RIVISTA DI
DIRITTI COMPARATI

Dati biometrici, tutela del singolo e opportunità di mercato*

Tommaso Sica

SOMMARIO: 1. Introduzione. - 2. Nozione di dato personale e di dato biometrico. - 3. Riconoscibilità del soggetto per mezzo della raccolta di dati biometrici. - 4. Il caso *Bridges* e l'esperienza inglese. - 5. L'approccio negli altri modelli di *common law*. - 6. Il caso *ClearView AI* e la risposta svedese, tedesca e italiana. 7. Le tecniche di riconoscimento biometrico nella Proposta di Regolamento sull'intelligenza artificiale del 2021. - 8. Nuove forme di biometria.

1. Introduzione

Le tematiche riconnesse alla biometria, oltre ad aver captato l'attenzione dei legislatori europei, si stanno altresì gradualmente imponendo nel dibattito pubblico. Da un lato, v'è chi evoca spettri distopici associati alla sorveglianza di massa[1]; dall'altro, invece, chi, forse con maggiore prudenza, intravede anche i vantaggi che tale tecnologia potrebbe apportare[2].

Allo stesso modo, è di frequente evidenziata l'imprudenza con cui molti utenti si raffrontano a tali mezzi: basti pensare, a titolo meramente esemplificativo, ai cc.dd. *wearable*, ossia i dispositivi che, una volta indossati, rilevano, registrano e tracciano i movimenti, i battiti cardiaci, la pressione sanguigna, la qualità del sonno e così via enumerando[3].

---

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a *double-blind peer review*.

[1] Si pensi alle polemiche associate all'utilizzo di sistemi di rilevamento biometrico a Hong Kong, su cui v. J. Li, *China's Facial-Recognition Giant Says It Can Crack Masked Faces during the Coronavirus*, in *Quartz*, 2020, disponibile al seguente link: https://qz.com/1803737/chinas-facial-recognition-tech-can-crack-masked-faces-amid-coronavirus/

[2] Cfr. M.B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 *UC Irvine Law Review* 107 (2019).

[3] L.J. Kyun, *Wearable device for oral biodata collection and analysis* in *Nuovo dir. soc.,* 2020, p. 1079 ss.; V. Zeno Zencovich, *Ten legal perspectives on the "big data revolution*", in *Conc. e merc.,* 2016, p. 29 ss.; E.C. Pallone, "Internet of Things" *e l'importanza del diritto alla* "privacy" *tra opportunità e rischi* in *Cib. e dir.*, 2016, p. 163 ss.; E. Germani - L. Ferola, *Il* wearable computing *e gli orizzonti futuri della* privacy, in *Dir. inf.,* 2014, p. 75 ss.

All'interno della discussione un ruolo centrale è assolto dalle tecniche di riconoscimento facciale, che consentono, sulla base dei punti del volto, di riconoscere un individuo, differenziandolo in modo univoco dagli altri consociati[4].

Anche in questo caso, le notizie sugli sviluppi tecnologici più recenti sollevano non pochi e preoccupanti interrogativi. La Cina, da anni, utilizza massivamente tecnologie invasive di riconoscimento per mezzo di dati biometrici, sia in ambito pubblico sia nel settore privato[5]: una tendenza che ha assunto dimensioni inquietanti, a cui la nuova legislazione nazionale sta provando a dare una risposta[6].

È evidente, però, che il dilemma tra *total control*, tipico dei regimi totalitari, e *absolute freedom*, su cui si basa la regolazione di stampo

[4] Sul riconoscimento facciale cfr. il report della European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27 novembre 2019, disponibile al seguente link: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf. V. anche A. Mascolo, *Riconoscimento facciale e autorità pubbliche*, in *Giorn. dir. amm.,* 2021, p. 308 ss. e L. Scaffardi, "Next Generation Prüme", *le scelte strategiche della UE: dall'ampliamento nello scambio dei dati genetici all'introduzione del riconoscimento facciale*, in *federalismi.it*, 2021, p. 200 ss.

[5] La Corte Suprema del Popolo della Repubblica Popolare Cinese, con la decisione del 27 luglio 2021, si è pronunciata sull'uso di tecnologie per il riconoscimento facciale, affermando che la raccolta e l'analisi dei dati attraverso il tracciamento facciale, per scopi di lucro, può avvenire solo con il consenso dell'interessato. Peraltro, l'ordinamento cinese si è recentemente dotato di una nuova normativa in materia di protezione dei dati personali, su cui si rinvia, per ulteriori approfondimenti, a D. Clementi, *La legge cinese sulla protezione delle informazioni personali: un GDPR con caratteristiche cinesi?*, in *Dir. comp.*, 2022, p. 1 ss. È da notare che, a differenza di quanto potrebbe credersi, le nuove disposizioni prevedono una serie di garanzie per i cittadini che sono assimilabili a quelle previste, a livello europeo, dal Regolamento UE n. 2016/679. In generale, sul fenomeno di "europeizzazione" della privacy fuori dal territorio dell'Unione europea, v. S. Mercer, *The Limitations of European Data Protection As A Model for Global Privacy Regulation*, 114 *American Journal of International Law Unbound* 20 (2020); P.M. Schwartz, *Global Data Privacy: The E.U. Way*, in 94 *New York University Law Review* 771 (2019); M. Scott – L. Cerulus, *Europe's New Data Protection Rules Export Privacy Standards Worldwide,* in *Politico.eu*, 31 gennaio 2018.

[6] Nell'ambito degli ordinamenti giuridici appartenenti alla *western legal tradition*, molte critiche sono state sollevate anche all'approccio statunitense, soprattutto a seguito dell'introduzione delle varie normative antiterroristiche, successive ai fatti dell'11 settembre 2001. Sul punto, in chiave critica, v. S.M. Hoque, *Government responses to terrorism: critical views of their impacts on people and public administration,* in 62 *Public Administration Review* 170 (2002); D. Lyon, *Technology vs. "Terrorism": circuits of city surveillance since September 11 ,* in 27 *International Journal of Urban and Regional Research* 666 (2003); nonché, nell'ambito della letteratura giuridica in lingua italiana, v. G. Frosio, *Cosa resta della privacy? – diritto alla riservatezza dell'"uomo medio" dopo l'11 settembre*, in *Cib. e dir.*, 2005, p. 222 ss.

neoliberista, ha determinato una polarizzazione probabilmente fuorviante. Difatti, le opzioni regolatorie attuate hanno ingenerato la convinzione che la biometria e il riconoscimento facciale siano, di per sé, tecniche pericolose, che espongono i cittadini a rischi ingiustificati[7].

Invero, la tecnologia, è appena il caso di ricordarlo, è ontologicamente neutrale, sicché una sua connotazione positiva o negativa non può che essere il frutto dell'utilizzo concreto che della tecnologia stessa si pone in essere[8]. Del resto, ma anche questa è affermazione scontata, l'intervento normativo dovrebbe ambire proprio al raggiungimento di un duplice effetto: quello della fissazione di limiti invalicabili a tutela dei diritti fondamentali, senza mortificare, al tempo stesso, lo sviluppo tecnologico[9]. Un approccio paternalistico e ultra-protezionistico potrebbe determinare un ritardo tecnologico negli ordinamenti che dovessero decidere di adottarlo: un esempio, in tal senso, è rappresentato dalla rallentata espansione del *cloud computing* in Europa, che ha costretto, e tuttora costringe, imprese e pubbliche amministrazioni ad affidare i propri dati a soggetti stabiliti fuori dall'Unione Europea, con un evidente pregiudizio sia sotto il profilo economico sia sotto quello dell'effettività della tutela dei diritti coinvolti[10].

---

[7] Cfr. J. Chandra Joshi – K.K. Gupta, *Face Recognition Technology: A Review*, in 1 *Iup Journal of Telecommunications* 53 (2016); R. Victoria - V. Petrescu, *Face Recognition as a Biometric Application*, 3 *Journal of Mechatronics and Robotics* 237 (2019); M.G. Galterio et al., *A Review of Facial Biometrics Security for Smart Devices*, in 7 *Computers* 37 (2018); I. Berle, *Facial Recognition Technology. Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images,* New York, 2020.

[8] V., ad es.,T. Wu, *Network Neutrality, Broadband Discrimination* in *Journal of Telecommunications & High Technology Law*, 2003, p. 141 ss., 2003; S. Sica - V. Zeno-Zencovich, *Manuale di diritto dell'informazione e della comunicazione*, IV ed., Padova, 2015, p. 365 ss.; G. Giannone Codiglione, *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali*, in *Dir. inf.*, 2015, p. 909 ss.; L. D'Acunto (a cura di), *Net (or not) Neutrality? Web e regolazione,* Napoli, 2017.; F. Mattassoglio, *Algoritmi e regolazione. Circa i limiti del principio di neutralità tecnologica*, in *Riv. reg. merc.,* 2018, p. 226 ss.

