

La tutela del dato genomico in Italia nel caso specifico della fenotipizzazione del DNA forense. Prospettive di normazione

Monica De Angelis, Luca Megale*

THE PROTECTION OF GENOMIC DATA IN ITALY IN THE SPECIFIC CASE OF FORENSIC DNA PHENOTYPING: REGULATORY PROSPECTS

ABSTRACT: The paper explores the use of Forensic DNA Phenotyping (FDP) in Italy and the EU, an investigative technique that infers physical characteristics from biological traces. It highlights how FDP raises significant concerns regarding the protection of genetic data and the risk of discrimination. The relevant legislation is examined to underline the potential violation of privacy and the lack of a specific regulatory framework governing its use and providing adequate safeguards. The paper also assesses the impact of artificial intelligence in support of FDP, warning of an amplification of the associated risks. Suggestions are put forward to balance public security with the right to personal data protection.

KEYWORDS: forensic DNA phenotyping; genomic data protection; proportionality principle; artificial intelligence; privacy

ABSTRACT: Il contributo esplora l'uso della fenotipizzazione del DNA forense (FDP) in Italia e nell'UE, una tecnica investigativa che deduce caratteristiche fisiche da tracce biologiche. Viene evidenziato come l'FDP sollevi rilevanti preoccupazioni riguardo alla protezione dei dati genetici e al rischio di discriminazione. Viene esaminata la normativa rilevante per sottolineare la potenziale violazione della privacy e la mancanza di un quadro normativo specifico che ne regoli l'uso e offra adeguate garanzie. Il contributo valuta anche l'impatto dell'intelligenza artificiale a supporto della FDP, paventando un'amplificazione dei rischi. Vengono proposti suggerimenti per bilanciare la sicurezza pubblica con il diritto alla protezione dei dati personali.

* Monica De Angelis: Professore associato di diritto amministrativo presso l'Università Politecnica delle Marche. Mail: m.deangelis@staff.univpm.it. Luca Megale: Assegnista di ricerca in diritto amministrativo presso l'Università LUMSA di Roma. Mail: l.megale@lumsa.it. Lo scritto rappresenta il risultato di una riflessione congiunta degli autori; tuttavia, Monica De Angelis ha redatto i §§ 1. e 6., mentre Luca Megale ha redatto i §§ 2., 3., 4., e 5. Il presente contributo è frutto della ricerca svolta dagli autori nell'ambito del Progetto "Legal, ethical and social challenges of the Forensic DNA Phenotyping in Italy (LetFor)", codice proposta: 2022TL8TAE_001 - CUP: J53D23005950006. Finanziato dall'Unione Europea – NextGenerationEU a valere sul Piano Nazionale di Ripresa e Resilienza (PNRR) – Missione 4 Istruzione e ricerca – Componente 2 Dalla ricerca all'impresa – Investimento 1.1, Avviso Prin2022 indetto con DD N. 104 del 2/2/2022. Contributo sottoposto a doppio referaggio anonimo.

PAROLE CHIAVE: fenotipizzazione del Dna forense; protezione dei dati genomici; principio di proporzionalità; intelligenza artificiale; privacy

SOMMARIO: 1. Introduzione. La Fenotipizzazione del DNA Forense (FDP): un caso emblematico tra progresso tecnologico e sfide normative – 2. La FDP: il dato genomico tra quadro normativo e rischio di abusi – 3. L'intersezione tra FDP e intelligenza artificiale: potenziali vantaggi e rischi amplificati – 4. Le garanzie nel trattamento dei dati FDP: consenso, stretta necessità e sfida della proporzionalità – 5. Prospettive future: suggerimenti per una normazione bilanciata e resiliente della FDP – 6. Alcune ulteriori riflessioni. Il caso della FDP come sfida della normazione sulle tecnologie moderne.

1. Introduzione. La Fenotipizzazione del DNA Forense (FDP): un caso emblematico tra progresso tecnologico e sfide normative

Il progresso scientifico e tecnologico pone costantemente interrogativi, la cui risposta non è di facile individuazione, e non è esente il settore sanitario (a maggior ragione se correlato all'ambito della sicurezza pubblica e investigativa). La fenotipizzazione del DNA forense (FDP), pur rappresentando un avanzamento significativo nelle tecniche investigative, ne è un chiaro esempio. Tale tecnica, che consente di dedurre caratteristiche fisiche da tracce biologiche trovate sulla scena del crimine, solleva infatti rilevanti preoccupazioni riguardo alla tutela dei dati sanitari e al rischio di discriminazione. La FDP, pur non permettendo l'identificazione certa di un individuo, consente infatti di dedurre¹ alcune caratteristiche fenotipiche con un certo grado di probabilità². Nel contesto investigativo, la FDP – partendo dal materiale biologico trovato in una scena del crimine – mira a restringere la ricerca a un gruppo di possibili sospettati accomunati da tratti genetici simili, così da guidare le indagini di polizia in casi senza sospetti noti³. Le risultanze divengono dunque la base dell'attività di polizia.

Si pensi al caso della Polizia di Edmonton (Canada) che ha diffuso sui propri canali social il ritratto, generato digitalmente⁴, di un sospettato. In mancanza di piste concrete, l'autorità si è rivolta a un'impresa privata per analizzare il DNA trovato sulla scena del crimine e ricostruire le caratteristiche fisiche dell'individuo attraverso la tecnica della FDP. L'immagine mostrava precisamente il viso di un uomo, là dove le informazioni fornite dal DNA indicavano solo che il soggetto aveva possibili origini dall'Africa orientale,

¹ Si parla, nello specifico, di inferenza probabilistica. Sul punto, si veda G. SAMUEL, B. PRANSACK, *The regulatory landscape of forensic phenotyping in Europe*, VISAGE, Novembre 2018.

² M. BOTTO, *Il DNA da "prova regina" a "testimone biologico"? I controversi effetti delle nuove frontiere dell'analisi genetico-forense sulla governance of crime*, in *La legislazione penale*, 23 gennaio 2025, 13.

³ Nelle più comuni pratiche di polizia e giudiziarie, il DNA è utilizzato per accertare l'identità di un sospetto. La FDP non ha invece finalità di prova confermativa, ma un'utilità investigativa in casi di mancanza di sospetti. Si vedano, tra gli altri, M. KAYSER, *Forensic DNA Phenotyping: Predicting human appearance from crime scene material for investigative purposes*, in *Forensic Science International: Genetics*, 18, 2015, 33-48; P.M. SCHNEIDER *et al.*, *The use of forensic DNA phenotyping in predicting appearance and biogeographic ancestry*, in *Dtsch. Arztebl. Int.*, 51-52, 2019, 873 – 880; G. SAMUEL E B. PRANSACK, *Forensic DNA phenotyping in Europe: views "on the ground" from those who have a professional stake in the technology*, in *New Genet. Soc.*, 38, 2019, 119 – 141.

⁴ Il caso è affrontato, offrendo anche altri esempi, da A. DURKIN, *Estimating a Face: What Predicting Appearance from DNA Reveals About the Need to Regulate Genetic Investigations*, in *Washington Law Review*, 101, 2022, 1241 ss. Il contributo ha anche il merito di analizzare il quadro regolatorio e le pronunce giurisprudenziali nell'incertezza data dalla frammentazione normativa dei singoli Stati USA, arrivando a proporre un intervento federale.



una carnagione scura e occhi di colore marrone o nero. La condotta ha suscitato vive critiche per la marcata superficialità con cui l'immagine è stata prodotta sulla base di indicazioni meramente sommarie. Se si vuole vedere un'esperienza domestica, si consideri il «caso Gambirasio»: qui la FDP è stata utilizzata per scoprire il colore degli occhi del sospettato ignoto, come richiamato anche dalla pronuncia della Corte di Assise di Appello di Brescia⁵.

Questo metodo, sebbene rappresenti un chiaro avanzamento nelle tecniche investigative, solleva perplessità giuridiche (oltre che etiche) poiché l'uso di informazioni probabilistiche derivanti dal DNA potrebbe comportare rischi di discriminazione o pregiudizio nei confronti di determinati gruppi di persone⁶, senza considerare la possibile erosione della fiducia dei privati nelle forze di polizia.

Ad esempio, vi è il rischio di un *confirmation bias* insito nell'attività investigativa; vale a dire, l'errore cognitivo che potrebbe portare, ad esempio, a concentrarsi solo sul primo sospetto in linea con le caratteristiche anticipate dalla FDP, ignorando altri possibili individui. Parimenti, si manifesta il rischio di *implicit bias*, per cui qualora l'analisi FDP indichi una specifica pigmentazione della pelle, le indagini potrebbero eccessivamente focalizzarsi su individui appartenenti a quel gruppo etnico, anche a fronte di successive prove divergenti. Sussiste altresì il pericolo di *tunnel vision*, ovvero la tendenza a concentrarsi su un'unica teoria investigativa, disattendendo la natura meramente probabilistica dei risultati.

