

SABRINA EL SABI

LA TUTELA DELLA *PRIVACY* NEL TRATTAMENTO DEI DATI BIOMETRICI E GENETICI PER SCOPI DI PUBBLICA SICUREZZA. SPUNTI DI DIRITTO COMPARATO

SOMMARIO: 1. Introduzione. — 2. GDPR e trattamento dei dati biometrici e genetici. — 3. La pronuncia della CGUE nella Causa C-205/21. — 4. Dati biometrici e genetici tra GDPR e Direttiva LED: discipline a confronto. — 5. L'*Artificial Intelligence Act* e i dati biometrici. — 6. Il principio di proporzionalità e il rischio di pregiudizi ai diritti e alle libertà dell'individuo. — 7. Il trattamento dei dati biometrici e genetici nell'esperienza americana: *law enforcement* e il IV Emendamento. — 8. Brevi cenni conclusivi.

1. INTRODUZIONE.

Negli ultimi anni si è diffusa sempre più la necessità di raccogliere dati biometrici e genetici per il loro peculiare utilizzo nel mondo della ricerca scientifica e, soprattutto, nel più complesso universo digitalizzato, dettato dal costante progresso tecnologico. In tal modo, il repentino sviluppo di questo specifico settore — che determina la traslazione fra dato e persona, quando la disciplina sulla tutela dei dati personali incrocia la materia dei dati biometrici e genetici — ha reso alquanto complessa l'opera di qualificazione di tali peculiari tipologie di dati e, in modo più incisivo, del loro trattamento¹. Nello specifico, occorre soffermarsi sul più comune e tradizionale uso che di questa particolare categoria di dati viene fatto: la lotta alla criminalità e la tutela della pubblica sicurezza. Proprio a riguardo, particolare questione — peraltro di recente sottoposta al vaglio della Corte

* Il presente lavoro è stato realizzato nell'ambito del progetto di ricerca "Assistenza olistica Intelligente per l'Active ageing in ecosistemi indoor e outdoor - AmICA", Università degli studi di Bari "Aldo Moro".

¹ F. ROSSI DAL POZZO, *La tutela dei*

dati personali nella giurisprudenza della Corte di giustizia, in *Quaderni Aiusde*, 1, 2019, 127 ss., consultabile al seguente link <https://www.aisdue.eu/rossi-dal-pozzo-la-giurisprudenza-della-corte-di-justizia-sul-trattamento-dei-dati-personali/>.

lussemburghese ² — è emersa con riferimento alla possibilità di raccogliere coattivamente i dati biometrici e genetici, in modo da consentire il loro utilizzo per finalità strettamente connesse alla pubblica sicurezza (prevenzione, lotta al crimine e la sua contestuale repressione). Le questioni pregiudiziali più interessanti sottoposte alla Corte riguardano, più nel dettaglio, la violazione della *privacy*, dovuta alla registrazione “sistematica” dei dati biometrici e genetici anche degli accusati formalmente di reato, nonché la possibilità di ottenere coattivamente detti dati nel caso in cui la persona sia indagata per un reato doloso procedibile d’ufficio. L’autorità competente, sostiene la CGUE, è tenuta pertanto a verificare e a dimostrare che tale raccolta sia assolutamente/strettamente necessaria per il conseguimento degli obiettivi specifici perseguiti e, inoltre, che tali obiettivi non possono essere raggiunti mediante misure che costituiscono « un’ingerenza meno grave nei diritti e nelle libertà della persona interessata ³ ».

2. GDPR E TRATTAMENTO DEI DATI BIOMETRICI E GENETICI.

Prima di entrare nel merito della questione, occorre soffermarsi sulla evoluzione della nozione di dati biometrici e genetici, tracciando brevemente la disciplina che regola tale “particolare” categoria di dati ⁴.

Per lungo tempo, queste tipologie di dati personali, nonostante le differenti nozioni ⁵ — sì divergenti, ma con caratteristiche

² V., *infra*, par. 3.

³ Cfr. Corte giust. UE, 26 gennaio 2023, C-205/21, *procedimento penale a carico di V.S.*, ECLI:EU:C:2023:49, punto 35 della pronuncia, consultabile al seguente link <https://curia.europa.eu/juris/document/document.jsf?jsessionid=E062811C425824B19762D73075B061F0?text=&docid=269704&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=245630>. Sulla questione, si consulti la nota di B. RUBIS, *Sistemi di autenticazione mediante l'utilizzo di dati biometrici*, in questa Rivista, 2023, 264 ss.

⁴ In proposito, tra gli strumenti giuridici che attualmente regolamentano il trattamento dei dati biometrici e genetici in tutta Europa rilevano: il Regolamento (UE) 2016/679 (GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, la Direttiva (UE) 2016/680 sulla protezione dei dati per le autorità di polizia e di giustizia penale (Direttiva LED), il Regolamento (UE) 2018/1725, 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, nonché, in seguito alla sua modernizzazione avvenuta nel 2018, la Convenzione del Consiglio d’Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale del 1981 (Convenzione 108).

⁵ Sulle diverse nozioni di “dati biometrici” si considerino quella fornita dal Comitato Nazionale per la Bioetica (CNB), secondo cui la biometria è, quindi, i dati biometrici sono considerati una nuova tecnica « di identificazione o “misurazione” dell’essere umano attraverso la rilevazione di determinate caratteristiche fisiche e comportamentali che vengono tradotte in sequenze matematiche e conservate in banche dati elettroniche » (CNB, *L’identificazione del corpo umano: profili bioetici della biometria*, 2010, 3, consultabile al link <https://bioetica.governo.it/it/pareri/pareri-e-risposte/1-identificazione-del-corpo-umano-profilo-bioetico-della-biometria/>); quella del Gruppo di lavoro — WP193 — Articolo 29 per la tutela dei dati personali, parere 3/2012, su-

comuni — già fornite da diverse istituzioni e autorità, sono state oggetto di incertezza definitoria.

Tuttavia, la lunga evoluzione di cui è stata protagonista tale categoria di dati (con riguardo, nello specifico, alla qualificazione giuridica dei medesimi) è culminata definitivamente con l'avvento del GDPR, il quale ha introdotto una definizione dei medesimi all'interno dell'art. 4, par. 1, nn. 13) e 14).

Dunque, per “dati biometrici” si intendono quei « 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, par. 1, n. 14); i “dati genetici”, invece, sono quei « dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione » (art. 4, par. 1, n. 13).

A ben vedere, la natura indelebile dell'informazione genetica e le sue potenziali implicazioni per il trattamento discriminatorio la rendono particolarmente sensibile ⁶.

In generale, i dati biometrici sono quei dati personali che

gli sviluppi nelle tecnologie biometriche, che li ha identificati come quei dati ricavati da « proprietà biologiche, aspetti comportamentali, caratteristiche fisiologiche, tratti biologici o azioni ripetibili laddove tali caratteristiche 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 » (consultabile nell'apposito archivio presente al seguente link https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec6); infine, quella indicata nel 2014 dall'Autorità Garante per la protezione dei dati personali, la quale, nelle *Linee guida in materia di riconoscimento biometrico e firma grafometrica* (consultabili al seguente link <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3132361>), ha ripreso la descrizione di dati biometrici fornita dal Gruppo di lavoro.

Quanto ai “dati genetici”, differenti nozioni sono, invece, state fornite dalla stessa Autorità Garante nel 2007, per la quale si considerava dato genetico « il dato che, indipendentemente dalla tipologia, riguarda la costituzione genotipica di un individuo, ovvero i caratteri genetici trasmissibili nell'ambito di un gruppo di individui legati da vincoli di parentela » (si veda, in proposito,

L'autorizzazione al trattamento dei dati genetici del 22 febbraio 2007 [1389918], reperibile al seguente link <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1389918>); dal Consiglio d'Europa nel 1997, secondo cui tale espressione « si riferisce a tutti i dati, di qualunque tipo, che riguardano i caratteri ereditari di un individuo o che sono in rapporto con quei caratteri che formano il patrimonio di un gruppo di individui affini » (così la Raccomandazione N. R (97) 5 del Comitato dei ministri agli stati membri, relativa alla protezione dei dati sanitari, adottata dal Comitato dei ministri il 13 febbraio 1997 e consultabile al seguente link <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1798880>); e, infine, dall'Unesco nel 2003, nella Dichiarazione internazionale sui dati genetici umani, per cui, all'art. 2, i dati genetici umani sono « *Information about heritable characteristics of individuals obtained by analysis of nucleic acids or by other scientific analysis* » (disponibile al seguente link <https://www.unesco.org/en/legal-affairs/international-declarations-on-human-genetic-data>).

⁶ Cfr. A. IANNUZZI-F. FILOSA, *Il trattamento dei dati genetici e biometrici, in dirittifondamentali.it*, 2, 2019, 2 ss., consultabile al seguente link <https://dirittifondamentali.it/2019/07/11/il-trattamento-dei-dati>

derivano da caratteristiche fisiche o comportamentali uniche e, pertanto, identificative di ciascun individuo (si pensi alle impronte digitali, alla particolare conformazione fisica della mano o del volto, dell'iride o della retina, alla firma grafometrica ⁷ nonché al timbro e alla tonalità della voce). Di conseguenza, oltre alle loro specificità, i dati in questione hanno delle caratteristiche tali da identificare in modo univoco una persona fisica ⁸.

Il Regolamento, pertanto, non ha fatto altro che uniformare la disciplina ⁹, non solo individuando una precisa nozione universale del dato biometrico e genetico, ma soprattutto tracciando una regolamentazione sul loro utilizzo, disposta ex art. 9 del predetto Regolamento, rubricato appunto "Trattamento di categorie particolari di dati personali".

Nello specifico, soffermando l'attenzione sui dati biometrici, può rilevarsi che i medesimi vengono più attualmente impiegati per quanto concerne quei dispositivi destinati ad uso personale di tecnologie informatiche e di *software*.

Ad esempio, le impronte digitali sono utilizzate ormai da tempo come strumento di autenticazione per l'attivazione di dispositivi elettronici, mentre appare più recente l'introduzione di tecnologie destinate al riconoscimento facciale, alla scansione dell'iride e al riconoscimento della struttura vascolare dell'occhio o del palmo delle mani ¹⁰.

In concreto, tali particolari dati personali possono essere raccolti mediante l'impiego di sistemi informatici di riconoscimento biometrico, il cui funzionamento si fonda prevalentemente su due elementi: una componente *hardware* acquisisce il dato biometrico (si pensi, ad esempio, al sensore per il riconoscimento dell'impronta digitale integrato in molti modelli di *smartphone* di ultima generazione); successivamente, interviene un *software* che consente, attraverso l'impiego di algoritmi, di analizzare i dati rac-

genetici-e-biometrici/; E. J. KINDT, *Having Yes, Using No? About the New Legal Regime for Biometric Data*, in *Computer Law and Security Review*, 3, 2018, 12 ss.; C. JASSERAND, *Legal Nature of Biometric Data: From 'Genetic' Personal Data to Sensitive Data: Which Changes Does the New Data Protection Framework Introduce?*, in *European Data Protection Law Review (EDPL)*, 2 (3), 2016, 297 ss.; R. DUCATO, *I dati biometrici*, in V. CUFFARO-R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 1301 ss.

⁷ Si veda G. D. FINOCCHIARO, *La metafora e il diritto nella normativa sulla cosiddetta "firma grafometrica"*, in questa Rivista, 1, 2013, 1 ss.

⁸ Così, G. ZICCARDI-P. PERRI, *Diziona-*

rio Legal Tech, Milano, Giuffrè, 2020, 314 ss.

⁹ B. WONG, *Delimiting the Concept of Personal Data After The GDPR*, *Legal Studies*, in *The Journal of the Society of Legal Scholars*, 39 (3), 2019, 517 ss.; M. SHABANI-P. BORRY, *Rules for Processing Genetic Data For Research Purposes in View of the new EU General Data Protection Regulation*, in *European Journal of Human Genetics*, 26, 2, 2018, 149 ss., consultabile al seguente link <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5838983/>; G.D. FINOCCHIARO, *Introduzione del Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civili commentate*, 1, 2017, 1 ss.

¹⁰ V. ancora A. IANNUZZI-F. FILOSA, *Il trattamento dei dati genetici e biometrici*, cit., 2 ss.

colti e di confrontarli con quelli acquisiti e conservati precedentemente nella banca dati del sistema, in modo da associare il dato raccolto alla specifica persona e identificarla sulla base di tali informazioni ¹¹.

Dunque, l'impiego dei dati biometrici e genetici, la cui principale caratteristica, come ormai noto, è data dalla loro unicità, mira al perseguimento di uno scopo ben preciso: facilitare la vita dell'individuo. Si pensi all'utilizzo dei dati biometrici per l'accesso a luoghi di lavoro riservati ¹² oppure, come anticipato, al loro utilizzo come misura di sicurezza per i dispositivi elettronici (sbloccare lo *smartphone* o il *tablet* con l'impronta digitale e/o attraverso il riconoscimento facciale).

Tuttavia, dall'utilizzo di questi dati possono derivare non solo effetti positivi, connessi al ruolo di ausiliari da questi svolto — con l'obiettivo di incrementare e facilitare il livello di sicurezza — ma anche una serie di effetti negativi: l'adozione illimitata dei medesimi porterebbe ad una insensibilità delle conseguenze che il trattamento dei dati particolari possa avere sulla vita dei soggetti, essendo immediatamente evidenti soltanto le agevolazioni nella quotidianità ¹³.

Inoltre, la numerosa quantità di informazioni che possono raccogliersi sugli individui, ad opera dell'elaborazione dei dati biometrici e genetici nonché dalla natura unica del DNA, presuppone l'esercizio di un conforme controllo sui medesimi mediante il ricorso ad efficaci meccanismi di protezione della *privacy* ¹⁴.

Pertanto, come è facilmente intuibile, l'utilizzo di questa delicata tipologia di dati personali richiede la rigida osservanza di una serie di cautele, al fine di evitare che si verifichino dei pregiudizi a danno dei soggetti interessati ¹⁵.

In effetti, se da un lato, i sistemi di riconoscimento biometrico

¹¹ V. GPDP, *Linee-guida in materia di riconoscimento biometrico e firma grafometrica*, Serie generale — n. 280, 2014, 84 ss., consultabile al seguente link <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/3556992>.

¹² L. VIZZONI, *Badge, algoritmi e identificazione dei lavoratori: la Cassazione e il trattamento dei dati biometrici*, in *Responsabilità Civile e Previdenza*, 4, 2019, 1230 ss. Sul trattamento dei dati biometrici nei luoghi di lavoro si veda, altresì, F. CONTE, *Il trattamento dei dati biometrici nei luoghi di lavoro. Analisi comparata tra l'esperienza italiana e tedesca*, in questa Rivista, 2023, 309 ss.

¹³ L. CALIFANO, *I diritti e le garanzie degli interessati nel regolamento europeo 2016/679*, in *Cultura giuridica e diritto vivente*, 10, 2022, 1 ss., consultabile al link

<https://journals.uniurb.it/index.php/cgd/article/view/3394/2973>.

¹⁴ P. TARALLO, *GDPR, che si intende per dati personali: natura, tipologie e qualità dei dati sensibili*, in *Agenda Digitale*, 2019, consultabile al seguente link <https://www.agendadigitale.eu/cittadinanza-digitale/gdpr-che-si-intende-per-dati-personali-natura-tipologie-e-qualita/>.

