Nazzaro AC, 'La tutela dei dati biometrici tra GDPR e AI ACT' (2024) 2 EJPLT, 37 – 53.
DOI: https://doi.org/10.57230/EJPLT242ACN

EJPLT
ISSN 2704-8012



La tutela dei dati biometrici tra GDPR e AI ACT

The protection of biometric data between the GDPR and the AI ACT

ANNA CARLA NAZZARO
Professore Ordinario di Diritto Privato
Università degli studi Internazionali di Roma

Abstract

Il saggio analizza la tutela dei dati biometrici nell'ambito del GDPR e dell'AI ACT, evidenziando il delicato equilibrio tra protezione della privacy e innovazione tecnologica. Viene esaminata la definizione di dato biometrico e il suo utilizzo per identificazione, autenticazione e categorizzazione, con particolare attenzione ai rischi legati alla discriminazione e all'uso improprio. Si affrontano i divieti di raccolta indiscriminata e le implicazioni etiche dell'impiego dell'IA nel riconoscimento facciale e nell'analisi delle emozioni. Infine, si discute il ruolo della valutazione d'impatto e la necessità di un approccio regolatorio che tuteli i diritti fondamentali.

The essay explores the protection of biometric data within the framework of the GDPR and the AI ACT, highlighting the delicate balance between privacy protection and technological innovation. It examines the definition of biometric data and its use for identification, authentication, and categorization, with a focus on the risks of discrimination and misuse. The paper addresses the bans on indiscriminate data collection and the ethical implications of AI in facial recognition and emotion analysis. Finally, it discusses the role of impact assessment and the need for a regulatory approach that safeguards fundamental rights.

* Questo articolo è stato presentato alla ReCEPL Annual Conference "Diritto privato e sviluppo tecnologico sostenibile: le nuove categorie tra Italia e Argentina", 21 ottobre 2024, Università degli Studi Suor Orsola Benincasa.

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Dati biometrici; identificazione biometrica; Bias algoritmico; riconoscimento facciale

Summary: 1. Definizione di dato biometrico. – 2. Segue: Identificazione univoca della persona. – 3. Identificazione, autenticazione e categorizzazione. – 4. Dal rilevamento biometrico al rilevamento delle emozioni. – 5. Dati biometrici e personalità dell'individuo. – 6. Qualità del dato, pericolo di *bias* e valutazione d'impatto.

1. Definizione di dato biometrico.

La definizione di dato biometrico necessita di essere distinta da altre definizioni (come, ad esempio, quella di dato sanitario) ed è fondamentale determinarne l'autonomia rispetto al concetto di dato personale.

A tal fine è d'obbligo partire dalla normativa, denominata comunemente AI ACT (Reg. 2024/1689/UE) [1], che si occupa di stabilire regole uniformi sull'intelligenza artificiale e di sviluppare un ecosistema di fiducia attraverso un quadro giuridico per un'IA affidabile[2].

L'AI ACT, nella versione pubblicata in GU dell'UE il 12 luglio 2024 e che sarà applicabile in maniera parziale, a decorrere dal 2 febbraio 2025, all'art. 3, n. 34, in tema di definizioni, si appresta a qualificare dati biometrici i «dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici».

Questa formulazione, che riprende quasi pedissequamente la definizione già contenuta nel Reg. 2016/679/UE (GDPR)[3], acquista un rilievo centrale nel tema che si sta trattando poiché aiuta a delimitare la nozione creando una

[1] Regolamento 2024/1689/UE del Parlamento europeo e del Consiglio, 13.06.2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti 300/2008/CE, 167/2013/UE, 168/2013/UE, 2018/858/UE, 2018/1139/UE e 2019/2144/UE e le direttive 2014/90/UE, 2016/797/UE e 2020/1828/UE (regolamento sull'intelligenza artificiale).

[2] L'obiettivo è ripreso anche dalla Commissione europea nel *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia* (COM(2020) 65), 19.02.2020.

[3] La definizione, infatti, è conforme a quella contenuta nell'art. 4, punto 14, GDPR: «dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici». La definizione contenuta nel GDPR è, dunque, più specifica rispetto a quella contenuta nell'AI ACT anche se, come si vedrà, l'identificazione del soggetto è necessaria anche nell'ambito di quest'ultimo sistema di norme. Ulteriori definizioni sono contenute nell' art. 3, n.13, Direttiva 2016/680/UE del Parlamento europeo e del Consiglio, 27.04.2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, la quale lì indica come «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 o i dati dattiloscopici»; ripresa pedissequamente nell'art. 5, n. 18 del Regolamento 2018/1725/UE del Parlamento europeo e del Consiglio, 23.10.2018 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE.

correlazione di *genus ad speciem* tra dati biometrici e dati personali[4] allorché si afferma che i primi sono una particolare tipologia di dati personali[5]. E la specificità sta nel processo di estrazione che deve essere un trattamento tecnico specifico, relativo alle caratteristiche di una persona. Non, dunque, la caratteristica in sé (che altrimenti sarebbe dato personale), ma quella caratteristica isolata e resa fruibile in un certo modo da uno specifico trattamento tecnico.

Essa, peraltro, non è una inutile puntualizzazione perché, l'individuazione di quale debba essere il trattamento che consente di accedere alla nozione di dato biometrico, e dunque all'applicazione di una disciplina molto scrupolosa e restrittiva[6], non è di poco conto ed è già stata oggetto di pronunce da parte di autorità di controllo.

L'esempio che viene subito alla mente è il noto caso di Clearview AI[7], la società statunitense la cui attività è stata sanzionata da diversi garanti degli Stati europei[8] per violazione del GDPR. Ma ciò che qui interessa è il funzionamento della tecnologia di Clearview AI che si basa sulla disponibilità di un (enorme) database di immagini di persone, creato dalla società attraverso lo *scraping* di immagini via web e relative informazioni[9]. Dalle immagini si ottengono rappresentazioni vettoriali del volto che riproducono le caratteristiche identificative delle persone[10], rappresentazioni poi indicizzate

[4] La necessità di coordinamento tra le due discipline è messa in risalto da D. IACOVELLI, M. FONTANA, *Nuove sfide della tecnologia e gestione dei rischi nella proposta di regolamento europeo sull'intelligenza artificiale: set di training, algoritmi e qualificazione dei dati. Profili critici*, in *Il diritto dell'economia*, 2022, III, 107-138; G. CERRINA FERONI, *Intelligenza artificiale e ruolo della protezione dei dati personali*, intervento a Key4biz 14.02.2023; G. CONTALDI, *Intelligenza artificiale e dati personali*, in *Ordine internazionale e diritti umani*, 2021, V, 1193-1213.

[5] Con ciò non si vuole comunque affermare che l'una sia generale e l'altra speciale poiché entrambe sono dirette a tutelare valori attinenti alla persona umana. Per queste riflessioni cfr., C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di Bio Diritto*, 2021, III, 415-437.

[6] La regolamentazione dei dati biometrici è oggi contenuta in numerosi atti normativi. Oltre al già citato GDPR, si segnalano la Direttiva 2016/680/UE sulla protezione dei dati per le autorità di polizia e di giustizia penale (Direttiva LED), il Regolamento 2018/1725/UE, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati e la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale del 1981 aggiornata nel 2018. Sono poi fornite differenti definizioni di dati biometrici da: Comitato Nazionale per la Bioetica (CNB), *L'identificazione del corpo umano: profili bioetici della biometria*, 2010, 3, consultabile al *link https://bioetica.governo.it/it/pareri/pareri-e-risposte/l-identificazione-del-corpo-umano-profilibioetici-della-biometria/*; Gruppo di lavoro WP193 — Articolo 29 per la tutela dei dati personali, parere 3, 27.04.2012, consultabile al link *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec6;* Garante per la protezione dei dati personali, la quale, *Linee guida in materia di riconoscimento biometrico e firma grafometrica,* 2014, consultabili al seguente *link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3132361*.

[7] Sul quale v., F. LALA, *Data collection via web scraping: privacy and facial recognition after Clearview*, in *i-lex Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale*, Vol. 16, II, 2023, 34 - 45.