La FDP non è, peraltro, una tecnica priva di possibili errori. Sebbene i risultati dell'analisi indichino quale sia la probabilità maggiore di un tratto (ad esempio, occhi azzurri), esiste una concreta possibilità che la risultanza più probabile non corrisponda a quella reale⁷. Senza considerare che i profili erroneamente ritenuti appartenere a un autore del reato possono, in realtà, provenire da fonti esterne, come il personale presente sulla scena del crimine o altri individui che introducono involontariamente una contaminazione⁸. Lo scritto si propone dunque di analizzare l'impatto sull'ordinamento giuridico del rapido sviluppo delle tecnologie di fenotipizzazione del DNA forense, con particolare attenzione al tema del trattamento dei dati sanitari per finalità di pubblico interesse (quale la tutela della sicurezza pubblica). Tale caso, pur non essendo isolato, costituisce un microcosmo di una sfida ben più ampia che il diritto moderno è chiamato ad affrontare: la regolamentazione delle nuove tecnologie. Esiste infatti una discrasia tra i tempi rapidi del progresso scientifico e quelli più lenti del legislatore e dell'amministrazione, rendendo ardua la costruzione di una cornice normativa adeguata. Le nuove tecnologie hanno un impatto pervasivo sul bilanciamento tra diritti fondamentali. Temi come la privacy, l'etica, la sicurezza dei dati, la discriminazione e la responsabilità sono costantemente messi in discussione, come si è visto nel caso della FDP. L'incertezza sul quadro regolatorio, pur non limitando l'impiego della tecnica da parte delle autorità, pone seri interrogativi sulle garanzie offerte ai soggetti interessati. Le informazioni genomiche sono infatti immutabili,

⁵ Si veda M. BOTTO, *Il DNA da "prova regina" a "testimone biologico"? I controversi effetti delle nuove frontiere dell'analisi genetico-forense sulla governance of crime*, cit., 15.

⁶ M. KAYSER, *Forensic DNA Phenotyping: Predicting human appearance from crime scene material for investigative purposes*, cit., 40.

⁷ NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, *Law Enforcement Use of Probabilistic Genotyping, Forensic DNA Phenotyping, and Forensic Investigative Genetic Genealogy Technologies: Proceedings of a Workshop*. Washington, DC, The National Academies Press, 2025, 55 ss. In particolare, Rebecca Brown ha segnalato, nel corso del convegno, come negli Stati Uniti la polizia abbia usato evidenze preliminari (fornite dalla FDP) per richiedere un test del DNA a centinaia di individui di origine ispanica solo poiché residenti nell'area.

⁸ S. CARSON et al., *The potential for investigator-mediated contamination to occur during routine search activities*, in *Forensic Sci. Med. Pathol.*, 18(3), 2022, 299 – 310.

uniche e capaci di rivelare dati sensibili sulla salute, sul fenotipo e su aspetti personali, passati e futuri, dell'individuo e dei suoi familiari⁹.

L'evoluzione della ricerca scientifica richiede, pertanto, come si vedrà, una sorta di “modulazione normativa”: il caso della FDP, con la sua rapida evoluzione e l'incertezza scientifica in alcuni aspetti dei suoi risultati, rende palese questa necessità di cautela e gradualità. La problematica è ulteriormente amplificata dalla crescente intersezione con l'Intelligenza Artificiale (IA), ove i sistemi – utilizzati per esaminare ampi set di dati genomici e creare modelli predittivi – rischiano di introdurre o amplificare *bias* e di minare la trasparenza, l'affidabilità e la validità dei risultati prodotti¹⁰. Questo solleva nuove e complesse domande sulla trasparenza, affidabilità e sorveglianza di massa, assimilando l'uso della FDP, in contesti di ordine pubblico, alla sorveglianza biometrica¹¹. Ciò si collega direttamente alla questione della responsabilità per le azioni generate da macchine con capacità cognitive autonome, un tema che il diritto fatica a inquadrare con le categorie tradizionali. Questioni di questo genere, che spaziano dalla protezione dei dati sanitari alla polizia di sicurezza come attività amministrativa preventiva¹², richiedono un'analisi approfondita dello stato dell'arte in UE e in Italia circa la tutela del dato genomico, i poteri riconosciuti alle autorità coinvolte e le garanzie per i soggetti.

La presente indagine si concentrerà sulla protezione dei dati sanitari e sull'attività di polizia di sicurezza, intesa quale funzione amministrativa prevalentemente preventiva. Essa non si estenderà alla legittimità

⁹ Sulla mancanza di una nozione sui dati genetici e il concetto di “unico e irripetibile” (tranne nei casi di gemelli), si veda A. IANNUZZI, F. FILOSA, *Il trattamento dei dati genetici e biometrici*, in S. SCAGLIARINI (a cura di), *Il “nuovo” codice in materia di protezione dei dati personali. La normativa italiana dopo il d.lgs. 101/2018*, Torino, 18 ss. Si veda anche C. JASERAND, *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*, 2 (3), 2016, 297 ss.

¹⁰ N. TERRADO-ORTUÑO, P. MAY, *Forensic DNA phenotyping: a review on SNP panels, genotyping techniques, and prediction models*, in *Forensic Sciences Research*, 10, 1, 2025. M.A., KATSARA et al., *VISAGE Consortium. Evaluation of supervised machine-learning methods for predicting appearance traits from DNA*, in *Forensic Sci Int Genet.* 2021. M. BARASH et al., *Machine learning applications in forensic DNA profiling: A critical review*, in *Forensic Science International: Genetics*, 69, 2024.

¹¹ M. COQUET, N. TERRADO-ORTUÑO, *Forensic DNA phenotyping: privacy breach, bias reification and the pitfalls of abstract assessments of rights*, in *Int. J. Police Sci. Manag.*, 25, 2023, 265. Ad esempio, lo strumento potrebbe andare oltre la descrizione dei tratti somatici di un soggetto, arrivando a fornire informazioni sullo stato di salute di un individuo unicamente sulla base della sua presenza in un determinato luogo. Negli ultimi anni, i progressi sono stati significativi. La previsione dell'aspetto del DNA include il colore degli occhi, dei capelli e della pelle, ma anche il colore delle sopracciglia, eventuali lentiggini, la struttura dei capelli, l'eventuale perdita di questi negli uomini e la statura. Inoltre, si è ora in grado di identificare l'ascendenza biogeografica continentale e subcontinentale, sino a stimare l'età del DNA e a identificare la predisposizione a malattie. Si veda, M. KAYSER ET AL., *Recent advances in Forensic DNA Phenotyping of appearance, ancestry and age*, in *Forensic Sci. Int. Genet.*, 65, 2023, 102870 ss. Una società operante nel settore afferma di essere arrivata a poter ricostruire la morfologia del volto. Si veda: <https://parabon-nano-labs.com/>.

¹² Indipendentemente dal fatto che l'evento costituisca un illecito penale o amministrativo, il potere di polizia ha infatti lo scopo di prevenire i rischi per la sicurezza pubblica. Cfr. P. VIRGA, *La potestà di polizia*, cit., 6.



dell'accertamento tecnico nel procedimento penale¹³, ma sarà guidata dal principio di legalità¹⁴, il quale impone che la legge disciplini le modalità di svolgimento dell'azione amministrativa per prevenire abusi¹⁵. Non si omette di considerare la normativa generale in materia di trattamento dei dati personali, con particolare riferimento alle disposizioni sui dati genetici; tuttavia, come meglio si spiegherà nel § 2, la ricerca si concentra prevalentemente sulla disciplina più direttamente connessa al caso in esame, ossia quella relativa al trattamento dei dati per finalità di polizia.

Al fine di contribuire ad un dibattito in fase crescente, l'analisi offerta da queste pagine mira a delineare i dubbi sul possibile uso della tecnica con una revisione della normativa domestica e a proporre suggerimenti utili per declinare le necessarie garanzie in un possibile disegno di legge in materia di utilizzo della FDP.

2. La FDP: il dato genomico tra quadro normativo e rischio di abusi

Prima di concentrarsi sulla normativa rilevante in materia di FDP, è opportuno comprendere il contesto in cui si muove, vale a dire i dati genetici. Un genoma racchiude materiale ereditario che rappresenta l'intero insieme di "istruzioni" necessarie a formare un organismo, rimanendo largamente invariato dal concepimento sino alla morte¹⁶. Alcuni geni determinano caratteristiche osservabili (vale a dire, fenotipi),

¹³ Sul punto si rinvia ai lavori di esperti del settore scientifico disciplinare di riferimento, ad es. M. BOTTO, *Il DNA da "prova regina" a "testimone biologico"? I controversi effetti delle nuove frontiere dell'analisi genetico-forense sulla governance of crime*, cit. Peraltro, lo scritto identifica – correttamente – anche altri usi di interesse nell'ambito investigativo, come nel caso dell'identificazione delle vittime di disastri su larga scala. Si veda anche F. SANVITALE, *Quello che il legislatore non dice in tema di prova genetica. Dalla banca dati nazionale del DNA al familial searching*, in *La legislazione penale*, 18 aprile 2024, 1 ss.

¹⁴ La legge, come noto, non solo stabilisce limiti per l'attività amministrativa, ma deve disciplinare anche le modalità di svolgimento dell'azione, con l'obiettivo di prevenire eventuali abusi. L'uso della FDP va letto dunque anche in funzione al principio di legalità, là dove «le norme regolano, altresì, le modalità di svolgimento dell'attività amministrativa di prevenzione, nonché le decisioni e la relativa efficacia che l'Autorità di polizia può adottare»: così R. URSI, *Il parametro della pericolosità e i poteri di polizia di sicurezza*, in *Amministrativ@mente*, 3, 2022, 54 e 57 ss. È noto, infatti, che l'attività di prevenzione della polizia si esercita nei casi e nei modi espressamente indicati dalla legge. In questo senso la Corte cost., 18 marzo 1957, n. 45, ma anche O. RANELLETTI, *La polizia di sicurezza*, in V.E. ORLANDO (a cura di), *Primo trattato completo di Diritto amministrativo italiano*, IV, Milano, 1904, 348.