[9] Cfr. tra i tanti contributi in dottrina, C. Blasi Casagran, *Global Data Protection in the Field of Law Enforcement: An EU Perspective*, London, 2016; S. Gutwirth - Y. Poullet - P. De Hert, - C. De Terwangne - S. Nouwt, *Reinventing Data Protection?*, Berlin, 2009.

[10] Le questioni poste dal *cloud computing* sono ben riassunte nel volume Aa.Vv., *Il Digital Single Market e i Cloud Services. Tutela e circolazione dei dati nell'Economia Digitale. Un approccio interdisciplinare a Cloud e Big Data*, Milano, 2018. V. anche R. Torino, Cloud Computing Contracts. *L'inadempimento contrattuale e il Mercato Unico Digitale*, in M. Franzosi – O. Pollicino – G. Campus (a cura di), *Il* Digital Single Market *e i* Cloud Services, Roma, 2018, p. 355 ss.; V. Boncinelli, M*odelli tecnici e disciplina giuridica del c.d.* "cloud computing" (Cloud computing: technical models and legal frameworks) in *Riv. it. inf. dir.,* 2021, p. 29 ss.; A. Martini, *Dalla "nuvola" al negozio: il contratto di "cloud computing"*

Il ricorso alla biometria, coniugato con le tecnologie di intelligenza artificiale, ha peraltro sollevato un'ulteriore questione, che incide direttamente sul funzionamento dei principali servizi di internet. Il riferimento è al rapporto che intercorre tra tali nuove tecnologie e i principi democratici e, segnatamente, alla circostanza per cui il ricorso a strumenti automatizzati di riconoscimento possa aprire il campo a forme, anche surrettizie e involontarie, di discriminazione[11].

Il presente scritto, esaminando talune recenti soluzioni informatiche immesse sul mercato, che prevedono l'utilizzo di dati biometrici per il riconoscimento degli individui senza conservazione dei dati stessi, intende fornire una prospettiva innovativa, che tenga conto delle novità tecnologiche pensate in un'ottica di maggiore *compliance* rispetto alla normativa vigente e di minimizzazione nel trattamento e nella *retention* dei dati[12].

2. Nozione di dato personale e di dato biometrico

Sulla scorta di quanto premesso, la prima questione da affrontare attiene alla natura dei dati biometrici e alla sussumibilità degli stessi nell'alveo della nozione di dato personale.

Occorre pertanto prendere le mosse proprio dalla definizione di dato personale, qualificato dal Regolamento UE n. 2016/679 (GDPR), all'art. 4, n. 1, come "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)*; *si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo*

in *Nuova giur. civ. comm.,* 2020, II, p. 970 ss.; A. Mantelero, *Il* cloud computing, in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, Milano, 2019, p. 509 ss.

[11] Sul punto, v., diffusamente, G. Resta, *Algoritmi, diritto, democrazia* in *Giustiziacivile.com*, 11 aprile 2019; Id., *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. dir.,* 2019, p. 218 ss.; T. Numerico, *Social network e algoritmi di machine learning: problemi cognitivi e propagazione dei pregiudizi*, in *Sistemi intelligenti*, 2019, p. 469; nonché J.G. Cavazos *et al.*, *Accuracy Comparison Across Face Recognition Algorithms: Where Are We On Measuring Race Bias?*, in *IEE Transactions on Biometrics, Identity, Profile*, 4 giugno 2020, disponibile al seguente link: http://arxiv.org/abs/1912.07398 e J. Kleinberg - J. Ludwig - S. Mullainthan - C.R. Sunstein, *Discrimination in the Age of Algorithms*, *NBER Working Paper n. 25548*, 2019.

[12] Sull'incidenza dei dati personali sulle modalità di conoscenza e organizzazione del diritto da parte dei giuristi v. Zeno-Zencovich, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *MediaLaws – Riv. dir. media*, 2018, p. 32 ss.

come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"[13].

Il legislatore europeo, muovendosi nella scia tracciata dalla direttiva n. 95/46/CE, ha prediletto una definizione onnicomprensiva, in grado di includere qualsivoglia informazione che, direttamente o indirettamente, consenta di risalire all'identità di una persona fisica[14].

Similmente, anche la nozione di dato biometrico è modellata in maniera ampia, abbracciando "*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*" (art. 4, n. 14 del GDPR)[15]. Tale definizione, da leggere necessariamente in combinato disposto con quella di dato personale, presenta un approccio descrittivo: anche in questo caso il GDPR ha preferito adottare una formula non ancorata alle soluzioni tecnologiche esistenti, che possa rivelarsi quindi flessibile alle innovazioni[16].

I dati biometrici rientrano altresì nella categoria dei dati particolari, così come regolati all'art. 9, par. 1 del GDPR, il quale statuisce che: *"è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici,*

[13] Sul dato personale, così come modellato dal GDPR, la letteratura è piuttosto ampia. Si vedano, tra gli altri, V. Cuffaro – R. D'Orazio – V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019; G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019; R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, cit.; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo,* Torino, 2016; G. Riccio – G. Scorza – E. Belisario (a cura di), *GDPR e Normativa Privacy. Commentario*, Milano, 2018; S. Sica – V. D'Antonio – G. Riccio (a cura di), *La nuova disciplina europea della privacy*, Padova, 2016; E. Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019; N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Bologna, Padova, 2019; L. Califano – C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017.

[14] Non a caso, la dottrina ha evidenziato che il legislatore comunitario non avrebbe voluto dettare un'elencazione chiusa degli elementi che consentono l'identificazione di un soggetto. Cfr. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., p. 7.

[15] F. Fontanarosa, *Dati biometrici e tutela della "privacy" tra divergenze giuridiche ed esigenze di unificazione*, in *Ann. dir. comp.*, 2019, III, p. 807 ss.; A. Iannuzzi - F. Filosa, *Il trattamento dei dati genetici e biometrici* in *Dir. fond.*, 2019, p. 24; G. Formici, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, in *DPCEonline.it*, 9 luglio 2019; L. Cuomo, *Profili giuridici del trattamento biometrico dei dati*, in *Riv. it. med. leg.*, 2014, p. 43 ss.

[16] F. Fontanarosa, *Dati biometrici e tutela della "privacy" tra divergenze giuridiche ed esigenze di unificazione,* cit., p. 808.

dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona"[17].

Nella ricostruzione normativa occorre però ricordare anche quanto esposto nel "*Working document on biometrics"* (WP80), adottato nel 2003 - quando ancora era vigente la Direttiva n. 95/46/CE - che, oltre ad offrire una panoramica sul concetto di sistema di rilevamento biometrico, già rispondeva affermativamente al quesito relativo alla riconducibilità nel *genus* dei dati personali della *species* dei dati biometrici[18]. Nello specifico, il *Working Party*, anche alla luce del considerando n. 26 della Direttiva n. 95/46/CE[19], concludeva che nella maggior parte dei casi i dati biometrici trattati mediante i sistemi di rilevamento sono dati personali, pur precisando che essi perdono tale qualifica allorquando, come un *template,* siano memorizzati in modo tale che il titolare del trattamento non possa utilizzare mezzi ragionevoli per identificare l'interessato[20].

Successivamente, nel WP136, "*Parere 4/2007 sul concetto di dati personali*", lo stesso *Working Party* definiva i dati biometrici come "*proprietà biologiche, caratteristiche fisiologiche, tratti biologici o azioni ripetibili laddove tali caratteristiche e/o azioni sono tanto proprie di un certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità"*[21]. Esempi tipici di dati biometrici sarebbero quindi le impronte digitali, la struttura della retina e del volto, la voce, ma anche la forma della mano, gli elementi caratteristici delle vene o perfino alcune capacità profondamente radicate nella persona o altre caratteristiche comportamentali (a titolo esemplificativo: la firma, la pressione esercitata

[17] Il par. 2 dell'art. 9 GDPR prevede tuttavia una serie di eccezioni che derogano al divieto di cui al par. 1 della medesima norma.

[18] La valutazione del *Working Party* era basata sulla nozione di dato personale fornita dalla Direttiva n. 95/46/CE, ove è dato leggere, all'art. 2 alla lett. a): *"«dati personali»: qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale*".

[19] A mente del quale: "(…) *per determinare se una persona è identificabile, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona; che i principi della tutela non si applicano a dati resi anonimi in modo tale che la persona interessata non è più identificabile* (…)".