¹⁵ G. GIANNONE CODIGLIONE, *Risk-based approach e trattamento dei dati personali*, in S. SICA-V. D'ANTONIO-G. M. RICCIO (a cura di), *La nuova disciplina della privacy*, Padova, CEDAM, 2016, 55 ss.; Id., *La tutela della riservatezza*, in S. SICA-V. ZENO-ZENCOVICH (a cura di), *Manuale di diritto dell'informazione e della comunicazione*, Milano, Wolters Kluwer - CEDAM, 2019, 281 ss.; V. ZENO-ZENCOVICH, *Do "Data Markets" Exist?*, in *MediaLaws*, 2, 2019, 13 ss.

favoriscono il livello di sicurezza per l'utente che fa uso dei dispositivi elettronici, dall'altro, trattandosi di dati "particolari", potrebbero generare effetti negativi per l'interessato, derivanti dall'indebito o non autorizzato utilizzo dei medesimi, scostandosi dai propositi per cui sono stati concretamente acquisiti dal sistema.

Tali considerazioni risultano di preminente rilevanza ove si volesse riflettere sulla determinante incidenza dei dati biometrici (ed anche genetici) sulla libertà delle persone e sulla dignità umana ¹⁶.

Una delle ipotesi in cui verrebbe a configurarsi una conseguenza del genere riguarda il caso in cui il trattamento dei dati biometrici e genetici venga richiesto soprattutto per finalità penali (di prevenzione e di lotta alla criminalità), uno degli usi più tradizionali, appunto, che di tale specifica categoria di dati viene fatto ¹⁷.

Per queste ragioni, il GDPR, all'art. 9, par. 1, pone un generale divieto di trattamento dei « dati biometrici intesi ad identificare in modo univoco una persona fisica », introducendo così, per tali dati, una disciplina normativa particolarmente rigida. Tuttavia, tale disposizione viene mitigata, al par. 2 del medesimo articolo, per il tramite di un elenco tassativo di casi in cui il trattamento di tali dati è consentito al verificarsi di una delle seguenti ipotesi: quando l'interessato ha dato il proprio consenso esplicito al trattamento dei dati personali per uno o più specifici utilizzi (come avviene per il caso dell'autenticazione tramite impronta digitale e purché la legge, nazionale o europea che sia, non vieti comunque il trattamento di tali dati per determinate finalità); quando tale trattamento è effettuato nell'ambito di rapporti di lavoro e di previdenza; quando l'impiego di questi particolari dati personali si rende necessario per proteggere un interesse vitale dell'interessato o di un'altra persona fisica, quando il soggetto cui i dati si riferiscono si trova in una situazione di incapacità, fisica o giuridica, di prestare direttamente il proprio consenso per tale utilizzo; nell'ambito di un procedimento giudiziario e, in particolare, per accertare, esercitare o difendere un diritto, tanto in sede amministrativa quanto stragiudiziale; per motivi di particolare interesse pubblico, di ricerca scientifica o storica, previsti dalla legge, e purché l'impiego di dati biometrici risulti proporzionato

¹⁶ 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*, 68, 109, 3, 2022, 123 ss., consultabile al seguente link <https://www.ildirittodelleconomia.it/2023/01/08/danil-a-iacovelli-marco-fontana-nuove-sfide-della-tecnologia-e-gestione-dei-rischi-nella-pro>

posta-di-regolamento-europeo-sull'intelligenza-artificiale-set-di-training-algoritmi-e-qualifica/.

¹⁷ L. SCAFFARDI, *Dati genetici e biometrici: nuove frontiere per le attività investigative*, in L. SCAFFARDI (a cura di), *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, Torino, Giappichelli, 2018, 37 ss.

alla finalità perseguita, rispetti il diritto alla protezione dei dati e siano comunque previste delle misure di sicurezza appropriate per tutelare i diritti fondamentali e gli interessi del soggetto cui questi dati si riferiscono; nel settore della sanità pubblica, per finalità di sicurezza sanitaria, per il controllo e l'allerta, per la prevenzione o il controllo di malattie trasmissibili e, in generale, per tutelarsi da altre minacce gravi alla salute delle persone.

Invero, la varietà delle ipotesi derogatorie sopra esaminate, in cui il GDPR consente il superamento del generale divieto di utilizzo dei dati biometrici, mette in evidenza l'apertura da parte del legislatore europeo all'utilizzo e alla circolazione dei dati personali, a scapito della predisposizione di rigidi sistemi di tutela ¹⁸.

Per questo motivo, la realizzazione, nell'ambito del GDPR, di un più adeguato e proficuo impianto di protezione, da riconoscersi in ogni fase del trattamento e che precede la raccolta dei dati personali, ha provocato effetti positivi. E dunque, relativamente ai dati biometrici, il Regolamento può considerarsi lo strumento utilizzato per costruire una solida base di cautele che consentono di procedere all'utilizzo di una categoria di dati la cui possibile applicazione ed utilità è assolutamente evidente ¹⁹.

Vi è inoltre da sottolineare che, in un settore come quello oggetto di disamina, i dati biometrici e genetici non rappresentano soltanto « i primi sensori dei rischi legati all'uso delle nuove tecnologie » ²⁰, ma fanno emergere una serie di ambiguità e incertezze che si riflettono sulla protezione dei diritti individuali anche quando il loro trattamento sia richiesto dalla autorità competente per motivi connessi alla prevenzione, alla lotta al crimine e alla sua repressione. Ciò, induce, pertanto, a riflettere sull'opportunità di adottare la disciplina più adeguata e delineare un più chiaro coordinamento tra fonti normative europee e fonti nazionali ²¹.

3. LA PRONUNCIA DELLA CGUE NELLA CAUSA C-205/21.

Lo sviluppo tecnologico « pur apparendo particolarmente affascinante si rivela spesso fortemente minaccioso, incidendo sui

¹⁸ F. FILOSA, *Dati genetici e biometrici, manca all'appello l'intervento del Garante*, in *Agenda Digitale*, 2019, consultabile al seguente link <https://www.agendadigitale.eu/sicurezza/dati-genetici-in-standby-manca-allappello-lintervento-del-garante/>.

¹⁹ 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*, cit., 106 ss.

²⁰ F. PIZZETTI, *La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni*, in *MediaLaws*, 1, 2018, 123 ss.

²¹ L. CHIEFFI, *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee*, in *federalismi.it*, 4, 2018, 2 ss., consultabile al seguente link https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=35745&content=&content_author=.

diritti e sulle libertà fondamentali ». Ciò è stato appositamente evidenziato nel rinvio pregiudiziale che ha offerto, ancora una volta ²², alla Corte di giustizia l'opportunità di interpretare uno strumento del diritto dell'Unione europea dedicato alla protezione dei dati personali e concepito come mezzo di salvaguardia ²³.

« In un certo senso, la presente causa costituisce una declinazione, nel settore della protezione dei dati personali, del principio secondo cui è meglio rischiare di salvare un colpevole che condannare un innocente » ²⁴.

Difatti, dall'esame della nozione di dati biometrici e genetici e, contestualmente, dall'analisi della disciplina sulla raccolta di tali dati personali, è stato possibile appurare che l'utilizzo o il trattamento dei suddetti dati solleva particolari questioni per quanto concerne i dati biometrici e genetici raccolti per ragioni di sicurezza pubblica e di polizia, con riferimento a quei soggetti che abbiano commesso reati e, soprattutto, anche nei riguardi di coloro che vengano accusati di un reato doloso perseguibile d'ufficio.

In tal senso, di particolare interesse è stata la decisione della CGUE ²⁵, chiamata a pronunciarsi nell'ambito di un procedimento penale bulgaro per frode fiscale, commesso da un'organizzazione criminale ²⁶.

A tal proposito, il giudice *a quo*, nutrendo dubbi sulla compatibilità con il diritto europeo delle disposizioni legislative e rego-

²² V. Corte giust. UE, 12 maggio 2021, C-505/19, *W.S. c. Bundesrepublik Deutschland*, EU:C:2021:376, punto 111, consultabile al seguente link <https://curia.europa.eu/juris/document/document.jsf?jsessionid=AE4B77C1D82DA04EC050AC16F224F501?text=&docid=241169&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=3818776>.

²³ F. ROSSI DAL POZZO, *La tutela dei dati personali nella giurisprudenza della Corte di giustizia*, cit., 127 ss.

²⁴ V. punto 1, conclusioni dell'avvocato generale Giovanni Pitruzzella, presentate il 30 giugno 2022, documento disponibile al seguente link <https://curia.europa.eu/juris/document/document.jsf?jsessionid=E062811C425824B19762D73075B061F0?text=&docid=261934&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=245630#Footnote3>.

²⁵ Cfr., ancora, Corte giust. UE, 26 gennaio 2023, C-205/21, *procedimento penale a carico di V.S.*, ECLI:EU:C:2023:49, consultabile al seguente link <https://curia.europa.eu/juris/document/document.jsf?jsessionid=E062811C425824B19762D73075B061F0?text=&docid=269704&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=245630>.

²⁶ I fatti che hanno dato origine alle questioni pregiudiziali riguardavano una persona fisica, formalmente accusata di aver partecipato ad un'organizzazione criminale costituita a fini di lucro, per commettere in maniera concordata delitti in territorio bulgaro. A seguito di tale messa in stato di accusa formale, la polizia bulgara invitava l'accusata a sottoporsi alla raccolta dei suoi dati dattiloscopici e fotografici nonché, ai fini della loro registrazione, ad un prelievo di campioni per l'elaborazione del suo profilo del DNA (come previsto dal diritto interno), sussistendo elementi probatori sufficienti a desumerne la colpevolezza. Tuttavia, dinanzi a siffatta richiesta, la stessa si opponeva al prelievo e alla registrazione che la riguardava (cui seguiva la compilazione di un apposito modulo di dichiarazione in cui indicava di essere stata informata della sussistenza dei fondamenti di legge per procedere a tale registrazione, ma di non acconsentirvi). Pertanto, le autorità di polizia provvedevano ad adire il giudice del rinvio

lamentari del diritto bulgaro applicabili alla registrazione da parte della polizia, sospendeva il procedimento e sottoponeva alla CGUE diverse questioni pregiudiziali ²⁷, tra cui: l'efficace recepimento nella legislazione nazionale dell'art. 10 della Direttiva LED (sul trattamento dei dati biometrici e genetici per finalità di pubblica sicurezza e di polizia), da valutarsi unitamente al "conforme" — ma più generico — art. 9 del GDPR; la compatibilità della normativa nazionale all'art. 6, lett. a) della Direttiva LED, letto in combinato disposto con l'art. 48 della Carta di Nizza (d'ora innanzi Carta), relativamente all'obbligo per il giudice di ordinare la raccolta coercitiva di dati personali qualora un soggetto accusato di un reato intenzionale perseguibile d'ufficio si rifiuti di collaborare volontariamente al rilevamento di tali dati; infine, la compatibilità delle norme di diritto europeo con quelle di diritto interno le quali prevedono, come regola generale, lo scatto di fotografie per la schedatura, il rilevamento dell'impronta digitale e il prelievo di campioni di DNA per tutte le persone accusate di un reato doloso perseguibile d'ufficio.

Ai fini di questo scritto è opportuno concentrarsi soltanto su determinate e specifiche questioni.

In particolare, la CGUE si è trovata ad argomentare sui predetti quesiti prendendo in considerazione tanto l'art. 9 del GDPR quanto l'art. 10 della Direttiva LED, trattandosi della raccolta di dati genetici e biometrici, di natura particolarmente sensibile.

A ben vedere, il principale interrogativo sollevato ha ad oggetto proprio la chiarezza e la specificità della normativa nazionale in tema di trattamento di dati biometrici e genetici per finalità di

(*Spetsializiran nakazatelen sad* — Tribunale specializzato per i procedimenti penali, Bulgaria) affinché autorizzasse l'esecuzione coercitiva della registrazione da parte della polizia.

²⁷ V. punto 50 della pronuncia: « 1) Se l'art. 10 della Direttiva LED sia efficacemente recepito nella legislazione nazionale (...) con il riferimento alla disposizione analoga di cui all'articolo 9 del GDPR;

2) Se sia soddisfatto il requisito previsto nell'art. 10, lett. a), della Direttiva LED, in combinato disposto con gli artt. 52, 3 e 8 della Carta di Nizza (d'ora in poi "Carta"), secondo cui una limitazione dell'integrità e della protezione dei dati personali deve essere prevista dalla legge, allorché esistono disposizioni nazionali tra loro contraddittorie in merito alla legittimità di un trattamento di dati genetici e biometrici a fini di registrazione da parte della polizia;

3) Se sia compatibile con l'art. 6, lett. a), della Direttiva LED, in combinato disposto con l'art. 48 della Carta, una normativa

nazionale — l'art. 68, par. 4, [dello ZMVR] — che prevede l'obbligo per il giudice di ordinare la raccolta coercitiva di dati personali (scatto di fotografie per schedatura, rilevamento dell'impronta digitale e prelievo di campioni per l'elaborazione di un profilo del DNA), qualora una persona accusata di un reato intenzionale perseguibile d'ufficio si rifiuti di collaborare volontariamente al rilevamento di tali dati, senza che il giudice possa valutare la sussistenza di un fondato motivo che abbia portato tale persona al compimento del reato di cui viene accusata;

4) Se sia compatibile con gli artt. 10, 4, par. 1, lett. a) e c), e 8, parr. 1 e 2, della Direttiva LED una legge nazionale — l'art. 68, parr. da 1 a 3, [dello ZMVR] — che prevede come regola generale lo scatto di fotografie per la schedatura, il rilevamento dell'impronta digitale e il prelievo di campioni per l'elaborazione di un profilo del DNA per tutte le persone accusate di un reato intenzionale perseguibile d'ufficio ».

prevenzione e di lotta alla criminalità. La questione, dunque, verte sul corretto recepimento nel diritto bulgaro dell'art. 10 della Direttiva LED che autorizza, a determinate condizioni, il trattamento dei dati biometrici e genetici²⁸. Ciò in quanto la contestata disciplina nazionale fa esplicito riferimento non alla Direttiva LED, quanto piuttosto al GDPR, emergendo, di conseguenza, dubbi sulla compatibilità del diritto comunitario con la legge interna²⁹.

Alla luce di tali elementi, gli interrogativi emersi hanno portato a domandarsi se sia possibile ritenere che, nonostante il riferimento all'art. 9 del GDPR, il trattamento di tali particolari dati a fini penali sia ammissibile nel diritto nazionale, tenuto conto del fatto che esso è chiaramente autorizzato dall'art. 10 della Direttiva LED, anche se quest'ultima non è menzionata dalle disposizioni nazionali³⁰.

Inoltre, nell'ambito del contesto in esame, qualora si dovesse ritenere che l'art. 10 della Direttiva LED sia stato correttamente trasposto nel diritto nazionale o che esista un valido fondamento in tale diritto per il trattamento di dati biometrici e genetici, è stato sollevato un ulteriore interrogativo: se il requisito di cui all'art. 10, lett. a), di tale Direttiva, secondo cui un simile trattamento deve essere autorizzato dal diritto dell'Unione o dello Stato membro, sia soddisfatto qualora sussista una contraddizione tra le disposizioni del diritto nazionale applicabili³¹.

