La Protezione Dei Dati Personali Italiana ("Garante Italiano"), "docweb 9751362 – n.ro 50/2022, registro provvedimenti", 10 febbraio 2022, disponibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9751362 (ultimo accesso in data 20 marzo 2023).

[14] Cfr. Autorità Garante Per La Protezione Dei Dati Personali Greca ("Garante Greco"), "Provvedimento 35/2022 – n.ro 1809", 13 luglio 2022, disponibile in lingua greca al link: https://www.dpa.gr/sites/default/files/2022-07/35_2022%20anonym_0.pdf (ultimo accesso in data 20 marzo 2023).

[15] Cfr. Commission Nationale De L'Informatique Et Des Libertés ("Cnil"), "Provvedimento No. SAN-2022-019", 17 ottobre 2022, disponibile in lingua inglese al link: https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_the_restricted_committee_no_san-2022 019_of_17_october_2022_concerning_clearview_ai.pdf (ultimo accesso in data 20 marzo 2023).

[16] Cfr. Garante Italiano, provvedimento cit., sezione 2, par. 34.

[17] Cfr. Garante Italiano, provvedimento cit., sezione 3.2. Cfr. Garante Greco, provvedimento cit., par. 12. Cfr. Cnil, provvedimento cit., parr. 18-42.

Del pari, le Autorità di controllo hanno poi preso atto che Clearview non ha sedi in Europa e che, dunque, il trattamento è effettuato da un titolare del trattamento (*i.e.* la stessa società statunitense) non stabilito nell'Unione. Tutte hanno dunque riconosciuto, sulla base del combinato disposto degli articoli 55 e 56 del GDPR, di essere Autorità competenti a trattare del tema, non trovando applicazione il famigerato *one stop mechanism*[18].

Venendo al cuore delle decisioni, le Autorità di Controllo hanno valutato come implicito il fatto che le foto fossero state rastrellate senza consenso degli interessati e, dunque, mancasse la base giuridica di cui all'articolo 6 lett. a) del GDPR. Tutte hanno inoltre constatato la mancanza delle altre basi giuridiche di trattamento previste dagli articoli 6 lett. b), c), d) ed e) del GDPR; di conseguenza, hanno esaminato se ci potesse essere un legittimo interesse alla raccolta dei dati da parte di Clearview sulla base dell'articolo 6 lett. f) del GDPR. Ciò anche a fronte di un'implicita difesa operata dalla società statunitense per cui essa non farebbe null'altro che indicizzare informazioni reperite sul web e già di dominio pubblico ai fini di dare corso al suo business[19]. A riguardo, le Autorità di controllo hanno tutte concluso che la circostanza che i dati siano disponibili pubblicamente su Internet non giustifica di per sé la legittimità della raccolta delle immagini da parte di soggetti terzi[20], a prescindere da come quei dati vengano poi utilizzati. Occorrerebbe invece sempre operare un bilanciamento di interessi (proprio sulla base dell'art. 6 lett. f) del GDPR). Tale analisi, condotta da tutte le Autorità di controllo nei diversi procedimenti, ha concluso che gli interessi economici di Clearview debbano necessariamente flettere rispetto a diritti quali la riservatezza degli interessati, che verrebbero invece gravemente messa a rischio dal sistema di riconoscimento facciale elaborato dalla società statunitense. Di conseguenza, in tutti i pronunciamenti è stato osservato, *inter alia*[21], come Clearview tratti i dati

[18] Cfr. Garante Italiano, provvedimento cit., sezione 3.3. Cfr. Garante Greco, provvedimento cit., par. 13. Cfr. Cnil, provvedimento cit., parr. 43-48.

[19] Cfr. Garante Italiano, provvedimento cit., sezione 2, par. 2.

[20] Cfr. Garante Italiano, provvedimento cit., sezione 3.6.2. Cfr. Garante Greco, provvedimento cit., par. 16. Cfr. Cnil, provvedimento cit., parr. 60-68.