¹⁵ La ricerca sul tema della sicurezza pubblica ha subito periodi di interesse più o meno intensi, ma è certamente ricco il dibattito nel complesso. Si parte dalla sicurezza come ordine della conservazione (G. D. ROMAGNOSI, *Introduzione al diritto pubblico universale*, II, V, Prato, 1838, 445 ss. e G. MANNA, *Principi di diritto amministrativo*, con appendici e note di G. Telesio, I, III, Napoli, 1876, 2 ss.), poi contrapposta all'attività sociale (V. E. Orlando, *Introduzione al diritto amministrativo*, *Primo trattato completo del diritto amministrativo italiano*, V. E. ORLANDO (a cura di), I, Milano, 1900, 63 ss.), sino ad essere letta come distinta dall'attività di conservazione e benessere (O. RANELLETTI, *La polizia di sicurezza*, in V.E. ORLANDO (a cura di), *Primo trattato completo di Diritto amministrativo italiano*, IV, Milano, 1904, 207 ss., e *Concetto della polizia di sicurezza*, in *Arch. giur.*, LX, 1898, 432-462, LXI, 3-29 (ora in *Scritti giuridici scelti*, I, Napoli, 1992, 129 ss.). Si vedano, non meno rilevanti e con interpretazioni talvolta contrastanti, S. ROMANO, *Principi di diritto amministrativo*, III, Milano, 1912, 244 ss; P. VIRGA, *La potestà di polizia*, Milano, 1954, 6; G. ZANOBINI, *Corso di diritto amministrativo*, V, *Le principali manifestazioni dell'attività amministrativa*, III., Milano, 1959, 72 ss.; G. CORSO, voce *Polizia di sicurezza*, in *Dig. Disc. Pubb.*, XI, Torino, 1996, 319 ss.; A. CHIAPPETTI, voce *Polizia* (dir. pubbl.), in *Enc. Dir. Treccani*, XXXIV, Milano, 1985, 120 ss. Meno risalenti, anche per una ricostruzione del dibattito dottrinario, si vedano R. URSI, *La sicurezza pubblica*, Bologna, 2022 e S. RAIMONDI, *La sicurezza pubblica*, Torino, 2023.

¹⁶ National Institute of standards and technology, *NIST Internal Report, NIST IR 8432*, dicembre 2023, 3 ss.

come il colore dei capelli o degli occhi, il gruppo sanguigno e i tratti del viso. Per di più, i fenotipi possono riguardare la predisposizione o la presenza di determinate condizioni mediche, come l'anemia falciforme, la fibrosi cistica, nonché forme di distrofia muscolare o certi tipi di tumore. Il genoma consente, inoltre, di identificare informazioni significative non solo sull'organismo in analisi, ma anche sui parenti del soggetto¹⁷.

I dati genetici assumono sempre maggiore attenzione anche alla luce dell'avanzamento delle conoscenze tecnico-scientifiche¹⁸, con un impatto sempre più pervasivo sul bilanciamento tra diritti fondamentali – aggravato da soventi lacune nel quadro normativo¹⁹.

Nello specifico ambito sanitario, le tecnologie emergenti – come nel caso in trattazione – hanno un impatto sui temi della privacy, dell'etica, della sicurezza dei dati, della discriminazione e della responsabilità. Pertanto, l'evoluzione della ricerca scientifica richiede una normazione tecnica per identificare e regolare fenomeni e impatti complessi e incerti, in modo agile e adattabile a nuove situazioni: «[il] bilanciamento tra il ruolo del diritto e le potenzialità tecnologiche è indispensabile, non solo perché altrimenti il diritto non svolgerebbe la funzione di regolazione cui è chiamato, ma anche perché rischierebbe di votarsi all'inefficacia e al mancato rispetto nella realtà concreta»²⁰. È infatti indiscutibile come il progresso sanitario, in termini tecno-scientifici, sia strettamente legato all'esistenza di un adeguato quadro normativo, ove rileva sia la qualità sostanziale dell'intervento normativo, sia il *quando* (si chiama ad una nuova disciplina quando vi sono effetti non tutelati dal quadro vigente, che deve così passare gradualmente da un certo grado di flessibilità ad una maggiore coerenza²¹). Allo stesso tempo, onde evitare impatti negativi su diritti fondamentali, «la storia ha dimostrato che la scienza non può procedere senza diritto»²².

Cosa accade in UE e, più in particolare, in Italia? Dai risultati di un progetto di ricerca del 2018 finanziato dall'UE²³ si evince che alcuni Stati membri si sarebbero dotati di un'apposita normativa in materia di FDP; in alcune ipotesi questa ha introdotto un divieto (ad esempio, Francia e Germania), in altre ha riconosciuto la liceità del trattamento (ad esempio, Austria – solo in via residuale, e Paesi Bassi). La già citata ricerca evidenzia come la FDP sia spesso usata nella prassi, ma non esplicitamente autorizzata (Polonia, Spagna, Svezia, Repubblica Ceca, Ungheria, Italia, Slovacchia e Regno Unito – al tempo ancora parte dell'Unione). Uno studio più recente aggiorna leggermente il quadro descritto: il divieto riguarda ora anche il Belgio (si può determinare solo il genere), mentre sarebbe ora lecito l'uso della FDP anche in Francia (solo in casi

¹⁷ S. RODOTÀ, *Trasformazioni del corpo*, in *Pol. dir.*, 1, 2006, 7, là dove afferma che «attraverso i dati genetici di una sola persona, ci si impadronisce dei corpi di un intero gruppo biologico». Si vedano anche E. STEFANINI, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, Padova, 2008; V. ZENO-ZENCOVICH, *La "comunione" di dati personali. Un contributo al sistema dei diritti della personalità*, in *Dir. inf.*, 2009, 7 ss.

¹⁸ Si veda N. TERRADO-ORTUNO E P. MAY, *Forensic DNA phenotyping: a review on SNP panels, genotyping techniques, and prediction models*, cit., 19.

¹⁹ Sul tema della regolamentazione del progresso tecnologico in sanità, si veda M. DE ANGELIS, *Alcune questioni giuridiche sulla regolamentazione del progresso tecnologico in sanità*, in *Diritto & Questioni pubbliche*, XVIII, 2017, 195 – 225.

²⁰ F. FAINI, *Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione*, *Federalismi.it*, 16, 2020, 82.

²¹ M. DE ANGELIS, *Alcune questioni giuridiche sulla regolamentazione del progresso tecnologico in sanità*, cit., 203 – 204.

²² R. FERRARA, *Trattato di Biodiritto*, Milano, 2010, 52.

²³ G. SAMUEL E B. PRAINSACK, *The regulatory landscape of forensic phenotyping in Europe*, *VISAGE*, Novembre 2018.



gravi e in seguito ad un intervento giudiziario), Germania (solo per raccogliere informazioni specifiche, quale colore di occhi, capelli e pelle) e Svezia (solo per i casi di omicidio)²⁴.

Ciò che rileva è però che, in larga parte dei casi, la tecnica viene dunque utilizzata e raramente sulla base di una normativa specifica che offra garanzie all'individuo con riguardo alla tutela dei propri dati.

Quanto all'Italia, non ci si sofferma sul bilanciamento del diritto alla protezione dei dati genetici e l'accertamento dei reati in termini generali (sebbene una recente ricostruzione della disciplina rilevante abbia rappresentato un quadro normativo preoccupante²⁵), ma sull'acquisizione di materiale biologico su una scena di un delitto, con un dubbio bilanciamento favorevole per l'accertamento dei reati o la sicurezza pubblica, rispetto alla tutela dei dati personali (peraltro, sanitari). Sull'acquisizione del materiale biologico, i pareri sono contrastanti: da un lato, non sarebbe possibile poiché si tratterebbe di un aggiramento delle garanzie previste²⁶; dall'altro, sarebbe possibile in mancanza di un espresso divieto²⁷.

In tali fattispecie, risulta di primaria importanza determinare l'ambito di legittima operatività delle misure e le relative modalità di attuazione. La discrezionalità conferita alle autorità pubbliche è regolata dal *principio di proporzionalità*, il quale impone una ponderazione tra la tutela dei dati personali (là dove, peraltro, nella nozione di libertà rientra anche la tutela della sfera individuale del soggetto e quindi la riservatezza²⁸) e la necessità di perseguire un interesse pubblico di rilevante entità.

Per comprendere come la normativa applicabile interviene sulla tecnica in analisi, si ritiene utile guardare prima alle disposizioni di carattere Unionale (generale sul trattamento dei dati e specifica sulle funzioni di polizia) e poi nazionale.

Dalla Carta dei diritti fondamentali dell'Unione europea si evince che ogni persona ha diritto al rispetto della propria vita privata e familiare²⁹. Non vi è dunque possibilità di ingerenza da parte di un'autorità pubblica, salvo specifica previsione legislativa necessaria a fini di pubblica sicurezza e difesa dell'ordine e prevenzione dei reati³⁰.

²⁴ H. WESTERMARK et al., *The Regulation of the use of DNA in Law Enforcement*, Bern, 2020.

