dirittifondamentali.it

Dirittifondamentali.it - Fascicolo 2/2019
Data di pubblicazione – 11 luglio 2019

Il trattamento dei dati genetici e biometrici[*]

di
Antonio Iannuzzi e Francesca Filosa [*]

1. Premessa

Il presente contributo si propone di analizzare il tema della tutela dei dati genetici e biometrici alla luce delle disposizioni del decreto legislativo n.196/2003, Codice in materia di protezione dei dati personali, come modificato dal decreto legislativo n. 101/2018, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)».

Il richiamo costante alle disposizioni del Regolamento UE 2016/679 (d'ora in avanti Regolamento), è necessario ed indispensabile per l'ovvia considerazione della portata generale della fonte europea.

---

[*] Lo scritto è destinato ad essere pubblicato 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*, Giappichelli, Torino. Il presente lavoro è frutto di una riflessione comune. In ogni caso, i parr. 2.1, 2.2 e 4 sono stati materialmente redatti dal Prof. Antonio Iannuzzi, i parr. 3 e 5 dalla Dott.ssa Francesca Filosa, il par. 1 da entrambi gli autori.

[*] Professore associato di Istituzioni di diritto pubblico presso l'Università Roma Tre; Dottoranda di ricerca presso l'Università degli Studi di Roma Tre.

La specificità delle previsioni del Codice in materia di protezione dei dati personali rispetto al trattamento dei dati genetici e biometrici, così come indicato nell'art. 2-*Septies*, si scorge, invece, nell'individuazione di misure di garanzia che devono essere adottate dall'Autorità Garante per la protezione dei dati personali (d'ora in avanti anche Autorità Garante). In particolare, si tratta di linee guida, autorizzazioni e provvedimenti generali che, oltre a determinare il corretto e lecito trattamento di tali dati particolari, individuano anche le misure di sicurezza adeguate che devono essere adottate.

Nonostante la mancanza di misure di garanzia aggiornate, per il presente lavoro sono stati esaminati gli ultimi provvedimenti e le autorizzazioni generali adottate da parte dell'Autorità Garante, a seguito della conclusione del periodo di sottoposizione a consultazione pubblica, così come indicato nello stesso art. 2-*septies* del Codice in materia di protezione dei dati personali. Inutile sottolineare che sarà fondamentale, per ridisegnare il nuovo regime di trattamento di tale tipo di dati personali, la revisione di tali provvedimenti e autorizzazioni, che risulta in corso di svolgimento presso l'Autorità Garante.

2. *"Unico e irripetibile": la nozione di dati genetici e biometrici si spinge fino alle radici dell'elementi costitutivi dell'ordine fisico dell'essere umano*. 2.1. *La mancanza di una definizione univoca ed esaustiva di dati genetici*

La difficoltà nell'individuazione di una convenzione definitoria è dovuta sia al fatto che manca nel panorama giuridico attuale una qualificazione normativa condivisa di tali categorie di dati, sia al fatto che il progresso della ricerca scientifica e l'evoluzione della tecnologica ampliano continuamente le possibilità di acquisizione e di elaborazione di questi dati vanificando ogni tentativo di fornire un'immagine statica della categoria.

Negli ultimi anni, i dati genetici e biometrici sono stati oggetto del dibattito giuridico principalmente in virtù delle peculiarità derivanti dal loro utilizzo nel campo della ricerca scientifica, per i dati genetici, e in quello delle nuove tecnologie, per i dati biometrici.

Nonostante le difficoltà poc'anzi messe in luce, non può di certo essere obliterato l'apporto definitorio tangenzialmente fornito da singole norme o da provvedimenti rintracciabili nell'ordinamento giuridico interno o sovranazionale.

In Italia, una prima definizione è traslabile dalla disciplina in tema di tutela del diritto alla *privacy*[1]. L'autorizzazione al trattamento dei dati genetici del 22 febbraio del 2007[2], adottata dal Garante per la protezione dei dati personali, definisce come «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*»[3].

Rivolgendo lo sguardo, invece, al contesto europeo ed internazionale, già nel 1997 il Consiglio d'Europa, con la Raccomandazione n. R (97) 5[4], e l'UNESCO nel 2003, con la Dichiarazione internazionale sui dati genetici umani[5], hanno reso una

[1] Come sostenuto dalla migliore dottrina, il concetto di *privacy* si è esteso fino a ricomprendere «l'insieme delle regole sulla circolazione delle informazioni personali, rafforzando la rilevanza costituzionale di tale diritto» S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica del diritto privato*, 1997, 588. Sul punto si veda anche M. TIMIANI, *Un contributo allo studio sul diritto alla riservatezza*, in *Studi parlamentari e di politica costituzionale*, 2012, 52 s., il quale afferma che con il termine privacy si esplicita il più ampio concetto derivante dalla tutela della riservatezza e dal diritto alla protezione dei dati personali. La riservatezza intesa come "diritto ad essere lasciato solo", il secondo quale diritto a tutelare le informazioni e i dati che riguardano l'individuo, concedendogli il più ampio potere di controllo su di esse definito come "*habeas data*". Come è stato osservato da L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, 2016, 10 e ss, la tutela della riservatezza è un diritto di complessa definizione poiché ha subito una espansione contenutistica legata oltre che ad interpretazioni giurisprudenziali, anche e soprattutto alla progressiva dimensione socio-relazionale degli individui.

[2] Autorizzazione al trattamento dei dati genetici, 22 febbraio 2007, doc. web n. 1389918, reperibile su www.gpdp.it e pubblicato in Gazzetta Ufficiale n. 65 del 19 marzo 2007.

[3] L. CALIFANO, *Il trattamento dei dati genetici: finalità di ricerca, esigenze di sicurezza e diritto alla protezione dei dati personali*, in *Cultura giuridica e diritto vivente*, in www.ojs.uniurb.it/index.php/cgdv 2017, 1. Come affermato da E. STEFANINI, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, Padova, 2008, 4, tale definizione è rilevante perché non solo riconosce il primo riferimento normativo al "gruppo biologico", ma «rivela la scelta definitoria compiuta dal Consiglio d'Europa nella nozione più ampia di dato genetico come informazione che attiene al patrimonio genetico della persona, a prescindere dalla fonte da cui è tratta».

[4] 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),

[5] La Dichiarazione internazionale sui dati genetici umani, del 16 ottobre 2003, stabilisce alcuni principi riguardanti la raccolta, il trattamento, l'utilizzo e l'archiviazione di dati ricavati dall'analisi di campioni biologici. Lo scopo di tale dichiarazione è quello di definire i principi fondamentali per la tutela di quei diritti dell'individuo che rischiano di essere lesi da un uso

definizione di dato genetico[6], solo parzialmente coincidenti: il primo organismo ha definito i dati genetici come «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», mentre il secondo come le «informazioni sulle caratteristiche ereditarie degli individui ottenute dall'analisi degli acidi nucleici o da altre analisi scientifiche».