[21] Non si analizzeranno le parti dei provvedimenti che hanno portato le Autorità di Controllo a rilevare altresì la violazione da parte di Clearview delle disposizioni del GDPR relative all'obbligo di designazione di un rappresentante nell'Unione europea o in tema di diritto di accesso o di cancellazione dati. Per una disamina di tali aspetti si rimanda alla lettura dei singoli provvedimenti.

che emergono dalle immagini raccolte su Internet senza una base giuridica e, dunque, in chiara violazione del GDPR. Analoghe sono anche state le domande di condanna che hanno colpito la società statunitense. In particolare, tutte le Autorità di Controllo: *i)* hanno disposto il divieto di prosecuzione del trattamento posto in essere da Clearview; *ii)* hanno richiesto la cancellazione dei dati utilizzati dal software; *iii)* in considerazione della gravità della condotta, hanno comminato a Clearview una sanzione principale altissima e identica, pari a venti milioni di euro[22].

In considerazione di tutto quanto sopra, il GDPR sembrerebbe essersi rivelato strumento utile per la tutela dei cittadini europei. All'atto pratico, restano però alcune perplessità di fondo in relazione all'effettiva deterrenza di tale strumento in casi come questo. È pur vero che attraverso il GDPR, in virtù delle tre decisioni citate, sono stati imposti alla società statunitense uno stop delle sue attività e sanzioni per un importo *monstre* di sessanta milioni di euro (*i.e.* venti milioni di euro per ogni provvedimento). Resta da valutare, però, se tali misure impatteranno realmente sull'attività della società statunitense. È noto, infatti, che l'*enforcement* del GDPR possa risultare ostico nei confronti di società extra-UE[23] (come, per l'appunto, Clearview). Vi è dunque il concreto rischio che i provvedimenti citati e le relative sanzioni possano rimanere "sulla carta".

3. *Il valore aggiunto che potrebbe portare la proposta di Regolamento sull'intelligenza artificiale in casi come quello di Clearview*

Il presente Contributo si pone anche l'obiettivo di provare a immaginare come verrebbe affrontata una questione come quella di specie con la proposta di Regolamento sull'intelligenza artificiale ("AI Act"), che rego-

[22] Cfr. Garante Italiano, provvedimento cit., sezione 5, parr. 20-23. Cfr. Garante Greco, provvedimento cit., par. 19. Cfr. Cnil, provvedimento cit., p. 15 (primi due *bullet point*). In aggiunta alla menzionata sanzione principale il Garante Italiano e il CNIL hanno affiancato anche alcune sanzioni ancillari. A riguardo, si rimanda alla lettura dei singoli provvedimenti.

[23] Cfr. A. Azzi, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation", «Jipitec», vol. 9, n. 2, 2018, p. 132, par. 46.

la altresì il riconoscimento biometrico[24]. Sistemi di riconoscimento facciale come quello di Clearview verranno dunque sottoposti al vaglio di questo nuovo formante legislativo una volta approvato.

La proposta di Regolamento sull'intelligenza artificiale utilizza uno schema piramidale, dividendo i sistemi di intelligenza artificiale in: *i*) pratiche proibite; *ii*) sistemi a rischio elevato; e *iii*) sistemi a basso rischio[25]. Ai nostri fini, rilevano le prime due categorie. L'AI Act distingue infatti i sistemi di riconoscimento biometrico (e dunque anche facciale) in sistemi vietati e sistemi ad alto rischio.

Nel dettaglio, sono vietati i sistemi utilizzati per l'identificazione di soggetti «in tempo reale»[26] in spazi pubblici per fini di contrasto alla criminalità[27]. Uno strumento come Clearview non potrebbe dunque essere immesso sul mercato se fosse impiegato per perseguire tali finalità[28]. Nella presente analisi, tuttavia, non ci si dilungherà su questa tipologia di strumenti di sorveglianza. Essi possono certamente incidere in maniera rilevante su diritti fondamentali delle persone[29]; tuttavia, il loro effettivo impatto dovrebbe forse essere ridimensionato in quanto implicherebbero una costante capacità di presenza delle forze di polizia a seguito di allarmi lanciati in tempo reale dai sistemi di riconoscimento facciale che, probabilmente (almeno in questo momento storico), non è ancora del tutto realistica[30].

[24] Un sistema di identificazione biometrica remota è «un sistema di IA finalizzato all'identificazione a distanza di persone fisiche mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento, e senza che l'utente del sistema di IA sappia in anticipo se la persona sarà presente e può essere identificata». Cfr. Commissione Europea, COM (2021) 206 *final*, cit., art. 3 par. 36.