²⁵ F. SANVITALE, *Quello che il legislatore non dice in tema di prova genetica. Dalla banca dati nazionale del DNA al familial searching*, cit.

²⁶ C. FANUELE, *L'acquisizione occulta di impronte digitali e materiale biologico*, in A. SCALFAI (a cura di), *Le indagini atipiche*, Torino, 2019, 413.

²⁷ M. MONTAGNA, *Accertamenti tecnici, accertamenti personali occulti e prelievo del DNA*, in A. GAITO (a cura di), *La prova penale*, 2, Milano, 2008, 88 ss. Quanto al tema della classificazione degli elementi di prova, non affrontato in questo contributo, la Corte Europea dei Diritti dell'Uomo ha tracciato un percorso interpretativo chiaro a partire dalla sentenza della Grande Camera nel caso Saunders c. Regno Unito (1996), la quale rappresenta una pietra miliare nell'elaborazione concettuale della distinzione tra prove volontà-dipendenti e volontà-indipendenti. La Corte ha infatti stabilito che il diritto di tacere e il diritto di non contribuire alla propria incriminazione, pur non essendo espressamente menzionati nell'art. 6 CEDU, costituiscono elementi essenziali del giusto processo, strettamente connessi alla presunzione di innocenza.

²⁸ All'art. 7 della Corte di giustizia dell'Unione europea, *Carta dei diritti fondamentali dell'Unione europea*, Ufficio delle pubblicazioni dell'Unione europea, 2020, si legge che «ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni».

²⁹ Art. 7, Corte di giustizia dell'Unione europea, *Carta dei diritti fondamentali dell'Unione europea*, Ufficio delle pubblicazioni dell'Unione europea, 2020.

³⁰ Art. 8, *Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, Roma, 4 novembre 1950, le cui limitazioni sono applicabili conformemente all'art. 52, par. 3 della Carta dei diritti fondamentali dell'Unione europea.

Guardando al Regolamento (UE) 2016/679 (GDPR), questo specifica che i dati personali relativi alla salute includono i dati genetici e i campioni biologici, in quanto capaci di rivelare informazioni relative allo stato di salute passata, presente o futura³¹. Inoltre, lo stesso testo evidenzia che i rischi per i diritti e le libertà delle persone fisiche («discriminazioni, pregiudizio alla reputazione, perdita di riservatezza dei dati personali [...], o qualsiasi altro danno economico o sociale significativo»³²) possono derivare dal trattamento dei dati genetici. Vi è poi, più precisamente, un divieto generale di trattamento di tale categoria di dati³³, fatti salvi alcuni specifici casi³⁴. Tra questi, il consenso esplicito per una o più finalità specifiche; un trattamento necessario per finalità di sicurezza e protezione sociale (se autorizzato dal diritto UE o nazionale) – ma in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'individuo; e un trattamento necessario per l'esercizio delle funzioni giurisdizionali³⁵. Dal dato normativo emerge così la necessità di un fondamentale bilanciamento tra integrità e dignità della persona, e l'uso del dato per interessi collettivi – in un'ottica così di proporzionalità. Per quanto attiene alla disposizione riguardante il trattamento dei dati personali relativi a condanne penali e reati non è in discussione – per la pratica in esame – che questo avvenga già sotto il controllo di un'autorità pubblica, come richiesto dalla normativa³⁶.

Con specifico riferimento ai dati genetici, è stata da altri criticata una interpretazione troppo restrittiva della definizione contenuta nel GDPR, là dove mancherebbe un riferimento alla raccolta e all'analisi del materiale biologico e delle caratteristiche fenotipiche come parte del concetto di dati genetici³⁷. È, inoltre, stato analizzato da attenta dottrina come la struttura fondamentale del GDPR, ossia l'idea che i dati siano collegati a un interessato concreto³⁸, non si adatti particolarmente bene ai dati genetici. Ciò sempre poiché i dati genetici non sono collegati esclusivamente a un solo interessato, ma a più persone che condividono una parte della propria struttura biologica: tale caratteristica non si concilia bene con le assunzioni alla base del GDPR³⁹.

³¹ Considerando 35; art. 4, 13): «i 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», Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

³² Considerando 75, Regolamento (UE) 2016/679.

³³ Si veda l'art. 9 (1), Regolamento (UE) 2016/679.

³⁴ Si veda l'art. 9 (2), Regolamento (UE) 2016/679.

³⁵ Sul punto, S. MELCHIONNA, F. CECAMORE, *Le nuove frontiere della sanità e della ricerca scientifica*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. 101/2018*, Milano, 2019, 585 ss.

³⁶ Art. 10, Regolamento (UE) 2016/679.

³⁷ M. SHABANI E 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), 152; M. TAYLOR, *Genetic data and the law: a critical perspective on privacy protection*, Cambridge, 2012, 46.

³⁸ Art. 4(1), Regolamento (UE) 2016/679.

³⁹ Sul punto, A. PANAGIOTOPOULOS, *Genetic information and communities*, in *European Data Protection Law Review*, 4(4), 2018, 459.

Inoltre, gli Stati membri hanno la possibilità di introdurre ulteriori limitazioni al trattamento, per quanto tale previsione non trovi concorde parte della dottrina⁴⁰. Quanto al consenso, più rigoroso per le categorie “speciali” di dati, come quelli relativi alla salute⁴¹, vi è necessità di una «volontà libera, specifica, informata e inequivocabile»⁴², nonché revocabile agevolmente e in qualsiasi momento⁴³.

Vi è, per di più, il tema della «limitazione della finalità»⁴⁴: è proibita una elaborazione secondaria di dati per uno scopo diverso da quello concordato⁴⁵. È chiaro come, nel caso di specie, vi sia la necessità di un (non agevole) bilanciamento tra il diritto di protezione di dati personali sanitari e le finalità di sicurezza e ordine pubblico, da considerarsi in ossequio al principio di proporzionalità alla luce della relativa funzione sociale⁴⁶. Nell'utilizzo della tecnica non appare realisticamente possibile operare una distinzione tra l'acquisizione di informazioni da un soggetto imputato e quella da un soggetto terzo estraneo. Il pericolo è il cosiddetto *massive screening*, pratica che violerebbe il principio di proporzionalità⁴⁷. Sempre in base alla normativa UE sulla protezione dei dati personali, appare *prima facie* complicata la liceità del trattamento dei dati estratti con la tecnica in analisi del fenotipo. Considerando che il DNA estratto contiene dati sanitari, non sarebbe in alcun modo possibile ottenere un consenso esplicito, in tutte le ipotesi in cui il materiale viene raccolto sulla base della presenza in un luogo oggetto di un reato. Parimenti non è possibile per l'individuo revocare liberamente un ipotetico consenso rilasciato o richiedere l'accesso al dato, non potendo essere a conoscenza di ogni luogo e momento in cui “perde” del DNA.

L'analisi di cui sopra rispetto al GDPR è opportuna ma sommaria poiché, come di recente ribadito anche dalla Corte di giustizia dell'Unione europea, qualora il trattamento dei dati sia finalizzato alla prevenzione, all'indagine, all'accertamento o al perseguimento di reati, non trova applicazione il GDPR, bensì la direttiva del 2016, riguardante il trattamento dei dati personali a fini di prevenzione, indagine, accertamento

⁴⁰ Il tema è la mancanza di uniformità a livello UE. Sul punto, si veda P. GUARDA, I dati sanitari, in V. CUFFARO et al., (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 600.

⁴¹ Art. 9, 1), Regolamento (UE) 2016/679.

⁴² Art. 4, n. 11, Regolamento (UE) 2016/679. Peraltro, all'art. 7, par. 3, si chiede di dimostrare che il consenso sia “presentato in modo chiaramente distinguibile dalle altre materia, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro”.

⁴³ Considerando 32, Regolamento (UE) 2016/679.

⁴⁴ Art. 5, Regolamento (UE) 2016/679.

⁴⁵ Per approfondire sul punto, si veda M. DONNELLY E M. McDONAGH, *Health Research, Consent and the GDPR Exemption*, in *European journal of health law*, 26 (2), 2019, 97-119.

⁴⁶ Considerando 4, Regolamento (UE) 2016/679.

⁴⁷ Ad esempio, la sentenza n. 238/1996 della Corte Costituzionale ha dichiarato l'illegittimità costituzionale dell'art. 224, comma 2, del codice di procedura penale nella parte relativa ai provvedimenti coattivi per l'esecuzione di perizie, con particolare riferimento al prelievo ematico forzato. L'indeterminatezza della norma è stata giudicata in contrasto con il principio secondo cui nessuna restrizione della libertà personale è ammissibile se non per atto motivato dell'autorità giudiziaria e nei soli casi e modi previsti dalla legge.

e perseguimento di reati⁴⁸ (c.d. direttiva polizia)⁴⁹. Tale orientamento conferma quanto espressamente previsto sia dal considerando 19 del GDPR sia dai considerando da 9 a 12 della direttiva medesima.