[8] Il progetto è stato anche al centro di casi giurisprudenziali soprattutto statunitensi: cfr, Circuit Court of Cook County, Illinois, May 28, 2020, No. 9337839, citata da F. LALA, *Data collection via web scraping: privacy and facial recognition after Clearview*, cit., 40 ss., ove anche una rassegna delle decisioni dei Garanti europei.

[9] Sul funzionamento specifico cfr. P DAUVERGNE, *Identified, Tracked, and Profiled*, Cheltenham, 2022. 59 - 68.

[10] Su tali tecniche cfr., E. SACCHETTO, *Brevi riflessioni sui fondamenti e limiti del rapporto fra automated faced-based human recognition technology e procedimento penale*, in *Intelligenza artificiale e diritto: una rivoluzione?*, Vol. II, *Amministrazione, responsabilità, giurisdizione*, a cura di A. PAJNO, F. DONATI, A. PERRUCCI, Bologna, 2022, 541 ss., cui si rinvia per una sintetica ed efficace spiegazione del funzionamento del riconoscimento facciale tramite *software*; in argomento v. anche L. ALGERI, M. TORRE, *Aspetti definitori e delimitazione della materia*, in *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, a cura di G.M. BACCARIM, P. FELICIONI, Milano, 2023, 96 ss.

in modo da permetterne l'utilizzo come motore di ricerca: il matching è semplice, basta avere l'immagine della persona che si vuole cercare (trasformata anch'essa in un modello vettoriale) e compararla con i modelli indicizzati nel database. Per fare ciò Clearview adotta un algoritmo di machine learning per la creazione e comparazione dei modelli.

Il caso in oggetto che come noto costituisce uno dei primi casi presi in considerazione da Autorità Garanti, rappresenta proprio un indicatore per la definizione di dato biometrico poiché sicuramente le fotografie di persone fisiche non possono essere considerate *tout court* come dati biometrici ai sensi della definizione del GDPR (ripresa dall'AI ACT[11]), in quanto è necessario un «trattamento tecnico specifico». Nel caso di Clearview, quindi, le immagini di persone fisiche identificabili (e i metadati associati) contenute nel *database* "raschiato" dal web sono dati personali, ma non biometrici. Diventano dati biometrici quando ad essi viene applicato il trattamento vettoriale che permette di ottenere il modello delle immagini nel database e dell'immagine sonda da sottoporre a comparazione[12]. Solo all'esito di questo processo possiamo essere sicuri di essere in presenza di dati biometrici.

2. Segue: Identificazione univoca della persona.

Dal confronto tra la definizione adottata dal GDPR e quella dell'AI ACT emerge tuttavia un altro elemento necessario alla definizione e cioè la possibilità di identificazione univoca di una persona.

Tale conclusione è stata di recente ribadita dalla Corte di Cassazione che in un noto caso che vedeva coinvolto un Istituto universitario ha confermato la sanzione del Garante Privacy affermando il principio di diritto secondo cui «In tema di trattamento dei dati personali, ai sensi dell'art. 9 del GDPR, ricorre un trattamento di dati biometrici, come definiti dall'art. 4, n.14 dello stesso Regolamento, quando i dati personali sono ottenuti mediante un trattamento tecnico automatizzato specifico, realizzato con un software che, sulla base di riprese e analisi delle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, le elabora, evidenziando comportamenti o elementi anomali, e che perviene a un esito conclusivo, costituito da un elaborato video/foto che consente (o che conferma) l'identificazione univoca della persona fisica, restando irrilevante la circostanza che l'esito finale del trattamento sia successivamente sottoposto alla verifica finale di una persona fisica»[13].

---

[11] Non è questo l'unico punto di contatto tra le due normative, anzi nell'ambito dell'AI ACT è palesemente indicato che la sua applicazione non pregiudica quella del GDPR. Per queste riflessioni v., P. FALLETTA E A. MARSANO, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR*, in *Riv. It. Inf. dir.*, 2024, I, 1-19.

[12] Per queste riflessioni cfr., Garante per la protezione dei dati personali, *Verifica preliminare. Sistema di rilevazione delle immagini dotato di un software che permette il riconoscimento della persona (morfologia del volto)*, 15.03.2018, n. 155, ove si specifica che «nel caso del riconoscimento facciale, il presupposto perché il trattamento delle immagini possa essere qualificato come trattamento biometrico è che i confronti finalizzati al riconoscimento dell´individuo (verifica dell´identità, nel caso in esame) siano automatizzati mediante l´ausilio di appositi strumenti software o hardware (che non sussistono nel caso di specie».

[13] Cass. Civ., sez. I, 13.05.2024, n. 12967 che ha cassato con rinvio la decisione di Trib. Milano, 20.10.2022, n. 8174, con la quale il Tribunale aveva accolto il ricorso di un istituto universitario avverso un provvedimento

Dunque, per accedere alla nozione, e alla disciplina, del dato biometrico c'è anche da verificare la nozione di identificazione biometrica [14] ossia il riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati.

In realtà, già sotto il vigore del solo GDPR, il dato biometrico è sempre stato legato indissolubilmente alla individuazione univoca di una persona fisica e lo stesso AI ACT, richiamando l'art. 4, punto 14, del GDPR, mostra di non volersi discostare da tale nozione[15].

Del resto, oltre a tutta la dottrina unanime sul punto, anche se non sempre con una motivazione ben definita, già l'EDPB, nelle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video [16], al punto 76, evidenziava alcune componenti qualificanti nella definizione e nel trattamento dei dati biometrici, sulla base della definizione all'articolo 4 e per l'applicazione dell'art. 9 del GDPR. In particolare, altre alla «natura dei dati», che devono essere relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e ai «mezzi e modalità del trattamento» per cui i dati devono essere ottenuti da un trattamento tecnico specifico, si poneva l'accento sulla «finalità del trattamento», ossia l'identificazione univoca della persona.

Dunque, il dato biometrico che interessa ai nostri fini era già unanimemente considerato dalla dottrina e dal legislatore come quello che consente una correlazione tra dato biologico-fisico e identificazione univoca della persona[17],

---

del Garante privacy (n. 317 del 16 settembre 2021) che aveva individuato la violazione degli artt. 5, par. 1, lett. a), c) ed e), 6, 9, 13, 25, 35, 44 e 46, del Regolamento, nonché 2-*sexies* del Codice, per aver utilizzato un sistema di rilevamento del volto degli studenti durante esami a distanza al fine di controllarne la regolarità. Secondo il Garante il consenso espresso dagli studenti non poteva reputarsi una valida base giuridica del trattamento perché non avrebbe rappresentato una "manifestazione di volontà libera" (art. 4, par. 1, n. 11) del Regolamento), in ragione dello squilibrio della posizione degli studenti rispetto al titolare del trattamento (cfr. considerando n. 43 del Regolamento). Il Tribunale aveva confutato il ragionamento del Garante negando *in nuce* la classificazione del dato come biometrico, poiché nel caso di specie si sarebbe trattato di una semplice comparazione di immagini fotografiche, mentre affinché occorra la fattispecie di trattamento di dati biometrici sarebbe stato necessario che da una foto o da un video si ricavino caratteristiche biologiche per derivarne un modello matematico del volto del soggetto ritratto, a fini di riconoscimento. Ciò che mancava, a detta del Tribunale, nel caso concreto, era la finalità di identificazione. La Cassazione, invece, disattende tale conclusione poiché riconosce nel complesso sistema tendente ad individuare comportamenti anomali integra un autonomo e articolato trattamento dei dati biometrici acquisiti ed elaborati dallo stesso software, e attiene anche alla conferma dell'identità della persona fisica esaminata.

[14] Già nel 2014, l'allegato A del Provvedimento generale prescrittivo in tema di biometria, che definisce le Linee-guida in materia di riconoscimento biometrico e firma grafometrica, Allegato al Provvedimento del Garante per la Protezione dei dati personali, 12.11.2014, distingueva tra dato biometrico e identificazione, specificando che il procedimento di identificazione consiste nella «ricerca in un archivio, per confronto biometrico, di uno o più modelli biometrici corrispondenti al dato acquisito».

[15] L'esigenza di coordinamento è molto sentita dallo stesso legislatore dell'AI ACT che al considerando 7 avverte come la definizione debba essere interpretata conformemente a («*in light of* ») quella fornita dal GDPR e dalle direttive di settore.