Per rispondere ai quesiti sulla sottomissione della raccolta dei dati all'una o all'altra disciplina europea, trattati congiuntamente

²⁸ Sulla questione, il giudice *a quo* ha rilevato che, in virtù del suo art. 2, par. 2, lett. d), il Regolamento, ponendo un divieto esplicito, non si applica al trattamento dei dati biometrici e genetici effettuato dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati, poiché è la Direttiva LED, conformemente al suo art. 1, par. 1, a disciplinare un siffatto trattamento (v. punto 40 della pronuncia).

Infine, aggiunge che l'art. 51 della legge sulla protezione dei dati personali bulgara (ZZLD) non può, di per sé, fondare l'ammissibilità di un trattamento di dati biometrici e genetici, dovendo quest'ultima essere prevista dal diritto dell'Unione o dal diritto nazionale v. punto 11 conclusioni dell'avvocato generale).

²⁹ G. MILIZIA, *La raccolta dei dati biometrici e genetici di una persona accusata di reato è una violazione della privacy*, in *Diritto & Giustizia*, 14, 2023, 39; P. ROSSI, *No a raccolta "sistematica" di dati biometrici di persone accusate di un reato doloso perseguibile d'ufficio*, in *NT+Diritto - Il Sole*

24ore, 2023, consultabile al seguente *link* <https://ntplusdiritto.ilsole24ore.com/art/no-raccolta-sistematica-dati-biometrici-persone-accusate-un-reato-doloso-perseguibile-d-ufficio-AEDHepaC>.

³⁰ V. punti 41 e 42 della pronuncia.

³¹ Si rileva una contraddizione tra l'articolo 25 *bis* della legge sul Ministero degli Affari Interni (ZMVR) che, riferendosi all'art. 9 del GDPR, sembrerebbe non autorizzare il rilevamento di dati biometrici e genetici, e l'art. 68 dello ZMVR, che diversamente lo autorizza.

In effetti, l'articolo 27 dello ZMVR precisa che i dati registrati dalla polizia ai sensi dell'art. 68 della suddetta legge possono essere utilizzati « solo » nel contesto della salvaguardia della sicurezza nazionale, della lotta contro la criminalità e della tutela dell'ordine pubblico (v. punto 30 della pronuncia). Secondo il governo bulgaro, i dati raccolti durante la registrazione da parte della polizia saranno trattati ai fini del procedimento penale in cui la persona interessata è stata accusata, ma anche per « altri fini connessi alla lotta contro la crimina-

dalla CGUE, la sentenza evidenzia che, quando il trattamento dei dati è appunto orientato alla prevenzione, all'indagine, all'accertamento o al perseguimento di reati, questi non saranno disciplinati dal GDPR, bensì dalla Direttiva LED, essendo previsto sia nel considerando 19 del GDPR sia nel considerando da 9 a 12 della Direttiva stessa ³².

In merito alla questione, si è altresì posto l'ulteriore problema della assoluta/stretta necessità del trattamento dei dati soggetti al campo di applicazione dell'art. 10 della Direttiva LED ³³.

Ciò comporta, da un lato, la definizione del livello di necessità richiesto e, dall'altro, l'introduzione nel *test* della necessità anche del principio della minimizzazione dei dati personali (art. 5, par. 1, lett. c) GDPR, secondo cui i dati personali raccolti e trattati devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità perseguite dal loro trattamento) sancito dall'art. 4, par. 1, lett. c) di tale Direttiva ³⁴.

In particolare, la CGUE, soffermandosi sull'art. 10 della citata Direttiva, ha dedotto da tale carattere che l'autorizzazione alla raccolta di tali dati può avvenire solo in presenza di « un'adeguata giustificazione della sua necessità » ³⁵.

Ciò che viene evidenziato dalla fattispecie *de quo* e che rende la disamina del caso particolarmente rilevante, consiste nel fatto che tale raccolta di dati può essere legalmente concordata solo in un numero limitato di ipotesi e che la necessità deve essere rigorosamente valutata. Tale obbligo di valutazione della necessità ha lo scopo di garantire una maggiore tutela delle persone rispetto al trattamento dei loro dati sensibili. Trattasi di un requisito rafforzato che si rende necessario in presenza di gravi ingerenze nel diritto alla protezione dei dati personali ³⁶, rispetto a quanto consentito nell'ambito del regime generale applicato ai dati non particolari. Fondamentale, quindi, il concetto della rigorosa necessità, che deve essere costantemente tenuto presente.

Pertanto, si richiama l'obbligo dei giudici nazionali di ricercare un'interpretazione del diritto interno conforme alla normativa

lità » (v. punto 60 conclusioni dell'avvocato generale), e se del caso, a fini di confronto. A prima vista, tali finalità sembrerebbero corrispondere a quelle menzionate all'art. 1, par. 1, della Direttiva LED, in particolare ai fini di indagine e accertamento dei reati.

³² T. WAHL, *CJEU: Systematic Collection of Biometric and Genetic Data Contrary to EU Law*, in *eu crim*, 2023, consultabile al seguente link <https://eu crim.eu/news/cjeu-systematic-collection-of-biometric-and-genetic-data-contrary-to-eu-law/>.

³³ V. punto 41 della pronuncia, in cui

viene evidenziato che l'art. 10 della Direttiva LED dispone che il trattamento dei dati biometrici e genetici volti ad identificare in modo univoco una persona fisica « è autorizzato solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e soltanto (...) se autorizzato dal diritto dell'Unione o dello Stato membro » (v. punto 41 della pronuncia).

³⁴ V. punti 42 e 43 conclusioni dell'avvocato generale.

³⁵ V. punto 46 della pronuncia.

³⁶ V. punto 44 della pronuncia.

europea e, in particolare, « che rispetti l'effetto utile della Direttiva » ³⁷.

Più segnatamente, una volta valutata l'esistenza di disposizioni in grado di soddisfare il requisito di cui all'art. 10, lett. a) di detta Direttiva, sarà responsabilità dell'autorità competente verificare se, in realtà, tali disposizioni non abbiano un ambito di applicazione diverso da quelle nazionali, contraddicendosi vicendevolmente ³⁸.

La Corte, dunque, conclude rispondendo alle prime due questioni sollevate, relative alla compatibilità della normativa nazionale con quella europea e all'autorizzazione da parte dell'autorità competente della raccolta di dati biometrici, che il rinvio operato dalla normativa nazionale al GDPR, e non alla Direttiva LED, non stravolge quanto disposto dall'art. 10, lett. a) della Direttiva, essendo compito del giudice nazionale interpretarla correttamente, purché dall'interpretazione di tutte le disposizioni applicabili del diritto nazionale risulti in modo sufficientemente chiaro, preciso ed inequivocabile che il trattamento dei dati biometrici e genetici in questione rientra nell'ambito di applicazione della Direttiva, e non del Regolamento.

Prosegue, inoltre, rilevando che la raccolta e il trattamento dei dati biometrici e genetici (quali le fotografie, le impronte digitali e il prelievo di campioni per l'elaborazione di un profilo del DNA), a fini di lotta contro la criminalità e di tutela dell'ordine pubblico, è autorizzata dal diritto dello Stato membro, purché il diritto di tale Stato contenga una base giuridica sufficientemente chiara e precisa per autorizzare detto trattamento.

Poiché, la raccolta e il trattamento dei suddetti dati costituiscono una grave ingerenza nel diritto alla protezione dei dati personali, sono autorizzati solo se « strettamente necessari » (garantendo una maggiore tutela della persona rispetto al trattamento dei loro dati sensibili) per il perseguimento di obiettivi legati alle forme gravi di criminalità, che il diritto nazionale deve chiaramente identificare. Ne discende che la natura e il numero dei dati personali trattati devono essere strettamente adeguati e coerenti con l'obiettivo e le finalità perseguite, ovvero la sicurezza e la difesa nazionale ³⁹.

Per di più, un'ulteriore incompatibilità tra discipline è emersa,

³⁷ V. punto 72 della pronuncia.

³⁸ P. Rossi, *No a raccolta "sistematica" di dati biometrici di persone accusate di un reato doloso perseguibile d'ufficio*, cit., consultabile al seguente link <https://ntplusdiritto.ilsole24ore.com/art/no-raccolta-sistematica-dati-biometrici-persone-accusate-un-reato-doloso-perseguibile-d-ufficio-AEDHepaC>.

³⁹ V. punto 58 conclusioni dell'avvocato generale. Cfr., ancora, G. MILIZIA, *La raccolta dei dati biometrici e genetici di una persona accusata di reato è una violazione della privacy*, cit., 39 s., la quale mette in evidenza che il diritto nazionale deve conformarsi ad una delle finalità della Direttiva LED dovendo, altresì, indicare gli obiettivi concreti perseguibili che possono contri-

nel caso di specie, anche in considerazione del fatto che, l'art. 6, lett. a) della Direttiva LED, obbliga gli Stati membri, « se del caso e nella misura del possibile », a operare una chiara distinzione tra i dati delle diverse categorie di interessati, quali: « le persone per le quali vi sono fondati motivi di ritenere che abbiano commesso o stiano per commettere un reato »⁴⁰.

L'obiettivo di tale disposizione è quello di non far subire la stessa ingerenza nel diritto fondamentale alla protezione dei dati personali sia alle vittime di reati sia alle persone sospettate di averli commessi⁴¹.

Sulla base di tali considerazioni, è stata dichiarata la liceità del prelievo coatto di tale particolare categoria di dati personali « purché il diritto nazionale garantisca successivamente un controllo giurisdizionale effettivo delle condizioni di tale imputazione, da cui deriva l'autorizzazione ad effettuare tale raccolta »⁴².

4. DATI BIOMETRICI E GENETICI TRA GDPR E DIRETTIVA LED: DISCIPLINE A CONFRONTO.

Come illustrato precedentemente⁴³, dalle questioni esaminate si evince che tra le due normative sussiste una stretta connessione,

buire alla realizzazione di tale scopo. Devono, inoltre, essere specificati concretamente i motivi per cui, nonostante si tratti di un'ingerenza grave, il trattamento di tali dati, e in particolare dei dati genetici, appare strettamente necessario a tal fine. Il diritto nazionale deve, peraltro, enunciare chiaramente le condizioni del trattamento in tutte le sue dimensioni, ossia dalle condizioni della raccolta alle condizioni di accesso e di cancellazione dei dati, fino alla determinazione specifica e strettamente limitata dell'ambito di applicazione personale della misura di raccolta e di trattamento. Il regime così definito deve risultare idoneo a proteggere efficacemente i soggetti dai rischi di abuso rappresentati, in particolare, dal trattamento dei dati biometrici e genetici.

⁴⁰ V. punti 18 e 27 conclusioni dell'avvocato generale.

⁴¹ V. punto 83 della pronuncia. La CGUE, proseguendo nella disamina, si pronuncia anche sulla terza questione pregiudiziale, rilevando che, nel sollevarla, l'organo giudiziario bulgaro aveva contestato la normativa nazionale secondo cui, qualora una persona sia indagata per un reato doloso e si rifiuti di collaborare volontariamente alla raccolta dei suoi dati biometrici e genetici ai fini della relativa registrazione, ciò legittimerebbe il tribunale penale ad autorizzare un trattamento coattivo di tali dati,

senza poter valutare se ci siano fondati motivi volti a definire la commissione del reato per cui venga indagato l'interessato (sul punto v. Court of Justice of the European Union, Press release No. 16/23, *The Systematic Collection of Biometric and Genetic Data of Any Accused Person in Order for Them to be Entered in a Police Record is Contrary to the Requirement of Ensuring Enhanced Protection with Regard to the Processing of Sensitive Personal Data*, in [curia.europa.eu](https://curia.europa.eu/jcms/jcms/J_2_7052/en/), consultabile al seguente link https://curia.europa.eu/jcms/jcms/J_2_7052/en/). Il giudice del rinvio precisa che quasi tutti i reati previsti dal codice penale rientrano nella categoria dei reati intenzionali/reati perseguibili d'ufficio. Di conseguenza tutte le persone accusate di un reato intenzionale perseguibile d'ufficio devono sottoporsi alla registrazione da parte della polizia).

In effetti, trattandosi di gravi ingerenze e di dati sensibili che richiedono una protezione rafforzata, sono emersi degli interrogativi che hanno portato a chiedersi il motivo per il quale non si attenda la condanna per i fatti oggetto di imputazione prima di procedere alla registrazione da parte della polizia dei dati personali del soggetto, il che rafforzerebbe, almeno, la selettività della misura (V. punto 63 conclusioni dell'avvocato generale).

⁴² V. punto 101 della pronuncia.

⁴³ V., *supra*, par. 3.

poiché entrambe contengono disposizioni che disciplinano il trattamento di categorie particolari di dati personali, considerati dati sensibili, inclusi quelli genetici e biometrici ⁴⁴.

Tuttavia emergono distinzioni quanto al campo di applicazione della medesima disposizione, oggetto di disamina: mentre il GDPR riguarda la protezione delle persone fisiche circa il trattamento dei dati personali, nonché la libera circolazione di tali dati, la Direttiva LED è volta 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 ⁴⁵.

A ben vedere, volendo fare un confronto tra le due normative, il Regolamento generale sulla protezione dei dati, non si applica al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati, trattamento, questo, riservato alla Direttiva.

A tal proposito, appare opportuno evidenziare che nell'Unione europea l'implementazione del GDPR è stata accompagnata dalla predisposizione della Direttiva LED, nata dall'esigenza di assicurare un livello uniforme ed elevato di protezione dei dati personali delle persone fisiche, agevolando lo scambio di tali dati tra le autorità competenti degli Stati membri, per garantire una maggiore efficacia giudiziaria in materia penale e di polizia.

Nel dettato della suddetta Direttiva, il divieto generale di trattamento dei dati biometrici sancito all'art. 9, par. 1, GDPR non trova attuazione nei casi di prevenzione e lotta alla criminalità o di esecuzione di sanzioni; nei casi in cui sia necessario prevenire o salvaguardare minacce alla pubblica sicurezza e sempre che i dati siano trattati dalle autorità competenti a fini di prevenzione, indagine e accertamento. Inoltre, queste Autorità sono autorizzate a predisporre il trattamento di dati biometrici con finalità di identificazione univoca solo se le tre condizioni cumulative definite all'art. 10 vengano rispettate. In presenza di un quadro giuridico chiaro ed un uso proporzionato di questi sistemi, si è ritenuto fondamentale garantire alle autorità di polizia l'accesso a queste tecnologie in funzione della tutela della pubblica sicurezza ⁴⁶.

⁴⁴ V. punto 62 della pronuncia.

⁴⁵ Si guardi, in proposito, il Parere del GPD del sullo schema di decreto legislativo recante Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio - 22 febbraio 2018 [8005333], consultabile al seguente link <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/8005333>.

⁴⁶ V. K. KUKAVA-S. CHIKHAIDZE-N. AKHILADZE, IDFI - *Institute for Development of Freedom of Information, Processing of Biometric and Genetic Data - European Standards*, 2022, 10 ss., consultabile al seguente link https://idfi.gelen/processing_of_biometric_and_genetic_data.

L'accesso ad immagini facciali ⁴⁷, impronte digitali o altri dati biometrici, se configurato all'interno di un'esigenza di interesse pubblico si può ritenere un'ingerenza necessaria nella vita delle persone per consentire di individuare e perseguire crimini, identificare sospetti e agevolare indagini giudiziarie ⁴⁸.