L'art. 4 del Regolamento, infine, fornisce il più recente tentativo di inquadramento della categoria, stabilendo che i «*dati genetici sono 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*»"[7].

La differente prospettiva dischiude, a ben vedere, un minimo comune denominatore relativamente alla riconducibilità ai caratteri essenziali e significativi dei «dati personali particolari»[8], che sono rintracciabili in tutte le definizioni precedentemente proposte. Infatti, i dati genetici presentano caratteristiche tali da renderli unici. Sono capaci di fornire, sia in nel presente che nel futuro, informazioni di tipo scientifico, medico e personale sempre attuali, la cui validità e utilizzabilità permane per tutta la vita dello stesso individuo, ma anche per ogni altra persona a lui biologicamente "vicina". Proprio per questo motivo, il trattamento dei dati genetici richiede una speciale tutela legale.

Come noto, i dati in esame hanno potenzialità di trattamento molto importanti: sono in grado di rivelare non solo la discendenza e i legami di parentela, ma anche

---

improprio dei dati genetici. Si tratta del diritto di non discriminazione, della tutela della riservatezza, del diritto alla salute e dell'autodeterminazione. Per un ulteriore approfondimento sul punto, si veda, I.R. PAVONE, *Diritti dell'uomo e genetica*, in *Enc. giur.*, Agg. XV, Roma, 2007, *ad vocem*.

[6] Articolo 29 - Gruppo di lavoro per la tutela dei dati personali, *Documento di lavoro sui dati genetici*, adottato il 17 marzo 2004, reperibile su www.gpdp.it, doc web n. 1337087.

[7] Art. 4, punto 13) del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[8] È lo stesso Reg. UE 2016/679 che all'articolo 9 disciplina il trattamento dei dati personali particolari. Al primo paragrafo di tale articolo elenca una serie di dati considerati particolari, tra cui anche i dati genetici.

i caratteri che rendono distinguibile un individuo da un altro e ancora possono svelare informazioni dei consanguinei dello stesso.

Le peculiarità di questi dati possono, quindi, scindere il legame fra trattamento dei dati e soggetto titolare degli stessi, con importanti ricadute anche relativamente alla disciplina giuridica del consenso.

È inoltre possibile ottenere facilmente oppure estrarre da "materie prime"[9] informazioni genetiche dell'individuo, che possano essere utilizzate da un numero crescente di soggetti, i quali possono trattare lecitamente tali dati e a scopi diversi[10].

La specificità di utilizzo dei dati genetici mostra che l'orizzonte giuridico della tutela della *privacy* è importante ma parziale: in questo ambito vengono in rilievo anche altri interessi meritevoli di tutela, per cui effettivamente si può affermare che in «punto di diritto la questione si sposta sul corretto bilanciamento fra le libertà individuali e le esigenze pubbliche»[11]. La disciplina relativa alla protezione di questa categoria di dati si pone al punto di intersezione fra la tutela della salute, la libertà di ricerca e di sperimentazione scientifica, e la sicurezza pubblica, ponendo in essere situazioni la cui regolazione presuppone complesse operazioni di bilanciamento.

Un ulteriore profilo problematico che il regime giuridico dei dati genetici involge è quello relativo al profilarsi di scelte difficili legate al riconoscimento del diritto a sapere o di un diritto speculare a non sapere, soprattutto in riferimento alla possibilità di analisi predittive relative alla predisposizione genetica a malattie particolarmente gravi[12].

---

[9] Nel Documento di lavoro sui dati genetici, per materie prime si intendono i tessuti e tutta la materia biologica dalla quale si possono ricavare informazioni genetiche.

[10] Articolo 29 - Gruppo di lavoro per la tutela dei dati personali, *Documento di lavoro sui dati genetici*, adottato il 17 marzo 2004, reperibile su www.gpdp.it, doc web n. 1337087. Il Gruppo Articolo 29 ha precisato che i dati genetici devono essere trattati secondo finalità determinate, esplicite e legittime ed in modo compatibile con le stesse. Inoltre, il Regolamento all'art. 9, par. 2, lett. a), stabilisce che il trattamento dei dati particolari, può avvenire solo previo il consenso per specifiche finalità.

[11] L. CALIFANO, *Il trattamento dei dati genetici*, cit., 2.

[12] Ancora L. CALIFANO, *op. cit*., p. 2. Sul punto anche E. STEFANINI, *op. cit*., 7, afferma che la stessa ricerca scientifica oltre ad individuare notevoli benefici per la salute pubblica e la collettività in generale, può rappresentare un importante rischio per i diritti fondamentali, come il diritto alla *privacy*, inteso, in questo senso come diritto di non sapere. La stessa A. precisa anche che «nel

2.2. *Alla ricerca di una definizione di dati biometrici*

Analogamente ai dati genetici, anche per i dati biometrici, prima dell'entrata in vigore del Regolamento, non era possibile rinvenire una definizione normativa. Oggi, finalmente, l'art. 4, punto 14), li definisce come «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici»

L'Autorità Garante nelle Linee guida in materia di riconoscimento biometrico e firma grafometrica[13], ha ripreso la medesima descrizione fornita nel Parere 3/2012 del Gruppo di lavoro WP29[14], che identifica i dati biometrici come quelli 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».

Già nel 2010 in ambito nazionale, il Comitato nazionale per la bioetica, aveva individuato la "biometria" come 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»[15]. Dal parere appena citato, si evince, infatti, che con lo sviluppo delle nuove tecnologie, l'impiego della biometria si è esteso a diversi ambiti e settori che per certi versi possono rendere più semplici determinate procedure, si pensi ad esempio all'utilizzo della biometria per consentire l'accesso a determinati luoghi di lavoro ad un numero ristretto di soggetti oppure all'utilizzo in alcuni specifici campi come la tutela della salute, la

---

rispetto del diritto di autodeterminazione, all'individuo deve essergli riconosciuto il diritto di non essere messo a conoscenza di informazioni che potrebbero determinare effetti devastanti sul libero sviluppo della sua personalità».

[13] Autorità Garante per la protezione dei dati personali, Linee guida in materia di riconoscimento biometrico e firma grafometrica, allegato A al Provvedimento del Garante del 12 novembre 2014, reperibile in www.gpdp.it, doc web n. 3563006.

[14] Articolo 29 - Gruppo di lavoro per la tutela dei dati personali, Parere 3/2012 sugli sviluppi nelle tecnologie biometriche, WP193, adottato il 27 aprile 2012.

[15] Comitato Nazionale per la Bioetica, *L'identificazione del corpo umano: profili bioetici della biometria*, 26 novembre 2010, 3.

prevenzione delle frodi sanitarie ed ancora la protezione delle informazioni mediche riservate[16].