[25] Per una panoramica su tali aspetti, cfr. P. Severino, *Intelligenza artificiale: politica, economia, diritto, tecnologia*, Roma, Luiss University Press, 2022, pp. 136-140.

[26] In questo caso, ci si basa su un uso immediato del materiale rilevato dal sistema.

[27] Cfr. Commissione Europea, COM (2021) 206 *final*, cit., art. 5 par. 1 l. d).

[28] *Ivi*, art. 5 par. 1 l. d) *(i)*, *(ii)*, *(iii)*. Nell'AI Act sono tuttavia previste alcune eccezioni "generose" che rendono possibile l'uso dei citati sistemi negli spazi pubblici per ricerche mirate di vittime di reati, per prevenire attacchi terroristici e per localizzare o identificare soggetti che siano sospettati di aver commesso gravi crimini.

[29] Cfr. G.G. Fuster, M.N. Peeters: "Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence", 2021, disponibile al link https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697191/EPRS_STU(2021)697191_EN.pdf (ultimo accesso in data 20 marzo 2023), p. 33.

[30] Cfr. A. Monti, "Chi ha paura della AI-powered Face Recognition?", «repubblica.it», 2023, disponibile al link https://www.repubblica.it/tecnologia/blog/strate-

Ci si concentrerà, invece, sulla restante fetta di sistemi di riconoscimento facciale che l'AI Act definisce come ad alto rischio. Tra questi, la proposta di Regolamento di intelligenza artificiale include[31] i sistemi biometrici «in tempo reale» non utilizzati per fini repressivi, quali quelli che consentono la possibilità ad attori privati di utilizzare tecnologie di riconoscimento facciale per regolare gli ingressi in determinati spazi pubblici (come supermarket, stadi e scuole[32]). Del pari, ricomprende altresì i sistemi biometrici utilizzati «a posteriori» dalle forze di polizia che confrontano materiale, come filmati ripresi da telecamere a circuito chiuso, che sono stati generati in precedenza (ad esempio, per identificare *ex post*, attraverso l'ausilio di immagini, un soggetto che abbia commesso un crimine)[33]. È evidente come questa tipologia di software sia particolarmente diffusa nella società[34]; non a caso, Clearview ne fa ampia promozione sul proprio sito Internet[35]. Soprattutto per tali sistemi vale dunque la pena di verificare che valore aggiunto possa essere fornito dall'AI Act rispetto all'attuale regolamentazione.

Si nota che, per essere immessi sul mercato, tali sistemi devono soddisfare i seguenti requisiti, previsti dal titolo III capitolo 2 dell'AI Act[36]: *i)* prova di utilizzo di dati di alta qualità per evitare qualsiasi tipo di *bias* nel funzionamento dell'algoritmo di riconoscimento[37]; *ii)* elaborazione del-

gikon/2023/01/16/news/chi_ha_paura_della_aipowered_face_recognition-383781689/ (ultimo accesso in data 20 marzo 2023).

[31] Cfr. Allegato III della Commissione Europea, COM (2021) 206 *final* cit., disponibile al link https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0006.02/DOC_2&format=PDF (ultimo accesso in data 20 marzo 2023), art. 1 l. a).

[32] Cfr. T. Madiega, H. Mildebrath, "Regulating facial recognition in the EU", 2021, disponibile al link https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf (ultimo accesso in data 20 marzo 2023), p. 26.

[33] *Ibidem*.

[34] T. Klosowski, op. cit.

[35] Cfr. https://www.clearview.ai/ (ultimo accesso in data 20 marzo 2023).

[36] Cfr. G. Finocchiaro, "La regolazione dell'intelligenza artificiale", «Rivista trimestrale di diritto pubblico», fascicolo 4, 2022, pp. 1093, 1094.

[37] Cfr. Commissione Europea, COM (2021) 206 *final*, cit., art. 10. I sistemi di riconoscimento facciale presentano un ampio margine di errore nell'identificazione di soggetti come le giovani donne e le persone di carnagione scura. Queste categorie sarebbero infatti sottorappresentate nei sistemi di addestramento degli algoritmi. È invece rile-

la necessaria documentazione tecnica[38]; *iii)* obbligo di tracciamento del funzionamento del sistema[39]; *iv)* trasparenza[40]; *v)* meccanismi di supervisione umana che assicurino sempre la possibilità di *double check*[41] di una persona in carne ed ossa sulle operazioni effettuate dal sistema; e *vi)* robustezza e accuratezza del sistema, anche in termini di cybersecurity[42]. Si tratta dunque di importanti presidi, come è stato rilevato da alcuni commentatori[43]. È altrettanto interessante notare, però, come nell'AI Act vi siano delle novità sensibili, che riguardano soprattutto il controllo sull'osservanza di tali requisiti.