Per questo, spetta al diritto nazionale dei singoli Stati membri regolamentare in maniera dettagliata la registrazione e la conservazione di questi dati per scopi biometrici da parte delle pubbliche autorità. Attualmente, manca nel diritto interno degli Stati europei una precisa normativa sulla conservazione dei dati biometrici, nonostante la creazione di banche dati e il rischio di una loro possibile registrazione — in assenza di una chiara base legale — sia aumentato in misura esponenziale.

Alla luce di tali elementi, è fondamentale tenere a mente tale distinzione ai fini di una più precisa disamina della pronuncia in oggetto.

A ben vedere, nel caso di specie, il giudice del rinvio si è interrogato sull'ammissibilità nel diritto nazionale bulgaro del trattamento dei dati biometrici e genetici a fini penali, nonostante il riferimento all'art. 9 del GDPR, tenuto conto del fatto che esso è chiaramente autorizzato dall'art. 10 della Direttiva LED (anche se quest'ultima non è menzionata dalle disposizioni di diritto interno) ⁴⁹.

Pertanto, è in tale contesto che il giudice del rinvio ha richiesto alla Corte indicazioni relative all'interpretazione di detta condizione, domandando, da un lato (con la sua prima questione) se si possa ritenere che tale art. 10 sia stato correttamente trasposto da una disposizione di diritto nazionale, che fa riferimento solo all'art. 9 del GDPR e il cui tenore letterale, invece, corrisponde a quello di detto art. 10; dall'altro, in caso di risposta affermativa (con la sua seconda questione), domandando se si possa ritenere che la raccolta di dati genetici e biometrici, ai fini della loro registrazione da parte della polizia, sia « autorizzata dal diritto dello Stato membro », ai sensi della lett. a) di tale articolo e, dunque, « previst[a] dalla legge », ai sensi dell'art. 52, par. 1, della Carta (quando le disposizioni di diritto nazionale che costi-

⁴⁷ Cfr. F. PAOLICCI, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *MediaLaws*, 1, 2021, 204 ss., consultabile al link <https://www.medialaws.eu/rivista/riconoscimento-facciale-e-diritti-fondamentali-e-la-sorveglianza-un-giusto-prezzo-da-pagare-2/>; J. SARABDEEN, *Protection of the Rights of the Individual When Using Facial Reco-*

gnition Technology, in *Heliyon*, 8, 2022, 1 ss., consultabile al link seguente <https://www.sciencedirect.com/science/article/pii/S2405844022003747>.

⁴⁸ Ancora, G. MILEZIA, *La raccolta dei dati biometrici e genetici di una persona accusata di reato è una violazione della privacy*, cit., 39 s.

⁴⁹ V., *supra*, par. 3.

tuiscono la base giuridica di tale trattamento sembrano enunciare norme contraddittorie)⁵⁰.

In primo luogo, a supporto di tale questione, il considerando 19 del GDPR prevede espressamente che, il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, inclusa la salvaguardia e la prevenzione di minacce alla sicurezza pubblica, e la libera circolazione di tali dati, costituisce oggetto di uno specifico atto dell'Unione. Pertanto, il relativo Regolamento non dovrebbe applicarsi ai trattamenti effettuati per tali finalità, bensì i suddetti dati dovrebbero essere disciplinati più segnatamente dalla Direttiva LED.

Ne consegue che, mentre un trattamento di dati biometrici e genetici da parte delle autorità competenti a fini rientranti nell'ambito di applicazione della Direttiva può essere autorizzato purché, conformemente ai requisiti enunciati all'art. 10 di quest'ultima, « strettamente necessario, soggetto a garanzie adeguate e previsto dal diritto dell'Unione o dello Stato membro, ciò non avviene necessariamente nel caso di un trattamento di questi stessi dati rientrante nell'ambito di applicazione del GDPR »⁵¹.

Inoltre, dalla giurisprudenza della Corte⁵² risulta che non può sussistere alcun equivoco quanto alle disposizioni del diritto dell'Unione in forza delle quali il diritto nazionale può autorizzare un trattamento di dati biometrici e genetici, come quello di cui al procedimento principale, e quanto alle condizioni applicabili cui tale autorizzazione è soggetta. Infatti, le persone interessate e i giudici competenti devono essere in grado di determinare con precisione, le condizioni a cui tale trattamento può aver luogo nonché le finalità alle quali esso può giuridicamente rispondere.

Pertanto, sebbene il legislatore nazionale abbia la facoltà di prevedere, nell'ambito del medesimo strumento legislativo, il trattamento di dati personali a fini rientranti nell'ambito della Direttiva LED nonché ad altri fini che rientrano nel GDPR, esso ha per contro l'obbligo di accertarsi dell'assenza di ambiguità quanto all'applicabilità dell'uno o dell'altro di tali due atti dell'Unione alla raccolta dei dati biometrici e genetici⁵³.

A tal riguardo, appare opportuno sottolineare, in particolare, che l'art. 9, par. 2, della Direttiva non esclude il trattamento dei dati biometrici e genetici da parte delle autorità competenti, nell'ambito di compiti diversi da quelli eseguiti per le finalità di cui all'art. 1, par. 1, di detta Direttiva. Analogamente, l'art. 9 del GDPR, che si applica al trattamento di tali dati, purché esso non rientri nelle eccezioni tassativamente elencate al suo art. 2, par. 2,

⁵⁰ V. punto 57 della pronuncia.

⁵¹ V. punti 60-63 della pronuncia.

⁵² V. punto 65 della pronuncia.

⁵³ V. punti 66-67 della pronuncia.

non lo vieta in modo assoluto, a condizione che tale trattamento corrisponda a una delle situazioni enunciate all'articolo 9, paragrafo 2, di detto regolamento. In tali circostanze, il giudice del rinvio è tenuto a verificare se il riferimento al GDPR nelle disposizioni nazionali non riguardi, in realtà, trattamenti di dati effettuati dalle autorità competenti a fini diversi da quelli rientranti nell'ambito di applicazione della Direttiva LED, in modo da non individuare contraddizioni con quelle disposizioni che prevedono il trattamento di tali dati a fini che rientrano nell'ambito della suddetta Direttiva ⁵⁴.

Tanto chiarito, la Corte ha rilevato che la circostanza per cui l'atto legislativo nazionale contenente una simile base giuridica faccia riferimento al GDPR, e non alla Direttiva LED, « non è di per sé idonea a rimettere in discussione l'esistenza di una simile autorizzazione alla raccolta e al trattamento dei dati personali di un soggetto accusato formalmente di un reato intenzionale perseguibile d'ufficio, purché dall'interpretazione di tutte le disposizioni applicabili del diritto nazionale risulti in modo sufficientemente chiaro, preciso ed inequivocabile che il trattamento di dati biometrici e genetici in questione rientra nell'ambito di applicazione di tale Direttiva, e non di tale Regolamento » ⁵⁵.

5. L'ARTIFICIAL INTELLIGENCE ACT E I DATI BIOMETRICI.

Alle disposizioni innanzi esaminate deve altresì affiancarsi la proposta di regolamento sull'Intelligenza Artificiale del 21 aprile 2021 ⁵⁶ che mira a garantire la conformità dell'IA sviluppata e utilizzata in Europa, ai diritti e ai valori dell'Unione (ad esempio in materia di supervisione umana, sicurezza, *privacy*, trasparenza, non discriminazione e benessere sociale e ambientale) ⁵⁷. L'obiettivo prospettato dalla Commissione è quello di affrontare tale tematica dotandosi di un *corpus* normativo che sia uniforme per tutti gli Stati membri ⁵⁸.

In un contesto come quello fino ad ora delineato, appare dunque

⁵⁴ V. punto 73 della pronuncia.

⁵⁵ V. punto 76 della pronuncia.

⁵⁶ Cfr. Commissione europea, 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 COM(2021) 206 final - {SWD(2021) 84 final} - {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}, consultabile al seguente link <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52021PC0206>.

⁵⁷ Le norme mirano a promuovere l'adozione di un'IA incentrata sull'uomo,

che sia affidabile e che tuteli la salute, la sicurezza, i diritti fondamentali e la democrazia dai suoi effetti dannosi.

⁵⁸ Attualmente, a seguito delle modifiche apportate al testo dell'*AI Act* (specificamente, Emendamento 3, Considerando 1), viene meglio specificato che: « Lo scopo del presente regolamento è promuovere la diffusione di un'intelligenza artificiale antropocentrica e affidabile e garantire un livello elevato di protezione della salute, della sicurezza, dei diritti fondamentali, della democrazia e dello Stato di diritto, nonché dell'ambiente, dagli effetti nocivi dei sistemi di intelligenza artificiale nell'Unione, soste-

imprescindibile l'analisi di tale proposta (il cui testo è stato recentemente approvato dal Parlamento europeo, modificato in alcune sue parti ⁵⁹) relativamente alla disciplina sul trattamento dei dati biometrici, da confrontarsi con il GDPR.

Per tali ragioni, è opportuno mettere in evidenza, nel particolare ambito dei dati biometrici, la connessione intercorrente tra la proposta di regolamento e la disciplina del GDPR, che permette di sperimentare l'applicazione delle categorie previste dalla proposta su tecnologie già esistenti e già oggetto di attenzione da parte delle autorità nazionali per la protezione dei dati personali; motivo per il quale è assolutamente necessario che la proposta si misuri con il Regolamento.

Il cardine del futuro *Artificial Intelligence Act* (d'ora innanzi *AI Act*) risiede nella definizione di un modello regolatorio finalizzato alla gestione ottimale dei rischi insiti nell'utilizzo dei dispositivi di

nendo nel contempo l'innovazione e migliorando il funzionamento del mercato interno. Il presente regolamento istituisce un quadro giuridico uniforme, in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso dell'intelligenza artificiale (IA) in conformità ai valori dell'Unione e garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di intelligenza artificiale (sistemi di IA), salvo espressa autorizzazione del presente regolamento. Alcuni sistemi di IA possono anche avere un impatto sulla democrazia, sullo Stato di diritto e sull'ambiente. Tali preoccupazioni sono affrontate specificamente nei settori e nei casi d'uso critici elencati negli allegati del presente regolamento ».

⁵⁹ Cfr. *Committee on the Internal Market and Consumer Protection Committee on Civil Liberties, Justice and Home Affairs, Draft Compromise Amendments on the Draft Report Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD))*, 9/05/2023, *chrome-extension://efabmnnnibpcajpcglcfeindmkaj/https://www.europarl.europa.eu/meetdocs/2014_2019/plnrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf*.

Si consulti, in proposito, il testo emendato della proposta di regolamento, appro-

vato il 14 giugno 2023 dal Parlamento europeo in sede plenaria (*Artificial Intelligence Act*, noto anche come *AI Act*). A ben vedere, il Parlamento europeo (con 499 voti a favore, 28 contrari e 93 astensioni) ha approvato la proposta di regolamento che ha ampliato l'elenco dei divieti sugli usi intrusivi e discriminatori dell'IA. Per gli emendamenti in tema di dati biometrici si veda il seguente link https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_IT.html; nonché *News European Parliament, MEPs Ready to Negotiate First-Ever Rules for Safe and Transparent AI*, 2023, disponibile al seguente link <https://www.europarl.europa.eu/news/en/press-room/2023/0609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai>.

Si vedano sul punto, inoltre, la Relazione - A9-0188/2023 del Parlamento Europeo, *Relazione sulla 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, del 22 maggio 2023, disponibile al seguente link https://www.europarl.europa.eu/doceo/document/A-9-2023-0188_IT.html; nonché *Emendamenti del Parlamento europeo, approvati il 14 giugno 2023, alla 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 (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD))(1), 14/06/2023, consultabile al seguente link https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_IT.html.

IA con l'obiettivo primario di tutela dei diritti fondamentali e di salvaguardia del processo democratico ⁶⁰.

Difatti, dal testo del regolamento emergono « una serie di limitazioni nell'identificazione delle tecnologie biometriche incluse nel relativo campo di applicazione, che hanno provocato una serie di ambiguità e incertezze. Ciò si riflette sulla protezione dei diritti individuali, inducendo ad una riflessione sull'opportunità di adottare scelte più nette in merito alle tecnologie vietate e a quelle ad alto rischio, al fine di delineare un più chiaro coordinamento con altre fonti normative — a partire dal GDPR » ⁶¹. Le tecnologie biometriche incluse nella disciplina del regolamento IA sono pertanto esclusivamente quelle che non solo coinvolgono i dati personali, ma sono altresì connotate dalla specifica nozione di dati biometrici, propria del diritto europeo dei dati personali ⁶². Quest'ultima considera soltanto i dati personali frutto di un trattamento tecnico specifico che ne consentono o confermano l'identificazione univoca ⁶³.

Da ciò discende il carattere neutrale della proposta rispetto ai dati regolati, considerando tecnologie che possono impiegare i dati personali e non personali. Coerentemente con questo approccio, il regolamento IA si propone di non interferire con la normativa europea in materia di dati personali (precisando nella relazione di accompagnamento della proposta che questa non pregiudica il GDPR e nemmeno la Direttiva LED). Le previsioni del nuovo regolamento, pertanto, devono essere coerenti con il contesto

⁶⁰ Così, G. RESTA, *Cosa c'è di 'europeo' nella Proposta di Regolamento UE sull'intelligenza artificiale?*, in questa Rivista, 2, 2022, 335 ss.; G.D. FINOCCHIARO, *La proposta di Regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in questa Rivista, 2, 2022, 303 ss.

⁶¹ V. 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*, cit., 108 ss.; G. CERRINA FERONI, *Intelligenza artificiale e ruolo della protezione dei dati personali. L'analisi di Ginevra Cerrina Feroni (Garante Privacy)*, 2023, consultabile al link <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9855742>.

⁶² Cfr. Emendamento 63, proposta di regolamento, Considerando 33-bis (nuovo): « Poiché i dati biometrici costituiscono una categoria speciale di dati personali sensibili ai sensi del regolamento (UE) 2016/679, diversi casi critici d'uso di sistemi biometrici e basati su elementi biometrici dovrebbero

essere classificati come ad alto rischio. È pertanto opportuno classificare come ad alto rischio i sistemi di IA destinati a essere utilizzati per l'identificazione delle persone fisiche e i sistemi di IA destinati a essere utilizzati per trarre conclusioni sulle caratteristiche personali delle persone fisiche sulla base di dati biometrici o basati su elementi biometrici, compresi i sistemi di riconoscimento delle emozioni, ad eccezione di quelli vietati a norma del presente regolamento. Non dovrebbero essere inclusi 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, a un dispositivo o a locali (verifica "uno a uno"). Non si dovrebbe ritenere che i sistemi biometrici e basati su elementi biometrici previsti dal diritto dell'Unione per consentire misure di cybersicurezza e di protezione dei dati personali presentino un rischio significativo di pregiudicare la salute, la sicurezza e i diritti fondamentali ».

⁶³ *Ibidem*, 132 ss.

esistente del diritto europeo della protezione dei dati personali e con le garanzie ad esso connesse, che continuano ad applicarsi anche con il rango di diritti fondamentali, in base al dettato della Carta di Nizza (art. 8) e della giurisprudenza della CGUE.

● Occorre, a questo punto, soffermarsi sull'analisi della disciplina dei dati biometrici.

In particolare, la proposta di regolamento, così come emendata, oltre ad individuare la nozione di dati biometrici, fornisce altresì una definizione dettagliata dei “sistemi di IA” che si basano su dati biometrici, costituenti i primi sensori dei rischi legati all'uso delle nuove tecnologie.