È necessario non sottovalutare l'enorme impatto di tali sistemi sui diritti fondamentali degli interessati[17] perché, con l'uso generalizzato dei dati biometrici, in modo particolare, il riconoscimento del volto, dell'impronta delle dita o dello schema delle vene[18], che hanno già raggiunto un livello ottimale di sviluppo e un utilizzo "senza limiti", è sicuramente verificabile il rischio che gli interessati diventino insensibili agli effetti che il loro trattamento possa avere sulla loro vita, proprio perché l'impiego di queste tecnologie di recente creazione agevola l'andamento della vita quotidiana[19].

Le applicazioni biometriche sono maggiormente utilizzate a fini di autenticazione e verifica automatica[20] di un individuo e si possono distinguere in due categorie principali: una di tipo fisico e fisiologico, che misura le caratteristiche fisiologiche di una persona, un'altra di tipo comportamentale, legata alla misurazione del comportamento di una persona[21].

3. Il quadro normativo

La Direttiva 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[22], anche conosciuta come "direttiva madre", non riconosceva la specificità dei dati genetici e

[16] Ivi, p. 4 e 5.

[17] Com'è stato puntualmente messo in luce in Articolo 29 - Gruppo di lavoro per la tutela dei dati personali, Parere 3/2012 sugli sviluppi nelle tecnologie biometriche, WP193, adottato il 27 aprile 2012, p. 9.

[18] Ivi. P. 3.

[19] Articolo 29 - Gruppo di lavoro per la tutela dei dati personali, *Documento di lavoro sui dati genetici*, adottato il 17 marzo 2004, reperibile su www.gpdp.it, doc web n. 1337087, p. 2.

[20] Attraverso l'autenticazione, il sistema certifica l'identità della persona grazie all'elaborazione di dati biometrici che si riferiscono all'individuo autore della domanda e prende una decisione si/no. Con l'identificazione il sistema riconosce l'individuo autore della domanda distinguendolo da altre persone i cui dati biometrici sono a loro volta registrati.

[21] Ivi., p. 3 e 4.

[22] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995)

biometrici e li faceva, perciò, rientrare nella generale categoria dei dati personali[23], che ricomprendeva «*qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale*»[24].

È vero, infatti, che le informazioni genetiche e le misure di identificazione biometrica o la loro traduzione digitale in un modello sono elementi che permettono di identificare una persona fisica, poiché sono in grado di fornire informazioni che rendono un individuo identificato o identificabile proprio per loro stessa natura[25].Bisogna precisare, però, che, come già detto sopra, i dati genetici possono fornire un quadro dettagliato della condizione fisica e del relativo stato di salute di una persona e dei suoi affini e, pertanto, sono considerati "dati relativi alla salute". Non è diverso il caso dei dati biometrici, i quali sono in grado di rivelare l'origine razziale o etnica, in particolare riguardo a quei sistemi basati sul riconoscimento del volto.

In tale prospettiva, la direttiva 95/46/CE, per dare risalto alla sensibilità della tipologia dei dati personali in esame, prevedeva delle prescrizioni specifiche mirate a garantire un livello di protezione più elevato. Trattandosi di categorie particolari di dati, dovevano essere assoggettate alle disposizioni dell'art. 8 della stessa direttiva.

Il d.lgs. n. 196/2003, recante "Codice in materia di protezione dei dati personali" (d'ora in avanti anche Codice *privacy*), recependo le indicazioni dettate dalla direttiva, all'interno di un corpus normativo ora abrogato, aveva costruito una efficace cornice normativa per il trattamento dei dati genetici e biometrici, innanzitutto considerando l'informativa e il consenso. Alla base v'era il

[23] Sul punto si veda anche L. CHIEFFI, *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2018 215, nt. 40.

[24] Art. 2, lett. *a)*, direttiva 95/46/CE.

[25] Sul punto si vedano i contributi dell'Articolo 29 - Gruppo di lavoro per la tutela dei dati personali, Documento di lavoro sulla biometria del 2003 e Documento di lavoro sui dati genetici del 2004, reperibili su www.gpdp.it

riconoscimento dell'autodeterminazione informativa, per cui l'interessato avrebbe potuto elaborare una scelta individuale, libera e consapevole, solo dopo aver ricevuto una dettagliata informativa che avesse illustrato in modo chiaro le finalità del trattamento, il periodo di conservazione dei dati genetici, l'elencazione dei diritti dell'interessato, l'eventuale possibilità di limitare l'ambito di comunicazione di tali dati e il trasferimento dei campioni biologici ed anche l'eventuale utilizzo di tali dati per ulteriori scopi. È facilmente desumibile che il trattamento dei dati genetici e dei campioni biologici, poteva avvenire solo previo consenso informato dell'interessato[26]. Inoltre, l'art. 90 del Codice *privacy*, anch'esso ad oggi abrogato dal decreto legislativo n. 101 del 2018[27], prevedeva che il trattamento dei dati genetici poteva realizzarsi successivamente al rilascio di una apposita autorizzazione del Garante per la protezione dei dati personali, sentito il Ministro della salute, che acquisiva, a tal fine, il parere del Consiglio superiore di sanità. Tale autorizzazione doveva individuare anche ulteriori elementi da includere nell'informativa all'interessato, con particolare riguardo alla specificazione delle finalità perseguite e dei risultati conseguibili, anche in relazione alle notizie inattese conoscibili per effetto del trattamento dei dati e al diritto di opporsi al medesimo trattamento per motivi legittimi.

L'Autorizzazione generale per il trattamento dei dati genetici[28], adottata per la prima volta nel febbraio 2007, compie due importanti operazioni: in primo luogo, mette in connessione l'istituto del consenso con le finalità lecite del trattamento dei dati genetici ed in secondo luogo, assimila i dati genetici ai dati sensibili.

[26] L. CALIFANO, *op. cit*., 3.

[27] D. lgs. 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"

[28] Garante per la protezione dei dati personali, Autorizzazione n. 8/2014, Autorizzazione generale al trattamento dei dati genetici, 11 dicembre 2014, doc. web. n. 3632835 In, www.gpdp.it. Successivamente, l'Autorità Garante ha adottato l'Autorizzazione n. 8/2016, Autorizzazione generale al trattamento dei dati genetici del 15 dicembre 2016. Attualmente il testo dell'Autorizzazione al trattamento dei dati genetici è sottoposta a consultazione pubblica.

In merito al consenso, l'Autorizzazione generale, precisa che «i dati genetici possono essere trattati e i campioni biologici utilizzati soltanto per gli scopi indicati nella presente autorizzazione e rispetto ai quali la persona abbia manifestato previamente e per iscritto il proprio consenso informato».

Quindi, è chiaro che il trattamento dei dati genetici è considerato lecito solamente se l'interessato ha rilasciato il proprio consenso informato, rispetto alle finalità indicate nella stessa autorizzazione, ossia: la tutela della salute dell'interessato e di terzi appartenenti alla stessa linea genetica dell'interessato nonché la ricerca scientifica e statistica, finalizzata alla tutela della salute dell'interessato, di terzi o della collettività in campo medico, biomedico ed epidemiologico e anche nel settore della sperimentazione di farmaci[29].