[20] Testualmente: "*in cases where biometric data, like a template, are stored in a way that no reasonable means can be used by the controller or by any other person to identify the data subject, those data should not be qualified as personal data".*

[21] Il testo integrale del parere è consultabile al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1496512.

sui tasti, le modalità di movimento, il timbro della voce)[22]. Peculiarità dei dati biometrici è che li si può considerare sia come contenuto delle informazioni relative ad una particolare persona, sia come elemento atto a stabilire una relazione tra un'informazione e una persona[23]. Essi assolvono dunque la funzione di "identificatori", in quanto, in seguito al loro collegamento univoco con la persona cui si riferiscono, essi possono essere impiegati per individuare una persona fisica[24]. Siffatta doppia natura si riscontra anche nei dati del DNA che forniscono informazioni sul corpo umano e consentono il riconoscimento univoco e inequivocabile, mentre i campioni di tessuti umani costituiscono mere fonti da cui vengono estratti dati biometrici, ma non sono di per sé dati biometrici (ad esempio, le impronte digitali sono dati biometrici, ma non lo è il dito)[25].

Se quindi i dati biometrici possono essere assurgere al ruolo di identificatori, occorre contestualmente verificare anche le modalità concrete attraverso cui avviene l'accertamento del soggetto. Siffatto processo, difatti, si realizza tramite i c.d. "mezzi di identificazione", che consentono la riconducibilità del dato personale al soggetto, il quale, a seguito di tale operazione, viene quindi identificato. Si può osservare inoltre come nel WP193 "*Opinion 3/2012 on developments in biometric technologies*", i sistemi di rilevamento biometrico facciano riferimento alle applicazioni che usano la

[22] Sull'autenticazione biometrica si v. S. Bisi, *Il corpo come password: alcune considerazioni in tema di sistemi di autenticazione biometrica*, in *Cib. e dir.*, 2005, p. 1 ss.; M. Sala, *Autenticazione e cifratura di dati biometrici* in *Gnosis*, 2016, p. 194 ss.; A. Cavo, *Acquisizione del consenso informato in ambito diagnostico tramite firma biometrica e "*data protection*"*, in *Resp. civ. prev.,* 2019, p. 318 ss.

[23] La ricostruzione è avallata anche dalla giurisprudenza di legittimità. Ad esempio, Cass. civ., 15 ottobre 2018, n. 25686, in *Resp. civ. prev.*, 2019, p. 1225, con nota di L.Vizzoni, sostiene che si configura un trattamento di dati personali ai sensi del d.lg. n. 196/2003 nel caso di installazione di un sistema di rilevazione biometrica (basato sull'archiviazione della geometria della mano) che, attraverso un algoritmo, consenta di risalire al lavoratore al quale appartiene il dato e, quindi, di identificarlo indirettamente.

[24] In merito al rapporto tra persona e identità si vedano, tra gli altri, S. Rodotà, *Il corpo "giuridificato",* in Aa.Vv. (a cura di) *Trattato di Biodiritto - Il governo del corpo*, I, Milano, 2011, p. 51 ss. e F. Di Marzio, Hybris, vanitas, jus. *Rifare l'umano*, in *Giust. civ.,* 2018, I, p. 99.

[25] L. Morrison, *Portraits of Automated Facial Recognition: On Machinic Ways of Seeing the Face,* Bielefeld, 2019; K.A. Gates, *Our Biometric Future. Facial Recognition Technology and the Culture of Surveillance*, New York, 2011.

tecnologia biometrica, in particolare quelli che consentono l'identificazione automatica e/o la verificazione di un soggetto[26].

Per *biometric identification* si intende proprio quel meccanismo che permette l'identificazione di un individuo da un sistema biometrico attraverso l'associazione di un dato biometrico a un numero presente all'interno di un database (*one to many matching process),* là dove, invece, i concetti di *verification/authentication* evocano tipicamente quel processo di comparazione tra un dato biometrico raccolto al momento della verificazione e il *biometric template,* conservato nel *device*[27].

Difatti, dal già menzionato Considerando 26 della Direttiva n. 95/46/CE si desume che la sola possibilità di distinguere una persona non è sufficiente per considerare tale persona "identificabile". Nel caso in cui, tenendo conto dell'insieme dei mezzi che possono essere ragionevolmente utilizzati da chi tratta i dati per identificare la persona, tale possibilità non esista o sia trascurabile, allora ne deriva che la persona non deve essere considerata "identificabile" e che le informazioni non si configurano come "dati personali"[28].

3. Riconoscibilità del soggetto per mezzo della raccolta di dati biometrici

Sempre con riguardo al meccanismo di identificazione del soggetto, il WP80 fornisce un esempio in tema di dati relativi alla ricerca farmacologica. Lo scenario che viene immaginato è quello di un ospedale che trasferisce dati anonimi di pazienti ad una società che si occupa di ricerca scientifica[29]. Nello specifico, i pazienti non sono associati a un dato anagrafico, bensì a una serie di numeri, e non vi è alcun pericolo di risalire alla persona, in

[26] Article 29, Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, 27 aprile 2012, disponibile al link: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

[27] M.B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, cit., p. 107.

[28] V. D'Antonio, *Biometria, dati genetici e* privacy: *profili giuridici*, Salerno, 2004; nonché Id., *I dati genetici*, in F. Cardarelli-S. Sica-V. Zeno Zencovich (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, 2004, p. 337 ss.

[29] Sul trattamento dei dati relativi alla salute si rinvia a C. Perlingieri, *eHealth and Data*, in R. Senigaglia – C. Irti – A. Bernes (eds.), *Privacy and data protection in software services*, New York, 2021, p. 127 ss.

quanto le informazioni che vengono conferite non permettono tale processo. Da siffatto esempio il WP80 evince che, nel caso *de quo*, considerato che il soggetto che conduce la ricerca non è in grado di rapportare la stringa di numeri concernente il singolo caso medico al paziente corrispondente, né tantomeno mostra alcuna intenzione di voler procedere in tal senso, i dati trattati secondo tali modalità non possono essere qualificati come dati personali.

Alla luce di quanto esposto, il titolare del trattamento, mediante la soluzione tecnologica di rilevamento dei dati biometrici, potrebbe realizzare un sistema che non sia in grado di risalire all'identità dei soggetti, attesa l'irreversibilità del processo di cifratura[30]. Per essere più precisi occorre considerare quelle soluzioni tecnologiche, già presenti sul mercato, che compiono sì l'identificazione del soggetto per mezzo del dato biometrico (ad esempio attraverso i punti del volto), ma che non consentono la loro identificazione in un momento successivo: difatti, per ottenere tale ultimo risultato sarebbe necessario venire a conoscenza del *template* originario del dato biometrico, il quale tuttavia, dopo la sua creazione, viene immediatamente distrutto sul dispositivo dell'utente[31]. Non viene inoltre creato alcun *database* centralizzato che possa raccogliere informazioni riconducibili agli utenti e il trattamento del dato biometrico - che, lo si ripete, avviene sul *device* dell'utente – è di tal guisa limitato al momento della trasformazione in stringhe numeriche, impedendo da un lato il rischio di *data breach*, dall'altro lato la diffusione e la trasmissione delle informazioni biometriche cc.dd. grezze.

---

[30] V. C. Irti, *Personal data, non-personal data, anonymised data, pseudonymised data, de-identified data*, in R. Senigaglia – C. Irti – A. Bernes (eds.), *Privacy and data protection in software services*, cit., p. 49 ss.

[31] Tra le varie soluzioni presenti sul mercato, si segnalano quelle in cui non avviene né la conservazione del dato personale, né la sua migrazione, successiva al momento della *caption*, dal dispositivo dell'utente. In altri termini, il processo di *enrollement*, con trattamento del dato biometrico (il volto dell'utente) avviene all'interno del dispositivo dell'utente stesso. Successivamente, avviene la scomposizione facciale e la trasmissione di codici che migrano su server di proprietà della società che gestisce il *device*. La società effettua, per conto del proprio cliente, il match dei risultati ai fini dell'identificazione dell'utente, senza tuttavia ricorrere al dato biometrico iniziale, che non è visibile – e, quindi, non è trattato – dalla società stessa, né in qualità di titolare del trattamento, né eventualmente di responsabile dello stesso. Occorre inoltre precisare, giacché trattasi di processo che incide sull'applicabilità della normativa in materia di dati personali, che, sebbene vi sia l'utilizzo degli elementi crittografici dei dati, le chiavi per decriptare tali informazioni sono sconosciute allo stesso titolare del trattamento.