Sulla questione, la direttiva prevede che «in linea di principio dovrebbe essere vietata qualunque discriminazione basata su caratteristiche genetiche»⁵⁰. La Corte di Giustizia – sempre nella medesima occasione – ha confermato che i dati genetici e biometrici costituiscono categorie particolari di dati considerati ad alto rischio⁵¹. Ciò in virtù della sensibilità delle informazioni di natura genetica e il possibile utilizzo e riutilizzo improprio e non autorizzato⁵². Inoltre, il trattamento di dati genetici è considerato autorizzato solo se soggetto a garanzie adeguate, nonché autorizzato dal diritto UE o nazionale, per salvaguardare un individuo o se il trattamento riguarda dati resi manifestamente pubblici⁵³. La Corte, in particolare, si sofferma sulla necessaria presenza di «un’adeguata giustificazione della sua necessità (del trattamento, ndr)»⁵⁴. Si tratta di un requisito rafforzato, imposto dalla necessità di fronteggiare gravi ingerenze nel diritto alla protezione dei dati personali⁵⁵, che va oltre le garanzie previste dal regime generale applicabile ai dati non particolari. Affermare che il trattamento dei dati sia possibile è tutt’altro che scontato: il trattamento è autorizzabile solo se «strettamente necessario, soggetto a garanzie adeguate e previsto dal diritto dell’Unione o dello Stato membro»⁵⁶. Spetta così alla decisione dei singoli Stati come procedere per la raccolta, analisi e conservazione di tale categoria dati, includendo idonee garanzie e un uso dei dati che identifichi dettagliatamente la finalità del trattamento (è chiaro che, così, il rischio di disarmonizzazione è fortemente probabile).

Calando l’analisi sul quadro domestico, il testo della già citata direttiva polizia è stato recentemente modificato prevedendo che la liceità del trattamento possa essere basata su atti amministrativi generali che

⁴⁸ Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. Altre normative affrontano il tema dei dati genetici. Tra queste, la Proposta di Regolamento del Parlamento europeo e del Consiglio relativa allo scambio automatizzato di dati per la cooperazione di polizia (“Prüm II”), che modifica le decisioni del Consiglio 2008/615/GAI e 2008/616/GAI e i regolamenti (UE) 2018/1726, 2019/817 e 2019/818 del Parlamento europeo e del Consiglio, COM/2021/784 final. La proposta affronta però, più precisamente, il tema delle banche dati, mentre il presente scritto si sofferma più nello specifico sull’analisi dei dati sanitari a seguito della raccolta, non tanto sulla loro condivisione. Sul punto, si rimanda comunque a F. SANVITALE, *Quello che il legislatore non dice in tema di prova genetica. Dalla banca dati nazionale del DNA al familial searching*, cit. Stesso discorso si applica al *Regolamento (UE) 2025/327 sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847*, Gazzetta ufficiale dell’Unione europea, L 327/1.

⁴⁹ Corte di giustizia dell’Unione europea, sentenza 19 gennaio 2023, causa C-205/21, ECLI:EU:C:2023:34, pubblicata il 27 febbraio 2023.

⁵⁰ Considerando 23, Direttiva (UE) 2016/680.

⁵¹ Corte di giustizia dell’Unione europea, sentenza 19 gennaio 2023, causa C-205/21, ECLI:EU:C:2023:34, pubblicata il 27 febbraio 2023.

⁵² *Ibid.* Come osserva S. Deplano, *Il campione biologico di un’identificata persona. Profili di sistema*, in questa *Rivista*, 1/2022, 45 ss., «non appare più corretto ritenere il distacco del tessuto del corpo ne sancisca la totale autonomia del soggetto-fonte: il profilo dell’appartenenza insiste sul bene ma è indissolubilmente legato a quello informativo, ovvero attinente ai dati personali che dal materiale biologico si ricavano».

⁵³ Art. 10, Direttiva (UE) 2016/680.

⁵⁴ V. punto 46 della pronuncia.

⁵⁵ *Ibid.*

⁵⁶ V. punti 60-63 della pronuncia.



individuano i dati e le finalità del trattamento⁵⁷. Per le categorie particolari di dati personali (come nel nostro caso), il trattamento è, tuttavia, autorizzato solo se previsto dalla legge e strettamente necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato⁵⁸. I regolamenti possono essere infatti usati solo per casi in cui si risponde alla salvaguardia di un interesse vitale dell'interessato o di altra persona fisica, o se i dati sono stati resi manifestamente dall'interessato⁵⁹. Non può essere dunque applicabile alla raccolta e analisi di DNA di persone sconosciute. Tale considerazione è rafforzata da un possibile parallelismo con il riconoscimento facciale nei luoghi pubblici. Nelle linee guida del Comitato europeo per la protezione dei dati sull'uso della tecnologia di riconoscimento facciale nel settore delle attività di contrasto, è esplicito che il fatto che una fotografia sia stata resa pubblica non implica che i relativi dati, ricavabili dalla fotografia con mezzi tecnici specifici, si considerino manifestamente pubblici⁶⁰. Inoltre, anche la normativa domestica prevede l'obbligo per il titolare di adottare tutte le misure adeguate a fornire all'interessato le informazioni necessarie sul trattamento, tra cui il titolo giuridico del trattamento (informazioni che devono presentate, peraltro, in forma concisa, intellegibile e facilmente accessibile)⁶¹. Non è certamente il caso della FDP, in cui non si conosce neanche l'identità dell'interessato al momento della raccolta e analisi del DNA.

Anche la normativa nazionale generale sulla protezione dei dati personali non migliora la certezza del quadro normativo, là dove prevede – in termini sommari – che il trattamento dei dati genetici è «consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale»⁶². La stessa normativa stabilisce che i dati genetici possono essere trattati secondo le condizioni, già viste, delineate dal GDPR, e «in conformità alle misure di garanzia disposte dal Garante»⁶³. Tali misure di garanzia dovrebbero essere disposte dal Garante con cadenza almeno biennale (un provvedimento che deve essere anche posto in consultazione pubblica). Il Garante ha così il ruolo di indicare al titolare come trattare i dati genetici. Anche in questo caso, la peculiarità della normativa nazionale, come di recente modificata, è infatti che il trattamento dei dati sanitari possa essere ammesso persino da atti amministrativi generali⁶⁴, ma va motivato l'interesse pubblico rilevante e le misure adottate per tutelare i diritti e gli interessi dell'individuo (e, peraltro, anche dei suoi familiari). Dal relativo provvedimento del Garante emerge una visione ancor più rafforzata dell'elemento del consenso al trattamento dei dati genetici (es. nel caso di investigazioni difensive è richiesto il consenso, un'espressa disposizione di legge o un provvedimento dell'autorità giudiziaria in conformità alla legge)

⁵⁷ Art. 5, decreto legislativo 18 maggio 2018, n. 51 di attuazione della direttiva (UE) 2016/680, come aggiornato dall'art. 9, comma 5, del D.L. 8 ottobre 2021, n. 139, convertito con modificazioni dalla l. 3 dicembre 2021, n. 205.

⁵⁸ Sul punto, si veda Corte di Giustizia dell'Unione Europea, 20/11/2025, *Policejní prezidium () and génétiques*, C-57/23, ECLI:EU:C:2025:905.

⁵⁹ Art. 7, decreto legislativo 18 maggio 2018, n. 51.

⁶⁰ Comitato europeo per la protezione dei dati, Linee guida 05/2022 sull'uso della tecnologia di riconoscimento facciale nel settore delle attività di contrasto, adottate il 26 aprile 2023.

⁶¹ Art. 10 e 11, decreto legislativo 18 maggio 2018, n. 51.

⁶² Art. 60, Decreto Legislativo 30 giugno 2003, n. 196, recante il 'Codice in materia di protezione dei dati personali', come modificato dal Decreto Legislativo 10 agosto 2018, n. 101, in attuazione del Regolamento (UE) 2016/679, e dal D.L. 2 marzo 2024, n. 19, convertito con modificazioni, dalla L. 29 aprile 2024, n. 56.

⁶³ Art. 2-septies, Decreto Legislativo 30 giugno 2003, n. 196.

⁶⁴ Art. 2 -sexies, come modificato dall'art. 9, comma 1, lett. B, n. 1, d.l. n. 139 del 2021.

che non considera però un caso come quello in trattazione⁶⁵. La revoca del consenso deve, per di più, essere assicurata, là dove nel caso di specie non è chiaramente possibile.

La Corte di Giustizia dell'Unione europea ha ben specificato che «il trattamento dei dati biometrici e genetici da parte delle autorità di polizia [...], è autorizzato dal diritto nazionale se quest'ultimo contiene una base giuridica sufficientemente chiara e precisa»⁶⁶. Come già anticipato, al contempo, la Corte ricorda che l'esistenza di un numero sufficiente di elementi di prova rappresenta un fondato motivo per la raccolta coercitiva dei dati genetici. Sorge dunque l'interrogativo circa l'operatività di tali misure in assenza di un fondato motivo, condizione che si verifica quando l'identità dell'individuo è ignota e l'attività investigativa è avviata proprio sulla base della FDP.

La decisione della Corte è netta nell'affermare che la normativa UE osta a una

normativa nazionale che prevede la raccolta sistematica di dati biometrici e genetici di qualsiasi persona formalmente accusata di un reato doloso perseguibile d'ufficio, ai fini della loro registrazione, senza prevedere l'obbligo, per l'autorità competente, di verificare e di dimostrare, da un lato, che tale raccolta è strettamente necessaria per il raggiungimento dei concreti obiettivi perseguiti e, dall'altro, che tali obiettivi non possono essere raggiunti mediante misure che costituiscano un'ingerenza meno grave nei diritti e nelle libertà della persona interessata⁶⁷.