■ Quanto al concetto di dati biometrici viene espressamente disposto che tale nozione è da considerarsi « in linea e dovrebbe essere interpretata in modo coerente con la nozione di dati biometrici di cui all'art. 4, punto 14, del GDPR (...) ». Riguardo, invece, ai sistemi di IA che si basano su dati biometrici, trattasi di « dati aggiuntivi derivanti da un trattamento specifico in relazione ai segnali fisici, fisiologici o comportamentali di una persona fisica, quali ad esempio le espressioni facciali, i movimenti, la frequenza cardiaca, la voce, la pressione esercitata sui tasti o l'andatura, che possono o non possono consentire o confermare l'identificazione univoca di una persona fisica »⁶⁴.

L'introduzione dei sistemi di intelligenza artificiale volti al trattamento dei dati biometrici ha peraltro sollevato questioni connesse ai diritti e alle libertà fondamentali.

Come anticipato, il trattamento dei dati biometrici degli individui ricorre attualmente con frequenza, e prende in considera-

⁶⁴ Cfr. Emendamento 21, Considerando 7, alla proposta di regolamento sull'IA, consultabile al seguente link https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_IT.html, che elimina il riferimento all'articolo 3, punto 18), del regolamento (UE) n. 2018/1725 del Parlamento europeo e del Consiglio e all'articolo 3, punto 13), della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio e integra ulteriormente la definizione. Tra le novità introdotte nel testo modificato vengono altresì in evidenza: l'Emendamento 22, Considerando 7-bis della proposta, che espressamente stabilisce che « La nozione di “identificazione biometrica” utilizzata nel presente regolamento dovrebbe essere definita come il riconoscimento automatico di caratteristiche fisiche, fisiologiche, comportamentali e psicologiche di una persona, quali il volto, il movimento degli occhi, le espressioni facciali, la forma del corpo, la voce, il linguaggio, l'andatura, la postura, la frequenza cardiaca, la pressione sanguigna, l'odore, la pressione esercitata sui ta-

sti, le reazioni psicologiche (rabbia, angoscia, dolore, ecc.), allo scopo di determinare l'identità di una persona confrontando i suoi dati biometrici con quelli di altri individui memorizzati in una banca dati (identificazione “uno a molti”), indipendentemente dal fatto che la persona abbia fornito il proprio consenso »; l'Emendamento 23, Considerando 7-ter, che individua la nozione di categorizzazione biometrica utilizzata nel presente regolamento e che dovrebbe essere definita come « l'assegnazione di persone fisiche a categorie specifiche o la deduzione delle loro caratteristiche o dei loro attributi, quali il genere, il sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, l'origine etnica o sociale, la salute, l'abilità mentale o fisica, i tratti comportamentali o di personalità, la lingua, la religione o l'appartenenza a una minoranza nazionale o l'orientamento sessuale o politico, sulla base dei loro dati biometrici o dei dati basati su elementi biometrici o che possono essere dedotti da tali dati »; l'Emendamento 186, art. 3 — punto 33, che dispone

zione attività banali (ad esempio sbloccare lo *smartphone*), ma soprattutto attività più articolate come la profilazione o la sorveglianza da remoto in tempo reale ⁶⁵. E proprio la sorveglianza applicata al riconoscimento facciale per fini di prevenzione e repressione dei reati ha catturato l'attenzione del Consiglio dell'Ue che nelle proprie linee guida ha segnalato l'intrusività che essa comporta quanto al diritto alla vita privata e alla dignità delle persone, unitamente al rischio di ripercussioni negative su altri diritti umani e sulle libertà fondamentali ⁶⁶.

A tal proposito, centrale, nella proposta di regolamento sull'IA, è il tema dei sistemi di riconoscimento attraverso dati biometrici in tempi reali collocati negli spazi accessibili al pubblico ⁶⁷.

Ciò che appare, inoltre, rilevante riguarda il fatto che la proposta avanzata dalla Commissione Europea, nella valutazione dei sistemi di IA, presenta distinti livelli di rischio (inaccettabile, alto, limitato o minimo) ⁶⁸.

Il livello di rischio inaccettabile, poiché viola i valori del-

che « i dati biometrici sono quelli definiti all'articolo 4, punto 14, del regolamento (UE) 2016/679 »; Emendamento 187, art. 3 — punto 33-*bis*, che fornisce la definizione di « dati basati su elementi biometrici », ovvero, « quei dati aggiuntivi ottenuti da un trattamento tecnico specifico in relazione ai segnali fisici, fisiologici o comportamentali di una persona fisica »; e infine, l'Emendamento 188, art. 3 — punto 33-*ter*, il cui riferimento va alla « identificazione biometrica », da intendersi quale « riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali e psicologiche al fine di stabilire l'identità di una persona confrontando i dati biometrici di tale persona con i dati biometrici di persone in una banca dati (identificazione uno a molti) ».

⁶⁵ Cfr. L. GIACOBBE, *Dati biometrici, il nodo del rapporto tra AI e libertà: quali regole in Europa*, in *Agenda Digitale*, 2021, disponibile al seguente link <https://www.agendadigitale.eu/cultura-digitale/dati-biometrici-il-nodo-del-rapporto-tra-ai-e-liberta-quali-regole-in-europa/>.

⁶⁶ Cfr. European Council, *Artificial Intelligence Act: Council Calls for Promoting Safe AI that Respects Fundamental Rights*, 2022, consultabile al seguente link <https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/>, in cui viene specificato che « scopo del futuro AI Act è quello di garantire che i sistemi di IA immessi sul mercato dell'UE e utilizzati nell'Unione siano sicuri e rispettino il di-

ritto vigente in materia di diritti fondamentali e valori dell'Unione ». Nello specifico, il riferimento va alle criticità mosse dai Paesi membri e dalle rispettive autorità per la protezione dei dati personali relativamente alle tecnologie di video sorveglianza che utilizzano dispositivi di riconoscimento facciale sulle quali il ricorso all'impianto complessivo del GDPR non sembra sufficiente.

⁶⁷ In altre parole, la Commissione non intende chiudere definitivamente le porte ai trattamenti effettuati mediante dispositivi di riconoscimento facciale in tempo reale e pur considerando il loro utilizzo su un piano di rischio non accettabile lascia margini di applicazione sia pure minimi agli Stati membri.

⁶⁸ Confronta la relazione di accompagnamento della proposta di regolamento della Commissione, 5.2. « Illustrazione dettagliata delle singole disposizioni della proposta », 5.2.2. « Pratiche di intelligenza artificiale vietate (Titolo II) », disponibile al link <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52021PC0206>. In particolare, il testo che è stato sottoposto a votazione è incentrato su una scala di rischio per regolamentare le applicazioni di intelligenza artificiale, a quattro livelli: minimo (videogiochi abilitati per l'IA e filtri anti-spam) per cui non è previsto alcun intervento, limitato (*chatbot*), alto (assegnazione di punteggi a esami scolastici e professionali, smistamento dei *curricula*, valutazione dell'affidabilità delle prove in tribunale, chirurgia assistita da robot) e inaccettabile (tutto ciò che rappresenta una « chiara minaccia per la sicurezza, i mezzi di sussistenza e i diritti

l'Unione e i diritti fondamentali, vieta tutte le pratiche incluse all'interno di questa categoria, potendo determinare una manipolazione del comportamento umano. Tra le fattispecie valutate all'interno del livello di rischio inaccettabile, previsti nell'art. 5, c'è l'uso di sistemi di identificazione biometrica in tempo reale negli spazi pubblici inerente i casi in cui l'IA venga considerata una minaccia alla sicurezza e ai diritti fondamentali delle persone.

In proposito, è interessante proprio quanto disposto all'interno del considerando 18, emendato lo scorso 13 giugno 2023, in cui viene espressamente evidenziato che « L'uso di sistemi di IA per l'identificazione biometrica remota "in tempo reale" delle persone fisiche in spazi accessibili al pubblico è particolarmente invasivo dei diritti e delle libertà delle persone interessate e può in ultima analisi avere ripercussioni sulla vita privata di un'ampia fetta della popolazione, farla sentire costantemente sotto sorveglianza, collocare le parti che impiegano l'identificazione biometrica in spazi accessibili al pubblico in una posizione di potere incontrollabile e scoraggiare in maniera indiretta l'esercizio della libertà di riunione e di altri diritti fondamentali che costituiscono l'essenza dello Stato di diritto. *In effetti (si evidenzia all'interno del considerando)*, le inesattezze di carattere tecnico dei sistemi di IA destinati all'identificazione biometrica remota delle persone fisiche possono determinare risultati distorti e comportare effetti discriminatori. Ciò diviene particolarmente rilevante quando si trattano aspetti quali l'età, l'etnia, il sesso o la disabilità. L'immediatezza dell'impatto e le limitate opportunità di eseguire ulteriori controlli o apportare correzioni in relazione all'uso di tali sistemi, che operano "in tempo reale", comportano inoltre un aumento dei rischi per quanto concerne i diritti e le libertà delle persone oggetto di attività di contrasto. *Ne discende che* l'uso di tali sistemi in spazi accessibili al pubblico dovrebbe pertanto essere vietato. Analogamente, anche i sistemi di IA utilizzati per l'analisi di filmati registrati in spazi accessibili al pubblico attraverso sistemi di identificazione biometrica remota "a posteriori" dovrebbero essere vietati, a meno che non vi sia un'autorizzazione giudiziaria preventiva concernente il loro uso a fini di contrasto, ove strettamente necessario per la ricerca mirata connessa a uno specifico reato grave già avvenuto e previa autorizzazione giudiziaria ».

Partendo da queste premesse si giunge alla conclusione che l'utilizzo dei dispositivi di riconoscimento facciale viene bandito dalla proposta di regolamento ⁶⁹.

delle persone », come l'assegnazione di un 'punteggio sociale' da parte dei governi) integralmente vietato.

⁶⁹ Prima delle modifiche apportate alla proposta lo scorso giugno 2023, l'uso di tali sistemi ai fini dell'applicazione della legge

Attualmente, l'art. 5 dell'*AI Act* emendato, pone dei divieti ad una più ampia serie di pratiche di intelligenza artificiale ⁷⁰.

Le norme seguono un approccio basato sul rischio e stabiliscono obblighi per i fornitori e gli operatori dei sistemi di IA a seconda del livello di rischio che può generare.

I sistemi di intelligenza artificiale, considerati a rischio inaccettabile vengono totalmente vietati, quando costituiscono una minaccia per le persone, e comprendono i seguenti casi ⁷¹: la manipolazione comportamentale cognitiva di persone o gruppi vulnerabili specifici (ad esempio, giocattoli attivati vocalmente che incoraggiano comportamenti pericolosi nei bambini); la classificazione sociale, ovvero la valutazione o la classificazione di persone fisiche sulla base del loro comportamento sociale, del loro *status* socio-economico o di caratteristiche personali; i sistemi di identificazione biometrica in tempo reale e a distanza, come il riconoscimento facciale.

Rispetto al testo iniziale, tale elencazione è stata ampliata per includere divieti sugli usi intrusivi e discriminatori dell'IA, tra cui: l'uso di sistemi di identificazione biometrica remota "in tempo reale" e "a posteriori" in spazi accessibili al pubblico (« a meno che non vi sia un'autorizzazione giudiziaria preventiva concernente il loro uso a fini di contrasto, ove strettamente necessario per la ricerca mirata connessa a uno specifico reato grave già avvenuto e previa autorizzazione giudiziaria » ⁷²); i sistemi di categorizzazione biometrica basati su caratteristiche sensibili (ad esempio genere, razza, etnia, cittadinanza, religione, orientamento politico); i sistemi di polizia predittiva (basati su profila-

era stato vietato, con l'eccezione di tre ipotesi tassative in cui l'uso di tali dispositivi fosse stato strettamente necessario per il perseguimento di un interesse pubblico sostanziale, la cui importanza avesse superato i rischi. Più segnatamente, si trattava della ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi (art. 5 — par. 1 — lett. d — punto i); della prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico (art. 5 — par. 1 — lett. d — punto ii); infine, in caso di rilevamento, localizzazione, identificazione o azione penale nei confronti di un autore o un sospettato di un reato di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/CAI del Consiglio, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni, come stabilito dalla legge di tale Stato membro (art. 5 — par. 1 — lett. d — punto iii).

⁷⁰ V. ancora, *News European Parliament, press releases, MEPs Ready to Negotiate First-Ever Rules for Safe and Transparent AI*, cit., disponibile al link <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai>.

⁷¹ A. CICCIA MESSINA, *Regolamento UE sull'intelligenza artificiale: come tutelare la privacy*, in IPSOA - Wolters Kluwer, 2023, consultabile al link <https://www.ipsoa.it/documents/quotidiano/2023/06/19/regolamento-ue-intelligenza-artificiale-tutelare-privacy>; A. LONGO, *Il Parlamento europeo approva l'AI Act, cosa cambierà per le nostre aziende?*, in *Ilsole24ore*, 2023, disponibile al link <https://www.ilsole24ore.com/art/il-parlamento-europeo-approva-l-ai-act-cosa-cambiera-le-nostre-aziende-AE2aw3gD#U4032345354665ZE>.

⁷² Cfr. Emendamento 41, proposta di regolamento sull'intelligenza artificiale, Considerando 18.

zione, ubicazione o comportamenti criminali passati); i sistemi di riconoscimento delle emozioni utilizzati dalle forze dell'ordine, nella gestione delle frontiere, nel luogo di lavoro e negli istituti d'istruzione; e l'estrazione non mirata di dati biometrici da Internet o da filmati di telecamere a circuito chiuso per creare *database* di riconoscimento facciale (in violazione dei diritti umani e del diritto alla *privacy*).

Un secondo livello di rischio comprende i sistemi di intelligenza artificiale che influiscono negativamente sulla sicurezza o sui diritti fondamentali, considerati ad "alto rischio" e suddivisi in due categorie: « i sistemi di IA che sono componenti di sicurezza di prodotti, o che sono essi stessi prodotti, e rientrano nell'ambito di applicazione della Direttiva 2001/95/CE, sulla sicurezza generale dei prodotti, è opportuno classificarli come sistemi ad alto rischio a norma del presente regolamento se il prodotto in questione è sottoposto alla procedura di valutazione della conformità, al fine di garantire la conformità ai requisiti di sicurezza essenziali, con un organismo terzo di valutazione della conformità a norma della suddetta pertinente normativa di armonizzazione dell'Unione (tali prodotti sono, in particolare, macchine, giocattoli, ascensori, apparecchi e sistemi di protezione destinati a essere utilizzati in atmosfera potenzialmente esplosiva, apparecchiature radio, attrezzature a pressione, attrezzature per imbarcazioni da diporto, impianti a fune, apparecchi che bruciano carburanti gassosi, dispositivi medici e dispositivi medico-diagnostici in vitro »⁷³; sistemi di intelligenza artificiale rientranti in specifici settori e che dovranno essere registrati nella banca dati pubblica dell'Ue)⁷⁴.

In particolare, tali sistemi ad alto rischio saranno valutati prima di essere messi sul mercato e durante tutto il loro ciclo di vita (trattasi di una valutazione d'impatto sui diritti fondamentali che si affiancherà alla valutazione di impatto *privacy* — DPIA — prevista dal GDPR⁷⁵).