[16] Comitato europeo per la protezione dei dati, Linee guida sul trattamento dei dati personali attraverso dispositivi video, versione 2.0, 29.01.2020, n. 3, disponibili al seguente link: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_it.pdf.

[17] In questo, già GDPR, art. 4, n. 14. Cfr., anche l'interpretazione della Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, che già nel 1981 all'art. 6 vietava il trattamento automatico dei dati a carattere personale che rivelano l'origine razziale, le opinioni politiche, le convinzioni religiose o altre convinzioni, nonché i dati a carattere personale relativi alla salute o alla vita sessuale.

ciò indipendentemente dal concetto di "identificazione biometrica" poi introdotto nel n. 35 del medesimo art. 3 dell'AI ACT e definito come "riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati". Infatti, le definizioni fornite nei riferimenti normativi fin'ora presi in considerazione contengono già *in nuce* il concetto di identificazione univoca[18].

Si deve però aggiungere che tale apparente perdita di centralità di questo concetto di identificazione nella definizione fornita dall'AI ACT, non deve essere inteso come irrilevanza di esso, anzi sembra rappresentare una rinnovata autonomia del requisito.

3. Identificazione, autenticazione e categorizzazione.

Sia chiaro comunque che identificazione non è autenticazione, ciò per espressa affermazione dello stesso considerando n. 15 che esclude dalle ipotesi di identificazione biometrica «i sistemi di IA destinati a essere utilizzati per la verifica biometrica, che include l'autenticazione, la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere e confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso di sicurezza a locali».

In questo senso, dunque, i sistemi che permettono di sbloccare gli smartphone con il volto o con le impronte digitali[19] non sono dati biometrici ai fini della normativa eurounitaria[20]. La distinzione non è nella modalità di rilevamento, ma nelle modalità di trattamento del dato e in particolar modo nel confronto di quel dato con un'entità di paragone laddove nel caso di autenticazione si opera un singolo confronto con un modello predefinito conservato nel dispositivo, nel caso invece di identificazione il confronto è più ampio e più invasivo e rischioso per la persona ed è relativo a banche dati esterne al sistema di riconoscimento.

[18] I problemi dell'identificazione biometrica sono soprattutto quelli legati alla possibilità di errore tanto che l'AI Act vieta l'identificazione biometrica remota «in tempo reale» che si verifica nei casi in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono contestualmente.

[19] La Corte europea dei diritti dell'uomo si è in vario modo occupata di tutelare i dati biometrici e, in particolar modo le impronte digitali (McVeigh, O'Neill and Evans v. the United Kingdom, 1981; Kinnunen v. Finland, 1993; S. and Marper v. the United Kingdom [GC], 2008; Dimitrov-Kazakov v. Bulgaria, 2011; M.K. v. France, 2013; Suprunenko v. Russia (dec), 2018; Gaughran v. the United Kingdom, 2020; P.N. v. Germany, 2020); Willems v. the Netherlands (dec.), 2021), o il timbro vocale (P.G. and J.H. v. the United Kingdom, 2001; Allan v. the United Kingdom, 2002; Doerga v. the Netherlands, 2004; Vetter v. France, 2005; Wisse v. France, 2005).

[20] In tal senso si era espresso anche il Garante per la Protezione dei dati personali italiano nel Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014. In un'altra interessante decisione (Garante per la protezione dei dati personali, *Installazione di apparati promozionali del tipo "*digital signage*" (definiti anche Totem) presso una stazione ferroviaria*, 21.12.2017) il Garante ha distinto tra "*face detection*", intesa come mero rilevamento del volto e "*face recognition*", ossia identificazione della persona, questa distinzione corrisponde a quella tra dati personali e dati biometrici.

Ovviamente anche nel caso di autenticazione si pongono problemi di tutela dei dati, poiché essi sono comunque come dati personali[21], ma non si reputa applicabile la disciplina più stringente prevista per i dati biometrici.

L'importanza centrale che assume nella definizione del dato biometrico lo scopo per cui si attua il trattamento diventa ancor più chiara con la nozione di "categorizzazione biometrica" di cui al 16 considerando e, all'art. 3, n. 40, come un sistema di IA che utilizza i dati biometrici di persone fisiche al fine di assegnarle a categorie specifiche[22]. In questa ipotesi, dunque, il medesimo rilevamento delle caratteristiche fisiologiche del soggetto è destinato alla creazione di categorie[23].

Appare chiaro, dunque, che la distinzione tra le definizioni riportare e fornite dall'AI ACT non risiede nella modalità di rilevamento dei dati, ma dalla finalità e dalle modalità del trattamento e, in particolar modo sembra che, stante la caratteristica di trattamento tecnologico delle fattezze dell'individuo, che serve a distinguere tale rilevamento dal semplice ritratto (sia esso anche fotografico), si possa discorrere di dato biometrico soltanto ove si sia in presenza di una identificazione della persona. Per vero, le sole norme analizzate non permettono immediatamente di raggiungere tale conclusione, potendosi immaginare tanto per l'autenticazione, quanto per la categorizzazione sistemi che sommano ad esse l'identificazione. Quest'ultima invece assume il ruolo di requisito dalla lettura congiunta, richiesta anche dall'AI ACT, delle norme del GDPR.

E, in questa prospettiva, l'AI ACT aggiunge una particolare attenzione alla finalità del trattamento la cui liceità non deriva più dal solo consenso dell'interessato, ma dal rispetto della normativa definita per quella particolare operazione. In altri termini, ciò che può essere lesivo della persona è la finalità del trattamento, cioè come viene trattato il dato e a quale scopo[24].

---

[21] Per queste riflessioni v., L. GRECO E A. MANTELERO, *Industria 4.0, robotica e* privacy-by-design*,* in *Dir. inf. e informatica*, 2018, VI, 875 - 900.

[22] Sul concetto di categorizzazione v., G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021, 35, il quale la definisce come un procedimento «consistente nell'estrarre le caratteristiche dall'immagine di una persona (conosciuta o meno) al fine di classificarla in una o più categorie in base agli attributi [come] età, sesso, abitudini di consumo». Significativo è l'esempio riportato delle consolle di gioco in grado, in alcuni casi, di categorizzare anche l'umore del giocatore.

[23] Sulle problematiche relative alla profilazione attraverso l'utilizzo di dati biometrici, v., P. PACILEO, *Profilazione e diritto di opposizione*, in Aa.Vv., *La nuova disciplina europea della privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, 179, che pone in risalto come gli strumenti di profilazione utilizzino sempre più le potenziali capacità individuali, relazionali, motivazionali ma anche individuando i gradi di soddisfazione personale, creando profili comportamentali dinamici di clienti per realizzare un'offerta mirata.

[24] In questo senso l'Autority canadese che si è occupata del caso Clearview ha utilizzato la locuzione "scopo inappropriato": Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta.

Forse questo è il passaggio ulteriore che, pur nel collegamento con il GDPR caratterizza l'AI ACT, neutrale dal punto di vista dei dati[25], ma interessato all'obiettivo per cui sono utilizzati[26].

In questo senso, il dato biometrico che può astrattamente essere utilizzato ai fini di identificazione e categorizzazione, rileva nella sua caratteristica di dato personale particolare, quando tale identificazione o categorizzazione permette l'identificazione della persona ed è utilizzata per finalità che possono reputarsi pericolose o lesive della dignità personale[27].

Tra gli scopi considerati pericolosi rientra (ed è dunque vietato) l'uso di sistemi di IA che creano o ampliano le banche dati di riconoscimento facciale mediante *scraping* non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso, che potrebbe creare un sistema di controllo di massa[28]. Tale divieto deriva dalla lettura congiunta di GDPR e AI ACT, che consente di desumere dalla interpretazione delle regole di entrambe le normative una disciplina molto restrittiva per tali dati biometrici con dei divieti specifici tra i quali, a norma dell'art. 5, anche la raccolta indiscriminata ("*untargeted scraping*") di immagini facciali allo scopo di creare o ampliare *database* di riconoscimento facciale[29].

---

[25] La scelta politica alla base della formulazione dell'AI ACT è stata quella di emanare un regolamento generale ed orizzontale, diretto a disciplinare il fenomeno dell'intelligenza artificiale senza tuttavia entrare troppo in tecnicismi che avrebbero condotto ad una rapida obsolescenza delle norme. In aggiunta, l'obiettivo degli organi dell'Unione era anche quello di rendere il modello europeo un riferimento globale atto ad essere implementato in tutto il resto del mondo, definendo regole applicabili con facilità in altri sistemi. Per queste riflessioni v., P. FALLETTA E A. MARSANO, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR* , cit., 3.