A tal riguardo, risulta interessante dare conto dell'orientamento della Corte di Giustizia dell'Unione Europea in ambito di dati personali, esplicitato nella decisione *C-582-14, Patrick Breyer c. Bundesrepublik Deutschland*[32]. La fattispecie era relativa alla registrazione e alla conservazione, da parte della convenuta, dell'indirizzo di protocollo Internet (ossia l'indirizzo IP) del sig. Breyer in occasione della consultazione fatta dal medesimo di vari siti internet dei servizi federali tedeschi. La questione principale verteva sulla possibilità di qualificare l'indirizzo IP come dato personale. La Corte concludeva affermando: "*L'articolo 2, lettera a), della direttiva 95/46 del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, dev'essere interpretato nel senso che un indirizzo di protocollo Internet dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale ai sensi di detta disposizione, qualora detto fornitore disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detta persona dispone*". In sostanza, nel caso appena delineato, proprio in quanto idoneo all'identificazione, l'indirizzo IP veniva considerato dato personale, sulla base della nozione dell'art. 2 della Direttiva n. 95/46/CE[33].

Si precisa, con riferimento alla sentenza, che la fattispecie risulta però differente rispetto a quella in cui i titolari raccolgono dati biometrici. Difatti, nel caso *Patrick Breyer* si discuteva del ruolo del fornitore dei servizi di media *online* e della legittimità della conoscenza di informazioni aggiuntive da parte del fornitore stesso; viceversa, nel caso di fornitori di servizi che raccolgono dati biometrici, questi ultimi non agiscono in qualità di fornitori di servizi di media *online* e non realizzano alcun trattamento di indirizzi IP. Il *discrimen*, quindi, è dato dalla circostanza per cui il titolare del trattamento venga, o

[32] *Patrick Breyer c. Bundesrepublik Deutschland*, Case *C-582-14*, 19 ottobre 2016.

[33] Risulta interessante anche il passo della decisione dove si afferma che: "*orbene, anche se il giudice del rinvio precisa, nella propria decisione di rinvio, che il diritto nazionale tedesco non consente al fornitore di accesso a Internet di trasmettere direttamente al fornitore di servizi di media online le informazioni aggiuntive necessarie all'identificazione della persona interessata, sembra tuttavia, ferme restando le verifiche che detto giudice dovrà compiere al riguardo, che esistano strumenti giuridici che consentono al fornitore di servizi di media online di rivolgersi, in particolare in caso di attacchi cibernetici, all'autorità competente affinché quest'ultima assuma le iniziative necessarie per ottenere tali informazioni dal fornitore di accesso a Internet e per avviare procedimenti penali*".

possa venire, a conoscenza di dati o di informazioni aggiuntive, nell'ambito di un servizio di mera autenticazione dell'utente[34].

4. Il caso *Bridges* e l'esperienza inglese

Occorre a questo punto rivolgere l'attenzione alle principali esperienze regolatorie straniere in tema di dati biometrici[35].

In Gran Bretagna, il Data Protection Act 2018, Section 205 (1) stabilisce che "*biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic data*". L'ICO (*Information Commissioner Office*, l'Autorità indipendente di controllo del Regno Unito) ha inoltre specificato che i dati biometrici rientrano all'interno delle categorie particolari di dati di cui all'art. 9 GDPR e ha altresì pubblicato una guida sul trattamento dei dati sensibili[36]. All'interno di quest'ultima, con riguardo ai dati biometrici, l'Autorità statuisce che, qualora si utilizzino immagini digitali degli individui, questo non implica automaticamente che ci si trovi dinanzi a un'ipotesi di trattamento di dati biometrici, anche nel caso in cui le immagini vengano utilizzate per finalità di identificazione. Secondo l'ICO, l'immagine rientra

[34] Cfr. F. Zuiderveen Borgesius, *The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition*, 3 *European Data Protection Law Review* 130 (2017).

[35] In Spagna, nel giugno 2020, è stato pubblicato da parte dell'Autorità Garante spagnola (AEPD), in collaborazione con l'EDPS (*European Data Protection Supervisory)*, un documento che ricostruisce gli equivoci più comuni relazionati all'uso della biometria e che valuta come tali equivoci incidano sulla protezione dei dati personali. La posizione è molto critica nei confronti dell'uso della biometria in generale; in particolare, si afferma che le tecniche utilizzate, come *l'hash* o il *biohash*, non siano totalmente accurate, in quanto è comunque probabile che possa essere compiuta un'operazione di reversibilità. Si consiglia quindi di eliminare totalmente il *template* biometrico, al quale si è applicato l'algoritmo di trasformazione: *"para añadir seguridad al tratamiento de la información biométrica, es recomendable eliminar el patrón biométrico"*. Cfr. AEPD, *14 equívocos con relación a la identificación y autenticación biométrica*, disponibile al seguente link: https://www.aepd.es/sites/default/files/2020-06/nota-equivocos-biometria.pdf. In generale, sui compiti delle autorità indipendenti nel trattamento algoritmico dei dati personali, v. A. Zoppini, *Il ruolo e le funzioni delle* authorities *nel trattamento algoritmico dei dati*, in Aa.Vv., *Il trattamento algoritmico dei dati tra etica, diritto ed economia. Atti del 14° Convegno nazionale*, Napoli, 2020, p. 291 ss.

[36] ICO, *What is special category data?*, disponibile al seguente link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/ .

tra i dati biometrici soltanto allorquando venga impiegata per creare un *template* digitale oppure un profilo, che a sua volta viene adoperato come strumento per effettuare automaticamente l'identificazione, attraverso un *matching* del volto e dell'immagine stessa: "*all biometric data is personal data, as it allows or confirms the identification of an individual. Biometric data is also special category data whenever you process it "for the purpose of uniquely identifying a natural person. This means that biometric data will be special category data in the vast majority of cases"*[37].

L'Autorità prosegue, quindi, sostenendo che i dati biometrici acquisiscono la qualifica di dati personali laddove consentano o confermino l'identificazione di un soggetto. Di contro, essi rientrano nelle categorie speciali di dati personali qualora il trattamento sia compiuto unicamente al fine di identificare il soggetto. In definitiva, nella maggior parte dei casi, i dati biometrici, secondo l'ICO, costituiscono una categoria speciale di dati.

Sempre nell'ordinamento inglese, il *leading case* è probabilmente rappresentato dalla sentenza della High Court of Justice, che, nel caso "*Bridges*" ha esaminato l'utilizzo di un algoritmo di "*automated Facial Recognition technology"* da parte delle forze di polizia[38].

La Corte ha statuito che, anche se il rilevamento dell'informazione biometrica sia stato limitato ad una conservazione per un lasso temporale ridotto, questo non esclude che il sistema debba esser vagliato alla luce della conformità rispetto all'art. 8 della Carta di Nizza[39]. A tal proposito, è infatti sufficiente che vi siano la raccolta del dato biometrico (*caption*), la conservazione e il trattamento, anche momentaneo, del dato stesso. Di tal guisa, financo la mera memorizzazione temporanea di dati biometrici renderebbe applicabile l'articolo 8 della Carta di Nizza, non rilevando l'uso successivo delle informazioni memorizzate[40].

---

[37] V. nota 35.

[38] Case No: CO/4085/2018-*Bridges, R (On Application of)* v. The *Chief Constable of South Wales Police [2019]* EWHC 2341. Sul caso, v. *amplius* M. Zalnieriute, *Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State*, 22 *Columbia Science and Technology Law Review* 284 (2021).

[39] Del quale val la pena riportare testualmente il disposto: "*1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.*

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

[40] In applicazione del precedente *S. and Marper v. United Kingdom* (2009) 48 *EHRR* 50.

Nel caso di specie, il *software* si limitava alla sola raccolta dell'immagine del viso per verificare se ci fosse un *match* tra tale dato e l'immagine contenuta nel *database*: la realizzazione di tale processo - anche in caso di cancellazione successiva per assenza di compatibilità – è stata ritenuta dalla pronuncia in esame come elemento rilevante al fine di stabilire se si sia in presenza, o meno, di un dato personale[41]. Si è affermato, quindi, che il meccanismo in uso in tale ipotesi rientrasse nel trattamento dei dati personali facenti parte di una delle categorie speciali, secondo quanto previsto dall'art. 35, par. 8, lett. b) del Data Protection Act [42].

Difatti, la sentenza sostiene che per identificazione non si debba far riferimento al mero riconoscimento, "*but also to what may allow to "individualise" or single out (and thus allow to treat differently) one person from others. This "individualization" could be done, for instance, by referring to him or her specifically, or to a device or a combination of devices (computer, mobile phone, camera, gaming devices, etc.) on the basis of an identification number, a pseudonym, biometric or genetic data, location data, an IP address, or other identifier*".