Pur senza voler considerare il consenso esplicito richiesto dal GDPR e le limitazioni alla finalità del trattamento, la normativa domestica non interviene dunque per autorizzare esplicitamente il trattamento in esame⁶⁸. Come è garantito il rispetto della vita privata? Chiaramente, non si può ridurre tutto alla mancanza di necessità del consenso per l'intrusione nella libertà corporale. Non si tratta infatti, con riguardo alla tecnica in analisi, di una semplice raccolta di campione biologico, con conservazione e "semplice sovrapposizione" successiva con il DNA di un possibile sospettato. Nel nostro caso, si procede direttamente all'analisi del campione a sé stante (con estrapolazione contestuale dei dati sanitari dell'individuo) per generare un profilo da cui far partire l'indagine. Il trattamento del dato sanitario avviene senza specifiche garanzie (ad esempio, come e per quanto tempo vengono conservati i dati dell'individuo e come circolano tra le autorità coinvolte?). Si pone così il quesito se qualsiasi materiale biologico o oggetto da cui sia possibile estrarre DNA, rinvenuto in un luogo che diverrà successivamente scena di un crimine, possa essere liberamente raccolto e analizzato nell'ambito di attività investigative. Peraltro, senza garanzie e limiti di tempo per l'estrazione delle informazioni sanitarie presenti in tale materiale?

In tale prospettiva, non si ravvisa il rispetto del principio di proporzionalità nel bilanciamento degli interessi coinvolti, né la garanzia di trasparenza nell'attività delle autorità pubbliche circa il trattamento dei dati personali.

Inoltre, la Corte apre anche ad un altro tema, sottolineando come prevedere un'autorizzazione al trattamento dei dati genetici «solo se strettamente necessaria» voglia dire una valutazione della limitazione delle finalità e la minimizzazione dei dati (e tale pratica, nel caso del dato genetico, appare essere tutt'altro

⁶⁵ Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d. lgs. 10 agosto 2018, n. 101, n. 146 del 5 giugno 2019, come aggiornato dal Provvedimento del 13 febbraio 2015, n. 66.

⁶⁶ Corte di Giustizia dell'Unione europea, Comunicato stampa n. 16/23, 26 gennaio 2023, p. 2. La sentenza è Corte di Giustizia dell'Unione Europea, sentenza del 26 gennaio 2023, causa C-205/21, ECLI:EU:C:2023:49.

⁶⁷ *Ivi*, 4.

⁶⁸ Come richiesto dall'art. 10, Direttiva (UE) 2016/680.



che semplice e richiederebbe una valutazione caso per caso vista l'unicità dei geni⁶⁹). Non si può dunque condurre una raccolta dei dati in modo indifferenziato e generalizzato.

Oltre ai problemi legati alla proporzionalità, trasparenza e riservatezza, vi sarebbe dunque anche un tema di principio di legalità, vale a dire definire i poteri affidati alle autorità e le modalità di esercizio degli stessi, declinare la discrezionalità assegnata, il numero, le categorie e lo status dei soggetti coinvolti. Il tema del principio di legalità è anche, chiaramente, da leggere rispetto alla volontà del soggetto interessato.

3. L'intersezione tra FDP e intelligenza artificiale: potenziali vantaggi e rischi amplificati

Gli impatti della FDP sono diversi e significativi e vanno oltre il mero trattamento illegale dei dati sanitari dell'individuo e la mancanza di trasparenza, proporzionalità e tutela della riservatezza da parte delle autorità pubbliche coinvolte. Un utilizzo improprio della tecnica può portare ad una discriminazione basata sulla falsa identificazione data da una gestione errata delle procedure nei laboratori e alla falsificazione delle informazioni genomiche.

Il contesto va peggiorando là dove sono impiegati sistemi di intelligenza artificiale per esaminare ampi set di dati genomici. Vi è il rischio di *bias* e, inoltre, un processo di analisi dei dati genetici automatizzato va a minare ancor di più la trasparenza e dunque l'affidabilità e la validità dei risultati prodotti.

L'applicazione di modelli predittivi è una realtà concreta: essi sono sviluppati per supportare la comprensione tra genotipo (vale a dire, la costituzione genetica di un organismo) e fenotipo (vale a dire, l'insieme delle caratteristiche di un organismo). In particolare, un laboratorio statunitense ha sviluppato un sistema suddiviso sostanzialmente in due parti: i) estrazione dei dati – si analizzano grandi set di dati genetici contenenti informazioni su migliaia di individui per identificare le varianti genetiche più rilevanti associate a una caratteristica fisica. Questo processo richiede settimane di calcolo su centinaia di computer e seleziona solo le varianti con il maggiore impatto biologico; ii) modellazione dei dati – tramite algoritmi di apprendimento automatico viene creata un'equazione matematica che rappresenta la struttura genetica della caratteristica fisica⁷⁰. Le previsioni vengono testate su soggetti noti e di cui, naturalmente, si conoscono i fenotipi, per valutare l'accuratezza del modello e scartare tratti improbabili. Il DNA di un ignoto può così essere inserito nel sistema per ottenere una previsione dei tratti del soggetto di interesse. Lo sviluppo del sistema è stato finanziato dal Dipartimento della Difesa degli Stati Uniti e sarebbe stato utilizzato già da più di cento autorità tra Stati Uniti resto del mondo⁷¹ al fine di supportare l'attività investigativa.

Si è anticipato, in introduzione, il parallelismo tra la presenza di materiale biologico in luogo e la raccolta e analisi del suo DNA, con la presenza fisica di un individuo all'esterno e la possibilità di essere inclusi in un'attività di sorveglianza di massa. Si ritiene così opportuno affrontare il tema guardando al Regolamento UE sulla regolazione dell'intelligenza artificiale.

⁶⁹ Sul punto, si veda A. SANTUOSSO, I. A. COLUSSI, *La banca dati del DNA: questioni in tema di alimentazione, trattamento e accesso, presupposti, cancellazione e tempi di conservazione* (art. 5-15, l. n. 85/09), in *Politica del diritto*, 2011, 437 ss.; A. M. CAPITTA, *Conservazione dei DNA profiles e tutela europea dei diritti dell'uomo*, in *Archivio penale*, 2013, 141.

⁷⁰ Si veda, dal sito del laboratorio, <https://snapshot.parabon-nanolabs.com/posters>.

⁷¹ *Ibid.*

Il Regolamento non contiene un riferimento esplicito all'applicazione dell'IA alle tecniche di analisi del DNA, il che non sorprende, data la novità e la fase di sviluppo di tali utilizzi. Questa lacuna, come già evidenziato in dottrina, solleva interrogativi sulla capacità del Regolamento di essere 'a prova di futuro'⁷². Parimenti, nel testo non si trova nulla con riguardo ai termini "DNA", "genoma", "dati genetici". Occorre dunque allargare la prospettiva ai dati sanitari e, anche qui, non si è più fortunati. L'attenzione è principalmente sull'uso di sistemi di IA per valutare l'accesso all'assistenza sanitaria, nonché per l'individuazione, la diagnosi, la prevenzione, il controllo e il trattamento di malattie⁷³.

Non ci si può dunque esimere da un esercizio interpretativo sulle disposizioni del Regolamento che più si avvicinano all'uso dell'IA nell'ambito della FDP. A una lettura superficiale, si potrebbe provare ad affermare la rilevanza del divieto dell'uso di un sistema di IA per valutare o classificare le persone fisiche per un determinato periodo di tempo sulla base di caratteristiche personali, inferite o previste⁷⁴. Nello specifico, con riguardo al trattamento pregiudizievole o sfavorevole in contesti non collegati all'originale raccolta o generazione dei dati. Si tratterebbe, tuttavia, di una chiave di lettura quanto meno estensiva di una disposizione scritta avendo in mente il tema del *social scoring* e della polizia predittiva⁷⁵.

Più rilevante, invece, il divieto di uso di IA per la categorizzazione biometrica e la classificazione delle persone per trarre deduzioni o inferenze in merito a razza o orientamento sessuale⁷⁶. Il divieto è però solo, per l'appunto, con riguardo ai dati biometrici (che, inoltre, pone come eccezione la categorizzazione di tali dati nel settore delle attività di contrasto). Lo stesso ragionamento vale per il divieto di utilizzare l'identificazione biometrica in spazi accessibili a fini di attività di contrasto⁷⁷. A tal riguardo, sono fatte salve la ricerca di persone scomparse o la prevenzione di una minaccia specifica, reale, attuale o prevedibile di un attacco terroristico e la localizzazione o identificazione di una persona sospettata di aver commesso un reato. Tale divieto si avvicina ancora di più al caso della FDP, ma non racchiude l'uso di dati genetici (solo biometrici). Lo stesso vale per la classificazione come sistema ad alto rischio dell'uso della biometria⁷⁸.

Per le pratiche considerate ad alto rischio, vi è il caso dell'attività di contrasto, dove potrebbe rilevare l'uso di sistemi da parte delle autorità di contrasto (o per loro conto) per la profilazione delle persone fisiche nel corso dell'indagine, dell'accertamento e del perseguimento di reati⁷⁹. Quest'ultima parrebbe essere la casistica che più si avvicina alla FDP, ma occorre comprendere in modo più approfondito l'accezione del termine "profilazione". Il Regolamento rimanda, per tale definizione, al GDPR, il quale descrive l'attività come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti riguardanti [...] la salute, l'ubicazione o gli spostamenti di detta persona fisica»⁸⁰. La descrizione potrebbe dunque effettivamente essere pertinente e— sebbene con un

⁷² L. MEGALE E N. RANGONE, *Risks Without Rights? The EU AI Act's Approach to AI in Law and Rule-Making*, in *European Journal of Risk Regulation*, first view, 2025, 1-16.