[26] In questo senso, un ulteriore punto di contatto tra le due norme è l'approccio basato sul rischio che impone un comportamento di compliance al privato. Sul punto v., F. PIZZETTI, *GDPR e Intelligenza Artificiale. Codici di condotta, certificazioni, sigilli, marchi e altri poteri di soft law previsti dalle leggi nazionali di adeguamento: strumenti essenziali per favorire una applicazione proattiva del Regolamento europeo nell'epoca della IA*, in AA.VV., *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna, Studi in tema di Internet Ecosystem*, a cura di A. MANTELERO, D. POLETTI, Pisa, 2018, 69 - 97. E trova anche A.C. NAZZARO, *L'utilizzo dei Big data e i problemi di tutela della persona*, in *Rass. dir. civ.*, 2018, IV, 1239-1260.

[27] Tra le possibilità di lesione si ritrova anche la decontestualizzazione degli individui, nel senso che il soggetto potrebbe essere preso in considerazione soltanto per alcuni degli aspetti rilevati e non per la sua totale personalità. Per queste considerazioni v., G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 23 ss., che afferma come ciò può risolversi in una rappresentazione parziale e fuorviante della persona. Si aggiunga che il sistema del riconoscimento biometrico rende più netta la distinzione tra identificazione e identità poiché le fattezze biometriche sono normalmente decontestualizzate. Per queste riflessioni v., Gruppo di lavoro articolo 29, *Parere sugli sviluppi nelle tecnologie biometriche*, 27.04.2012, n. 3, 6, disponibile al link: https://www.garanteprivacy.it/documents/10160/2150354/wp193.pdf, che chiarisce come la prima consiste nel confronto dei dati biometrici della persona con una serie di modelli biometrici conservati in una banca dati mentre la seconda consiste nel confronto con un unico modello biometrico conservato in un dispositivo; Il tema era stato già affrontato dal Comitato Nazionale per la Bioetica, *L'identificazione del corpo umano: profili bioetici della biometria*, 26.11.2010, 14 ss., che addirittura discorre del corpo umano come password, chiarendo con ciò la limitata utilizzazione degli strumenti di autenticazione biometrica.

[28] Tale controllo è verosimile soprattutto a fronte di sistemi politici meno improntati ai valori espressi nella nostra Carta costituzionale come, ad esempio, quello cinese dove esiste un "*Social Credit System*" attraverso il quale ogni cittadino riceve in modo automatizzato un punteggio di affidabilità. La circostanza è denunciata da G. MOBILIO, Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative, cit., 11 ss. e 208 ss., il quale mette anche in evidenza la particolare pericolosità per la libertà dell'individuo delle tecnologie di riconoscimento facciale.

[29] Il percorso seguito dall'AI ACT non è stato tuttavia lineare. Infatti, soprattutto con riferimento ad alcune utilizzazioni delle tecniche di riconoscimento facciale, in particolare con riferimento al riconoscimento delle emozioni facciali, si è passato da un divieto assoluto ad una soluzione più mite. Per tali riflessioni v., M.

Si tratta della nota tematica del divieto di *webscraping*[30] e la necessità di spiegarne la ratio ove il legislatore pur ammettendo l'uso, anche se a certe condizioni di dati biometrici, vieta il *webscraping* di essi.

Per risolvere la questione sembra necessario puntare l'attenzione proprio sulle finalità del trattamento poiché il problema è che quando si raschiano dati personali dal web [31], la liceità del loro utilizzo può dipendere, e anzi necessariamente deve dipendere, dalla finalità della raccolta. La norma non vieta *tout court* lo *scraping*, ma la creazione o l'ampliamento tramite esso di banche dati di riconoscimento facciale.

Tale previsione è assolutamente in linea con il GDPR poiché l'art. 6, considera le basi giuridiche sempre in ragione del particolare contesto e della specifica finalità del trattamento. Così altro è il *webscraping* finalizzato ad addestrare l'AI[32], altro è quello utilizzato per ragioni di pubblica sicurezza, altro è quello utilizzato per ragioni commerciali e così via.

Di ciò è ben conscio il nostro Garante privacy, quando nelle linee guida del maggio 2024[33] «propone una diversa prospettiva, esaminando la posizione dei soggetti, pubblici e privati, gestori di siti *web* e piattaforme *online,* operanti quali titolari del trattamento di dati personali, che rendano pubblicamente disponibili, dati (anche personali) che vengono raccolti dai *bot* di terze parti». Tutto ciò nella consapevolezza che il funzionamento stesso del sistema di internet è basato su *web crawler,* cioè programmi che scandagliano sistematicamente il web al fine di raccogliere i dati contenuti nelle pagine web ed indicizzarli per garantire il funzionamento dei motori di ricerca.

Del resto, anche il comportamento illecito imputato nel noto caso Clearview AI non era tanto il *webscraping*, quanto l'utilizzo che si faceva dei dati rastrellati dalla rete[34].

Sembra a questo punto necessario rispondere ad una possibile obiezione e cioè che in fondo si tratterebbe di dati pubblici. L'obiezione sembra facilmente superabile oltre che per le ragioni oramai comunemente accolte dalla dottrina[35] anche perché il problema è la finalità dell'utilizzo di dati sensibili e il

---

MATTIOLI AND F. CABITZA, *Not in My Face: Challenges and Ethical Considerations in Automatic Face Emotion Recognition Technology*, in *Mach. Learn. Knowl. Extr.* 2024, VI, 2221.

[30] Per una definizione v., B. ZHAO, *Web Scraping*, in AA.VV., *Encyclopedia of big data*, a cura di L.A. SCHINTLER, C.L. MCNEELY, Cham, 2022, 951 - 953: «*Web scraping, also known as web extraction or harvesting, is a technique to extract data from the World Wide Web (WWW) and save it to a file system or database for later retrieval or analysis. Commonly, web data is scraped utilizing Hypertext Transfer Protocol (HTTP) or through a web browser. This is accomplished either manually by a user or automatically by a bot or web crawler*».

[31] Ciò deriva dal fatto che tutti i sistemi di AI riescono a funzionare soltanto se hanno a disposizione una enorme quantità di dati. G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale*, in *Riv. trim. dir. pubbl.*, 2022, IV, 1085 - 1099; C. COLAPIETRO, A. MORETTI, *L'Intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali*, in *BioLaw Journal – Rivista di BioDiritto*, 2020, III, 359 - 387. Il fenomeno, già prima dell'avvento dei sistemi di AI aveva impegnato gli studiosi di Big Data. Cfr. A.C. NAZZARO, L'utilizzo dei Big data, cit.

[32] Su quest'ultimo si evidenziano problemi legati alla titolarità dei dati utilizzati. Cfr., A.M. PARK , *Unfair Collection: Reclaiming Control of Publicly Available Personal Information from Data Scrapers Personal Information from Data Scrapers*, in *Michigan Law Review*, Vol. 120, V, 2022, 914 ss..; G. XIAO, *Bad Bots: Regulating the Scraping of Public Personal Information*, in *Harv. J.L. & Tech.,* Vol. 34, II, 2021, 702.

[33] Garante per la protezione dei dati personali, *Web scraping ed intelligenza artificiale generativa: nota informativa e possibili azioni di contrasto*, maggio 2024.

[34] La doppia valenza, in negativo e in positivo, degli strumenti di *webscraping* è evidenziata da F. LALA, *Data collection via web scraping: privacy and facial recognition after Clearview*, cit., 35.

[35] Oramai è generalmente accolta l'opinione che considera tutelati anche i dati pubblici nel rispetto della c.d. vita sociale privata. Cfr., L*ópez Ribalda and Others v. Spain* [GC], nos. 1874/13 and 8567/13, §§ 87-88, 17

Garante, proprio in questo documento di raccomandazione, non suggerisce ai gestori accorgimenti funzionali di evitare tout court il *webscraping* (che sarebbe un obiettivo irrealizzabile), ma individua possibili azioni di contrasto per fare in modo che tale *webscraping* sia utilizzato per finalità di addestramento della IA generativa in modo lecito.