Il legislatore europeo intende inserire nella classificazione delle applicazioni ad alto rischio anche i sistemi di IA che comportano danni significativi per la salute, la sicurezza, i diritti fondamentali

⁷³ Cfr. Emendamento 58, proposta di regolamento, Considerando 30.

⁷⁴ Tra le diverse aree si considerino: a) identificazione e categorizzazione biometrica di persone naturali; b) gestione e funzionamento di infrastrutture critiche; c) istruzione e formazione professionale; d) occupazione, gestione dei lavoratori e accesso all'autoimpiego; e) accesso e fruizione di servizi privati essenziali e servizi pubblici e vantaggi; f) forze dell'ordine; g) gestione delle migrazioni, asilo e controllo delle frontiere; h) as-

sistenza nell'interpretazione e applicazione legale della legge. Cfr. Emendamenti 63, Considerando 33-bis nuovo — 72, Considerando 40-bis nuovo.

⁷⁵ Cfr. Attualità Parlamento europeo, *Normativa sull'IA: la prima regolamentazione sull'intelligenza artificiale*, 2023, disponibile al link <https://www.europarl.europa.eu/news/it/headlines/society/20230601ST093804/normativa-sull-ia-la-prima-regolamentazione-sull-intelligenza-artificiale>.

delle persone o l'ambiente. Inoltre, all'elenco dei sistemi ad alto rischio sono stati aggiunti quei sistemi di IA che « sono destinati a essere utilizzati per influenzare l'esito di elezioni o *referendum* o il comportamento di voto delle persone fisiche nell'esercizio del loro voto alle elezioni o ai *referendum* » ⁷⁶.

Infine, vengono classificati i sistemi di intelligenza artificiale “a rischio limitato”, i quali dovranno rispettare requisiti minimi di trasparenza che consentano agli utenti di prendere decisioni informate e consapevoli.

Per tali ragioni, innanzi al rapido sviluppo tecnologico dei sistemi di intelligenza artificiale, l'Unione europea deve agire al fine di promuovere lo sviluppo dell'IA, affrontando contestualmente i rischi che comporta per la sicurezza e, in particolar modo, per i diritti fondamentali.

Si auspica, a questo punto, che le modifiche e le novità apportate al testo di regolamento ⁷⁷ — considerata la velocità dei cambiamenti tecnologici e delle possibili sfide che i sistemi di IA potrebbero presentare — possano essere utili per agevolare l'impegno dell'Unione a perseguire un approccio equilibrato, volto ad assicurare ai cittadini europei l'opportunità di beneficiare di nuove tecnologie sviluppate e operanti in conformità ai valori, ai diritti fondamentali e ai principi dell'Unione.

6. IL PRINCIPIO DI PROPORZIONALITÀ E IL RISCHIO DI PREGIUDIZI AI DIRITTI E ALLE LIBERTÀ DELL'INDIVIDUO.

Le premesse appena riferite possono contribuire ad inquadrare meglio la questione relativa al rispetto del contenuto essenziale dei diritti e delle libertà della persona interessata.

In tale sede, dunque, è opportuno chiedersi se il trattamento dei dati biometrici e genetici soddisfi il requisito di offrire garanzie adeguate per i predetti diritti e libertà.

A tal proposito deve sottolinearsi come nei casi inerenti la raccolta di dati biometrici e genetici per finalità di polizia sia necessario realizzare un bilanciamento tra diritti e interessi dando priorità all'esigenza di armonizzare la protezione dei diritti e delle libertà fondamentali delle persone fisiche.

Occorre esaminare il trattamento di tale particolare categoria di dati personali alla luce del principio di proporzionalità, strumento di bilanciamento fra diritti e libertà costituzionali, da leggersi anche quale parametro per gli interventi dell'autorità di polizia ⁷⁸.

⁷⁶ V. Emendamento 72, Considerando 40-bis (nuovo).

⁷⁷ Che adotta un approccio adeguato al futuro, che consente alle norme di adat-

tarsi ai cambiamenti dell'ecosistema digitale.

⁷⁸ D. IACOVELLI-M. FONTANA, *Nuove sfide della tecnologia e gestione dei rischi nella*

A ben vedere, l'art. 8, par. 1, della Carta, così come l'art. 16, par. 1, del TFUE stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano, come pur ricordato nel primo considerando del GDPR.

In effetti, nonostante i dati rappresentino una fondamentale risorsa, tuttavia, il loro utilizzo, il loro trattamento non deve pregiudicare e scavalcare la preminente tutela dei diritti e delle libertà individuali; motivo per il quale il principio di proporzionalità, in ipotesi del genere, si pone alla base del rispetto di tali diritti, finalizzato al perseguimento di uno scopo, prima di equilibrio, poi di giustizia ⁷⁹.

In particolare, risultano alquanto evidenti i conflitti, con i relativi pregiudizi, che possono derivare dal trattamento dei dati personali, rilevandosi la conseguente necessità di tutela dei soggetti che ne sono titolari. Il dato personale è infatti espressione della personalità dell'individuo ed oggetto di diritti fondamentali espressamente riconosciuti dall'art. 8 della Carta, nell'accezione di *privacy* come riservatezza, a garanzia del rispetto della vita privata e della vita familiare ⁸⁰.

Imprescindibile, dunque, in un'ipotesi del genere, la creazione di un ambiente affidabile attraverso la predisposizione di una serie di misure di salvaguardia che assicurino la protezione degli individui, nell'ambito dell'Unione europea.

Il riferimento va proprio al trattamento dei dati biometrici e genetici da parte dell'autorità competente per la salvaguardia e la garanzia della pubblica sicurezza. La questione, tuttavia, necessita di essere letta altresì in un'ottica legata alla protezione dell'individuo cui viene richiesta la raccolta di tali particolari

proposta di regolamento europeo sull'intelligenza artificiale: set di training, algoritmi e qualificazione dei dati. Profili critici, cit., 106 ss.; A. CARAVITA DI TORITTO, *La proporzionalità multilivello nel mercato "presidiato" dei dati personali*, in *MediaLaws*, 3, 2021, 160, consultabile al seguente link <https://www.medialaws.eu/rivista/la-proporzionalita-multilivello-nel-mercato-presidiato-dei-dati-personali/>.

⁷⁹ G. FORMICI, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, in *DPCE online*, 2, 2019, 1107 ss., disponibile al seguente link <https://www.dpceonline.it/index.php/dpceonline/article/view/729/668>.

⁸⁰ V. Defenseur des droits, *Report, Biometrics: The Urge to Safeguard Fundamental Rights*, 2021, consultabile al seguente link <chrome-extension://efaidnbmn>

[nibpcajpcgclefindmkaj/https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/rap-biometr-num-gb-24.09.21.pdf](https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/rap-biometr-num-gb-24.09.21.pdf). Inoltre, sul riconoscimento del diritto fondamentale alla protezione dei dati di carattere personale si vedano M. BASSINI, *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quaderni costituzionali*, 3, 2016, 587 ss.; M. BRKAN, *The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way through the Maze of the CJEU'S Constitutional Reasoning*, in *German Law Journal*, 20, 2019, 864 ss., disponibile al seguente link <https://www.cambridge.org/core/journals/german-law-journal/articles-sense-of-the-fundamental-rights-to-privacy-and-data-protection-finding-the-way-through-the-maze-of-the-cjeus-constitutional-reasoning/00621C26FA14CCD55AD0B4F4AD33ED09>.

categorie di dati, proprio al fine di giungere a quel bilanciamento tra diritti e interessi in gioco che tra loro paiono inconciliabili ⁸¹.

Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

Infatti, in assenza del rispetto di una necessaria proporzionalità, con riguardo agli obiettivi legittimi ad essi assegnati, i benefici che tali dati apportano sarebbero pregiudicati dalle gravi violazioni ai diritti e alle libertà che gli Stati devono garantire ⁸².

Nelle operazioni di trattamento dei dati genetici e biometrici è necessario e doveroso che il titolare del trattamento consideri l'applicazione dei principi di necessità, proporzionalità e minimizzazione dei dati, esplicitamente previsti dall'art. 5 del GDPR e valuti quali siano le misure tecniche e di sicurezza da applicare, affinché sia garantita una adeguata protezione dei dati ⁸³.

Nella sua decisione, la Corte ha stabilito che la Direttiva LED e la Carta ammettono una normativa nazionale che prevede che se una persona accusata di aver commesso un reato doloso di carattere generale rifiuta di collaborare volontariamente alla raccolta di dati biometrici e genetici ai fini della loro registrazione, il giudice penale competente è tenuto ad autorizzare la raccolta obbligatoria di tali dati senza poter valutare se sussistano gravi motivi per ritenere che la persona abbia commesso il reato di cui è accusata, a condizione che la legislazione nazionale garantisca un effettivo successivo controllo giurisdizionale dei termini di detto addebito ⁸⁴.

Inoltre, sempre con riferimento alla pronuncia oggetto di disamina, la Corte evidenzia che, in forza della Direttiva LED, gli Stati membri devono provvedere affinché sia operata una chiara distinzione tra i dati delle diverse categorie di interessati, in modo che non sia loro imposta indistintamente un'ingerenza della medesima intensità nel loro diritto fondamentale alla protezione dei propri dati personali a prescindere dalla categoria a cui appartengono.

Tuttavia, tale obbligo non è assoluto, ma viene precisato che l'esistenza di un numero sufficiente di elementi di prova della colpevolezza di una persona « costituisce fondato motivo per

⁸¹ E. STEFANINI, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, Padova, CEDAM, 2008, 4 ss.; F. PIRAINO, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civili commentate*, 40, 2, 2017, 369 ss.

⁸² V. punto 55 conclusioni dell'avvocato generale.

⁸³ F. FILOSA, *Dati genetici e biometrici, manca all'appello l'intervento del Garante*, cit., consultabile al seguente link <https://www.agendadigitale.eu/sicurezza/dati-genetici-in-standby-manca-allappello-lintervento-del-garante/>.

⁸⁴ G. FORMICI, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, cit., 1130 ss.

ritenere che quest'ultima abbia commesso il reato di cui trattasi » ⁸⁵.

Dunque, « solo la lotta alle forme gravi di criminalità e la prevenzione di minacce gravi alla sicurezza pubblica sono idonee a giustificare ingerenze gravi nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta (...). Pertanto, solo le ingerenze in tali diritti fondamentali che non presentano un carattere grave possono essere giustificate dall'obiettivo di prevenzione, ricerca, accertamento e perseguimento di reati in generale » ⁸⁶.

Dubbi, quindi, non sussistono e si ritiene del tutto ammissibile, che uno Stato membro stabilisca, come « categoria chiara », quella delle persone accusate, ovvero quelle rispetto alle quali sono raccolte prove sufficienti per ritenere che abbiano commesso un reato ⁸⁷.

Nel contesto del GDPR, per soddisfare il requisito di proporzionalità « la normativa su cui si fonda il trattamento deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura *de qua* e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente tali dati contro il rischio di abusi. Tale normativa dev'essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale e, in particolare, indicare in quali circostanze e a quali condizioni una misura che preveda il trattamento di tali dati possa essere adottata, garantendo così che l'ingerenza sia limitata allo stretto necessario » ⁸⁸. La suddetta normativa, inoltre, « deve fondarsi su criteri oggettivi per definire le circostanze e le condizioni » ⁸⁹ in cui una persona deve fornire i propri dati personali per il trattamento da parte delle autorità competenti.

Peraltro, l'art. 52, par. 1, della Carta prevede che possano essere apportate limitazioni all'esercizio dei diritti e delle libertà riconosciuti da quest'ultima, purché, in primo luogo, tali limitazioni siano previste dalla legge, in secondo luogo, rispettino il contenuto essenziale dei diritti e delle libertà in questione e, in terzo luogo, nel rispetto del principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

Pertanto, una limitazione all'esercizio del diritto a un ricorso effettivo sancito dall'art. 47 della Carta può essere apportata dal legislatore dell'Unione o, in mancanza di una normativa del-

⁸⁵ V. punto 85 della pronuncia.

⁸⁶ V. punto 50 conclusioni dell'avvocato generale.

⁸⁷ V. punto 28 della pronuncia.

⁸⁸ V. punto 56 della pronuncia.

⁸⁹ V. punto 57 della pronuncia.

l'Unione in materia, dagli Stati membri, ove le condizioni previste all'art. 52, par. 1, della Carta siano rispettate ⁹⁰.

L'esito cui si giunge, quindi, è quello di fondare la valutazione sull'ammissibilità del trattamento dei dati biometrici e genetici da parte delle autorità di polizia, nell'esercizio delle loro attività, sulla trasparenza e sulla precisione della base giuridica del diritto nazionale ⁹¹.

Diversamente, ciò comporterà una lesione dei diritti e delle libertà fondamentali dell'individuo, relativamente a quanto disposto dalla normativa sulla *privacy* ⁹².

In tutte queste ipotesi è necessario considerare il caso concreto e valutare se sussistono alternative al trattamento nella stessa misura efficaci e meno invasive, anticipando le conseguenze negative sui diritti e libertà delle persone interessate e adottando strumenti adeguati diretti a ridurre i relativi rischi.

7. IL TRATTAMENTO DEI DATI BIOMETRICI E GENETICI NELL'ESPERIENZA AMERICANA: LAW ENFORCEMENT E IL IV EMENDAMENTO.

Nel lungo dibattito che da tempo anima la riflessione giuridica in materia di protezione dei dati personali e, in particolar modo negli ultimi decenni quella sul trattamento dei dati biometrici e genetici, non può prescindersi dall'analisi delle questioni giuridiche legate al trattamento di tale particolare categoria di dati personali, analizzando trasversalmente, in un'ottica comparatistica, la disciplina sui dati biometrici e genetici dell'ordinamento europeo ⁹³ con quella dell'ordinamento statunitense ⁹⁴, a partire dalla loro emersione fino alle innovazioni più recenti.

⁹⁰ V. punto 33 conclusioni dell'avvocato generale. In tal senso, la normativa bulgara (art. 68 dello ZMVR) « sembra chiaramente idonea a realizzare l'obiettivo perseguito e non appare sproporzionata, a condizione che la persona accusata abbia effettivamente la possibilità di contestare la registrazione da parte della polizia in una fase successiva, dinanzi al giudice che ne ha ordinato l'esecuzione coercitiva o dinanzi ad un altro giudice » (v. punto 38 conclusioni dell'avvocato generale).

⁹¹ A. RICCI, *Sulla "funzione sociale" del diritto alla protezione dei dati personali*, in *Contratto e impresa*, 2017, 609 ss.

⁹² S. GIRARDI, *Dati biometrici. Quo vadis per un trattamento legittimo? — Le condizioni e gli adempimenti prescritti dal GDPR per scongiurare il rischio di pregiudizi ai diritti e alle libertà delle persone fisiche*, in *iQG - Altalex*, 2021, consultabile al seguente link [https://www.altalex.com/documents/news/2021/04/23/dati-biometrici-](https://www.altalex.com/documents/news/2021/04/23/dati-biometrici-quo-vadis-per-un-trattamento-legittimo)

[quo-vadis-per-un-trattamento-legittimo](https://www.federalismi.it/nv14/articolo-documento.cfm?artid=40640); G. DI LORENZO, *La circolazione dei dati personali tra tutela della persona e ordine giuridico del mercato*, in *federalismi.it*, 21, 2019, 2 ss., consultabile al link seguente <https://www.federalismi.it/nv14/articolo-documento.cfm?artid=40640>.