In primo luogo, l'AI Act prevede una fase precedente all'ingresso sul mercato per i sistemi considerati ad alto rischio. Il modello scelto dal Legislatore per effettuare tali controlli è la procedura di ottenimento della marchiatura "CE". L'AI Act prevede che, di norma, sia lo stesso soggetto che ha interesse a immettere il prodotto sul mercato a dover eseguire un'autovalutazione, per verificare la conformità del sistema ai citati requisiti previsti dal titolo III capitolo 2[44]. Tuttavia, per i sistemi di intelligenza artificiale destinati all'identificazione biometrica remota (come quello di Clearview), tale procedura di conformità, almeno di *default,* dovrebbe essere eseguita da enti terzi di certificazione del settore privato, denominati «organismi notificati»[45]. In questo caso, il vantaggio è rile-

vante che i database contengano campioni rappresentativi «di diverse età, genere e nazionalità, con l'inclusione di minoranze etniche». Cfr. M. Lo Monaco, J. Scipione, op. cit., p. 8. La norma in parola va dunque in questa direzione.

[38] Cfr. Commissione Europea, COM (2021) 206 *final*, cit., art. 11.

[39] *Ivi,* art 12.

[40] *Ivi,* art. 13.

[41] *Ivi,* art. 14. Questo articolo dell'AI Act riprende in parte quanto già previsto dall'articolo 22 del GDPR. Sulla necessità che l'intervento umano sia sempre posto a presidio di decisioni automatizzate, cfr. A. Oddenino, "Decisioni algoritmiche e prospettive internazionali di valorizzazione dell'intervento umano", «Saggi – DPCE online», n.1, 2020, disponibile al link https://www.dpceonline.it/index.php/dpceonline/article/view/894/868 (ultimo accesso in data 20 marzo 2023), pp. 199-217.

[42] *Ivi,* art. 15.

[43] Cfr. P. Severino, op. cit., p. 137.

[44] Cfr. C. Casonato, B. Marchetti, "Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale", «BioLaw Journal», n. 3, Settembre 2021, pp. 430-432.

[45] Cfr. Commissione Europea, COM (2021) 206 *final*, cit., art. 43 par. 1. La stessa disposizione prevede però che ci possano essere degli enti di settore a cui delegare la

vante[46]. E infatti, se tale prassi dovesse essere consolidata, la "tagliola" del menzionato controllo da parte degli «organismi notificati» potrebbe potenzialmente bloccare sistemi come Clearview *ex ante* (e prima della loro immissione sul mercato), se considerati non in linea con i menzionati parametri previsti dall'AI Act.

In seconda battuta, è altresì interessante notare come i sistemi ad alto rischio sarebbero comunque sottoposti a controllo anche dopo essere stati immessi in commercio attraverso un sistema di monitoraggio successivo[47]. A riguardo, si prevede che ogni Stato membro debba istituire un'autorità per la gestione di tale fase, deputata a verificare che qualsiasi sistema, una volta introdotto nel mercato, continui ad essere *compliant* con i menzionati requisiti previsti dal titolo III capitolo 2 dell'AI ACT per tutto il suo ciclo di vita[48]. Se così non fosse, l'Autorità di vigilanza designata potrebbe arrivare a disporre rimedi estremi, quali il ritiro dal mercato del sistema[49]. Anche questa, a ben vedere, non è una novità da poco. Nel caso Clearview, le Autorità di controllo, sulla base del GDPR, hanno infatti solamente potuto richiedere alla società statunitense di bloccare il

stesura di standard tecnici anche per i sistemi biometrici. In tal caso, quando il fornitore applica lo standard tecnico (ove promulgato) può scegliere di svolgere internamente la procedura di valutazione della conformità senza ricorrere agli «organismi notificati». Si è notato che, se così fosse, sarebbe improbabile che non si ricorresse all'applicazione di standard tecnici (una volta promulgati) e dunque risulterebbe fortemente depotenziata la figura degli «organismi notificati». Cfr., in tal senso, M. Veale, F. Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach", «Computer Law Review International», vol. 22, no. 4, 2021, p. 106, par. 64. È stato dunque caldeggiato di «prevedere l'obbligo generale di sottoporre i sistemi di IA ad alto rischio a una valutazione della conformità *ex ante* da parte di terzi». Cfr. European Data Protection Board, European Data Protection Supervisor, "Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale)", 2021, disponibile al link https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_it.pdf. (ultimo accesso in data 20 marzo 2023), pp. 14, 15, par. 37.