4. Dal rilevamento biometrico al rilevamento delle emozioni.

Tra i divieti di utilizzo di dati biometrici giustificati non dal dato in sé ma dalla finalità del trattamento rientrano anche l'uso di sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale, perché potrebbero essere fonte di discriminazioni basate su tali caratteristiche; l'uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione perché potrebbe essere considerato lesivo della libertà personale[36].

L'ipotesi da ultimo riportata apre la strada ad ipotesi ulteriori di rilevamento di caratteristiche fisiologiche, non strettamente fisiche che sono caratterizzate da una invasività maggiore sul corpo e sulla psiche dell'individuo. Tali casi sono stati già oggetto di valutazione da parte di autorità di controllo. Ad esempio l'Autorità nazionale per la protezione dei dati e la libertà d'informazione ungherese [37] ha censurato il comportamento di un istituto finanziario che analizzava le telefonate registrate dal servizio clienti e, tramite un sistema di *machine learning,* individuava lo "stato emozionale" della conversazione sulla base della voce, delle pause e del numero delle persone intervenute, con lo scopo di selezionare i clienti particolarmente insoddisfatti, da richiamare, per prevenire future lamentele e migliorare in generale i processi interni di gestione.

Anche in questa ipotesi, se oggi il problema può essere quello di definire i dati trattati in termini di dati biometrici o meno, all'esito dell'AI ACT, all'epoca dei fatti era quello di tutelare i soggetti coinvolti, utilizzando le norme in quel momento a disposizione, e l'Autority ungherese, utilizzando il GDPR e pur non qualificando i dati in questione come biometrici, perché non consentivano l'identificazione univoca della persona, ha considerato illegittimo il trattamento effettuato perché l'impresa non aveva provveduto ad informare adeguatamente gli interessati sui trattamenti effettuati, secondo un principio di trasparenza analogo a quello su cui è basata la disciplina dei «sistemi di riconoscimento delle emozioni» nel regolamento AI ACT[38].

October 2019; *Nikolay Sergeyevich Glukhin v. Russian Federation*, App no. 11519/20 (ECtHR, 4 July 2023), commentata da M. ZALNIERIUTE, *Glukhin v. Russia. App. No. 11519/20. Judgment*, in *American Journal of International Law*, Vol. 117, IV, 2023, 695 - 701.

[36] In quest'ultima ipotesi si tratta di un sistema di IA «finalizzato all'identificazione o alla deduzione di emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici».

[37] Nemzeti Adatvédelmi és Információszabadság Hatóság, 8.02.2022, n. 85-3/2022, in https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei.

[38] Tali tecniche rientrano, a norma dell'art. 5, tra le pratiche vietate ove siano utilizzate nell'ambito del luogo di lavoro e degli istituti di istruzione, tranne laddove l'uso del sistema di IA sia destinato a essere messo in

La pericolosità di questi sistemi di rilevamento delle emozioni per i diritti e le libertà delle persone può essere amplificata da utilizzazioni tese ad implementare strumenti predittivi e ciò anche muovendo da utilizzi che invece appaiono non soltanto leciti, ma anche auspicabili.

Le utilizzazioni più frequenti, sono proprio quelle ammesse dall'AI ACT che godono dell'eccezione dal divieto perché utilizzate per pubblica sicurezza e, in particolar modo, le tecniche dirette a garantire la sicurezza transfrontaliera. Tale tema è fortemente avvertito dal legislatore eurounitario tanto che si sono succeduti anche Regolamenti destinati a disciplinare l'utilizzo di dati biometrici alle frontiere [39]. In particolare, il Regolamento 2226/2017/UE istituisce un "sistema di ingresso/uscita" (EES), che registra e memorizza la data, l'ora, il luogo di ingresso e di uscita, nonché i dati biometrici dei cittadini di paesi terzi, con l'obiettivo di "Aumentare la sicurezza delle frontiere utilizzando tecnologie moderne, come l'intelligenza artificiale e le tecniche biometriche. Le norme contenute in tale regolamento sono di stringente applicazione tanto che dal necessario coordinamento con quanto previsto dalla Direttiva 2016/680/UE[40], che all'art. 10 richiede un consenso rafforzato per l'utilizzazione di dati biometrici anche da parte delle forze dell'ordine, deriva che il loro trattamento è «autorizzato solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e soltanto: *a*) se autorizzato dal diritto dell'Unione o dello Stato membro; *b*) per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; *c*) se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato».

In questa specifica applicazione, appare significativa una decisione della High Court of Justice gallese che nel 2019[41] ha affrontato il caso della legittimità dell'utilizzo da parte delle forze dell'ordine di un sistema di *Artificial face recognition* denominata AFR Locate [42]. La Corte, dopo aver riconosciuto

funzione o immesso sul mercato per motivi medici o di sicurezza e sono sottoposte, a norma dell'art. 50, a particolari obblighi di trasparenza. Ove ammesse, tali pratiche, sono comunque catalogate "ad alto rischio".

[39] Ad esempio il Regolamento 2022/991/UE, che modifica il Regolamento 2016/794/UE, si occupa di stabilire un'eccezione alle restrizioni riguardanti il trattamento automatizzato di dati biometrici intesi a identificare in modo univoco una persona, per consentire ad EUROPOL di prevenire e combattere la criminalità organizzata. Per questi dati v., V. VASTA, *Diritto dell'unione europea e intelligenza artificiale. Riflessi sul procedimento penale*, in *Riv. It. Dir. Proc. Pen.*, Vol. 67, I, 2024, 271 - 285.

[40] Relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

[41] Sentenza 4 settembre 2019, [2019] EWHC 2341, R (Bridges) c. CCSWP and SSHD.

[42] Il caso nasce da un progetto pilota che la polizia del Galles meridionale stava testando per l'intero Regno Unito, consistente nella raccolta di immagini digitali di volti ripresi in tempo reale in un contesto dinamico, confrontate con un database di soggetti sospettati o accusati di reati, in possesso delle forze dell'ordine. Nel caso in cui fosse avvenuto il *matching* e un operatore umano avesse confermato la correttezza della valutazione del software, le forze di polizia si sarebbero attivate per identificare il soggetto e procedere con la cattura o con la semplice segnalazione all'*intelligence.* Dato il numero di soggetti registrati e la sua ampia percentuale in considerazione della popolazione del Galles, la Corte si interroga sulla possibilità che il progetto integri gli estremi di un controllo di massa. Nonostante l'impiego dello strumento avvenisse in modalità esplicita, cioè avvertendo pubblicamente gli avventori della sua presenza, la Corte evidenzia che il trattamento dei dati personali non è assimilabile semplicemente ad un apparecchio fotografico installato in una pubblica piazza poiché viene analizzata l'informazione digitale che contiene l'immagine ne vengono estratti i dati facciali biometrici. Tale processo, a detta della Corte, sarebbe assibilabile ad una raccolta di impronte digitali o di DNA. Nonostante ciò, la Corte non reputa censurabile l'utilizzo dello strumento poiché rispetta sia l'art. 8 CEDU, sia le norme del GDPR. Per accurate riflessioni sulla sentenza v., A. PIN, *Non esiste la "pallottola d'argento": l'Artificial Face Recognition al vaglio giudiziario per la prima volta*, in *DPCE on line*,

l'importanza di accordare l'uso di tali strumenti nel campo della tutela di interessi pubblici, afferma anche il necessario bilanciamento con la protezione dei diritti individuali [43], soprattutto per gli aspetti che gli stessi giudici definiscono "inquietanti" per la capacità di trattare enormi quantità di dati. Tuttavia, reputa legittimo l'uso dello strumento poiché risulterebbero correttamente utilizzati gli strumenti previsti dal GDPR per tutelare la privacy dei soggetti coinvolti[44].

Tuttavia, le tecniche atte a creare c.d. confini "intelligenti" potrebbero comprendere non solo l'uso di tecnologie biometriche a fini di identificazione, ma anche sistemi di rilevamento delle emozioni per individuare soggetti che potenzialmente siano non completamente sinceri riguardo a quanto dichiarato alla frontiera.