⁷³ Allegato III, Regolamento (UE) 2024/1689, Gazzetta ufficiale dell'Unione Europea, L 2024, 13 giugno 2024.

⁷⁴ Art. 5, 1, c), Regolamento (UE) 2024/1689.

⁷⁵ Sul tema, si veda M. B. ARMIENTO, *La polizia predittiva come strumento di attuazione amministrativa delle regole*, in *Diritto amministrativo*, 4, 2020.

⁷⁶ Art. 5, 1, g), Regolamento (UE) 2024/1689.

⁷⁷ Art. 5, 1, h), Regolamento (UE) 2024/1689.

⁷⁸ Art. 5, 2, Regolamento (UE) 2024/1689.

⁷⁹ Allegato III, 6, Regolamento (UE) 2024/1689.

⁸⁰ Art. 4 (4), Regolamento (UE) 2016/679.



certo grado di interpretazione – si potrebbe affermare che l'uso dei sistemi di IA a supporto della FDP rientri tra le pratiche ad alto rischio, con i conseguenti limiti e garanzie.

Il ragionamento si complica, tuttavia, là dove il Regolamento sull'IA specifica esplicitamente che è fatta salva la direttiva 2016/680⁸¹, già menzionata come *lex specialis* del GDPR, che rimane dunque applicabile (con riguardo particolare anche all'articolo 13, ove si prevede che gli Stati membri devono mettere a disposizione dell'interessato informazioni quali la base giuridica per il trattamento, le finalità del trattamento, la possibilità di porre reclamo e di accesso, rettifica o cancellazione dei dati – fatte naturalmente salve le casistiche tali da compromettere l'indagine). La direttiva, per il caso in analisi, pone un divieto alla profilazione che porta alla discriminazione di persone fisiche sulla base dei dati genetici⁸². Una tale disposizione – decisamente esplicita – rende chiaramente più complicato inserire, in via meramente interpretativa, una casistica di uso dell'IA come ad alto rischio.

4. Le garanzie nel trattamento dei dati FDP: consenso, stretta necessità e sfida della proporzionalità

Al fine di valutare la possibilità di garantire un adeguato livello di trasparenza e proporzionalità nel trattamento, l'elemento più critico è senza dubbio il consenso, criterio che si rivela sostanzialmente inesigibile⁸³. Non c'è modo di garantire un consenso libero, specifico, informato e inequivocabile rispetto alla raccolta e analisi di una traccia di DNA di un individuo che rimane sconosciuto finché non identificato grazie alla correlazione tra altri elementi e, poi, al confronto con il DNA del soggetto sospettato. È vero anche che, secondo il considerando 37 della direttiva polizia, il consenso non è di per sé una base giuridica valida per il trattamento di dati sensibili nel contesto dell'applicazione della legge, ma solo una "garanzia aggiuntiva" – comunque mancante.

In ogni caso, come visto, la normativa italiana di recepimento della direttiva polizia autorizza al trattamento, se strettamente necessario, se assistito da garanzie adeguate a diritti e libertà dell'interessato e se previsto dalla normativa. Dunque, parrebbe si possa comunque andare avanti, anche senza un consenso esplicito. Immaginando l'esistenza di una normativa sul tema nei termini che si vedranno

⁸¹ Art. 26 (11), Regolamento (UE) 2024/1689.

⁸² Art. 11, Direttiva 2016/680.

⁸³ Il consenso, come analizzato diffusamente in dottrina (ex multis, M. DE ANGELIS, *Diritto a informare e a essere informati per l'appropriatezza delle cure. Uno sguardo diverso sul consenso informato*, in M. CERIONI E M. DE ANGELIS (a cura di), *Il diritto alla salute: tensioni e sviluppi*, Roma, 2022, 41-90), è riconosciuto come una procedura autonoma di manifestazione della volontà, sintesi dei diritti fondamentali all'autodeterminazione e alla salute, e si basa su un'informazione completa, chiara, esaustiva, comprensibile e soprattutto personalizzata. Esso rappresenta il tessuto stesso della relazione di cura, richiedendo una scelta libera, specifica, informata e inequivocabile, con possibilità di revoca in qualsiasi momento. Tuttavia, nel caso della FDP su tracce biologiche di individui sconosciuti, l'elemento del consenso si rivela sostanzialmente inesigibile perché non solo manca la possibilità di un dialogo informativo personalizzato con il soggetto, ma è impossibile per l'individuo manifestare una volontà consapevole, revocare il consenso o richiedere l'accesso al dato, poiché non è a conoscenza della raccolta e analisi del proprio DNA. Sebbene la Direttiva (UE) 2016/680 consideri il consenso una "garanzia aggiuntiva", l'assenza di tale pilastro dell'autodeterminazione, unitamente alla natura sensibile e immutabile dei dati genetici, rende ancora più imperativa la necessità di garanzie adeguate e di un rigoroso test di proporzionalità "caso per caso". La liceità del trattamento, in assenza di consenso esplicito, può essere ammessa solo se strettamente necessaria e prevista da una normativa nazionale che includa idonee e stringenti salvaguardie per i diritti e le libertà dell'interessato.

successivamente (par. 5), è il caso di verificare quando il trattamento possa essere considerato “strettamente necessario” e quali le garanzie minime.

Con riferimento all’accezione di “strettamente necessario” rispetto all’uso di dati genetici, l’avvocato generale Pitruzzella ha interpretato come giustificabile l’interferenza con il diritto alla protezione dei dati solo per casi di reati gravi⁸⁴. Nella sentenza di cui a tale opinione, la Corte ha però rappresentato come la raccolta sistematica di dati genetici di qualsiasi persona accusata di un reato perseguibile d’ufficio sia, in linea di principio, contraria al requisito di stretta necessità⁸⁵. Da ciò si deduce che, a maggior ragione, non è ammissibile una raccolta e analisi sistematica di dati genetici di individui non ancora sospettati del reato. La Corte ha inoltre osservato la condizione di stretta necessità deve essere letta insieme al principio di limitazione della finalità, minimizzazione dei dati e liceità. La necessità del trattamento implicherebbe, inoltre, che non esistano altri mezzi meno invasivi per raggiungere l’obiettivo del trattamento e che venga presa in considerazione la natura dell’obiettivo perseguito. Sono state poi fornite indicazioni per permettere al giudice del rinvio di valutare la condizione della stretta necessità nell’interpretazione del diritto nazionale, come «la natura o gravità del reato», il «casellario giudiziale della persona» e le «circostanze particolari» del reato. Il Comitato europeo per la protezione dei dati ha invece evidenziato che il trattamento di dati sensibili può essere considerato «strettamente necessario» solo quando l’interferenza con i diritti alla protezione dei dati è limitata all’essenziale, cioè quando è assolutamente indispensabile⁸⁶. È confermata dunque l’impossibilità di ammettere un trattamento generico o sistematico.

Si è così dinnanzi a un contesto fortemente incerto. È tutt’altro che chiaro se, pur in caso di una normativa specifica sulla materia, possa essere considerato lecito il trattamento dei dati genetici tramite la FDP. Le interpretazioni della Corte e del Comitato europeo per la protezione dei dati sembrano negare tale possibilità. Non sarebbe però corretto risolvere così la questione. Si tratta, è vero, di casi relativi al trattamento dei dati genetici, ma che non si può ritenere pienamente corrispondenti al bilanciamento dei diritti rispetto ad un caso, come quello della FDP, che rappresenta peculiarità che dovrebbero godere di un’interpretazione e un bilanciamento di interessi *ad hoc*. Sarebbe così da auspicare un intervento del Comitato europeo per la protezione dei dati (anche per un’interpretazione uniforme nel territorio UE), o quantomeno una valutazione del Garante nazionale. In virtù di un bilanciamento già per natura negativo per la tutela del dato (si rammenta la mancanza di un possibile consenso), sarebbe opportuno un aggiornamento delle prescrizioni relative al trattamento dei dati genetici, di cui all’allegato del provvedimento del Garante sul trattamento di categorie particolari di dati⁸⁷. L’aggiornamento dovrebbe fornire un bilanciamento specifico, da parte dell’Autorità, sull’uso della tecnica della fenotipizzazione del DNA forense, così da poter tener conto delle specificità del caso.

Si riconosce, allo stesso tempo, come un bilanciamento degli interessi in termini generali rischi di essere complicato, se non impossibile. Il compito dell’autorità sarebbe infatti anche quello di comprendere

⁸⁴ Parere dell’Avvocato Generale Pitruzzella nella causa C-205/21, VS contro *Ministerstvo na vatreshnite raboti*, 30 giugno 2022 (ECLI:EU:C:2022:507).

⁸⁵ Caso C-205/21, VS v *Ministerstvo*, para. 122.

⁸⁶ Comitato europeo per la protezione dei dati personali, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, 11 aprile 2017.