⁹³ E. J. KINDT, *A First Attempt at Regulating Biometric Data in the European Union*, in A. KAK (ed.), *Regulating Biometrics, Global Approaches and Urgent Questions*, in *AI Now Institute*, 2017, disponibile al seguente link <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ainowinstitute.org/regulatingbiometrics-kindt.pdf>; R. DUCATO, *I dati biometrici*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 1288 ss., spec. 1313.

⁹⁴ Così, G. GIANNONE CODICILIONE, *La tutela della riservatezza*, in S. SICA-V. ZENO-ZENCOVICH (a cura di), *Manuale di diritto*

In particolare, con riferimento alla disamina della regolazione dei sistemi biometrici all'interno del sistema americano, occorre, in via preliminare, precisare che negli Stati Uniti non è stata ancora implementata una legislazione federale unica e completa (nonostante l'ambizioso obiettivo di adottare un testo federale sulla *privacy* sembrerebbe — quasi — essersi concretizzato con la presentazione della prima bozza normativa dell'*American Data Privacy and Protection Act* — ADPPA — formalmente introdotta nella *House of Representatives* il 21 giugno 2022, ancora in attesa di approvazione e che parrebbe ispirarsi al modello del GDPR) volta a regolare anche la raccolta e il trattamento dei dati biometrici e genetici, riscontrandosi, piuttosto, una disciplina giuridica statale frammentaria adottata dagli Stati del Texas, dell'Illinois e di Washington.

In effetti, lo Stato di Washington nel 2017, dopo quello dell'Illinois e del Texas, ha approvato una legge sulla *privacy* biometrica e, più di recente, lo Stato della California ha migliorato la sua regolamentazione sulla protezione della *privacy* alla fine del 2018 con il *California Consumer Privacy Act* (CCPA), la cui disciplina ad oggi è stata modificata dal *California Privacy Rights Act* (CPRA) approvata nel 2020, legge, quest'ultima, spesso presentata come potenziale modello per una Legge statunitense sulla *privacy* e sul trattamento personale dei dati ⁹⁵.

Tali disposizioni, tuttavia, mettono in luce come l'utilizzo di tali sistemi riceva maggiori consensi nel settore pubblico rispetto a quello privato in cui si riscontra un orientamento fondato prevalentemente su una forte deregolamentazione.

Da ciò discende un paradosso sostanziale, tale per cui l'uso di questi sistemi, generalmente vietato nei contesti pubblici, viene invece sempre più normalizzato all'interno di quelli privati, con una disciplina sulla *privacy* decisamente meno articolata rispetto alla disciplina del GDPR europeo ⁹⁶.

dell'informazione e della comunicazione, Milano, Wolters Kluwer - CEDAM, 2020, 284 ss. Per un'analisi del quadro normativo statunitense relativo ai sistemi di autenticazione basati su dati biometrici si veda, ancora, B. RUBIS, *Sistemi di autenticazione mediante l'utilizzo di dati biometrici*, cit., 304 ss.

⁹⁵ V. D.L. BURESH, *Should Personal Information and Biometric Data Be Protected Under a Comprehensive Federal Privacy Statute That Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?*, in *Santa Clara High Technology Law Journal*, 38, 1, 2021, 39 ss., consultabile al seguente link <https://digitalcommons>

<http://law.scu.edu/chtlj/vol38/iss1/2/>; K. HILL-H. MURPHY, *Your DNA Profile Is Private? A Florida Judge Just Said Otherwise*, in *The New York Times*, 2019, disponibile al seguente link <https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html>.

⁹⁶ J. ANDREW-M. BAKER, *The General Data Protection Regulation in the Age of Surveillance Capitalism*, in *Journal of Business Ethics*, 2021, 168, 565 ss.; M. PATERSON-M. McDONACH, *Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data*, in *Monash University Law Review*, 44, 1, 2018, 1 ss.; E. W. CLAYTON-C.M. HALVERSON-N.A. SATHE-B.A. MALIN, *A Systematic Literature Review of*

A ben vedere, il modello statunitense si focalizza prevalentemente sul trattamento di dati biometrici e genetici effettuati per scopi commerciali da imprese private, e risultando, per questo, decisamente più attento alle pratiche di mercato ⁹⁷.

Come già anticipato, le incisive innovazioni che il settore delle tecnologie biometriche e genetiche ha subito nel corso degli anni hanno determinato la progressiva diffusione di tali dati nei diversi settori dell'agire pubblico e privato. I sistemi biometrici hanno campi di sviluppo e di applicazione ampi e variegati. Attualmente, come già rilevato, uno dei più diffusi usi di questa particolare categoria di dati, impiegati soprattutto nella quotidianità, riguarda l'accesso a specifici luoghi o servizi nonché il consenso dell'utilizzo di dispositivi elettronici nei settori più disparati: bancario, sanitario, commerciale, dell'istruzione e delle telecomunicazioni. Tuttavia, ciò che in questa sede interessa particolarmente concerne l'utilizzo dei dati biometrici per il perseguimento di finalità connesse alla lotta contro la criminalità (i cui obiettivi primari riguardano la prevenzione, l'indagine, l'accertamento e il perseguimento dei reati, inclusa la salvaguardia e la prevenzione di minacce alla sicurezza pubblica e la libera circolazione di tali dati).

Ed è proprio in tale settore che queste tecnologie svolgono un ruolo sempre più incisivo. Tuttavia, il costante sviluppo di questi sistemi (di determinazione soprattutto biometrica), all'interno dei vari settori, può rivelarsi altamente problematico e comportare numerosi rischi dovuti all'impiego degli stessi, soprattutto con riferimento al rispetto dei diritti e delle libertà fondamentali dei suoi "utenti" ⁹⁸.

Peraltro, questi dati, espressione della relazione fra corpo e identità, hanno sollevato (e sollevano tuttora) una serie di questioni fondamentali sia da un punto di vista etico che giuridico. Ne discende che una spropositata richiesta dell'utilizzo di tali dati, che esula da situazioni di stretta necessità, determinerebbe un incremento delle minacce alla tutela della *privacy* dei singoli individui.

Per tracciare l'evoluzione della disciplina in materia di biometria, all'interno dell'ordinamento europeo e statunitense, è necessario soffermarsi sulla forte relazione del settore in esame con la

Individuals' Perspectives on Privacy and Genetic Information in the United States, in *Plos One*, 2018, 10-11, consultabile al seguente link <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0204417>.

⁹⁷ Così L. STEWART, *Big Data Discrimination: Maintaining Protection of Individual Privacy Without Disincentivizing Businesses' Use of Biometric Data to Enhance Security*, in *Boston College Law Review*,

60, 1, 2019, 349 ss., consultabile al seguente link <https://lira.bc.edu/work/ns/8c89f3a2-3848-4b97-81f1-713bc7bad862>.

⁹⁸ Cfr. F. SELTA, *Genetic Data Misuse: Risk to Fundamental Human Rights in Developed Economies*, in *Legal Issues Journal*, 7 (1), 2019, 54 ss., consultabile al seguente link <https://www.legalissuesjournal.com/article/1491/>.

tutela della *privacy*. In effetti, se, da un lato, l'utilizzo da parte delle tecnologie della biometria mira a perseguire risultati positivi, dall'altro, ciò può provocare effetti negativi che andrebbero ad impattare sulla vita delle persone.

In tal senso, si spiega la ragione per cui il crescente e, oramai, sempre più costante utilizzo della biometria nella quotidianità degli individui ha portato a ritenere come imprescindibile l'inquadramento di una efficace regolamentazione che disciplini la sicurezza di questi sistemi. A tal proposito, si ritiene che l'elaborazione di una specifica disciplina statunitense sulla biometria introdurrebbe e riconoscerebbe maggiori tutele per i diritti e le libertà degli individui.

Volendo realizzare, dunque, un confronto tra l'ordinamento europeo e quello statunitense, va evidenziato che nella predisposizione di una disciplina in materia di biometria, tali ordinamenti adottano due approcci tra loro differenti. Nel primo, l'adozione del GDPR pone una solida ed avanzata disciplina sulla *privacy*, nel secondo sussistono, invece, ancora forti contraddizioni, non essendoci un'unica regolazione posta a tutela della *privacy* e, soprattutto, in materia di biometria ⁹⁹.

Tuttavia, la bozza del testo di legge federale infonde speranza inserendo una definizione tanto di "*biometric information*" quanto di "*genetic information*".

In effetti, l'ADPPA presentata al Congresso americano, volta ad incrementare la tutela in materia di *privacy*, metterebbe in luce alcuni aspetti e alcune disposizioni volte a replicare la disciplina europea sulla *privacy*, trovando posto, in alcuni articoli, anche la materia dei dati biometrici e genetici ¹⁰⁰.

La bozza di legge, infatti, definisce rispettivamente le "*biometric information*", come « *any covered data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that is linked or reasonably linkable to an individual, including (i) fingerprints; (ii) voice prints; (iii) iris or retina scans; (iv) facial or hand mapping, geometry, or templates; or (v) gait or personally identifying physical movements* »; e le "*genetic information*", quali « *any covered data, regardless of its format, that concerns an individual's genetic characteristics, including (A) raw sequence data that results from the sequencing of the complete, or a portion of the, extracted deoxyribonucleic acid (DNA) of an individual; or*

⁹⁹ L. TRUJILLO, *In the Absence of a Uniform Biometric Law: A Proposal Comparing Current Biometric Laws, Issues, and Future Solutions*, in *Southern Illinois University Law Journal*, 46, 2021, 161 ss.

¹⁰⁰ N. GIUSTI, *Privacy, gli Usa verso*

una svolta: novità e sviluppi nella legge e nella cultura, in *Agenda Digitale*, 2022, consultabile al seguente link <https://www.agendadigitale.eu/sicurezza/privacy/privacy-gli-usa-verso-una-svolta-novita-e-sviluppi-nella-legge-e-nella-cultura/>.

(B) *genotypic and phenotypic information that results from analyzing raw sequence data described in subparagraph* »¹⁰¹.

Di contro, nell'ordinamento europeo, il dato biometrico — in passato oggetto di riflessioni dottrinali, ma mai espressamente definito — con l'introduzione del GDPR ha finalmente ottenuto autonomia concettuale attraverso una serie di specifiche disposizioni (si pensi all'art. 4, par. 14, GDPR, introduttivo di una definizione *ad hoc* nonché agli artt. 6 e 9 GDPR, relativi, rispettivamente, alle condizioni di liceità per il trattamento e al trattamento di particolari categorie di dati personali).

Nonostante ciò, lacune normative sussistono tuttora relativamente alla raccolta, all'immagazzinamento e alla conservazione di tali informazioni in banche dati (si pensi alle agenzie europee quali l'Eurodac e l'Europol che dispongono quotidianamente la raccolta di dati biometrici di cittadini europei, e non solo, all'interno di politiche di sicurezza in materia di immigrazione clandestina o per la creazione di una banca dati biometrica comune a livello europeo fra le varie forze di polizia nazionali), lasciando agli Stati membri autonomia nell'adozione di regole nazionali aggiuntive, più rigide e specifiche, utilizzate per affrontare la regolamentazione del mercato relativa a queste tecnologie¹⁰².

Trattasi di dati la cui raccolta e conservazione¹⁰³, pur non essendo impiegate per svolgere funzioni di controllo una volta acquisiti, potrebbe costituire un'interferenza sproporzionata con il diritto alla vita privata delle persone, soprattutto qualora

¹⁰¹ Cfr. ADPPA, Sec. 2. *Definitions*, (3) e (18), consultabile al seguente link <http://www.congress.gov/bills/117/th-congress/house-bill/8152/text>.

¹⁰² V., a tal riguardo, D.J. SOLOVE, *Data is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data*, in *Northwestern University Law Review*, 2023, 2 ss., disponibile al link seguente https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198; A. M. CAPITTA, *Conservazione dei DNA profiles e tutela europea dei diritti dell'uomo*, in *Archivio Penale*, 1, 2013, 141 ss.; L. SCAFFARDI, *Giustizia genetica e tutela della persona. Uno studio comparato sull'uso (e abuso) delle Banche dati del DNA a fini giudiziari*, Padova, CEDAM, 2017, 19 ss.; E. GATTI, *Il DNA come strumento di identificazione, esigenze investigative e diritti della persona: uno sguardo alla giurisprudenza ed alla prassi*, in *Questione Giustizia*, 2021, consultabile al seguente link <https://www.questionegiustizia.it/articololil-dna-come-strumento-di-identificazione-esigenze-investigative-e-diritti-dell>

a-persona-uno-sguardo-alla-giurisprudenza-ed-alla-prassi.

¹⁰³ In proposito, si veda ancora l'art. 5, della proposta di regolamento che stabilisce regole armonizzate sull'intelligenza artificiale — Legge sull'intelligenza artificiale — e modifica alcuni atti legislativi dell'unione, {SEC(2021) 167 final} — {SWD(2021) 84 final} — {SWD(2021) 85 final, consultabile al seguente link <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206&from=IT> (analizzato *supra*, par. 5); Consiglio europeo, comunicato stampa 1008/22, 6 dicembre 2022, <https://www.consilium.europa.eu/it/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/>; nonché gli emendamenti alla predetta proposta, approvati il 14 giugno 2023, dal Parlamento europeo, consultabili al link seguente https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_IT.html. Sulla questione si consulti, altresì, V. CARREDDA, *Campioni biologici e Big Data: l'evoluzione del consenso*, in *Diritto di Famiglia e delle Persone (II)*, 3, 2022, 1071 ss.

vengano sottoposti a forme di trattamento automatizzate e siano conservati in *database* di polizia ¹⁰⁴.

Tuttavia, nel contesto europeo, nessun Paese membro ha ancora elaborato e introdotto un quadro giuridico di livello primario per i sistemi biometrici e genetici. Per cui, la mancanza di una legislazione nazionale specifica sulla biometria e sulla genetica che integri il modello europeo riflette le difficoltà che questi sistemi pongono ai legislatori nazionali (così come accaduto in Bulgaria). Da ciò si deduce, quale diretta conseguenza di tale aspetto, la necessità di trovare un equilibrio tra il sistematico trattamento dei dati biometrici e genetici e la protezione degli individui, non sempre così agevole da perseguire.

Diversamente, nell'ordinamento statunitense si assiste ad un approccio che si discosta fortemente dalla presenza di un'unica, rigida e mirata disciplina sulla *privacy* e sul trattamento dei dati biometrici e genetici, riconoscendo un ampio spazio di autonomia ai singoli Stati ¹⁰⁵.

Per questo, è apparsa auspicabile l'introduzione nella disciplina statunitense di alcuni istituti in materia della *privacy* disposti dalla disciplina europea.

Passando, invece, alla regolazione dei trattamenti di dati biometrici da parte di autorità di pubblica sicurezza, mentre negli Stati Uniti si assiste ad una fortissima deregolamentazione di tali sistemi (attribuendo un potere arbitrario estremamente ampio ad agenzie e organi federali e nazionali), in ambito europeo, anche l'uso di sistemi biometrici da parte di poteri pubblici viene regolamentato.