È proprio ciò che è accaduto nei casi di rilevamento delle emozioni alle frontiere. Si tratta di una evoluzione della tecnologia che ha prodotto anche strumenti di *Automatic Face Emotion Recognition* (FER), che sono dunque in grado di rilevare le emozioni, quantomeno quelle che modificano i dati biometrici[45].

Questi strumenti automatizzati di rilevamento degli inganni analizzano i dati biometrici di seconda generazione associati a stress, ansia e menzogna per supportare gli agenti di controllo delle frontiere. Sebbene non siano attualmente in funzione sistemi di rilevamento delle emozioni alle frontiere dell'UE, esiste un progetto, "*Intelligent Portable Control System*" (iBorderCtrl), che mira allo sviluppo di strumenti di rilevamento degli inganni e di strumenti di valutazione che, analizzando microespressioni, come ammiccamenti, aumento dell'arrossamento del viso o direzioni dei movimenti della testa, calcolano il rischio associato a ciascun soggetto. I sistemi iBorderCtrl mirano a identificare le persone che hanno mentito sulla loro identità, bagaglio, destinazione o altri piani di viaggio e classificano persone in viaggiatori "in buona fede" e "non in buona fede". Se una persona rientra in quest'ultima categoria, un funzionario di frontiera umano conduce un colloquio e ulteriori indagini[46].

2019, V, 3075- 3082. Per una rassegna della legislazione sul tema in Galles cfr., J. PURSHOUSE, L. CAMPBELL, *Automated facial recognition and policing: a Bridge too far?*, in *Legal Studies*, *Vol. 42, II,* 2022, 209 - 227.

[43] In questo senso non sembra sia accoglibile l'affermazione di chi reputa sicuramente giustificato l'uso di questi sistemi da parte delle forze dell'ordine e da verificare invece soltanto quando tale uso sia relativo a scopi commerciali. Cfr. B. MCNERNEY, Keep Your Fingerprints to Yourself: New York Needs a Biometric Privacy Law, in *St. John's Law Review*, 2022, Vol. 96, IV, 1039 - 1070.

[44] Un altro caso ha impegnato la Corte europea dei diritti umani (*Nikolay Sergeyevich Glukhin v. Russian Federation*, App no. 11519/20 (ECtHR, 4 July 2023) a seguito della contestazione di un cittadino russo che lamentava di essere stato sottoposto ad una tecnologia di riconoscimento facciale senza averne avuto notizia preventiva. In particolare, il ricorrente lamentava la violazione dell'art. 8 della Convenzione. Questo è stato il primo caso in cui la Corte ha affrontato i problemi legati all'uso di tale tecnologia ed ha espresso forti dubbi sul fatto che le disposizioni di legge nazionali che autorizzavano il trattamento dei dati personali biometrici, anche con l'ausilio della tecnologia di riconoscimento facciale, "in relazione all'amministrazione della giustizia" soddisfacessero il requisito della "qualità del diritto", poiché erano formulate in modo sommario e sembravano consentire il trattamento di tali dati in relazione a qualsiasi tipo di procedimento giudiziario. Il diritto nazionale, in altri termini, non conteneva limitazioni sulla natura delle situazioni che potevano dar luogo all'uso della tecnologia di riconoscimento facciale, sulle finalità previste, sulle categorie di persone che potevano essere oggetto di trattamento o sul trattamento di dati personali sensibili.

[45] Su questa tematica cfr., M. MATTIOLI AND F. CABITZA, *Not in My Face: Challenges and Ethical Considerations in Automatic Face Emotion Recognition Technology*, in *Mach. Learn. Knowl. Extr.* 2024, VI, 2201 - 2231.

[46] Il Progetto nasce dal finanziamento di un Programma Horizon ed è stato oggetto di decisioni del tribunale UE e della Corte di Giustizia dell'UE, 7 settembre 2023, C-135/22P, poiché un cittadino tedesco aveva chiesto

È palese che l'uso di questi sistemi di rilevamento biometrico dell'inganno è altamente rischioso poiché essi scontano una diversa caratterizzazione culturale delle modalità di esprimere, attraverso il volto, le proprie emozioni. Inoltre, essi non si fondano su solide basi scientifiche, ma piuttosto su una catena di ipotesi sulla relazione tra indicatori biometrici e intenzioni interne[47]. Uno dei problemi fondamentali di questi sistemi è che le emozioni sono fenomeni umani complessi che non possono essere chiaramente assegnati a un insieme di indicatori non verbali e verbali[48].

Ovviamente, anche tra i non giuristi, non mancano le obiezioni di chi reputa queste tecniche pericolose per le persone fisiche[49], soprattutto se si prende in considerazione la possibilità di errore[50] causato anche dalla presenza di *bias*[51].

5. Dati biometrici e personalità dell'individuo.

I problemi da valutare in ambito giuridico, tuttavia non sono solo quelli legati alla possibilità di errore dell'algoritmo.

---

il pieno accesso agli atti, negato dal Tribunale ed accolto parzialmente dalla Corte di giustizia (per la cui sentenza cfr., https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A62022CJ0135). La questione è efficacemente illustrata da F. De Simone, *Una nuova tipologia di misure di prevenzione: algoritmi, intelligenza artificiale e riconoscimento facciale*, in archiviopenale.it.

[47] Sul punto cfr., P. Grother, M. Ngan, K. Hanaoka, *Face Recognition Vendor Test (FVRT). Part 3: Demographic Effects*, U.S. Department of Commerce, National Institute of Standards and Technology, 2019, disponibile sul sito web *www.nvlpubs.nist.gov* che riporta uno studio molto significativo condotto dal *National Institute of Standards and Technology* degli Stati Uniti, secondo il quale l'utilizzo di molti *software* di riconoscimento facciale è affetto da numerosi errori relativamente alle donne afroamericane e asiatiche; J. Della Torre, *Quale spazio per i* tools *di riconoscimento facciale nella giustizia penale?*, in Aa.Vv., *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, a cura di G. Di Paolo, L. Pressacco, Napoli, 2022, 20 ss.. L'a. evidenzia come in questi casi non si tratti necessariamente di *bias*, ma del modo in cui sono costruiti gli algoritmi che sconta necessariamente difetti di selezione dei volti in fase di addestramento trasmettendo dunque alla macchina pregiudizi umani.

[48] Sul punto sono soprattutto le indagini di altre scienze a venire in soccorso. Cfr., M. Gendron, D. Roberson, J.M. van der Vyver; L.F Barrett, *Perceptions of emotion from facial expressions are not culturally universal: Evidence from a remote culture*, in *Emotion*, 2014, Vol. 14, II, 251 - 262.; J. Vincent, *Emotion Recognition Can't be Trusted*, in www.theverge.com, 2019; D. Matsumoto, *Cultural influences on the perception of emotion.*, in *J. Cross-Cult. Psychol.*, 1989, Vol. 20, I, 92 - 105.

[49] A. Katirai, *Ethical considerations in emotion recognition technologies: A review of the literature*, in *AI and Ethics*, 2024, Vol. 4, 927 - 948; K. Crawford, *Time to regulate AI that interprets human emotions*, in *Nature*, 2021, 592, 167 ss.

[50] La probabilità di errore è massima nelle ipotesi di *real time*, non a caso vietato dall'AI ACT, perché è stato provato che in queste ipotesi l'accuratezza dei tools può variare in modo significativo in base ad un'ampia gamma di fattori, come la qualità della fotocamera utilizzata, la luce, la distanza, la qualità dei dati immessi nel database (o dei dati ricavati dal flusso di video), o ancora l'etnia, l'età o il sesso del soggetto. Si deve tuttavia avvertire che il concetto di accuratezza utilizzato nel GDPR è differente dal medesimo concetto preso in considerazione nell'AI ACT laddove la prima normativa si riferisce all'accuratezza nella gestione dei dati, la seconda si occupa invece dell'accuratezza del risultato ottenuto dai dati processati. Per queste considerazioni v., C. Novelli, F. Casolari, P. Hacker, G. Spedicato, L. Floridi, *Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity*, in *Computer Law & Security Review*, 2024, Vol. 55, 1-16.