Il limite della tecnologia adoperata è dato dalla circostanza per cui il *software* utilizzato dalla polizia inglese raccoglieva l'immagine digitale e la processava attraverso un algoritmo matematico, al fine di produrre un *template* biometrico, ossia un'immagine del soggetto[43]. Di qui, tale ultima immagine veniva comparata con un altro dato biometrico, che invece era registrato in un *database*, con l'obiettivo di verificare la corrispondenza tra i due elementi.

Ciò posto, occorre verificare se, anche senza la conservazione delle immagini e, quindi, dei dati biometrici, la semplice creazione del *template* del dato biometrico possa essere considerata alla stregua di un'operazione sussumibile nella nozione di trattamento del dato e possa poi altresì

[41] "*Accordingly, the fact that the process involves the near instantaneous processing and discarding of a person's biometric data where there is no match with anyone on the watchlist (and such data is never seen by or available to a human agent) does not matter. (…) Article 8 is triggered by the initial gathering of the information. In the context of the interception of communications, the Strasbourg Court has treated the initial gathering of the information in question, its retention, and any subsequent use, as discrete interferences with Article 8*". Sul punto v. altresì *Amann v Switzerland* (2000) 30 *EHRR* 843 [GC].

[42] Tale norma individua la categoria: "*(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual*".

[43] V. P. Perlingieri, *Privacy digitale e protezione dei dati personali tra persona e mercato*, in *Foro nap.*, 2018, p. 481 ss.

ingenerare la riconducibilità all'interessato, nonostante tale dato sia immediatamente distrutto[44].

Difatti, come si illustrerà meglio nelle conclusioni, chi scrive è dell'avviso che sia necessario adottare una lettura meno formalistica della normativa applicabile, che non si limiti al tenore letterale, ma che si estenda in special modo alle finalità di tutela che il legislatore si è voluto prefissare. In tale ottica, dunque, gli esiti cui è pervenuta la giurisprudenza inglese sembrano poggiarsi su presupposti fallaci o, quanto meno, viziati da una indubbia rigidità.

5. L'approccio negli altri modelli di *common law*

Di assoluto interesse appare inoltre il modello regolatorio adottato dall'ordinamento statunitense sul punto, soprattutto ove si consideri che il dato biometrico non è ivi disciplinato a livello federale, ma soltanto attraverso singole leggi statali.

Tra queste ultime, si segnala il California Consumer Privacy Act del 2018 (CCPA), che presenta talune similitudini rispetto alla normativa europea[45].

Ai sensi della Sec. 3, Title 1.81.5., 1798.140, lett. (o) del CCPA per dato personale si intende ogni informazione "*that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household*". Tuttavia, il provvedimento normativo chiarisce che non sempre le categorie di informazioni così individuate possono essere considerate dati personali, ma rilevano come tali nel mero caso in cui identificano, sono connesse, descrivono o sono capaci di essere associate, ragionevolmente, direttamente o indirettamente, al soggetto.

Una delle categorie di dati che è valutata di natura personale è quella costituita dai dati biometrici, che sono definiti alla Sec. 3, Title 1.81.5., 1798.140., lett. (b) del CCPA come "*an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to*

[44] E.J. Kindt, *Biometric data processing: Is the Legislator Keeping up or Just Keeping up Appearances?*, in G. Gonzalez Fuster – R. Van Brakel – P. de Hert (eds.), *Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics,* Cheltenham, 2022, p. 375 ss.

[45] Sul punto v., per una disamina più accurata, J.M. Blanke, *Protection for 'Inferences Drawn': A Comparison Between the General Data Protection Regulation and the California Consumer Privacy Act*, 2 *Global Privacy Law Review* 81 (2020).

establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information". Nonostante la definizione molto ampia ed inclusiva del dato biometrico, il CCPA non prevede alcuna regola specifica in ordine al trattamento dello stesso e ciò che emerge come unico aspetto rilevante è l'inclusione nella categoria dei dati personali dell'informazione biometrica[46].

Inoltre, è utile in questa sede rimarcare che la natura di dato personale viene meno nel caso in cui l'informazione sia stata *de-identified*, e quindi non sia più riconducibile né direttamente né indirettamente al soggetto. Pertanto, quando una tecnologia definita *untraceable biometrics technology* viene adoperata, si esclude che il dato biometrico possa essere considerato dato personale, attesa la non riconducibilità ad un determinato soggetto.

Una definizione di dati biometrici più stringente è fornita dall'Illinois Biometric Information Privacy Act del 2008 (BIPA), che isola l'informazione biometrica "*regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers*"[47]. Peraltro, se, come statuito dalla pronuncia relativa al caso "*Rivera v. Google*", per *biometrics identifiers* si intendono "*retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry*", qualsiasi azione sia compiuta sui *biometrics identifiers* può sempre esser qualificata come dato personale, a condizione che sia possibile identificare il soggetto[48].

Si può dunque concludere che nel contesto ordinamentale statunitense il dato biometrico sia considerato alla stregua del dato personale, ma nella misura in cui esso consenta l'identificazione, re-identificazione o riconducibilità al soggetto, anche qualora ciò che residua dell'informazione sia un mero numero o comunque una rappresentazione matematica.

---

[46] E. Simons, *Putting a Finger on Biometric Privacy Laws: How Congress Can Stitch Together the Patchwork of Biometric Privacy Laws in the United States*, 86 *Brooklyn Law Review* 1100 (2021).

[47] Cfr. Illinois Biometric Information Privacy Act, Ch. 740, 14/10.

[48] Ciò, comunque, si potrebbe realizzare anche nei casi in cui l'informazione sia ridotta ad una "*mathematical representation*" o ancora più semplicemente ad "*a unique number assigned to a person's biometric identifier*" (*Rivera v. Google*, Inc., 238 (2017).

La normativa dello Stato dell'Illinois è stata peraltro oggetto di analisi in occasione di una *class action* attivata nei confronti di Facebook[49].

Nel 2010 Facebook aveva introdotto una tecnologia di riconoscimento facciale che scansionava le foto pubblicate dagli utenti per creare un *database* di strumenti di identificazione biometrica. Nell'agosto del 2015, i cittadini dell'Illinois Adam Pezen, Carlo Licata e Nimesh Patel intentavano una *class action* contro Facebook nel distretto settentrionale della California, sostenendo che tale tecnologia di riconoscimento facciale sarebbe stata in contrasto con l'*Illinois Biometric Information Privacy Act*[50].

Nell'agosto del 2019, la Corte d'Appello del *ninth circuit* ha ammesso l'azione di classe, riconoscendo i danni immateriali connessi alla violazione della privacy [51]. La società resistente si era però difesa sottolineando un presunto errore procedurale commesso dai giudici, consistente nella violazione della Rule 23(b)(3) del Federal Rules of Civil Procedure, in base alla quale l'azione può essere intrapresa se le violazioni si sono compiute "*primarily and substantially within*" il territorio dell'Illinois e, pertanto, non vi sarebbe stata una "predominanza" (ai sensi della normativa citata) che avrebbe determinato l'applicazione delle norme dello Stato.

Prima della pronuncia nel merito, Facebook ha definito transattivamente la controversia, offrendo 650 milioni di dollari, da suddividere tra i *plaintiffs* (circa 1,6 milioni di utenti Facebook), ma, quel che più rileva è che il caso potrebbe portare ad un rovesciamento totale delle

[49] Consol. Class Action Complaint, *Licata v. Facebook*, Inc., No. 3:15-cv-03747-JD (N.D. Cal. Aug. 28, 2015). Ma v. anche Class Action Complaint, *Pezen v. Facebook*, No. 1:15-cv-03484 (N.D. Ill. Apr. 21, 2015).

[50] Nello specifico in relazione al 740 Ill. Comp. Stat. 14/5(e).

[51] È interessante notare che anche l'art. 82 GDPR fa riferimento ai danni immateriali e non ai danni morali; sul punto, v., tra gli altri, S. Sica, *Commento all'art. 82*, in R. D'Orazio - G. Finocchiaro – O. Pollicino – G. Resta (a cura di), *Codice della privacy e data protection*, Milano, 2021; M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino 2019, p. 1017 ss.; E. Tosi, *La responsabilità civile per trattamento illecito dei dati personali*, in Id., *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano 2019, p. 619 ss.; F. Bilotta, *La responsabilità civile nel trattamento dei dati personali*, in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, cit., p. 445 ss. Sul tema più ampio del danno in ambito europeo e sulle differenti declinazioni dello stesso, v. F.D. Busnelli – G. Comandè -H. Cousy - D.B. Widmer et al., *Principles of European Tort Law: Text and Commentary*, New York, 2005, p. 24; nonché, nella dottrina italiana, *ex multis*, P.G. Monateri, *La responsabilità civile*, in R. Sacco (diretto da), *Trattato di diritto civile*, Torino, 1998, p. 101 ss. e M. Franzoni, *Il danno risarcibile*, in Id. (diretto da), *Trattato della responsabilità civile*, 2, II ed., Milano, 2010.

politiche adottate dalla *big tech* statunitense, la quale, in effetti, ha già sospeso i programmi di rilevamento delle immagini biometriche dei propri utenti.