Eppure vi è un numero sempre più elevato di soggetti pubblici attivamente coinvolti nel trattamento di dati biometrici per finalità di prevenzione del crimine, sicurezza e contrasto al terrorismo, di cui possono disporre senza alcuna giustificazione delle

¹⁰⁴ Si consulti C.M. CASCIONE, *La 'data retention' tra lotta al crimine e aspettative di privacy* [Nota a sentenza: CGUE, grande sez., 2016, (cause riunite C-203/15 e C-698/15)], in *Giustizia civile.com*, 4, 2, 2017, 1 ss.; *Id.*, *I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione data retention della Corte di giustizia e gli echi del datagate* (Commento a Corte giust.UE, grande sez., 8 aprile 2014, cause riunite C-293/12 e C-594/12), in *La nuova giurisprudenza civile commentata*, 30, 11, 2014, 1044 ss.

¹⁰⁵ A partire dal 2023 sono entrate (ed entreranno) in vigore una serie di leggi statali sulla *privacy* degli Stati Uniti.

Tra questi, il più significativo è il *California Privacy Rights Act* (CPRA), che modifica e rafforza il *California Consumer Privacy Act* (CCPA). Il CPRA è entrato in vigore il 1° gennaio 2023 e diventerà esecutivo a partire dal 1° luglio 2023. Altre leggi statali statunitensi che entreranno in vigore quest'anno includono il *Virginia Consumer Data Protection Act* (VDPA), il *Colorado Privacy Act* (CPA), il *Connecticut Data Privacy Act* (CDPA) e lo *Utah Consumer Privacy Act* (UCPA). Il VDPA è entrato in vigore il 1° gennaio 2023, il CPA e il CDPA, invece, entreranno in vigore il 1° luglio 2023. Infine, l'UCPA entrerà in vigore dal 31 dicembre 2023.

loro finalità e senza dover incorrere in alcun tipo di limitazione ¹⁰⁶.

Nello specifico, sebbene il governo federale da tempo si sia fatto promotore di iniziative di raccolta di dati biometrici, tuttavia l'assenza di un insieme di precise regole nell'adozione dei sistemi di riconoscimento biometrico ne rivela la fallacia. Infatti, queste tecnologie possono interferire notevolmente nella tutela della *privacy* delle persone coinvolte, attuando vere e proprie azioni di controllo e profilazione e venendo in contro al possibile (e probabile) rischio di interferenza delle primarie finalità di sicurezza e interesse pubblico ¹⁰⁷.

Inoltre, nel sistema statunitense, la materia in cui si riscontra maggiormente la lesione dei diritti e delle libertà degli individui è quella inerente il trattamento dei dati genetici. L'esempio più diffuso è quello connesso al prelievo di campioni di DNA. Ciò che in tale contesto, desta particolare preoccupazione riguarda proprio le informazioni sul corpo così raccolte e tutte le conseguenze che tali informazioni comportano sull'individuo. Per di più, l'archiviazione e, dunque, la conservazione in apposite banche dati, di tali informazioni consente di effettuare ricerche su larga scala sui sospettati per periodi di tempo indefiniti ¹⁰⁸.

Ciò genera una lesione del diritto dell'individuo secondo quanto disposto dal IV Emendamento della Costituzione americana, evidenziandosi la gravità della violazione dell'integrità fisica e della *privacy* derivante dal prelievo di campioni di DNA dagli indagati.

Difatti, il DNA, considerato uno dei più potenti strumenti di risoluzione dei crimini per le forze dell'ordine, ha subito un'evoluzione guidata dalla conservazione di una grande quantità di dati genetici in *database* governativi, pubblici e privati, e dall'emersione di nuove tecniche utilizzate per sfruttare queste risorse ¹⁰⁹.

Un fenomeno particolarmente diffuso, nel sistema statunitense, è quello che consente alle autorità di polizia di utilizzare sempre più spesso le banche dati genetiche, sia mediante la richiesta del profilo del DNA di un sospettato identificato da una banca dati

¹⁰⁶ W.A. LOGAN, *Policing Police Access to Criminal Justice Data*, in *Iowa Law Review*, 104, 2, 2019, 649 ss.

¹⁰⁷ J.P.M. GABA-J.J.M. ESTREMADURA, *Data Protection of Biometric Data and Genetic Data*, in *Ateneo Law Journal*, 64, 2020, 949 ss.

¹⁰⁸ I. VAN DER PLOEG, *Genetics, Biometrics and the Informatization of the Body*, in *Ann Ist Super Sanità*, 43, 1, 2007, 49 ss.

¹⁰⁹ J.W. HAZEL-C. SLOBOGIN, "A World of Difference"? *Law Enforcement, Genetic Data, and the Fourth Amendment*, in *Duke Law Journal*, 70, 4, 2021, 707 ss.; C. SLOBOGIN, *A Defense of Privacy as the Central*

Value Protected by the Fourth Amendment's Prohibition on Unreasonable Searches, in *Texas Tech Law Review*, 48, 2015, 143 ss.; A. REGALADO, *Hundreds of Crimes Will Soon Be Solved Using DNA Databases, Genealogist Predicts*, in *MIT Technology Review*, 2018, consultabile al seguente link <https://www.technologyreview.com/2018/09/13/140207/hundreds-of-crimes-will-soon-be-solved-using-dna-databases-genealogist-predicts/>; C. SLOBOGIN, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment*, U.S., The University of Chicago Press, 2007, 1 ss., spec. 21 ss.

sia, più comunemente, confrontando il DNA prelevato dalla scena del crimine con quello conservato in una banca dati nel tentativo di identificare il sospettato o un familiare del medesimo ¹¹⁰.

Pertanto, in un contesto del genere, appare di fondamentale rilevanza l'analisi della disciplina del IV Emendamento ¹¹¹ dal cui dettato letterale discende che il tentativo di valutare le aspettative della società in materia di *privacy* suggerisce che l'accesso alle informazioni genetiche da parte delle forze dell'ordine sia parificato o considerato più invasivo delle perquisizioni che si eseguono nelle abitazioni, controllando sms o la *mail* e, in modo più incisivo, quando il DNA di una persona viene prelevato dalle forze dell'ordine facendo uso di banche dati per fini inerenti la sicurezza pubblica ¹¹².

Sulla base di tale assunto, può dedursi che sia l'accesso della polizia a banche dati genetiche non governative sia l'uso di metodi occulti per raccogliere il DNA richiedono un'apposita autorizzazione giudiziaria ¹¹³.

Ciò nonostante, né la raccolta di campioni genetici né la loro analisi e il loro uso da parte delle forze dell'ordine sono stati oggetto di un'apposita regolamentazione.

Significativo, a riguardo è il noto caso *Maryland v. King* ¹¹⁴. Con tale sentenza, la Corte Suprema si è pronunciata sui presupposti di legittimità delle misure restrittive della libertà personale, oggetto della garanzia di cui al IV Emendamento, e sulle istanze di tutela della riservatezza che esse chiamano in causa. Tale caso riguarda Alonzo King arrestato (accusato e rinviato a giudizio) per aggressione nel 2009 e sottoposto al prelievo di un campione salivare, sulla base del *Maryland DNA Collection Act*, che dispone la predetta operazione a carico di tutti i soggetti arrestati, ma non ancora condannati, per una serie di crimini violenti. Il profilo genetico dell'arrestato coincideva con un campione raccolto nel 2003 e conservato nella banca dati CODIS (*Combined DNA Index System*, *software* che permette l'organizzazione dei dati relativi al DNA) per una violenza sessuale. Questa corrispondenza fu utiliz-

¹¹⁰ L.E. WOLF-L.M. BESKOW, *Genomic Databases, Subpoenas, and Certificates of Confidentiality*, in *Genetics in Medicine*, 21, 2019, 2681 ss.

¹¹¹ Che recita espressamente: « *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized* ».

¹¹² Cfr. J.W. HAZEL-C. SIOBOGIN, « *A World of Difference* »? *Law Enforcement, Genetic Data, and the Fourth Amendment*, cit., 711 ss.

¹¹³ S. HUNT-BLACKWELL, *You Have the Right to Remain Private: Safeguarding Biometric Identifiers in Civil and Criminal Contexts*, in *Tulane Journal of Technology and Intellectual Property*, 2022, 205 ss.

¹¹⁴ Si veda, in tal senso, 569 U.S. 435 (2013), disponibile al seguente link <https://www.law.cornell.edu/supremecourt/text/12-207>.

zata come unico elemento di prova per la condanna all'ergastolo ¹¹⁵.

L'imputato eccepiva l'incostituzionalità della legge del Maryland, la quale, prevedendo una limitazione della libertà personale irragionevole e non giustificata da uno specifico e circostanziato sospetto, avrebbe violato il IV Emendamento (che appunto tutela l'individuo soltanto dalle "perquisizioni irragionevoli").

La difesa di King e la pretesa incostituzionalità della pratica di prelievo del DNA mediante tampone salivare si fondarono interamente sulla differenza fra tale pratica e il rilevamento delle impronte digitali: mentre lo scopo del secondo intervento sarebbe quello di identificare il sospettato, il prelievo di DNA avrebbe come unica finalità quella di trovare un colpevole per casi irrisolti ¹¹⁶.

Si evidenzia nel dettaglio, in questo caso, la necessità da parte della Corte di bilanciare la pluralità di interessi pubblici meritevoli di tutela che fronteggiano la libertà personale e il diritto alla riservatezza del soggetto sottoposto al prelievo del DNA ¹¹⁷.

Le nuove tecnologie investigative hanno imposto al Supremo organo statunitense « un' *actio finium regundorum*, volta a ricondizionare l'equilibrio fra sicurezza e libertà: da un lato, esse rappresentano uno strumento di impareggiata efficacia attraverso cui lo Stato assolve i compiti di difesa sociale; dall'altro, non può ignorarsi la loro potenziale lesività al cospetto della pretesa dell'individuo a disporre di una sfera intima inattuabile per l'autorità » ¹¹⁸.

La Corte conclude, quindi, che il prelievo di DNA sia una « *reasonable search* », equiparabile al rilevamento delle impronte digitali e alle foto segnaletiche e, perciò, compatibile con il IV Emendamento. Prosegue evidenziando come le forze di polizia possano legittimamente raccogliere campioni di DNA da individui accusati di gravi reati (tra cui « *violence, attempted crimes of violence, burglaries, or attempted burglaries* ») ¹¹⁹.

¹¹⁵ D. DE LUNGO, *Libertà e sicurezza: Maryland v. King ovvero il IV Emendamento nell'era del DNA*, in *Diritti Comparati*, 2013, 1 ss., consultabile al link seguente <https://www.diritticomparati.it/liberta-e-sicurezza-maryland-v-king-ovvero-il-iv-emendamento-nellera-del-dna/>.

¹¹⁶ In tal senso, si v. A. ROTH, *Maryland v. King and the Wonderful, Horrible DNA Revolution in Law Enforcement*, in *Ohio State Journal Of Criminal Law*, 11, 2013, 295 ss.

¹¹⁷ Si veda, ancora, D. DE LUNGO, *Libertà e sicurezza: Maryland v. King ovvero il IV Emendamento nell'era del DNA*, cit., 1

ss., il quale specifica che tra gli interessi pubblici meritevoli di tutela vi rientrano quello all'identificazione dell'arrestato, alla garanzia della sicurezza del personale carcerario e dei detenuti, all'effettivo svolgimento del processo, al giudizio sulla pericolosità sociale nonché quello all'eventuale proscioglimento di individui erroneamente accusati.

¹¹⁸ *Ibidem*, cit., 4.

¹¹⁹ Cfr. D.H. KAYE, *Why So Contrived? Fourth Amendment Balancing, Per Se Rules, and DNA Databases after Maryland v. King*, in *The Journal of Criminal Law & Criminology*, 104, 3, 535 ss.

Dalla disamina, dunque, il sistema statunitense, quanto alla raccolta di dati personali — biometrici, ma soprattutto genetici — parrebbe molto meno restrittivo, prediligendo il fine della lotta alla prevenzione e alla criminalità, e tutelando gli individui soltanto in stringenti e limitati casi.

8. BREVI CENNI CONCLUSIVI.

Volendo trarre qualche sintetica considerazione da quanto fin qui esposto, potrebbe rilevarsi che il *fil rouge* che lega tutti i casi e le normative analizzate possa essere individuato nel forte bisogno di ripensare il ruolo del diritto in tema di trattamento di dati biometrici e genetici che, dinanzi all'avanzamento tecnologico, ha il compito non di frenarne lo sviluppo e le potenzialità, bensì di individuare il corretto bilanciamento tra diritti e interessi.

Nel contesto europeo siamo abituati, di fronte all'utilizzo dei dati personali, a vedere la garanzia della sicurezza come contrapposta alla tutela della *privacy* e alla protezione dei dati. Ciò evidenzia quanto le nuove tecnologie, mediante l'uso di dati, quali quelli biometrici e genetici, vengano impiegate per risolvere problematiche anche connesse all'ambito delle indagini o di prevenzione dei crimini, oltre che per rispondere ad altri bisogni fondamentali ¹²⁰.

Tale utilizzo non può che aprire a tutta una nuova serie di considerazioni e valutazioni sulla proporzionalità delle misure adottate. Compito del legislatore, del giudice e del giurista in generale, è far sì che, di fronte a queste prospettive, le garanzie costituzionali non debbano essere lese dal trattamento di dati, e ciò deve valere ancor più quando in gioco vi è la cessione di una parte dell'individuo stesso, come quella che avviene appunto mediante l'utilizzo di tale particolare categoria di dati. In questa ipotesi, assumerebbe grande valore la produzione di regole in grado di prevedere e arginare i rischi e le compressioni sproporzionate dei diritti fondamentali alla riservatezza e alla protezione dei dati, anche e soprattutto in un'era « *of ubiquitous dataveillance* » ¹²¹.

Per tale ragione, si individua l'esigenza di integrare, rendendolo il più completo possibile, il quadro normativo applicabile ai dati biometrici e genetici mediante il riconoscimento di apposite ed

¹²⁰ Cfr. A. CARAVITA DI TORITTO, *La proporzionalità multilivello nel mercato "presidiato" dei dati personali*, cit., 157 ss., consultabile al seguente link <https://www.medialaws.eu/rivista/la-proporzionalita-multilivello-nel-mercato-presidiato-dei-dati-personali/>.

¹²¹ Così, Y. McDERMOTT, *Conceptualizing the Right to Data Protection in an Era of Big Data*, in *Big Data and Society*, 1, 2017, 1 ss.

efficaci misure di garanzia (oltre alla promozione di regole deontologiche) ¹²².

Abstract

The paper proposes to analyze the processing of genetic and biometric data in the light of current European regulations. After a brief introduction on the concept of biometric and genetic data, the scope of application, as well as the protection and safeguard of this type of data, the focus shifts on the recent CJEU decision (Case C-205/21), which ruled on the “systematic” collection of biometric and genetic data by any person formally accused of an intentional offense subject to public prosecution, comparing the discipline of the GDPR with that of the Directive (EU) 2016/680 (the so-called Law Enforcement Directive)-(LED), followed by some remarks on the “AI Act” (recently amended and approved by the European Parliament).

Finally, the study analyzes, in a comparative perspective, the Privacy regulation in the U.S. legal system. In particular, it refers to the collection and use of biometric and genetic data, with regard to the infringement of the individual’s fundamental rights and freedoms resulting from the violation of the processing of this particular category of personal data.

¹²² V. F. FILOSA, *Dati genetici e biometrici, manca all’appello l’intervento del Garante*, cit., consultabile al seguente link

<https://www.agendadigitale.eu/sicurezza/dati-genetici-in-standby-manca-allappello-lintervento-del-garante/>.