[51] A. McStay, *Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy*, in *Big Data Soc.*, 2020, 7; T. Xu; J. White, S. Kalkan, H. Gunes, *Investigating bias and fairness in facial expression recognition*, in *Proceedings of the Computer Vision–ECCV 2020Workshops*, Glasgow, UK, 23-28 August 2020, Berlin/Heidelberg, 2020; 506 - 523; E. Kim, D. Bryant, D. Srikanth, A. Howard, *Age bias in emotion detection: An analysis of facial emotion recognition performance on young, middle-aged, and older adults*, in *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, Virtually, 19-21 May 2021, USA, 2021, 638 - 644; J. Buolamwini, T. Gebru, *Gender shades: Intersectional accuracy disparities in commercial gender classification*, in Proceedings of the *Conference on Fairness, Accountability and Transparency*, 23-24 February 2018, New York, 2018, 77 - 91.

Non si può dimenticare che i dati biometrici rappresentano una specificazione dei dati personali e sono dati sensibili ai sensi dell'art.9 del GDPR poiché rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, o ancora la salute o la vita sessuale o l'orientamento sessuale della persona[52]. Il loro trattamento è in principio vietato, tranne nel caso in cui si verifichi una delle condizioni previste dal secondo comma, tra cui rientra anche il consenso esplicito dell'interessato per una o più finalità specifiche (lett. a)[53], oppure nel caso in cui il trattamento risulti necessario per finalità stabilite dalla stessa norma[54].

Un caso specifico ha fatto molto scalpore proprio in Argentina dove, nell'agosto del 2023, l'Agenzia per l'accesso alla pubblica informazione (AAIP)[55] ha avviato un'indagine sulla liceità del trattamento dei dati personali da parte di una società di gestione di criptovalute, la Fondazione Worldcoin, la quale chiedeva ai clienti, dietro compenso in criptovaluta, di sottoporsi ad una procedura di scansione dei volti e delle iridi. Il problema riscontrato era la mancanza di una finalità dichiarata del trattamento[56]. La decisione dell'Autorità argentina di bloccare l'operazione commerciale si è fondata proprio sull'identificazione tra dato biometrico e dato sensibile[57].

Il progetto è, in realtà più ambizioso e avrebbe lo scopo di creare, proprio tramite la scansione dell'iride, che a detta degli studiosi sarebbe il dato biometrico più attendibile, una identità digitale per essere distinti con assoluta certezza da una AI.

Il problema è che le tecniche di rilevamento facciale collegate all'identità digitale, devono essere valutate nella consapevolezza del loro stretto rapporto con l'identità personale dell'individuo. In questo senso, nel progetto da ultimo riportato, la scansione del volto avrebbe reso possibile individuare la personalità di un individuo distinguendolo da una macchina, in quanto tale, senza personalità. Numerosi studiosi guardano con sospetto a queste tecniche

---

[52] Cfr. art. 9 co. 1. Infatti, i dati biometrici sono per gran parte strettamente identificativi della persona e contengono una impronta indelebile della persona. Per queste affermazioni cfr., S .EL SABI, *La tutela della* privacy *nel trattamento dei dati biometrici e genetici per scopi di pubblica sicurezza. Spunti di diritto comparato*, in *Dir. inf. e informatica*, 2023, V, 789 - 827. Lo stretto rapporto tra dati biometrici e personalità dell'individuo è rimarcata anche dal Gruppo di lavoro articolo 29, Parere sugli sviluppi nelle tecnologie biometriche, cit.

[53] In questo senso si è espressa Cass., Sez. Lav., 19.05.2023, n. 13873, in *Dir. § giust.*, che ha accolto la domanda di un lavoratore che chiedeva di dichiarare illegittimo un sistema di rilevazione biometrica, tramite impronta della mano, dell'accesso dei lavoratori da parte del datore di lavoro, perché il consenso prestato non era specifico. Tale consenso non esclude comunque limitazioni generali rispetto all'utilizzo di tali dati, tanto che il loro utilizzo quale corrispettivo di un servizio sarebbe da ritenersi in ogni caso sproporzionato. Così, G. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Dir. inf. e informatica*, 2020, III, 634 - 674.

[54] In particolare, il pericolo è di lesione di diritti personalissimi a causa di un potere incontrollabile che potrebbe derivare dalla tecnica dell'IA di processare questi dati personali. Cfr. L. STARK, J. HOEY, *The ethics of emotion in Artificial Intelligence systems*, in Proceedings of the 2021 ACM *Conference on Fairness, Accountability, and Transparency*, FAccT '21, 3 - 10 March 2021, New York, 782 - 793; Stark, L. The emotional context of information privacy. Inf. Soc. 2016, 32, 14–27; A. MCSTAY, *Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy*, cit., 7.

[55] Si tratta dell'equivalente dei Garanti privacy europei ed è l'Autorità esecutiva della legge 25.326 sulla protezione dei dati personali.

[56] Peraltro, è attualmente in discussione un progetto di legge per riformare profondamente la normativa in tema di dati personali che propone una specificazione maggiore anche delle finalità del trattamento.

[57] Il medesimo progetto è stato bloccato anche dalla Provincia di Buenos Aires che, tramite il Ministero della produzione, Scienza e Innovazione tecnologica, ha imposto una sanzione di 194 milioni di Pesos alla Worldcoin Foundation, perché non aveva previsto limiti di età alla partecipazione al progetto.

muovendo dall'assunto che il trattamento di dati biometrici può rivelarsi fortemente pericoloso, perché il volto sarebbe la finestra dell'anima [58] e, dunque, la sua scansione potrebbe permettere un controllo della personalità. Non sembra tuttavia che tale teoria colga nel segno, infatti il problema è sicuramente più pratico e la pericolosità dei dati ritraibili dalla scansione del volto e dalla sua fedele riproduzione potrebbe essere utilizzata per attribuire comportamenti non veri ai soggetti [59]. In questo senso gli strumenti di riconoscimento facciale permettono di violare il diritto ad una corretta e non infedele rappresentazione della propria identità che trova fondamento nell'art. 2 Cost. [60]. Un ulteriore pericolo è poi legato alla profilazione laddove la trasformazione delle sembianze umane in flussi di dati poi ricomposti e riconfigurati per confluire nel profilo assegnato, creano un sistema di forte spersonalizzazione e, nuovamente di assoluta mancanza di rispetto della complessa e complessiva personalità dell'individuo. Quest'ultimo, infatti, non può essere visto esclusivamente e isolatamente nella sua veste di consumatore, o utilizzatore di certe merci, o cliente finanziario con determinate caratteristiche, ma deve essere riguardato nel suo essere persona con specifici bisogni[61], poiché proprio nella necessità di distinguere tra identità e identificazione non sembra possibile accogliere l'opinione di quanti confondono l'identità digitale con gli strumenti di identificazione tecnologici o con le immagini, a volte usurpate, in ambito digitale[62], ma sembra necessario approdare ad una visione unitaria di identità personale che coinvolge anche comportamenti in ambito digitale.

6. Qualità del dato, pericolo di *bias* e valutazione d'impatto.

Da quanto riportato una linea comune definibile è la tematica della qualità del dato[63].

A ciò, tuttavia, sembra necessario aggiungere una riflessione sul problema delle correlazioni (a volte insospettabili) che l'algoritmo potrebbe individuare

---

[58] S. PORTER et al., *Is the Face a Window to the Soul? Investigation of the Accuracy of Intuitive Judgments of the Trustworthiness of Human Faces, in Canadian Journal of Behavioural Science*, 40, III, 2008, 171 ss.

[59] Il riferimento è alla nota tematica dei deepfake sulla quale v. M. CAZZANIGA, Una nuova tecnica (anche) per veicolare disinformazione: le risposte europee ai *deepfakes*, in *Medialaws*, 2023, 170 - 187; Garante per la protezione dei dati personali, Deepfake*: Il falso che ti «ruba» la faccia (e la* privacy), scheda informativa sui rischi della manipolazione digitale di volti e voci, in www.garanteprivacy.it, 2020; A. SANTANGELO, *Il futuro del volto nell'era dei deep fake*, in AA.VV. *Il metavolto*, a cura di M. LEONE, FACETS Digital Press, 2022, 19 ss.; D. HARRIS, *Deepfakes: False Pornography Is Here and the Law Cannot Protect You*, in *Duke Law & Technology Review*, 17, 2019, 99 ss.; V. AZZALI, N. ELLECOSTA, *La questione* deepfake *in Italia: una panoramica*, in *Medialaw*, 2023, 72 - 90.