6. Il caso ClearView AI e la risposta svedese, tedesca e italiana

Il conflitto tra l'approccio statunitense e quello europeo si è manifestato in tutta la sua evidenza nel caso ClearView AI.

Recentemente, il Garante per la protezione dei dati personali ha emesso probabilmente il provvedimento più importante in materia di biometria, che ha fatto anche il punto sul quadro regolamentare applicabile e, soprattutto sull'approccio dell'Autorità in *subiecta materia*[52].

Il provvedimento in questione trae origine da un'articolata indagine svolta dall'Autorità Garante a seguito di alcune segnalazioni ricevute da parte di cittadini che avevano ritrovato le immagini del proprio volto all'interno di un sito internet americano. I soggetti interessati lamentavano la circostanza per cui non avrebbero prestato alcun consenso né alla raccolta della propria immagine biometrica né, tantomeno, alla conservazione di tale dato[53].

L'intervento del Garante italiano, peraltro, ha fatto seguito alle indagini che erano già state precedentemente svolte sia dal Garante svedese, sia dall'Autorità Garante di Amburgo.

Nel primo caso, quello svedese, era stato sanzionato il comportamento della polizia locale, che aveva utilizzato il sistema di riconoscimento facciale offerto dalla società Clearview AI per finalità di indagine e di prevenzione dei reati[54]. Il principale profilo di interesse della vicenda svedese è correlato alla dimostrazione che, anche in caso di interesse pubblico al contrasto della criminalità, i diritti dei cittadini, in relazione ai dati biometrici, sono da considerarsi prevalenti. La polizia è stata difatti

---

[52] Garante Privacy, Provvedimento n. 50 del 10 febbraio 2022, disponibile al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9751362

[53] M.G. Stanzione, *Consenso e trattamento di dati personali nella dimensione europea*, in P. Stanzione (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, 2022, p. 77 ss.; R. Torino, *Il diritto di opposizione al trattamento dei dati personali e il diritto a non essere sottoposti a decisioni basate su trattamenti automatizzati e alla profilazione nel Regolamento (UE) 2016/679*, in *Cittadinanza Europea*, 2019, p. 45 ss.

[54] Il testo originale del provvedimento è disponibile all'URL: https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-polismyndigheten-cvai.pdf Per una sintesi, cfr. quanto riportato sul sito internet dell'European Data Protection Board, *Swedish DPA: Police unlawfully used facial recognition app*, 12 febbraio 2021.

sanzionata con un'ammenda del valore di 2,5 milioni di euro, nonché con l'obbligo di formare i propri membri affinché non si ripetano in futuro casi analoghi. Peraltro, l'autorità svedese ha imposto altresì l'obbligo di comunicare ai soggetti interessati il trattamento dei loro dati da parte delle forze di polizia[55].

Il provvedimento dell'autorità tedesca, invece, presenta forti analogie con quello italiano e origina da una segnalazione effettuata da un attivista, il quale aveva lamentato l'inserimento della propria immagine del volto nei database di Clearview[56]. Detta società, come appurato anche dalle indagini svolte dall'autorità italiana, raccoglie miliardi di immagini fotografiche e, di conseguenza, processa miliardi di dati biometrici, in parte raccolti da piattaforme di *social network* o da siti internet, senza il consenso dei soggetti interessati, i quali non sono neppure successivamente informati circa l'archiviazione della propria immagine nei *server*. Era stato inoltre accertato che la società statunitense alienava il proprio database non soltanto ad altre società private, ma anche ad alcune autorità pubbliche, che utilizzavano la banca dati di riconoscimento facciale per reperire ulteriori informazioni su persone sconosciute.

Nel caso tedesco l'istante presentava all'autorità di protezione dei dati di Amburgo una richiesta finalizzata ad ottenere la cancellazione delle proprie immagini, nonché dei valori matematici di *hash* corrispondenti al proprio profilo biometrico. L'Autorità tedesca, accogliendo il ricorso, ha stabilito il diritto dei cittadini dell'Unione Europea a non essere oggetto di rilevazione biometrica e ha ordinato la cancellazione dei dati.

Un profilo particolarmente interessante, anche in ottima comparatistica, è quello che attiene alla applicabilità del Regolamento europeo alla fattispecie e che è stato discusso sia nel provvedimento italiano sia in quello tedesco. Difatti, alla luce della propria sede sociale negli Stati Uniti, Clearview sosteneva che la normativa europea non potesse trovare applicazione nei suoi confronti. Di diverso avviso è stata l'Autorità di Amburgo, allorquando ha sostenuto che se le azioni di una società americana interessano cittadini europei, il titolare del trattamento è in ogni caso soggetto all'applicazione della normativa eurounitaria.

---

[55] Analoga è la vicenda che ha interessato, qualche mese dopo quella svedese, il Garante belga, che nel corso di un'ispezione ha appurato che i servizi della società che raccoglieva i dati erano utilizzati anche dalla polizia federale belga, così come confermato dal ministero dell'Interno. Quest'ultimo, peraltro, ha ammesso l'illegittimità dell'utilizzo di tali dispositivi, i quali, a seguito dell'intervento dell'Autorità a protezione dei dati personali, sono stati bloccati.

[56] Autorità di controllo tedesca del Land di Amburgo, decisione n. 545/2020.

La questione attiene, in sostanza, alla *vis attractiva* del GDPR e, in particolare, all'estensione di quest'ultimo oltre i confini territoriali dell'Unione europea[57], conformemente anche alle indicazioni della Corte di Giustizia[58]. È appena il caso di ricordare che prima dell'emanazione del GDPR, la normativa comunitaria trovava applicazione nel solo caso in cui si vi fosse un titolare del trattamento stabilito all'interno del territorio europeo ovvero nell'ipotesi in cui all'interno dei confini dell'Unione Europea fossero localizzati gli strumenti impiegati per il trattamento dei dati personali. Con l'avvento del GDPR, di contro, è stato ampliato l'ambito di applicazione oggettivo e soggettivo della normativa, mediante l'inserimento di quei servizi che, pur essendo fisicamente stabiliti fuori dall'UE, si rivolgono ai cittadini europei[59].

Allo stesso tempo, deve osservarsi che le determinazioni assunte dalle autorità garanti nazionali non esplicano i propri effetti al di fuori del territorio nazionale e, di conseguenza, non trovano applicazione in tutti gli ordinamenti appartenenti all'Unione europea, ma soltanto in quelli ove vengono proposti reclami o nei quali le autorità hanno avviato un'attività di indagine volta alla sanzione dei soggetti che raccolgono i dati biometrici[60].

---

[57] È opportuno ricordare che, sulla scorta delle indicazioni fornite dalle "Guidelines 3/2018 on territorial scope", adottate dallo European Data Protection Board il 12 novembre 2019, è richiesto che la condotta del "*titolare del trattamento, che determina i mezzi e gli scopi del trattamento stesso" sia idonea a dimostrare la sua intenzione di offrire beni o servizi a un interessato che si trova nell'Unione*" (cfr. par. 2.a delle Guidelines). Inoltre, il Considerando 23 del GDPR stabilisce che, "*mentre la semplice accessibilità del sito web del titolare del trattamento, del responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica o di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il titolare del trattamento è stabilito sono insufficienti per accertare tale intenzione, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione possono evidenziare l'intenzione del titolare o del responsabile del trattamento di offrire beni o servizi agli interessati nell'Unione*".

[58] Cfr. *Pammer/Reederei Karl Schlüter GmbH & Co e Hotel Alpenhof/Heller* (cause riunite C-585/08 e C-144/09) nella quale si indicano tra i fattori per valutare se un'attività commerciale svolta da un soggetto sia diretta nei confronti di uno Stato membro, il riferimento alla cittadinanza europea nell'ambito dell'offerta, la lingua utilizzata, la valuta per mezzo della quale possono essere effettuati i pagamenti, ecc.

[59] Una soluzione, peraltro, seguita anche da alcuni ordinamenti extracomunitari, da ultimo la Cina, che hanno adottato il medesimo modello, ricomprendendo nell'ambito di applicazione nazionale i trattamenti che avvengono al di fuori dei propri confini.