Relativamente alla natura particolare dei dati genetici, la stessa autorizzazione generale, li assimila ai dati sensibili, sottoponendoli quindi alle medesime garanzie, prima fra tutte, il consenso. Tale posizione si ricava dall'espresso rinvio agli artt. 23 e 26 del Codice *privacy*, oggi abrogati, ad opera dell'Autorizzazione generale, prevedendo necessariamente la forma scritta del consenso per il trattamento di questi dati.

A sostegno dell'orientamento dell'Autorità Garante, sulla natura dei dati genetici quali dati sensibili, si esprimono due documenti internazionali, già esaminati all'inizio del presente paragrafo: il parere del gruppo dei Garanti europei del 2004, che li riconosce come particolarmente sensibili, tanto da trattarli come dati particolari ai sensi delle previsioni dell'art. 8 della Direttiva madre e la

[29] Ivi, paragrafi n. 3 e 6. È opportuno precisare che il Regolamento (UE) n. 536/2014 del Parlamento Europeo e del Consiglio del 16 aprile 2014, sulla sperimentazione clinica di medicinali per uso umano e che abroga la direttiva 2001/20/CE, prevede espressamente negli artt. 28 e ss. che il soggetto interessato deve rilasciare il consenso informato per partecipare alla sperimentazione clinica ed inoltre definisce all' art. 4, par. 2, punto 21) il consenso informato come «espressione libera e volontaria di un soggetto della propria disponibilità a partecipare a una determinata sperimentazione clinica (…)».

Raccomandazione R(97)5[30] del Consiglio d'Europa, che individua una serie di prescrizioni specifiche per garantire agli stessi una maggiore protezione[31].

L'evoluzione normativa in tema, trova il suo sbocco nelle previsioni del Regolamento, che li disciplina all'art. 4.13 e 4.14 all'interno della sezione dedicata alle categorie particolari di trattamenti, mentre il loro trattamento è regolato dagli artt. 9 e 89 del Regolamento UE 2016/679.

L'articolo 9, al primo paragrafo, vieta il trattamento dei dati genetici e biometrici, a meno che non sia stato rilasciato il consenso. Il trattamento è lecito, invece, per finalità lavorative e previdenziali, qualora sia necessario tutelare un interesse vitale, per il raggiungimento delle finalità di legittime attività di fondazioni, associazioni o altri organismi senza scopo di lucro, qualora i dati personali particolari siano resi manifestamente pubblici dall'interessato, per lo svolgimento di attività difensive ed investigative, oppure per il raggiungimento di un interesse pubblico rilevante o, infine, per un interesse pubblico rilevante riguardante il sistema sanitario nazionale e regionale ed infine per scopi statistici o scientifici, così come precisamente disciplinato dall'art. 89[32]. L'art. 89 precisa, infatti, al secondo paragrafo, che per scopi di ricerca scientifica o storica, oppure per fini statistici, la disciplina regolamentare deve permettere agli Stati membri di introdurre deroghe e adeguamenti. In merito alle deroghe, potrebbero essere disapplicate le disposizioni del regolamento riguardanti l'esercizio dei diritti dell'interessato, in particolare il diritto alla rettifica, alla cancellazione, all'oblio, alla portabilità e l'opposizione al trattamento, subordinandole all'implementazione di specifiche garanzie e misure di sicurezza adeguate. In merito all'adeguatezza, bisogna considerare l'applicazione dei principi di necessità, proporzionalità e minimizzazione dei dati. Per quanto concerne, invece, l'applicazione delle misure tecniche adeguate, è

[30] 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).

[31] L. CALIFANO, *op. cit.*, 3 e 4.

[32] G. DRUETTA, *9. Trattamento di categorie particolari di dati personali*, in G. M. RICCIO, G. SCORZA, E. BELISARIO, *GDPR e normativa privacy commentario. Regolamento UE 2016/679 del 27 aprile 2016. Decreto di adeguamento – D. Lgs. n. 101/2018, Codice privacy – D. Lgs. n. 196/2003*, Milano, ed. Wolkers Kluwer, 2018, p. 93 e ss.

necessario valutare se procedere con la pseudonimizzazione[33] oppure con l'anonimizzazione[34], notando attentamente che attraverso il processo di pseudonimizzazione, i dati sono da considerarsi dati personali a tutti gli effetti[35].

In virtù di quanto previsto dall'art. 2-*septies* del Codice *privacy*, d. lgs. n.196/2003, così come novellato dal d. lgs. n. 101 del 2018, "*i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento (…) in conformità alle misure di garanzia disposte dal Garante*". Il comma successivo precisa che tali garanzie devono tener conto di una serie di fattori, tra cui le indicazioni contenute nelle linee guida e nelle raccomandazioni pubblicate dal Comitato europeo per la protezione dei dati, nonché dell'evoluzione scientifica e tecnologica e dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea.

4. L'utilizzo dei dati genetici nelle biobanche di ricerca fra salvaguardia della salute, tutela della riservatezza e libertà di ricerca.

Anche il riferimento alle biobanche è fortemente ambiguo e sfuggente dal punto di vista concettuale e definitorio[36], com'è reso evidente dalla circostanza che un progetto finanziato dall'Unione Europea ha prodotto, solo fino al 2010, circa ventisei definizioni[37].

---

[33] Così come definito da G. D'ACQUISTO e M. NARDI, in *Big Data e Privacy by Design. Anonimizzazione, Pseudonimizzazione e Sicurezza*, Torino, 2017, 38, la pseudonimizzazione «consiste nel sostituire un attributo, solitamente univoco, di un dato con un altro, ugualmente univoco e solitamente non immediatamente intellegibile». Attraverso questa tecnica, il processo di identificazione può essere più oneroso, ma è mantenuto inalterato il quadro di certezze per concatenare l'attribuzione del dato pseudonimo alla persona.

[34] Ancora G. D'ACQUISTO e M. NARDI, *op. cit.*, 35, definiscono il processo di anonimizzazione, volto ad impedire la re-identificazione della persona, avviene attraverso l'uso didue tecniche principali, la distorsione e la generalizzazione dei dati che introducono elementi di incertezza. La scelta di una o dell'altra tecnica deve avvenire secondo la disponibilità dei mezzi di cui gode il titolare del trattamento, che possono essere ripartiti in due classi: mezzi "ragionevolmente utilizzabili" e quelli "irragionevolmente utilizzabili".

[35] G. PEDRAZZI, *89. Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*, in G. M. RICCIO, G. SCORZA, E. BELISARIO, *op. cit.*, 656.

[36] Cfr. J. KAYE, *Regulating human genetic Databases in Europe*, in M. HAYRY, R. CHADWICK, V. ARNASON, G. ARNASON, *The ethics and governance of human genetic databases. European perspectives*, Cambridge, 2007, 92 ss.

[37] Come ha fatto notare A. SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, II ed., Padova, 2016, 157.

Stante, perciò, l'ampiezza del tema, i confini di questo contributo non consentono un'analisi approfondita del tema. È, però, fondamentale, in questa sede, almeno tracciare i contorni più rilevanti.