[60] Così, non da ora, Cass., sez. I, 22.06.1985, n. 3769.

[61] P. PERLINGIERI, La personalità umana nell'ordinamento giuridico, Napoli, 1972.

[62] Discorre di possibile traslazione tra dato e persona, nelle ipotesi di utilizzo di dati biometrici S. EL SABI, *La tutela della privacy nel trattamento dei dati biometrici e genetici per scopi di pubblica sicurezza. Spunti di diritto comparato*, cit., 789 - 827.

[63] Su questo tema sembra molto opportuna la precisazione della Legge argentina n. 25.326, dove si prevede uno specifico articolo (il n. 4) sulla qualità del dato. Il tema è affrontato da numerosa dottrina. Cfr., E. PELLECCHIA, *Profilazione e decisioni automatizzate al tempo della* black box society*: qualità dei dati e leggibilità dell'algoritmo nella cornice della* responsible research and innovation, in *Nuove leggi civ. comm.*, 2018, V, 1209-1236; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, 2016, 254 ss.; G. FINOCCHIARO, Intelligenza Artificiale e protezione dei dati personali, in Giur. it., 2019, VII, 1670 - 1677.

ed implementare. Per dirlo in una parola è il pericolo di *bias*[64]. Per cui se, ad esempio, un database di volti è collegato a statistiche che individuano in una certa etnia una maggiore possibilità di commettere crimini, allora la discriminazione è quasi inevitabile.

La soluzione, come oramai da un po' ci ha abituato il legislatore europeo, è l'*accountability*, ossia la responsabilizzazione dell'operatore professionista[65] che sarà quindi anche chiamato ad una valutazione di impatto per i sistemi ad alto rischio.

Tanto è previsto nell'AI Act che specifica che tale procedimento deve valutare l'impatto di quei comportamenti sui diritti fondamentali [66] specificando anche gli elementi di tale valutazione, tra cui anche le categorie di persone fisiche e gruppi verosimilmente interessati, i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati e le misure da adottare qualora tali rischi si concretizzino.

Sembra, tuttavia, che tale Valutazione di impatto sia diversa da quella prevista dall'art. 35 del GDPR che è invece relativa all'impatto dei trattamenti previsti sulla protezione dei dati personali, mentre la tutela dei diritti e delle libertà delle persone fisiche vengono presi in considerazione solo con riferimento al rischio presunto.

Quanto questa differenza terminologica, che ora si nota, sia poi traducibile in una differenza di contenuto e di responsabilità è ancora troppo presto per dirlo, certo è che gli elementi individuati dal GDPR al comma 7 dell'art. 35 sono ben diversi da quello desumibili dall'art. 27 dell'AI ACT.

Di sicuro è che l'utilizzo di dati biometrici potrebbe colorare diversamente la rischiosità per i diritti fondamentali.

L'importanza della valutazione d'impatto è stata rimarcata di recente in un parere emesso dal Comitato europeo per la protezione dei dati a seguito di una richiesta dell'Autorità di vigilanza francese sull'uso della tecnologia di riconoscimento facciale da parte degli operatori aeroportuali e delle compagnie aeree per l'autenticazione o l'identificazione biometrica dei passeggeri per semplificare il flusso di passeggeri negli aeroporti[67].

Come osservazione preliminare, il Comitato ricorda che l'uso dei dati biometrici e in particolare della tecnologia di riconoscimento facciale comporta rischi maggiori per i diritti e le libertà degli interessati [68] . Dunque, si

---

[64] Sul punto cfr., A. PIN, *Non esiste la "pallottola d'argento": l'Artificial Face Recognition al vaglio giudiziario per la prima volta*, cit., 3081 ss.; F. FAINI, *Big data, algoritmi e diritto*, in DPCE online, 2019, Vol. 40, III, 1869 ss.

[65] Tale responsabilizzazione porta anche ad imporre un costante controllo ed aggiornamento dei dati per non creare la situazione per cui continuino a perpetrarsi discriminazioni passate. Sul punto v., D. CARDON, *Che cosa sognano gli algoritmi.* Le nostre vite al tempo dei big data, Milano, 2016, 74.

[66] c.d. *fundamental rights impact assessment,* art. 27, AI ACT.

[67] Comitato europeo per la protezione dei dati, *Opinion on the use of facial recognition to streamline airport passengers' flow* (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR, n. 11, 2024, Version 1.1. Adopted on 23 May 2024.

[68] I rischi significativi evidenziati sono soprattutto relativi alla intermediazione della macchina. Infatti, un sistema di riconoscimento facciale rende le caratteristiche intrinseche del soggetto "leggibili dalle macchine," creando un collegamento permanente tra corpo e identità. Questo trattamento può amplificare le minacce alla privacy e alla sicurezza personale, specialmente in caso di violazioni o accessi non autorizzati. La maggiore pericolosità di un eventuale trattamento automatizzato di questi dati sta nel fatto che in ipotesi di *data breach*, i dati biometrici non possono essere "cambiati" come una *password*, quindi le persone colpite sono permanentemente esposte a questo tipo di rischio. Inoltre, il documento sottolinea anche che le tecnologie di riconoscimento facciale possono essere soggette a *bias* legati a età, genere e razza. Questi pregiudizi algoritmici possono portare a trattamenti ingiusti e discriminatori, specialmente contro

raccomanda, che prima di utilizzare tali tecnologie, i titolari del trattamento valutino l'impatto del trattamento in linea con i requisiti dell'art. 35 GDPR e considerino se esistono mezzi meno invasivi che possano raggiungere lo scopo legittimo del trattamento.

Il parere è poi molto articolato e valuta quattro possibili scenari che sono contraddistinti da un grado crescente di automazione. In tutte le ipotesi si conclude che si potrebbe ritenere che le misure scelte abbiano soddisfatto il principio di necessità se il titolare del trattamento può dimostrare che non esistono soluzioni alternative meno invasive che potrebbero raggiungere lo stesso obiettivo in modo altrettanto efficace[69].

Ovviamente, in questo caso, il riferimento era alla valutazione di impatto di cui al GDPR ed è puro esercizio di stile chiedersi cosa avrebbe detto l'EDPB se fosse stato in vigore l'AI ACT.

Ma più che interrogarci su questo, sembra opportuno riflettere sulla ragionevolezza dell'applicazione delle norme nel caso concreto e richiamare fortemente il ruolo di un interprete consapevole e coraggioso che superi la contrapposizione tra privacy e persona, in una corretta interpretazione della normativa sul trattamento dei dati personali per approdare finalmente a quella evoluzione dal diritto ad essere lasciati soli al diritto al controllo della circolazione dei dati. In questo senso assume un ruolo centrale il c.d. diritto all'autodeterminazione informativa ricavabile dell'art. 8 della Carta dei diritti fondamentali dell'Unione Europea che rappresenta il fondamento e il coordinamento delle normative di cui stiamo discutendo.

---

minoranze e gruppi vulnerabili, creando disuguaglianze nel modo in cui le persone sono identificate e trattate.

[69] Analogamente si è espresso il Garante italiano per la protezione dei dati personali, negando per ben 5 volte l'utilizzo di strumenti di riconoscimento facciale per il controllo della presenza dei lavoratori. Il Garante ha specificato che alla luce dei principi di minimizzazione e proporzionalità del trattamento, i datori di lavoro avrebbero dovuto optare per sistemi meno invasivi e rispettosi della sfera personale dei lavoratori. Si tratta dei seguenti provvedimenti: Provvedimento 22.02.2024, doc. web. n. 9995680. Ordinanza ingiunzione nei confronti di L'Igiene Urbana Evolution s.r.l., disponibile al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9995785; Provvedimento 22.02.2024, doc. web. n. 9995701, Ordinanza ingiunzione nei confronti di Airone società consortile a r.l., disponibile al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9995701; Provvedimento 22.02.2024, doc. web. n. 9995741, Ordinanza ingiunzione nei confronti di Blue Work s.r.l., disponibile al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9995741; Provvedimento 22.02.2024, doc. web. n. 9995762, Ordinanza ingiunzione nei confronti di DM Technology s.r.l., disponibile al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9995762; Provvedimento 22.02.2024, doc. web. n. 9995785, Ordinanza ingiunzione nei confronti di Unica s.r.l.s., disponibile al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9995785.