[60] Clearview è stata oggetto di una indagine anche da parte del CNIL, l'Autorità francese, che, nel dicembre 2021, ha disposto un ordine di blocco nei confronti della società

Ciononostante, a parte i numerosi interventi delle varie autorità nazionali, giova segnalare che il ricorso ai servizi di ClearView, con motivazioni analoghe, è stato considerato illegittimo anche dall'ICO nel Regno Unito[61] e dall'OAIC (Office of the Australian Information Commissioner), l'autorità competente sull'applicazione dell'*Australian Privacy Act*[62]. Infine, il *Privacy Commissioner* canadese ha egualmente bloccato l'applicazione, affermando che la stessa raccogliesse "*highly sensitive biometric information without the knowledge or consent of individuals*" e che "*collected, used and disclosed Canadians' personal information for inappropriate purposes, which cannot be rendered appropriate via consent*"[63]. Quest'ultima affermazione appare particolarmente pregnante, giacché spiega che, vista la tipologia di informazioni personali e l'utilizzo che ne viene compiuto, il consenso non potrebbe comunque costituire una base giuridica adeguata.

Venendo al caso italiano, il provvedimento del Garante privacy non si discosta di molto da quelli resi dagli omologhi europei ed anglosassoni appena considerati. Meritano, però, di essere analizzati in dettaglio alcuni elementi delle difese spiegate dalla società statunitense. *In primis*, facendo riferimento alle indagini svolte dal Garante svedese, ClearView ha sostenuto di non esser più interessata ad espandersi sul mercato europeo e che quelli utilizzati in Europa fossero dei meri strumenti di prova. La società ha inoltre contestato che fosse stato svolto un monitoraggio dei cittadini europei – precondizione per l'applicazione del GDPR, alla luce del Considerando n. 24 dello stesso –, dal momento che, a parte la raccolta e la conservazione del dato, non vi erano ulteriori trattamenti e, quindi, non si realizzava un effettivo monitoraggio, non essendo stato generato un profilo analitico dell'utente.

Ad ogni modo, il Garante, con il provvedimento in esame (n. 50 del 10 febbraio 2022), ha dichiarato illecito il trattamento di Clearview, disponendo il divieto di prosecuzione del trattamento stesso e di ulteriore raccolta, nonché la cancellazione dei dati comuni e biometrici, e la condanna

statunitense, ritenuta colpevole di un trattamento non fondato su una base giuridica adeguata, ai sensi dell'articolo 6 del GDPR, nonché per non aver risposto alle istanze formulate dai soggetti interessati ai sensi degli articoli 12,15 e 17 del GDPR.

[61] Il provvedimento sanzionatorio è disponibile al seguente link: https://ico.org.uk/action-weve-taken/enforcement/clearview-ai-inc-mpn/.

[62] Clearview AI, Inc. (Privacy) [2021] AICmr54 (14 october 2021), consultabile al seguente URL: https://www.oaic.gov.au/__data/assets/pdf_file/0016/11284/Commissioner-initiated-investigation-into-Clearview-AI,-Inc.-Privacy-2021-AICmr-54-14-October-2021.pdf

[63] Cfr. Office of the Privacy Commissioner of Canada, *Clearview AI's unlawful practices represented mass surveillance of Canadians, commissioners say*, February 3, 2021.

al pagamento della somma di venti milioni di euro a titolo di sanzione amministrativa pecuniaria.

7. Le tecniche di riconoscimento biometrico nella Proposta di Regolamento sull'intelligenza artificiale del 2021

Il quadro regolatorio sin qui prospettato va arricchito con il riferimento alle tecniche di riconoscimento biometrico operato dalla Proposta di Regolamento in materia di intelligenza artificiale, pubblicata dalla Commissione nel mese di aprile 2021[64].

Il modello regolatorio su cui si fonda quest'ultima appare proteso alla gestione efficiente dei rischi sottesi all'uso dei dispositivi di intelligenza artificiale, nell'ottica di garantire la tutela dei diritti fondamentali e la struttura democratica[65]. Il documento risponde altresì alle istanze, sempre più diffuse, di un intervento legislativo in grado di proteggere, per un verso, il buon funzionamento del mercato interno dei sistemi di intelligenza artificiale, per l'altro, il consolidamento dell'Unione Europea a livello globale come leader nello sviluppo di un'intelligenza artificiale sicura, affidabile ed etica[66]. Nello specifico, gli obiettivi espressamente dichiarati sono i seguenti: i) assicurare che i sistemi di IA immessi e utilizzati sul mercato dell'Unione siano sicuri e rispettino la normativa vigente in materia, nonché i diritti fondamentali e valori dell'Unione; ii) assicurare la certezza del diritto per facilitare gli investimenti e l'innovazione nell'intelligenza artificiale; iii) migliorare la *governance* e l'applicazione effettiva della normativa esistente in materia di diritti fondamentali e requisiti di sicurezza applicabili ai sistemi di IA; iv) facilitare lo sviluppo di un mercato unico per applicazioni di IA lecite, sicure e affidabili, nonché prevenire la frammentazione del mercato[67].

---

[64] 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, COM(2021) 206 final.

[65] Come sottolinea G. Resta, *Cosa c'è di 'europeo' nella Proposta di Regolamento UE sull'intelligenza artificiale?*, in *Dir. inf.*, 2022, p. 323 ss. "*questa impostazione è propria dell'approccio europeo sin dai primi documenti redatti dal Parlamento Europeo, dalla Commissione e dall'High Level Expert Group on Artificial Intelligence, tutti convergenti nel dare concreta attuazione alla linea giuspolitica per cui devono essere i diritti fondamentali (e il parco di valori europei che in essi si riflettono) a guidare lo sviluppo del mercato e non viceversa*".

[66] G. Finocchiaro, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Dir. inf.,* 2022, p. 303 ss.

[67] T.E. Frosini, *L'orizzonte giuridico dell'intelligenza artificiale*, in *Dir. inf.*, 2022, p. 5 ss.

Quanto alla biometria, essa è presa in considerazione soprattutto per quel che concerne le tecniche di identificazione. Innanzitutto, partendo dall'ambito definitorio, l'art. 3, n. 33, definisce i dati biometrici 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*"[68], là dove, invece il considerando n. 8 qualifica i sistemi di identificazione biometrica remota come sistemi di IA destinati "*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 sapere in anticipo se la persona interessata sarà presente e può essere identificata, a prescindere dalla tecnologia, dai processi o dai tipi specifici di dati biometrici utilizzati*"[69].

Lo stesso considerando n. 8 prosegue proponendo una distinzione, ribadita anche dall'art. 3, nn. 37 e 38, tra sistemi di identificazione biometrica remota "in tempo reale" e "a posteriori". Nei primi, il rilevamento dei dati biometrici, il confronto e l'identificazione vengono posti in essere istantaneamente o, in ogni caso, senza ritardi significativi, in quanto basati sull'uso di materiale "dal vivo" o "quasi dal vivo", come, ad esempio, i filmati generati da una telecamera o da un altro dispositivo con funzionalità analoghe. Di contro, nei sistemi di identificazione "a posteriori", i dati biometrici sono già stati rilevati e il confronto e l'identificazione avvengono soltanto con un ritardo significativo, come nel caso di telecamere a circuito chiuso o di dispositivi privati, che generano il filmato prima che il sistema sia utilizzato in relazione alle persone fisiche interessate.

Ciò posto, l'art. 5, par. 1, lett. d) vieta espressamente l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, a meno che e nella misura in cui tale uso sia strettamente necessario per uno dei seguenti obiettivi: i) la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi; ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico; iii) il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato di cui all'art. 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio in tema di mandato d'arresto europeo, punibile nello Stato membro interessato con una pena o

[68] In coerenza con il considerando n. 7, il quale chiarisce espressamente che la nozione di dati biometrici utilizzata nel testo del regolamento "*è in linea e dovrebbe essere interpretata in modo coerente*" con la nozione di dati biometrici di cui all'art. 4, par. 14, GDPR.

[69] La definizione è poi ribadita dall'art. 3, n. 36.

una misura di sicurezza privativa della libertà della durata massima di almeno tre anni.

In tali ipotesi l'uso del sistema di identificazione biometrica deve necessariamente tenere in considerazione la natura della situazione che dà luogo al possibile uso, con specifico riguardo alla gravità, probabilità ed entità del danno causato dal mancato uso del sistema, e le conseguenze dell'uso del sistema per i diritti e le libertà di tutte i soggetti coinvolti. L'uso è inoltre lecito soltanto se è autorizzato da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro in cui deve avvenire, salvo il caso di una situazione di urgenza straordinaria e giustificata, in cui è possibile iniziare a usare il sistema senza autorizzazione e richiedere l'autorizzazione solo in un momento successivo.