Intanto, la scelta di utilizzare il lemma «banca» non sembra particolarmente felice né particolarmente calzante perché conduce ad un'associazione, del tutto fuorviante, con gli istituti di credito, laddove, le biobanche, invece, pur nella varietà delle tipologie e delle finalità che perseguono, possono identificarsi come unità operative e di servizio, preposte a raccogliere, conservare, classificare, gestire e distribuire materiali biologici umani (cellule, tessuti, DNA) d'individui o gruppi d'individui sani o malati, per finalità biomediche (di ricerca, di diagnosi, di prevenzione o di terapia), all'interno dei presidi ospedalieri o centri di ricerca[38].

Lo scopo principale delle biobanche è rappresentato dalla possibilità che offrono di mettere in correlazione particolari profili genomici con reperti molecolari e con il profilo clinico della malattia[39]. Si possono distinguere in due categorie, a seconda che il materiale biologico sia conservato a scopo di ricerca oppure che sia conservato per uso clinico/terapeutico, vale a dire destinato all'applicazione sull'uomo.

Le problematiche giuridiche che le biobanche sollevano sono di grande portata. Per dare immediatamente una misura dei problemi evocati, si pensi solo alla possibilità di creare un database nazionale o locale che permetta schedature di massa, con le più diverse finalità, talune delle quali, tra l'altro, ad oggi neanche immaginabili perché soggette a trattamenti frutto di futuri sviluppi tecnologici. È solo appena il caso di far menzione ad un ulteriore elemento problematico che rende oltremodo difficile il compito di dare regolazione al fenomeno, ossia che a finalità diverse perseguite corrispondono necessariamente bilanciamenti mutevoli fra i principi e i diritti costituzionali che vengono, volta per volta, in riferimento[40].

---

[38] Comitato Nazionale per la Bioetica, *Parere sulle biobanche pediatriche*, 11 aprile 2014, 5.

[39] M. TOMASI, *Genetica e Costituzione. Esercizi di eguaglianza, solidarietà e responsabilità*, Napoli, 2019, 231 s.

[40] Si pensi anche alle complesse implicazioni delle biobanche a fini investigativi, la cui trattazione esula dall'oggetto del presente studio. Nell'ordinamento giuridico italiano la legge 30 giugno 2009, n. 85, ha previsto, per la prima volta, la disciplina della banca dati nazionale del

Nell'ordinamento italiano, le biobanche con finalità di ricerca e di diagnosi sono state oggetto dell'Autorizzazione generale al trattamento dei dati genetici adottata dall'Autorità garante che, all'art. 3, lett. *c)*, che rende legittimo il trattamento dei dati genetici per la «ricerca scientifica e statistica, finalizzata alla tutela della salute dell´interessato, di terzi o della collettività in campo medico, biomedico ed epidemiologico, anche nell´ambito della sperimentazione clinica di farmaci, o ricerca scientifica volta a sviluppare le tecniche di analisi genetica (sempre che la disponibilità di dati solo anonimi su campioni della popolazione non permetta alla ricerca di raggiungere i suoi scopi)».

Tale trattamento è subordinato all'ottenimento del consenso dell'interessato, salvo che nei casi di indagini statistiche o di ricerca scientifica previste dalla legge o dalla medesima autorizzazione.

Il rimedio della richiesta del consenso dell'interessato, tuttavia, non supera tutti i problemi suscitati dall'uso dei dati genetici custoditi nelle biobanche, soprattutto in riferimento all'evenienza di un uso pregiudizievole verso terzi derivante dal fatto che il genoma di un soggetto contiene, è bene ripeterlo, una serie di informazioni che riguardano anche gli appartenenti al suo gruppo biologico, che è costituito dai suoi consanguinei.

Un ulteriore profilo problematico è rappresentato dal fatto che le finalità future di utilizzo legate allo sviluppo tecnologico, ancora sconosciute al momento della raccolta del materiale genetico e all'espressione del consenso informato possono rendere inattuale o anacronistico il consenso inizialmente concesso perché non idoneo a coprire utilizzi futuri o futuribili. Per ovviare a queste difficoltà, troppo

DNA e del laboratorio centrale per la banca dati nazionale del DNA, a fini investigativi. L'intervento legislativo, tuttavia, si è limitato a prevederne l'istituzione senza darne compiuta disciplina. In assenza di ulteriore attuazione, i laboratori di analisi del DNA delle forze di polizia hanno continuato per lungo tempo ad operare in un regime di sostanziale autonomia normativa. Il vuoto normativo è stato finalmente colmato dal regolamento di attuazione della legge n. 85/2009, il d.P.R. 7 Aprile 2016, n. 87. In argomento, v. A. SANTOSUOSSO, 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 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, 2017.

incauto e foriero di problemi potrebbe risultare ammettere la liceità di un consenso aperto, c.d. *open consent*, espresso sulla base di un'informativa che genericamente metta il soggetto sull'avviso della possibilità di sviluppi futuri, perciò non prevedibili. In alternativa, è stato proposto un consenso dinamico che consente di coinvolgere il paziente anche in futuro con la possibilità di modificare l'opzione inizialmente espressa[41]. Una soluzione originale che si avanza in questa sede è quella di chiedere previamente al titolare dei dati se, in caso di sviluppi futuri frutto di analisi nuove effettuate sui suoi dati genetici, preferisce essere contattato o, in alternativa, vuole essere lasciato in pace. Non si può sottovalutare, infatti, la portata di stress e ansia che il solo primo contatto, foriero di notizie nuove ancora non comunicate, può arrecare ad un soggetto, In tal modo si consentirebbe, a monte, di far decidere all'interessato se chiudere del tutto la porta all'eventualità di comunicazioni future, di qualsiasi tipo, o se accettare un contatto, salvo poi riservarsi comunque l'ulteriore possibilità di esprimere il consenso o di negarlo.

Dilemmi etici e giuridici di ancor più difficile soluzione pongono le biobanche pediatriche, che si contraddistinguono per essere collezioni di materiali biologici di minori e che sono finalizzate alla ricerca scientifica. Il tema richiederebbe certamente una trattazione più ampia. Nell'economia del presente lavoro, molto utile a fornire un quadro delle implicazioni etiche e giuridiche appare il già citato parere del Comitato nazionale di bioetica dell'11 aprile 2014[42]. Il documento sviluppa nel dettaglio le problematiche principali che le biobanche pediatriche sollevano: quello relativo al consenso che è espresso dai genitori o dal minore/adulto, e quello, invece, legato all'alternativa fra il diritto a "sapere" e diritto a "non sapere" dei genitori e del rappresentante legale nel caso di analisi predittive sull'insorgenza di malattie gravi.

Per ciò che concerne il primo profilo problematico, si pongono problemi specifici per via del fatto che da una parte il materiale biologico non appartiene a chi lo cede e dall'altra che i minori non sono ancora in grado di esprimere un consenso

[41] A. SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., 167.