⁸⁷ Garante per la protezione dei dati personali, *Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell’art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101*, 2019, registro dei provvedimenti n. 146 del 5 giugno 2019.



quando l'utilizzo della tecnica è strettamente necessario rispetto ad altri possibili strade, meno invasive, che dipendono dalle specifiche circostanze. Viene così naturale pensare che un tale test di proporzionalità debba essere impiegato in un'analisi caso per caso. Questa soluzione non rappresenterebbe una novità, sebbene possa apparire come un'opzione desueta. È ciò che prevedeva l'art. 90 del codice privacy per i dati genetici, prima dell'abrogazione, là dove si richiamava ad una apposita autorizzazione del Garante, dopo aver sentito il Ministero della Salute che acquisiva il parere del Consiglio superiore di sanità⁸⁸. Sarebbe in tal modo possibile un'applicazione del principio di proporzionalità, nei termini di un «metodo equilibratore» che consente di realizzare una valutazione «caso per caso e con prudente apprezzamento, al fine di garantire, secondo un delicato ma giusto bilanciamento»⁸⁹. Si tratta infatti un bilanciamento di proporzionalità tutt'altro che scontato e che richiede un forte dinamismo. Una delle pronunce più significative sul tema del bilanciamento tra protezione dei dati personali ed esigenze di sicurezza pubblica è rappresentata dalla sentenza della Corte di giustizia dell'Unione Europea dell'8 aprile 2014, nelle cause riunite C-293/12 e C-594/12. Nella decisione, la Corte ha dichiarato l'illegittimità della direttiva 2006/24/CE, in quanto lesiva proprio del principio di proporzionalità. Tra i motivi, un obbligo di conservazione dei dati in modo indiscriminato e generalizzato, senza limitazione o eccezione in funzione dell'obiettivo di contrastare i reati gravi. Inoltre, mancava un criterio oggettivo che limitasse l'accesso ai dati raccolti esclusivamente a fini di indagine su reati sufficientemente gravi da giustificare una simile ingerenza nella sfera privata. La pronuncia valorizza il tema della protezione dei dati personali, anche in un settore come quello della lotta alla criminalità, in cui le libertà individuali possono subire limitazioni legittime per finalità di interesse generale⁹⁰.

5. Prospettive future: suggerimenti per una normazione bilanciata e resiliente della FDP

Fermi i dubbi sul possibile uso della tecnica con una mera revisione della normativa domestica, è opportuno guardare a quali garanzie minime dovrebbero essere assicurate⁹¹. Una proposta di legge sulla FDP dovrebbe, innanzitutto, prevedere l'obbligo di comunicare all'interessato (una volta identificato) la modalità per l'esercizio dei propri diritti, tra cui le finalità del trattamento, la base giuridica, il diritto di proporre reclamo, nonché la limitazione del trattamento, ove possibile⁹². Parimenti sono da prevedere termini per la conservazione dei dati o per un esame periodico, come anche la possibilità di trattamento solo fino al conseguimento delle finalità.

In linea con quanto indicato dall'avvocato Pitruzzella, sarebbe poi opportuno limitare la casistica d'uso della tecnica, come avviene ad esempio in Svizzera⁹³. La FDP potrebbe dunque essere usata, sempre «solo

⁸⁸ Una ricostruzione dello strumento delle autorizzazioni generali del Garante è in A. IANNUZZI E F. FILOSA, *Il trattamento dei dati genetici e biometrici*, cit., 8.

⁸⁹ Cons. Stato, VI, 13 agosto 2019, n. 5702.

⁹⁰ S. DE NITTO, *La proporzionalità nel diritto amministrativo*, Torino, 2023, 218 ss.

⁹¹ Chiaramente, come menzionato nel paragrafo introduttivo, non si affronta il profilo processual-penalistico e dunque il necessario raccordo con la normativa di settore.

⁹² Inteso rispetto alle eccezioni previste dalla direttiva polizia (es. compromissione delle indagini) per ritirare, limitare o escludere la comunicazione di informazioni (art. 13).

⁹³ *Federal Act on the Use of DNA Profiles in Criminal Proceedings and for Identifying Unidentified or Missing Persons (DNA profiles act)*, 20 giugno 2003, AS 20004 5269.

se strettamente necessario», in casi di reati gravi, quali l'omicidio e su bilanciamento degli interessi da parte del pubblico ministero, sentito il Garante per la protezione dei dati personali. Ancor meglio, un rafforzamento del bilanciamento sullo «strettamente necessario» sarebbe assicurato da un ritorno all'autorizzazione per questo caso specifico, già citata e ormai abrogata, dell'art. 90 del codice privacy rispetto ai dati genetici⁹⁴.

La limitazione delle finalità del trattamento può poi essere espressa anche in altri termini, vale a dire con riguardo alle caratteristiche fenotipiche che è consentito identificare tramite il DNA. Queste andrebbero limitate a quelle più scientificamente validate e utili a fornire indizi, quali colore degli occhi, dei capelli, la carnagione e la possibile età. In un contesto in cui il soggetto di cui si sta analizzando il DNA è sconosciuto, sarebbe da vietare l'analisi di possibili condizioni di salute o altre informazioni sensibili sull'individuo o la sua famiglia. Vi sarebbe poi la necessità di evitare analisi probabilistiche su elementi di cui l'affidabilità è ancora poco certa, dovendo certamente vietare la possibilità di fornire una bozza di volto sulla base delle capacità attuali della tecnica. La genotipizzazione probabilistica (che prevede l'utilizzo di sistemi di intelligenza artificiale) non pare essere ben bilanciata rispetto alle possibili conseguenze, vista l'attuale incertezza scientifica. Si limiterebbero così possibili eventuali *bias* e il possibile uso discriminatorio dello strumento, come in via interpretativa sembrerebbe già prevedere la normativa rilevante (sebbene, si è scritto – par. 3 – dell'incertezza sulla possibilità della FDP di rientrare tra le pratiche ad alto rischio secondo il regolamento UE sull'IA). La limitazione del trattamento sulla base solo di talune caratteristiche, e senza fornire immagini probabilistiche, favorirebbe un uso della FDP come mero strumento di accompagnamento iniziale.

Nella prospettiva sommariamente descritta, la tecnica dovrebbe essere ricondotta a una funzione ausiliaria e non sostitutiva dell'attività investigativa tradizionale, riducendo al minimo l'invasività sul piano dei diritti fondamentali. Solo un simile approccio precauzionale potrebbe garantire una legittimità sostanziale dell'uso della FDP all'interno di un ordinamento democratico e rispettoso dello Stato di diritto.

6. Alcune ulteriori riflessioni. Il caso della FDP come sfida della normazione sulle tecnologie moderne

Il caso della FDP è un esempio paradigmatico di una sfida più ampia che il diritto moderno si trova ad affrontare. Il progresso scientifico e tecnologico, specialmente in sanità, ma con evidenti ricadute anche nel settore della sicurezza pubblica, postula di continuo interrogativi le cui risposte non sono di semplice individuazione. Vi è una discrasia tra i tempi del progresso scientifico e quelli del legislatore e dell'amministrazione, rendendo difficile la costruzione di una cornice normativa adeguata.

Le nuove tecnologie hanno un impatto pervasivo sul bilanciamento tra diritti fondamentali. Temi come la privacy, l'etica, la sicurezza dei dati, la discriminazione e la responsabilità sono costantemente messi in discussione, come ben evidenziate nel caso della FDP. L'evoluzione della ricerca scientifica, dunque, richiede una "modulazione normativa": non si tratta solo di capire se normare, ma soprattutto come e quando intervenire.

⁹⁴ Una ricostruzione dello strumento delle autorizzazioni generali del Garante è offerta da A. IANNUZZI, F. FILOSA, *Il trattamento dei dati genetici e biometrici*, cit., 8.



Inizialmente, la normazione dovrebbe essere flessibile e solo quando gli esiti dell'innovazione tecnologica si sono stabilizzati, può risultare utile un impianto regolatorio più cogente. Il rischio di "geometrizzare tutta la vita" con regole rigide e anacronistiche può infatti ledere i diritti dei cittadini⁹⁵. Il caso della FDP, con la sua rapida evoluzione e l'incertezza scientifica in alcuni aspetti, rende palese questa necessità di cautela e gradualità. L'assenza di un quadro regolatorio organico non sta limitando l'impiego della tecnica, ma solleva interrogativi sulle garanzie, similmente a quanto avviene in altri settori del progresso tecnologico dove le norme esistenti sono spesso inadeguate o insufficienti.

Inoltre, la crescente intersezione con l'intelligenza artificiale, come in queste pagine anticipato per la FDP, amplifica ulteriormente queste problematiche. I sistemi di IA, se impiegati per esaminare ampi set di dati genomici, rischiano di introdurre o amplificare *bias* e minare la trasparenza e l'affidabilità dei risultati. Questo si collega direttamente alla questione della responsabilità per le azioni generate da macchine con capacità cognitive autonome, un tema che il diritto fatica a inquadrare con le categorie tradizionali.

In definitiva, le perplessità sull'impiego della tecnica con la sola revisione della normativa esistente e la proposta di garanzie normative necessarie per un futuro disegno di legge si integrano pienamente nella più ampia riflessione sulla necessità di un bilanciamento dinamico tra innovazione e tutela dei diritti fondamentali. L'obiettivo è sviluppare un approccio normativo che sia adattivo e resiliente, in grado di governare gli impatti delle nuove tecnologie, evitando che la mancanza di regole chiare o, al contrario, una normazione eccessivamente rigida, compromettano la tutela della persona e la fiducia nelle istituzioni.

Essays

⁹⁵ Così M. DE ANGELIS, *Diritto a informare e a essere informati per l'appropriatezza delle cure. Uno sguardo diverso sul consenso informato*, cit., 202.