[46] *Ivi*, p. 15, par. 37. Si afferma che l'inserimento nell'AI Act di «una previsione generale di condurre una valutazione obbligatoria della conformità a opera di terzi permetterebbe […] di accrescere ulteriormente la certezza del diritto e la fiducia in tutti i sistemi di IA ad alto rischio».

[47] Cfr. Commissione Europea, COM (2021) 206 *final*, cit., artt. 61-68.

[48] *Ivi*, art. 59 par. 2.

[49] *Ivi*, art. 65 par. 2.

trattamento dei dati ritenuto illegittimo[50]. Con l'AI Act, in un caso analogo, l'Autorità designata avrebbe altresì la possibilità di richiedere l'uscita dal mercato[51] del sistema se ritenuto non in linea con i requisiti di ingresso sopra menzionati.

Alla luce di tutto quanto sopra, si è osservato come la procedura di conformità *ex ante* e il sistema di monitoraggio *ex post* previsto dall'AI Act costituiscano una robusta base per l'*enforcement* di tale nuova normativa[52], che potrebbe dunque portare un valore aggiunto anche nella lotta ai sistemi di riconoscimento facciali considerati illegittimi.

4. *Possibili problematiche sul coordinamento tra il Regolamento generale per la protezione dei dati e la proposta di Regolamento sull'intelligenza artificiale in tema di riconoscimento facciale*

Nonostante quanto sopra osservato, resta un punto fondamentale da scandagliare, costituito dai rapporti e dai punti di contatto tra il GDPR e l'AI Act. A riguardo, si nota che il GDPR regola il trattamento dei dati personali mentre l'AI Act si riferisce a una regolamentazione della tecnologia[53] con cui il trattamento dei dati può avvenire. In base a questa considerazione, è logico pensare che i due strumenti debbano essere complementari l'uno all'altro[54]. In altre parole, posto un caso analogo, essi dovrebbero portare alle medesime conclusioni (pur da angolature differenti).

Alla luce di quanto sopra, si può pertanto verificare se, stante l'attuale dicitura della proposta di AI Act, il software utilizzato da Clearview sarebbe stato considerato come uno strumento che non può trovare spa-

[50] Cfr. Art. 58 par. 2 del GDPR.

[51] Cfr. N. Lomas, "Europe's AI Act contains powers to order AI models destroyed or retrained, says legal expert", su «techcrunch.com», 2022, disponibile al link https://techcrunch.com/2022/04/01/ai-act-powers/ (ultimo accesso in data 20 marzo 2023).

[52] Cfr. J. Mökander, M. Axente, F. Casolari, L. Floridi, "Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation", «Minds and Machines», 32, June 2022, p. 253.

[53] Cfr. Commissione Europea, COM (2021) 206 *final*, cit., p. 3, par. 8.

[54] Cfr. G. Cerrina Feroni, "Intelligenza artificiale e ruolo della protezione dei dati personali. L'analisi di Ginevra Cerrina Feroni (Garante Privacy)", su «key4biz.it», 2023, disponibile al link https://www.key4biz.it/intelligenza-artificiale-e-ruolo-della-protezione-dei-dati-personali/434983/ (ultimo accesso in data 20 marzo 2023).