[42] V. nt. 39.

informato. Il Comitato, perciò, raccomanda di non anonimizzare i campioni in modo irreversibile e di non consentire ai genitori o al rappresentante legale di di fornire un consenso "ampio" o "aperto", ma solo limitatamente ad una ricerca specifica o direttamente correlata (c.d. consenso parzialmente ristretto), previa informativa completa e dettagliata, «così che i cedenti possano valutare le finalità, la durata, i luoghi e le modalità di esecuzione del progetto scientifico nel quale viene impiegato il campione». Inoltre, fra le altre cose, «i genitori dovrebbero essere rassicurati sul piano gestionale e sulle modalità con cui la biobanca assicura la conservazione e la "confidenzialità" dei dati raccolti», mentre «esplicito dovrebbe essere il divieto di accesso ad alcuni soggetti terzi, quali assicurazioni e datori di lavoro».

Relativamente alla seconda questione problematica ritiene che il consenso informato dei genitori o del rappresentante legale relativo alla donazione dei campioni biologici debba prevedere esplicitamente che l'informativa sia data, se le ricerche forniscono informazioni sufficientemente fondate e attendibili di modo che, a fronte di benefici reali o potenziali, si possa configurare un «dovere del ricercatore di informare e un diritto/dovere di sapere dei genitori/rappresentante legale in ragione dell'interesse del minore, anche se ciò comporta un onere sul piano dei costi e sul piano organizzativo per le biobanche, oltre che un onere psicologico per i genitori stessi».

5. *L'utilizzo dei dati biometrici per l'accesso ai luoghi di lavoro e per motivi di sicurezza nazionale.*

Il diritto, nell'assumere il compito oneroso di regolamentare l'impiego delle nuove tecnologie, deve contemperare i potenziali benefici che esse possono offrire e i rischi per l'uomo, cercando di rinvenire un punto di equilibrio fra la libertà della ricerca scientifica e la tutela dei diritti della persona[43]. Gli esempi che dimostrano la

[43] Sul punto si veda L. CHIEFFI, *op. cit.*, 208 s. L'autore, a conferma di ciò, afferma che in assenza di adeguata regolamentazione e controlli, i reati di crimine informatico potrebbero moltiplicarsi e gli interessati vedrebbero lesi i loro diritti. Pensando al campo della biomedicina, se si facesse un uso incontrollato dei *software* utilizzati dalle strutture sanitarie, all'interno delle quali

complessità di questa operazione sono molti. Fra i tanti, sembra ancor più attuale e calzante, la discussione in Parlamento relativa al disegno di legge «Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo»[44], meglio conosciuto come "ddl concretezza". Di particolare interesse, ai fini del presente lavoro, è la previsione dell'articolo 2 rubricato «Misure per il contrasto all'assenteismo», il quale introduce tecniche di rilevamento biometrico e sistemi di videosorveglianza[45] per verificare l'osservanza dell'orario di lavoro[46].

La ragione di questa previsione è dovuta al fatto che il corpo di ognuno di noi, presenta delle caratteristiche uniche, per cui è considerato come una vera e propria *password*, grazie soprattutto allo sviluppo tecnologico che ha reso i mezzi e gli strumenti idonei al processo di identificazione univoca. Infatti, le caratteristiche fisiche e/o comportamentali[47] degli esseri umani, sono acquisite da sensori elettronici, elaborate da appositi algoritmi matematici[48] e trasformate in modelli numerici[49].

Sull'impiego delle tecnologie biometriche e di videosorveglianza, per contrastare il fenomeno dell'assenteismo, si è espressa anche l'Autorità Garante per la protezione

---

circolano notevoli quantità di dati sensibili, risulterebbe grave pregiudizio per la salvaguardia della riservatezza e per la salute stessa dei soggetti interessati.

[44] Senato della Repubblica, A.S. n. 920-A.

[45] L'art. 2 prevede quanto segue: «Ai fini della verifica dell'osservanza dell'orario di lavoro, le amministrazioni pubbliche (…) introducono, (…) sistemi di verifica biometrica dell'identità e di videosorveglianza degli accessi, in sostituzione dei diversi sistemi di rilevazione automatica, attualmente in uso, nel rispetto dei princìpi di proporzionalità, non eccedenza e gradualità sanciti dall'articolo 5, paragrafo 1, lettera *c),* del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016».

[46] Servizio Studi del Senato della Repubblica, XVIII Legislatura, Dossier del Servizio Studi sull'A.S. 920 –A "*Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo*", dicembre 2018 n. 82/1, 16.

[47] Così come precisato dallo stesso Comitato Nazionale per la Bioetica, si possono distinguere le nostre caratteristiche individuali attraverso quel che siamo (volto, impronte digitali, DNA etc.), e quel che facciamo (voce, andatura, firma etc.). Le prime riconducibili alle caratteristiche fisiche, mentre le altre a quelle comportamentali.

[48] Sulla rilevanza costituzionale degli algoritmi nelle decisioni rilevanti per la libertà è fondamentale la lettura di A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal - Rivista di BioDiritto*, 2019, 63 ss.

[49] Comitato Nazionale per la Bioetica, *L'identificazione del corpo umano: profili bioetici della biometria,* 26 novembre 2010, 4.

dei dati personali, che ha chiarito la sua posizione il 6 febbraio 2019 con l'audizione presso le Commissioni riunite I (Affari Costituzionali) e XI (Lavoro) della Camera dei Deputati. In tale sede il Presidente dell'Autorità, Antonello Soro, ha ribadito la necessità che il legislatore nazionale rispetti il diritto alla protezione dei dati e adoperi un bilanciamento secondo il canone della proporzionalità. Questo principio è centrale nel parere, infatti l'analisi compiuta dall'Autorità traccia un quadro completo delle disposizioni del Regolamento riguardo al trattamento dei dati biometrici[50], e sulla specifica riserva normativa nazionale in materia di lavoro, così come previsto dall'art. 88, par. 1 e 2. È da precisare che nel parere sono rese note le deroghe previste dell'art. 9, par. 2, che permettono di trattare le particolari categorie di dati ove sussista la necessità per il titolare di adempiere ad un obbligo legale o di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Inoltre, rispetto alle misure di garanzia sancite dall'art. 2-*septies* del Codice *privacy*[51], la previsione dell'art. 2 del ddl concretezza, non appare compatibile con i canoni di necessità e proporzionalità, poiché l'obbligo di impiegare in modo contestuale due sistemi di verifica per il rispetto dell'orario di lavoro eccede i limiti imposti dalla stretta necessità del trattamento rispetto al fine perseguito. Se l'introduzione di un sistema di verifica della presenza in servizio così invasivo quale quello biometrico è ritenuto efficace e affidabile, ne consegue che la videosorveglianza è da ritenersi ultronea per raggiungere lo stesso fine. Oltretutto non sembra essere proporzionale l'introduzione sistematica, generalizzata e indifferenziata per tutte le pubbliche amministrazioni, di sistemi di

[50] In particolare, il riferimento è all'art. 9 del Reg. UE 2016/679, il quale annovera tale tipologia di dati tra le categorie particolari di dati personali alle quali è riconosciuta una tutela rafforzata, in ragione dei rischi (di discriminazione, in particolare) ai quali un loro indebito utilizzo può esporre l'interessato.