Il controllo dell'autorità giudiziaria o amministrativa competente che rilascia l'autorizzazione consiste nell'accertamento circa la sussistenza, sulla base di prove oggettive, che l'uso del sistema di identificazione biometrica remota "in tempo reale" sia necessario e proporzionato al conseguimento di uno degli obiettivi summenzionati.

Le cautele appena esposte si rendono imprescindibili alla luce dell'invasività dei sistemi di identificazione biometrica, che, difatti, la Proposta annovera tra i "Sistemi di IA ad alto rischio", intesi come sistemi in grado di porre in pericolo i diritti fondamentali delle persone fisiche e che, di conseguenza, possono essere utilizzati soltanto in presenza di stringenti requisiti[70].

8. Nuove forme di biometria

L'analisi svolta nei paragrafi precedenti ha dimostrato che l'approccio normativo alla biometria è fondato sull'ambito definitorio, nel senso che la normativa in materia di privacy si preoccupa, innanzitutto, di offrire una qualificazione del dato personale, individuando le ipotesi nelle quali il coinvolgimento di uno specifico aspetto determina la caratterizzazione del dato comune.

Occorre allora domandarsi se tali definizioni, coniugate con quella di trattamento dei dati, siano idonee a disciplinare talune nuove forme di rilevazione del dato biometrico. Si allude, in particolare, a quelle nuove tecnologie che consentono – come si accennava in precedenza –

[70] L'elenco completo di tali sistemi è fornito dall'Allegato III alla Proposta, richiamato espressamente dall'art. 6, par. 2.

l'identificazione dell'utente per mezzo di un elemento biometrico, per una frazione di secondo, senza conservazione del dato e senza possibilità tecnica di risalire all'identità dell'utente stesso.

Ciò è reso possibile mediante un sistema c.d. di *privacy preserving*. Siffatta soluzione rientra difatti all'interno delle cc.dd. *untraceable biometrics technologies,* ossia le tecnologie che mettono in atto una modalità di trasformazione del dato biometrico, a partire dall'impronta digitale o dalla forma del volto, tale da non permetterne una successiva riconduzione al soggetto e quindi alla sua identità, preservandone così l'integrità e l'immodificabilità[71].

La soluzione consiste in una prima fase di *enrollement,* durante la quale l'utente effettua una registrazione del proprio dato biometrico su di un software attraverso il proprio dispositivo, generando un *template* dello stesso. Tale dato tuttavia non è soggetto ad alcuna registrazione o conservazione e viene immediatamente convertito e scomposto irreversibilmente in stringhe crittografate di numeri (*public keys)*, che sono inviate ad un insieme di nodi della rete proprietaria del titolare del trattamento. Il risultato della soluzione in esame è quello di veicolare nella rete una stringa numerica che non rappresenta l'impronta biometrica dell'utente, la quale viene trasformata in modo irreversibile per garantire l'impossibilità di associarla con l'utente stesso. Inoltre, la stringa è distribuita in quote diverse in vari nodi della stessa (*secret sharing*), cosicché ogni nodo non è in grado individualmente di ricostruire la stringa e viene impedita l'individuazione della transazione o dell'operazione sulla base delle informazioni di un solo nodo[72]. Il *template* iniziale creatosi dal dato biometrico viene poi distrutto, con la conseguente impossibilità di accesso al dato biometrico, nonché della sua conservazione, trasmissione o diffusione. Tuttavia, la circostanza per cui, seppur per un lasso temporale estremamente esiguo, l'informazione biometrica sia utilizzata, determina che si rientri nell'ambito di applicazione dell'art. 4 GDPR[73].

---

[71] Sul tema si vedano i saggi contenuti in P. Campisi (ed.), *Security and Privacy in Biometrics*, London, 2013.

[72] Sul rapporto tra tecniche crittografiche e nuove tecnologie si v., tra gli altri, F. Delfini, "Blockchain", "Smart Contracts" *e innovazione tecnologica: l'informatica e il diritto dei contratti* in *Riv. dir. priv.*, 2019, p. 167 ss.

[73] Cfr. art. 4 del GDPR, a mente del quale *"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"*.

Per un altro verso, la presenza di un dato personale e di un riconnesso trattamento comporta che l'eventuale anonimizzazione del dato avviene solo in un momento successivo al *matching* tra l'identità del soggetto e il dato biometrico utilizzato. Al riguardo, è appena il caso di rammentare che i dati anonimi non sono regolati da parte del GDPR, eccezion fatta per una menzione nel Considerando n. 26, dove si legge che "(…) *i principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca*".

Con il parere 5/2014, sulle tecniche di anonimizzazione, il *Working Party* afferma che l'anonimizzazione potrebbe costituire una strategia valida per preservare i vantaggi e attenuare i rischi; difatti, una volta che un insieme di dati viene reso effettivamente anonimo e le persone non sono più identificabili, le norme dell'Unione in materia di protezione dei dati non sono applicabili[74].

Le tecnologie in esame, quindi, potrebbero determinare un'anonimizzazione del dato, ossia una de-identificazione irreversibile dello stesso, ma soltanto in un momento successivo.

Si tratta, però, a parere di chi scrive, di considerare anche i vantaggi che tali forme di raccolta delle informazioni biometriche potrebbero

[74] Dalla lettura del parere citato nel testo emerge con chiarezza la difficoltà di creare un insieme di dati effettivamente anonimo a partire da un ampio agglomerato di dati personali, preservando al contempo tutte le informazioni necessarie per espletare l'attività richiesta. Ad esempio, un insieme di dati considerato anonimo potrebbe essere combinato con un altro insieme di dati in maniera tale da consentire l'identificazione di una o più persone. In merito all'anonimizzazione si segnalano, di seguito, alcuni tratti peculiari: i) essa può essere il risultato del trattamento di dati personali allo scopo di impedire irreversibilmente l'identificazione della persona interessata; ii) possono essere previste diverse tecniche di anonimizzazione, attesa l'assenza di norme prescrittive nella legislazione dell'Unione; iii) deve essere attribuita importanza agli elementi contestuali, e, segnatamente, all'insieme degli strumenti che possono essere ragionevolmente utilizzati per l'identificazione da parte del responsabile del trattamento o di altri, prestando particolare attenzione a ciò che ultimamente, allo stato attuale della tecnologia, è diventato "ragionevolmente utilizzabile" (dato l'incremento della potenza di calcolo e degli strumenti disponibili); iv) l'anonimizzazione presenta un fattore di rischio intrinseco, sicché occorre tenerne conto nel valutare la validità di qualsiasi tecnica di anonimizzazione – compresi gli impieghi possibili dei dati "resi anonimi" mediante tale tecnica – e vanno soppesate la gravità e la probabilità di tale rischio.

determinare in termini di minimizzazione dei dati e di esclusione della conservazione, nonché i loro utilizzi anche per finalità virtuose.

Si pensi, a titolo esemplificativo, alla possibilità di adottare tali tecnologie per identificare l'età dei minori e prevenirne l'accesso a siti riservati ai maggiorenni. Il Regno Unito, ad esempio, si accinge a varare una legge che impone ai siti pornografici di installare un dispositivo di verifica dell'età, prevedendo sanzioni, in caso di inottemperanza, che possono arrivare fino al 10 per cento del fatturato[75].

Probabilmente, adottare un'interpretazione assiologica delle definizioni di dati personali e di trattamento degli stessi dovrebbe condurre a incentivare l'uso di tali tecnologie, anziché a ostacolarle, nella consapevolezza che i rischi di distopie potrebbero essere temperati dall'uso dei dati per finalità sociali ed esclusivamente per un lasso di tempo minimo. In altri termini, possiamo ammettere che il trattamento dei dati si verifichi nel solo caso in cui vi siano dei rischi ai diritti e alle libertà dei cittadini e, occorre, quindi, ripensare tali definizioni, in un'ottica meno formalistica e più sostanzialistica?

***

ABSTRACT: The issues related to biometric data and the growing use of artificial intelligence technologies have reinvigorated the debate on the need to find solutions that do not violate the fundamental rights involved but, at the same time, do not completely forego the advantages that this technologies can give. By examining some recent IT solutions that envisage the use of biometric data for the recognition of individuals without data retention, this paper intends to provide an innovative perspective that takes into account technological innovations designed in the light of a greater compliance with the current legislation and the minimisation of data processing and retention.

KEYWORDS: biometric data - biometric identification systems - untraceable biometrics technologies - biometric templates

***

Tommaso Sica - Dottore di ricerca in diritto privato, Università degli Studi Roma Tre (tommaso.sica@uniroma3.it)

[75] Il testo della proposta, definito *Online Safety Bill*, è consultabile sul sito del Parlamento del Regno Unito, al seguente link: https://publications.parliament.uk/pa/bills/cbill/58-03/0004/220004.pdf.