zio sul mercato, come decretato dalle Autorità di controllo europee sulla base del GDPR. A riguardo, come menzionato, si andrebbero a valutare i requisiti previsti dal titolo III capitolo 2 dell'AI Act, conducendo, dunque, un'analisi *de facto*. Allo stato, non si può affermare con certezza che Clearview non sarebbe in grado di superare questa prova[55]. Resta invece da verificare se, sulla base dell'AI Act, si potrebbe giungere alle medesime conclusioni delle Autorità di controllo che, sulla base del GDPR, hanno considerato Clearview come uno strumento da vietare, avendo alimentato il suo database con foto raccolte su Internet senza chiedere consenso ai diretti interessati. A ben vedere, ciò non sembra operazione scontata. L'AI Act non si pronuncia in maniera chiara su questo specifico punto[56] e non vi sono divieti specifici a riguardo[57]. Occorrerebbe, dunque, rifarsi alle previsioni del GDPR (come interpretate dalle Autorità di controllo nelle decisioni contro Clearview) per arrivare a tale conclusione. Siffatta operazione non sembrerebbe però essere consentita. E infatti, l'AI Act si limita a precisare che esso «non pregiudica il regolamento generale sulla protezione dei dati»[58], senza però affermare chiaramente che

[55] Uno dei requisiti più rilevanti dell'AI Act è la dimostrazione di utilizzo di dati che evitino qualsiasi tipo di *bias* nel funzionamento dell'algoritmo. Cfr. Commissione Europea, COM (2021) 206 final, cit., art. 10. Clearview afferma sul suo sito internet di essere stata riconosciuto ufficialmente come il sistema di riconoscimento facciale più accurato negli Stati Uniti basandosi su un database di oltre trenta miliardi di immagini (rappresentativo di gran parte della popolazione mondiale). Cfr. https://www.clearview.ai/press-release-consecutive-nist-tests-confirm-superiority-of-clearview-ai-facial-recognition (ultimo accesso in data 20 marzo 2023). Tale affermazione andrebbe provata. È noto, però, che più un sistema viene alimentato, più può essere preciso. Cfr. M. Lo Monaco, J. Scipione, op. cit., p. 8. Non si può dunque escludere che la società americana possa dare prova che il suo software sia conforme al requisito in parola, oltre agli altri parametri previsti dall'AI Act.

[56] Si è affermato che l'AI Act «fails to elaborate on the conditions for the collection of personal data from publicly available sources for mandatory training, validation, and testing». Cfr. S. Barros Vale, "GDPR and the AI Act Interplay: lessons from FPF's ADM case-law report", su «FPF's blog», 2023, disponibile al link https://fpf.org/blog/gdpr-and-the-ai-act-interplay-lessons-from-fpfs-adm-case-law-report/ (ultimo accesso in data 20 marzo 2023).

[57] Si è rilevato che «il processo di *scraping*, ossia il rastrellamento di dati *open-source* su Internet, non è astrattamente vietato». Cfr. M. Lo Monaco, J. Scipione, op. cit., p. 5.

[58] Cfr. Commissione Europea, COM (2021) 206 final, cit. p. 4. L'EDPB e EDPS hanno dunque raccomandato «vivamente di precisare, all'articolo 1, che la legislazione dell'Unione in materia di protezione dei dati personali – in particolare l'RGPD [GDPR]… – si applica a qualsiasi trattamento di dati personali che rientri nell'ambito

il GDPR debba estendersi a qualsiasi trattamento di dati personali che rientri nell'ambito di applicazione dell'AI Act stesso. Inoltre, tra i requisiti dell'AI Act, per l'immissione e permanenza nel mercato dei sistemi di riconoscimento biometrico non è incluso il rispetto del GDPR[59].

Allo stato dell'arte, sulla base delle precedenti constatazioni, non necessariamente gli eventuali «organismi notificati» chiamati a valutare *ex ante* la legittimità del sistema avrebbero considerato Clearview come illegale, dal momento che acquisisce foto online in assenza di idonea base giuridica (che è invece punto comune a cui sono arrivate le Autorità italiana, greca e francese sulla base del GDPR). Del pari, anche nel controllo *ex post* (sulla sola base dell'AI Act) non necessariamente le autorità designate sarebbero arrivate a considerare quello strumento come illegale e dunque ad ordinare, ad esempio, il suo ritiro dal mercato.

Alla luce di tutto quanto sopra osservato, sembrerebbe dunque esserci un problema di coordinamento tra i due strumenti legislativi. Sistemi come Clearview potrebbero paradossalmente correre il rischio di essere considerati accettabili dall'AI Act e, allo stesso tempo, contrari ai principi espressi dal GDPR.