[51] Per misure di garanzia si intendono le autorizzazioni generali al trattamento dei dati in casi specifici, le quali devono essere adottate dal Garante per la protezione dei dati personali con cadenza almeno biennale, e devono tener conto in particolare: delle linee guida, delle raccomandazioni e delle migliori prassi pubblicate dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali; dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure; dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea.

identificazione biometrica per la rilevazione delle presenze, poiché particolarmente invasivi.

Il Garante conclude che l'utilizzo di sistemi di rilevazione biometrica, oltre che per specifiche previsioni di legge attentamente esaminate alla luce del criterio di proporzionalità e delle misure di sicurezza e di garanzia adeguate, sono ammessi in presenza di fattori di rischio specifici e quindi, per realizzare il fine del contrasto dell'assenteismo e della falsa attestazione della presenza in servizio bisognerebbe ricorrere a misure meno invasive rispetto alla sfera della persona[52].

Con il provvedimento in tema di biometria[53], adottato unitamente alle linee guida in materia di riconoscimento biometrico e firma grafometrica[54], l'Autorità Garante ha individuato le misure, organizzative, procedurali e soprattutto tecniche per assicurare che il trattamento dei dati biometrici avvenga nel rispetto della disciplina della tutela dei dati personali. In particolare, il provvedimento, per alcune tipologie di trattamento, prescrive la possibilità di semplificare alcuni adempimenti in ambito *privacy*, sempre nel rispetto delle misure di sicurezza. Si tratta di: *a)* autenticazione informatica (impronta digitale o emissione vocale); *b)* controllo di accesso fisico ad "aree sensibili" dei soggetti addetti e utilizzo di apparati e macchinari pericolosi con utilizzo dell'impronta digitale e topografia della mano (intendendo per aree sensibili aree in cui sono conservati oggetti di particolare valore, aree dove si svolgono processi produttivi pericolosi); *c)* utilizzo dell'impronta digitale o della topografia della mano a scopi facilitativi (biblioteche pubbliche, aree portuali riservate); *d)* sottoscrizione di documenti informatici (firma grafometrica, come base per la soluzione di firma elettronica avanzata) [55].

---

[52] Audizione del Presidente dell'Autorità Garante per la protezione dei dati personali nell'ambito dell'esame del disegno di legge C. 1433 recante interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo, presso le Commissioni riunite I (Affari Costituzionali) e XI (Lavoro) della Camera dei Deputati (6 febbraio 2019), in www.gpdp.it , doc web n. 9080870

[53] Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014, (Pubblicato sulla Gazzetta Ufficiale n. 280 del 2 dicembre 2014)

[54] Allegato A al Provvedimento del Garante per la protezione dei dati personali del 12 novembre 2014, in www.gpdp.it doc. web n. 3563006.

[55] Sul punto si veda V. FIORILLO, *Il provvedimento e le linee guida del Garante privacy in materia di biometria*, in *Democrazia e sicurezza*, 2015, 99.

In questa sede, è bene soffermarsi sul controllo di accesso fisico ad "aree sensibili" dei soggetti addetti e utilizzo di apparati e macchinari pericolosi. L'utilizzo dell'impronta digitale e della topografia della mano per il controllo dell'accesso ad aree ristrette o riservate, per l'apertura di varchi o di serrature a protezione di locali o per l'uso di determinati apparati e macchinari, è consentito per finalità di sicurezza, per la protezione patrimoniale o la tutela dell'incolumità di persone. Le stesse linee guida prevedono delle misure di sicurezza relative al ciclo di vita dei dati biometrici, ponendo particolare attenzione alla loro conservazione. Una volta ottenuto il campione biometrico, acquisito attraverso una sequenza di fasi di elaborazione a partire dal rilevamento di una determinata caratteristica biometrica, biologica o comportamentale, esso viene memorizzato all'interno di banche dati centralizzate per determinare l'identità dell'interessato. I dati biometrici sono, quindi, nella disponibilità del titolare del trattamento e conservati anche in forma di *Hardware Security Module* (HSM)[56], nelle postazioni di lavoro informatiche oppure sugli stessi dispositivi di acquisizione biometrica. Ma è possibile memorizzare il dato biometrico anche in dispositivi affidati alla esclusiva disponibilità dell'interessato, come nel caso dei *token* e delle *smart card*[57].

Alla luce della normativa vigente, europea ed italiana, in materia di protezione dei dati personali, il trattamento dei dati biometrici è lecito ai sensi del combinato disposto dell'art. 2-*septies*, co. 1, del Codice *privacy* e art. 9, par. 1, lett. *g)* del Regolamento, se necessario per motivi di interesse pubblico rilevante, nei quali rientra anche l'esame di una domanda di asilo presentata in uno degli stati membri dell'Unione europea e il contrasto all'immigrazione irregolare[58].

[56] *Hardware Security Module* (HSM) è un dispositivo fisico di elaborazione atto a generare, proteggere, conservare, gestire e revocare chiavi digitali per l'autenticazione forte.

[57] Linee-guida in materia di riconoscimento biometrico e firma grafometrica, Allegato A al Provvedimento del Garante del 12 novembre 2014, in www.gpdp.it doc web n. 3563006

[58] Il riferimento è alla Convenzione di Dublino, che ha lo scopo di facilitare l'azione degli Stati membri davanti alle difficoltà nell'individuare gli stranieri che avessero già presentato una domanda di asilo in un altro Stato membro.

Al fine di perseguire le violazioni penali, così come indicato nel Trattato di Prüm[59], i Pesi contraenti, si impegnano a creare e a gestire degli schedari nazionali[60]. In particolare, per agevolare lo scambio di informazioni tra i Paesi europei, è stato istituito il sistema Eurodac con il Regolamento n. 2725/2000/CE[61]. Eurodac è il primo database europeo biometrico, il cui scopo è quello di comparare le impronte dei richiedenti asilo e di coloro che attraversano irregolarmente le frontiere europee[62].

Diverso è invece il casellario centrale d'identità del Ministero dell'Interno, Dipartimento della pubblica sicurezza[63], il quale raccoglie nella sua banca dati i cartellini fotosegnaletici redatti dalle forze dell'ordine[64], avvalendosi del Sistema automatizzato di riconoscimento delle impronte digitali e palmari A.P.F.I.S. (*Automated Palmprint and Fingerprint Identification System*).

Tale sistema permette di memorizzare le fotografie, le immagini delle impronte e i dati anagrafici e biometrici delle persone sottoposte a rilievi solo nei casi consentiti dalla legge ed in particolare nell'ambito di prevenzione dei reati o di accertamenti effettuati nello svolgimento dei compiti di polizia giudiziaria[65].

Il regolamento di istituzione dell'Eurodac, con la raccolta dei dati biometrici, mira ad arginare il rischio che i richiedenti asilo possano formulare più domande in più Stati, riuscendo a stabilire quale sia lo Stato membro competente alla gestione della

[59] Il Trattato di Prüm, sottoscritto a Prüm, in Germania il 27 maggio 2005, da Belgio, Germania, Spagna, Francia, Lussemburgo, Paesi Bassi e Austria, ha ad oggetto «l'approfondimento della cooperazione transfrontaliera, in particolare al fine di lottare contro il terrorismo, la criminalità transfrontaliera e la migrazione illegale» ed è stato recepito dal Parlamento italiano con la legge 30 giugno 2009, n. 85.

[60] Il Trattato di Prüm prevede l'istituzione di schedari nazionali all'art. 2. Inoltre, per quanto riguarda i dati biometrici o dattiloscopici, l'art. 8 e ss., definiscono le corrette modalità di consultazione e gestione degli stessi dati.

[61] Regolamento (CE) n. 2725/2000 del Consiglio dell'11 dicembre 2000, che istituisce l'«Eurodac» per il confronto delle impronte digitali per l'efficace applicazione della convenzione di Dublino.

[62] V. FERRARIS, *Eurodac e i limiti della legge: quando il diritto alla protezione dei dati personali non esiste*, in *Diritto, Immigrazione e Cittadinanza*, 2017, 1 s.

[63] Il suddetto casellario è collocato presso la Direzione centrale anticrimine della Polizia di Stato ed è un Servizio di polizia scientifica.

[64] Si intende la polizia di Stato, l'Arma dei Carabinieri, Guardia di finanza e canali di cooperazione internazionale, quindi polizie straniere.

[65] C. LAUDO, F. RESTA, *Il trattamento dei dati personali per esigenze di giustizia, pubblica sicurezza e difesa e sicurezza dello Stato*, in G. BUSIA, L. LIGUORI, O. POLLICINO (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Canterano, 554.

domanda di asilo ricevuta. Eurodac è composto da una banca dati centrale informatizzata («Sistema centrale») e di una infrastruttura di comunicazione tra il Sistema centrale e gli Stati membri, dotata di una rete virtuale cifrata dedicata ai dati Eurodac. Ciascuno Stato membro, invia i dati al Sistema centrale che in tempo reale effettua il controllo relativo alla presenza o meno delle impronte inserite nel Sistema, attraverso un punto di accesso (il *focal point* nazionale). Se le impronte sono presenti, è indicata la classificazione e quando e dove le impronte della persona sono state già rilevate. Il *focal point* nazionale in Italia è il Servizio di polizia scientifica a Roma e l'autorità responsabile per Eurodac è la Direzione centrale anticrimine. Il sistema informativo è stato notevolmente modificato nel 2013, in linea con il Regolamento UE n. 603/2013[66], che oltre a specificare quali sono le tipologie di dati che possono essere raccolte, cercando di limitare l'impatto sulla vita degli individui e nel rispetto del principio di proporzionalità, così come specificato dal Garante europeo per la protezione dei dati personali[67], prevede una disposizione specifica per l'esercizio dei diritti dell'interessato.

In particolare, l'art. 29 del Reg. UE n. 603/2013 stabilisce che la persona debba essere informata «per iscritto, e dove necessario oralmente in una lingua che la persona comprende o che ragionevolmente si suppone a lei comprensibile» di quanto segue:

a) dell'identità del responsabile del trattamento;

[66] Regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013 , che istituisce l' «Eurodac» per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, e che modifica il regolamento (UE) n. 1077/2011 che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia.

[67] European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of "EURODAC" for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] [.....] (Recast version)*, 5.9.2012, disponibile al link https://edps.europa.eu/sites/edp/files/publication/12-09-05_eurodac_en.pdf.

b) dello scopo per cui i suoi dati saranno conservati in Eurodac, compresa una descrizione delle finalità del regolamento n. 604/2013[68] (cd. Dublino III) conformemente al diritto all'informazione disciplinato nell'articolo 4, nonché una spiegazione, in forma accessibile e con un linguaggio semplice e chiaro della possibilità di accesso delle autorità di polizia degli Stati membri e di Europol;

c) dei destinatari dei dati;

d) dell'esistenza di un obbligo di rilevamento delle impronte digitali per le persone che ricadono nelle Categorie 1 e 2[69];

e) del diritto di accesso ai dati che la riguardano e del diritto di chiedere che i dati inesatti che la riguardano siano rettificati o che i dati che la riguardano trattati illecitamente siano cancellati, nonché del diritto di ottenere informazioni sulle procedure da seguire per esercitare tali diritti, compresi gli estremi del responsabile del trattamento e delle autorità nazionali di controllo di cui all'art. 30, par. 1[70].

Il diritto per la protezione dei dati personali, e nei casi esaminati dei dati particolari o sensibili, non può prescindere dall'evoluzione scientifica e tecnologica, perciò, così come indicato nell'art. 2-*septies* del Codice *privacy*, l'Autorità garante deve adottare con cadenza almeno biennale un provvedimento che tenga conto di ciò. Inoltre, è facile notare che tutti i pareri emessi dalle Autorità garante, sia europea che nazionale, utilizzano come parametro il principio di proporzionalità.

In virtù dei casi esaminati, il legislatore per disegnare al meglio il quadro normativo di riferimento, dovrà necessariamente tener conto dei principi del Regolamento e del Codice in materia di protezione dei dati personali, in combinato

---

[68] Regolamento (UE) n. 604/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide.

[69] Secondo le disposizioni del Regolamento 603/2013, rientrano nella "categoria 1" i richiedenti protezione internazionali maggiori di anni 14 (art. 9), mentre, sono identificate nel Sistema Eurodac, come "categoria 2" le persone provenienti da Paesi terzi o gli apolidi di età non inferiore a 14 anni, che siano fermati dalle competenti autorità di controllo in relazione all'attraversamento irregolare via terra, mare o aria della propria frontiera in provenienza da un Paese terzo e che non siano stati respinti (art. 14).

[70] La previsione dell'art. 29 del Reg. UE 603/2013, sembra essere parte integrante della normativa in materia di protezione dei dati personali. Agli individui interessati, sono infatti riconosciuti gli stessi diritti previsti dal Regolamento UE 2016/679.

disposto con le previsioni dello Statuto dei Lavoratori[71] e soprattutto delle disposizioni costituzionali riguardanti la libertà degli individui. Il bilanciamento tra i diritti fondamentali diventa, anche in questo caso, essenziale.

[71] Il riferimento è all'art. 4 della Legge del 20 maggio 1970, n. 300, il quale prevede la possibilità di utilizzare strumenti che potenzialmente possono controllare i lavoratori solamente per motivi di sicurezza e tutela del patrimonio aziendale e che esplicitamente vieta l'utilizzo di strumenti invasivi per la rilevazione delle presenze.