5. *Conclusioni*

Nel complesso di quanto rilevato nel presente Contributo, sembra si possano segnare alcuni punti fermi. Il GDPR è un presidio assoluto e svolge un ruolo di tutela anche nel contrasto di software di intelligenza artificiale che operino in spregio alla legislazione in materia di dati personali. E infatti, in un caso come quello di Clearview, le Autorità di controllo hanno dimostrato di poter fornire una risposta compatta. È sta-

di applicazione della proposta stessa». Cfr. European Data Protection Board, European Data Protection Supervisor, op. cit., p. 9 par. 15).

[59] A questo riguardo, EDPB e EDPS osservano che «la conformità agli obblighi giuridici previsti dalla legislazione dell'Unione (compresa quella in materia di protezione dei dati personali) dovrebbe essere un prerequisito per ottenere l'autorizzazione all'immissione sul mercato europeo come prodotto munito della marcatura CE. A tal fine […] raccomandano di includere nel capo 2 del titolo III della proposta l'obbligo di garantire la conformità al RGPD [GDPR]». Cfr. European Data Protection Board, European Data Protection Supervisor, op. cit., p. 11 par. 23.

to infatti richiesto in tutti i Paesi in cui vi sono stati pronunciamenti (*i.e.*, Italia, Grecia e Francia) che la società statunitense cessasse l'illegittimo trattamento di dati basati sul rastrellamento di fotografie su Internet senza chiedere il consenso degli interessati. Sono poi state comminate alla suddetta società sanzioni pecuniarie ragguardevoli. Rimane però il problema della *enforceability* di queste decisioni, specie in un caso come quello di Clearview, che è società extra-europea.

A riguardo, l'AI Act potrebbe rivelarsi un valore aggiunto. Tale normativa pone infatti presidi ulteriori, che potrebbero impedire a questi strumenti di entrare in circolo *ex ante*. L'AI Act prevede inoltre un sistema di monitoraggio successivo e strumenti più forti di repressione rispetto al GDPR (come la possibilità di ordinare il ritiro dal mercato del sistema di intelligenza artificiale ritenuto illegale). Occorre però allo stesso tempo che i due strumenti (GDPR e AI Act) procedano di pari passo. Si è osservato, infatti, come al momento potrebbero esserci problemi di coordinamento tali da condurre a trattamenti differenti nell'analisi di software come quello di Clearview a seconda che si consideri una o l'altra normativa.

Si ritiene dunque che le valutazioni fornite dimostrino la necessità di caldeggiare un maggiore *fine tuning* tra i due formanti legali presi in considerazione in sede di finalizzazione dell'AI Act. Se il Legislatore europeo procederà in tale direzione, potrà essere raggiunto un risultato eccellente. Si otterrà infatti un atto legislativo (l'AI Act) che regola i sistemi di intelligenza artificiale in pieno ossequio a quanto previsto dalla legislazione in materia di protezione dei dati personali. Alternativamente, se il GDPR e l'AI Act (quando andrà a regime) dovessero configurarsi come due monadi non coordinate nel firmamento della "legislazione digital" si potrebbero determinare alcune criticità e, forse, si sarebbe persa un'occasione per lo sviluppo di un'intelligenza artificiale sostenibile, anche in un'ottica di salvaguardia dei dati personali.

Il caso Clearview: uno stress test per il Regolamento generale per la protezione dei dati e la proposta di Regolamento sull'intelligenza artificiale in relazione alle nuove sfide poste dal riconoscimento facciale

Partendo dal controverso caso Clearview AI, gli Autori si propongono di verificare quali siano le tutele previste ad oggi dalla legislazione europea in materia di riconoscimento facciale e, in particolare, dal GDPR. Il Contributo ha lo scopo di analizzare, dunque, come potrà cambiare il quadro di riferimento con la proposta di Regolamento sull'intelligenza artificiale, evidenziando il valore aggiunto e le maggiori tutele che detta normativa potrà eventualmente garantire in futuro in quest'ambito.

The Clearview's case: a stress test for the General data protection regulation and the proposed artificial intelligence Regulation in relation to the new challenges posed by facial recognition

Starting from the controversial Clearview AI's case, the Authors aim to analyse which safeguards are in place as of today in the European legislation regarding the facial recognition, focusing especially on the GDPR. The paper aims to analyze, therefore, how the framework may change with the proposed artificial intelligence Regulation, highlighting the added value and reinforced protections that said legislation may eventually guarantee in the future in this area.

Ciberspazio e Diritto vol. 24, n. 73 (1 - 2023), in questo numero: