progetto virtuoso, un nuovo assetto governamentale in termini di bilanciamento *bíos*/*mètron*.

6. Biometria e privacy

In materia di *privacy*, la ricerca in campo biometrico, biotecnologico, biostatistico e genetico offre un interessante *corpus* teorico-giuridico di riferimento su cui è necessario muoversi con cautela, in particolare quando le acquisizioni teoriche sono utilizzate a supporto di applicazioni in ambito biopolitico e biomedico, oppure come metodologie applicate che riguardano aspetti connessi al fenomeno della criminalità e del terrorismo. Una cautela che porta ad assumere un'assetto trans-generazionale e trans-nazionale, perdendo in questo mutamento il carattere della transitorietà della norma[157]

> «dovuto allo iato riscontrabile fra l'evoluzione della scienza, che procede secondo ritmi ormai convulsi e disciplina normativa, che deve invece rispettare i tempi procedurali, e recuperando la sua funzione precipua di strumento per la coesistenza»[158].

A distanza di oltre un secolo dalla teorizzazione del diritto alla *privacy*, l'evoluzione concettuale ha condotto sostanzialmente a due tendenze, da un lato, il passaggio "dalla *privacy* alla non discriminazione", dall'altro, il "passaggio dalla segretezza al controllo"[159].
Questo accrescimento in ordine alla spazialità e alla profondità è l'esito di un nuovo contesto sociale (digitale e globale), dove aumentano i rischi di trasferimento e divulgazione illecita o abusiva dei dati personali con una gravità potenzialmente maggiore qualora vengano trattati dati sensibili contenenti informazioni personali di carattere strutturale e permanente, come quelle genetiche e biometriche.
Nella cultura europea e nell'ambito della legislazione comunitaria, i dati biometrici sono considerati come «informazione concernente una persona fisica» poiché sono dati che, per la loro stessa natura, forniscono informazioni univoche su una determinata persona; in altri termini, nell'ambito dell'identificazione biometrica la persona è generalmente sempre riconoscibile da tutte le altre[160].
Sul piano formale, l'importanza di distinguere il trattamento dei dati biometrici dalla categoria più ampia dei dati personali è rilevata per la prima volta nel 2003 con l'attività del Gruppo di lavoro che ha coinvolto le Autorità Garanti dei paesi membri[161] e che ha portato all'elaborazione di un documento sui rischi derivanti dal ricorso, generalizzato e incontrollato, della biometria per il riconoscimento e l'identità delle persone e sul rischio che l'uso generalizzato dei dati biometrici

---

[157] A. Di Giandomenico, *La genetica e l'evoluzione del diritto*, in (Ed.), *Filosofia e politica dei diritti umani nel terzo millennio*, Milano, Giuffré, 2003, p. 515.
[158] *Ibidem.*
[159] S. Rodotà, *Tecnologie e diritti*, Bologna, Il Mulino, 1995, p. 108.
[160] L'identificabilità della persona dipende anche dalla disponibilità di altri dati i quali, insieme o separatamente, consentono l'identificazione del soggetto interessato. La possibilità di un'identificazione diretta mediante "uno o più elementi specifici caratteristici della sua identità fisica" è citata espressamente nella definizione di dati personali di cui all'art. 2, lett. a) della Dir. 95/46/CE.
[161] Sul punto cfr. il *Documento di lavoro sulla biometria*, Gruppo di lavoro per la tutela dei dati personali presieduto da S. Rodotà e istituito a norma dell'art. 29 della Direttiva 95/46/CE, Bruxelles, 13 giugno 2003.

renda la collettività insensibile agli effetti che questo processo può avere sulla vita quotidiana.
Nel documento emerge, tra gli altri, uno dei princìpi cardine della Direttiva sulla *privacy*, in particolare «l'impiego di sistemi biometrici non è lecito se non è proporzionato agli scopi che si vogliono raggiungere, in particolare nei casi in cui si propone di creare archivi centralizzati», e che «tali informazioni sono particolarmente delicate e il loro uso, se da un lato può contribuire a salvaguardare la *privacy* riducendo il ricorso ad altri dati personali, dall'altro può comportare rischi legati all'utilizzazione indebita o indiscriminata di informazioni desunte da tracce fisiche (es. impronta digitale, dell'iride ecc.) che una persona può lasciare anche senza rendersene conto»[162].
L'impiego della biometria richiede, infatti, il rispetto del principio di proporzionalità di ogni categoria di dati trattati con la finalità del rispettivo trattamento e i dati biometrici possono essere utilizzati solo se adeguati, pertinenti e non eccessivi. Si richiede, dunque, una valutazione accurata della necessità e della proporzionalità dei dati trattati. I dati biometrici, inoltre, contengono generalmente più informazioni di quante siano necessarie per l'identificazione, l'autenticazione e la verifica.
La Direttiva vieta l'ulteriore trattamento dei dati se incompatibile con la finalità per la quale i dati sono stati raccolti e prevede deroghe al divieto di trattare ulteriormente i dati per finalità ritenute incompatibili, solo quando si applicano condizioni specifiche espressamente previste e disciplinate dai singoli ordinamenti.
In linea generale è condivisa l'idea che il rischio di riutilizzo per finalità incompatibili di dati biometrici ottenuti da tracce fisiche lasciate da un individuo a sua insaputa (come ad esempio le impronte digitali) sia relativamente inferiore se i dati non sono memorizzati in basi di dati centralizzate, e quindi accessibili a terzi. L'archiviazione centralizzata dei dati biometrici aumenta il rischio che i dati siano utilizzati come chiave per collegare basi di dati distinte e ottenere profili dettagliati delle "abitudini" pubbliche e private della persona interessata.
Anche per il trattamento di questa tipologia di dati, dunque, così come per i dati genetici, occorre osservare i princìpi di liceità, finalità, proporzionalità.
Ogni tecnica biometrica utilizzata a scopo di autenticazione, di verifica o d'identificazione dipende, in misura maggiore o minore, dall'elemento biometrico considerato che in ogni caso deve essere: a) "universale", l'elemento biometrico è presente in tutte le persone; b) "unico", l'elemento biometrico deve essere distintivo per ogni persona; c) "permanente", ogni persona conserva il proprio elemento biometrico nel corso del tempo.
Sul piano socio-politico, oltre che legislativo, anche il Consiglio Europeo, preoccupato di dare un'impostazione omogenea e coerente al trattamento dei dati biometrici presenti nei documenti dei cittadini dei Paesi terzi (visti e permessi di soggiorno) e nei passaporti dei cittadini europei, presenta, nel 2004, una proposta di Regolamento sulle caratteristiche di sicurezza e sugli elementi biometrici presenti in questi documenti con l'obiettivo di stabilire un nesso sicuro, e giuridicamente vincolante, tra il titolare legittimo e il documento.

[162] *Ivi*, p. 2.

Nello stesso anno, il Parlamento Europeo adotta una Risoluzione legislativa, non vincolante, dal titolo "Norme sulle caratteristiche di sicurezza e sugli elementi biometrici nei passaporti dei Cittadini dell'Unione"[163], permettendo agli Stati membri di soddisfare le prescrizioni interne all'Unione Europea e quelle previste dal *Visa Waiver Program* [164] degli Stati Uniti, nel rispetto delle norme internazionali.
Ciò testimonia l'atteggiamento favorevole dei governi all'introduzione di passaporti biometricamente idonei ad assicurare certezza giuridica nella fase di identificazione della persona, ma con il divieto di istituire una banca dati centrale per la raccolta e la conservazione di dati biometrici. In effetti, la creazione di un database centralizzato violerebbe i principi di finalità e di proporzionalità contenuti nella Direttiva sulla *privacy* e aumenterebbe i rischi di eventuali abusi e incroci indebiti, oltre che accrescere i rischi riguardanti l'interconnessione di serie di dati attraverso l'utilizzo degli indicatori biometrici come "chiavi di accesso" ai database[165].
In Italia, la Costituzione detta limiti generali sull'acquisizione arbitraria d'informazioni riguardanti caratteristiche biometriche, prevedendo la libertà di tutela della propria salute e della propria integrità fisica e richiamando i limiti imposti dal rispetto della persona umana circa la costrizione a un determinato trattamento sanitario (articolo 32 Cost.), anche se in ambito processuale penale e in materia di tutela dell'ordine e della sicurezza pubblica, la facoltà di acquisire i dati biometrici dei cittadini è demandata all'autorità preposta anche se il concetto di acquisizione coattiva, ossia di dato acquisito contro la volontà dell'interessato, richiede delle distinzioni che portano a scindere le caratteristiche biometriche strettamente connesse alla sfera personale, intima e interiore del soggetto interessato (impronta digitale, riconoscimento dell'iride o della retina dell'occhio, ecc.) dalle caratteristiche biometriche che riguardano la parte "esteriore" della sfera personale del soggetto (riconoscimento dell'immagine del volto, dell'andatura, ecc.)[166].
Nella prima ipotesi, in considerazione dell'elevata invasività connessa all'acquisizione delle caratteristiche biometriche, è richiesta maggiore collaborazione da parte dell'interessato rispetto alla seconda ipotesi.
In linea generale non sono consentiti atti di acquisizione coattiva di impronte digitali e prelievi coattivi di campioni di sangue per effettuare accertamenti sull'identità del soggetto, individuare il gruppo sanguigno, il fattore Rh o il DNA, se non per giustificate necessità di cura e nei casi espressamente previsti dalle norme a tutela della salute.
Il legislatore italiano, in linea con l'orientamento comunitario, disciplina puntualmente questa particolare tipologia di informazioni personali, vincolando il trattamento all'obbligo di notifica presso l'Autorità Garante, come nel caso specifico dei «dati genetici, biometrici o dati che indicano la posizione geografica

[163] In argomento si veda la Risoluzione del Parlamento europeo. COM (2004) 0116; C5-0101/2004; 2004/0039 CNS.
[164] Si tratta del Programma di esenzione dall'obbligo del visto. È un programma del Governo degli Stati Uniti che permette ai cittadini di un paese di recarsi negli Stati Uniti, per turismo o affari, per un periodo di 90 giorni senza un visto.
[165] Secondo i contenuti della Relazione della Commissione per le libertà civili, la giustizia e gli affari interni presentata il 25/10/2004.
[166] Cfr. *Linee guida per l'impiego delle tecnologie biometriche nelle Pubbliche Amministrazioni* in «I Quaderni», CNIPA, n. 9/2004, p. 10.

di persone mediante una rete di comunicazione elettronica»[167], è ciò avviene a partire da 2003, con l'emanazione *Codice in materia di protezione dei dati personali*, fino all'emanazione del Decreto Legge n. 139 del 2021, Nuove modifiche al Codice privacy, in linea con il *General Data Protection Regulation* (GDPR, Regolamento europeo 2016/679).
L'impianto normativo italiano rappresenta, oggi, un complesso e sistematico sistema di tutela in materia di privacy e prescrive una disciplina particolarmente rigorosa che ha inizio con la definizione di dati sensibili e che prosegue con l'individuazione di regole che riguardano i soggetti pubblici, i privati e gli enti pubblici economici, lo stato civile, l'anagrafe, le liste elettorali, l'istruzione e il trattamento dei dati per scopi statistici o scientifici[168].
Riguardo alla disciplina dei trattamenti da parte di forze di polizia, i trattamenti biometrici sono inquadrati fra quelli che implicano maggiori rischi di danno all'interessato e che di conseguenza devono essere effettuati nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti dall'Autorità Garante, sulla base di una verifica preliminare e di preventiva comunicazione (si pensi ai dati in grado di rivelare l'appartenenza del soggetto a determinati gruppi razziali, le patologie a carico del soggetto, le caratteristiche fisiologiche di un determinato individuo).
Per ciò che attiene, invece, al trattamento delle informazioni di natura genetica, in Italia, l'Autorità Garante per il trattamento dei dati personali ha definito le regole per il trattamento dei dati genetici orientate al divieto di raccolta e utilizzazione di tali dati in particolare in tutti i rapporti di lavoro e nel settore assicurativo, se non in casi del tutto eccezionali specificamente previsti dalla legge, anche se la continua creazione di grandi banche dati contenenti informazioni genetiche espongono al rischio di utilizzazioni improprie, alla conservazione per periodi eccessivi, all'accesso abusivo.
Il primo lavoro, rilevante sul piano formale, che si occupa di dati genetici e biometrici risale al 2004 ed è un Documento di lavoro approvato dalle Autorità Garanti per la protezione dei dati dei Paesi dell'Unione Europea. Con questo documento si è inteso procedere a un approccio comune riguardo ai punti fondamentali e ai princìpi contenuti nella Direttiva 95/46/CE[169], oltre che una visione unitaria, condivisa e attiva circa le problematiche connesse all'impiego dei dati genetici all'interno di ciascun Paese, al fine di garantire il rispetto di eguaglianza e non discriminazione, nonché il diritto alla salute previsti e sanciti dalle più importanti fonti internazionali.
Il Documento di lavoro in materia di dati genetici concentra la sua analisi su alcuni punti fondamentali tra cui la definizione di dato genetico e delle relative conseguenze sul piano giuridico. Riguardo a questo primo punto, il Documento delle Autorità garanti definisce i dati genetici come una particolare categoria dei dati sensibili appartenente alla macro area dei dati personali e come tali soggetti all'applicazione della Direttiva europea sulla *privacy* ed al conseguente rispetto di

[167] Art. 37, comma 1, lett. a) del D.Lgs. n. 196/2003.
[168] Cfr. G. Rasi, *Il punto di vista dell'Autorità Garante per la tutela dei dati personali*, in VI Convegno «La Biometria entra nell'e-government», CNIPA, Roma 23 novembre 2004.
[169] 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*. Pubblicata in G.U. delle Comunità europee N. L 281/31 del 23 novembre 1995.

determinati princìpi generali[170], tra cui emergono il "principio di pertinenza e non eccedenza", al fine di evitare il ricorso al trattamento dei dati genetici se non strettamente necessario; il "principio di proporzionalità", il cui obiettivo riguarda la valutazione dei rischi connessi alle libertà fondamentali e ai diritti nel momento in cui tali dati vengono trattati; il "principio di finalità", al fine di evitare l'utilizzo dei dati genetici in maniera non consona alle finalità per cui sono raccolti; il "diritto di accesso" a tali dati da parte degli interessati; il "diritto all'informazione" degli interessati sui dati genetici che li riguardano.
Il Documento pone in rilievo un altro aspetto fondamentale legato ai dati genetici, ossia la possibilità di poter caratterizzare anche un "gruppo biologico"[171] portatore d'interessi giuridici rilevanti, fissando i criteri per l'utilizzazione del dato genetico e che sono stabiliti partendo dall'individuazione di particolari ambiti sociali.
Nell'alveo della ricerca medico-scientifica, riconosciuti e considerati gli sviluppi degli studi sul genoma umano, i Garanti mettono in rilievo i rischi connessi alla creazione di grandi banche di dati contenenti informazioni genetiche, cercando di porre divieti sull'utilizzazione impropria dei dati genetici, richiamando il principio di finalità al fine di evitare la conservazione per periodi eccessivi e il principio di pertinenza e non eccedenza per evitare la mancata adozione di idonee misure di sicurezza nella conservazione dei dati genetici[172].
In particolare, nell'ambito sanitario, i test genetici, diagnostici o predittivi possono essere compiuti soltanto con il consenso espresso, libero (in assenza di vincoli coercitivi a carico dell'interessato, come previsto dalla Direttiva) e informato.
Nel contesto lavorativo, il trattamento dei dati genetici è vietato in linea generale e di principio ed è previsto solo in casi eccezionali secondo specifiche norme di legge[173].
Nel settore assicurativo e previdenziale, il trattamento dei dati genetici è vietato in linea generale e di principio ed è previsto solo in casi eccezionali secondo specifiche norme di legge, considerato, anche in questo settore, l'elevato rischio di discriminazione.
Nell'ambito della sicurezza pubblica, del controllo e dell'accesso ad aree riservate, l'utilizzo dei dati genetici è finalizzato alle operazioni di identificazione per l'accertamento della paternità del soggetto interessato, o di un gruppo determinato di soggetti, previa somministrazione di un test genetico soggetto all'obbligo del consenso da parte degli interessati. Tuttavia, il sistematico ricorso a operazioni che rendono anonimi i dati genetici per ogni singolo trattamento può offrire, in molti casi, una risposta equilibrata al problema.
Oggi, è consentito utilizzare i dati genetici soltanto per finalità orientate alla tutela della salute dell'interessato e dei terzi appartenenti alla sua stessa linea genetica; per finalità di ricerca scientifica e statistica volta alla tutela della salute; per investigazioni difensive e difesa in sede giudiziaria, nonché per specifici

[170] Cfr. Autorità Garante per il trattamento dei dati personali, Documento *Newsletter n. 206/15-21 marzo 2004 - Dati genetici: prime linee guida dai Garanti europei.*
[171] Gruppo di soggetti legati da vincoli di consanguineità con l'interessato del trattamento. In tal senso si afferma che i dati genetici non appartengono solo all'interessato, essendo per loro stessa natura patrimonio comune dei consanguinei.
[172] Cfr. il *Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici*.
[173] In tal senso si è precedentemente espresso il *Gruppo Europeo per l'etica nelle scienze e nelle nuove tecnologie*, con il *Parere n. 18/2003*, mettendo in rilievo i rischi di discriminazione occupazionale legati all'impiego di test genetici di incerto valore predittivo.

adempimenti specifici previsti dalla normativa in materia di previdenza e di assistenza o di igiene e sicurezza sul lavoro o della popolazione.
Vi sono altri casi eccezionali in cui si può procedere al trattamento dei dati genetici, qualora non siano disponibili procedure alternative, come ad esempio i casi in cui i cittadini di Stati non appartenenti all'Unione europea, apolidi e rifugiati, si trovino [174] nell'impossibilità di fornire documenti ufficiali atti a provare i vincoli di consanguineità richiesti dalla Legge per ottenere il ricongiungimento con i propri familiari.
Inoltre, il trattamento dei dati genetici è di regola consentito solo dopo aver acquisito il consenso scritto dell'interessato e dopo averlo informato sugli specifici scopi perseguiti, sul diritto di opporsi al trattamento, sui risultati che s'intendono conseguire e sul periodo di conservazione dei dati e dei campioni biologici. Il consenso è sempre revocabile.
Sono richieste specifiche garanzie per l'esecuzione di *test*, *screening* genetici, ecc., come nel caso dei *test* di consanguineità [175], in questi ultimi casi sono previste particolari procedure sui contenuti dell'informativa [176], la necessità di fornire all'interessato un'adeguata consulenza genetica, il diritto di non conoscere i risultati dell'esame, le modalità di manifestazione del consenso e il periodo di conservazione dei dati e dei campioni biologici.
Non sono autorizzate indagini genetiche di paternità e di maternità condotte su minori all'insaputa di uno dei due genitori; per tali indagini l'autorizzazione richiede, quale presupposto di liceità, il consenso di ambedue i genitori.
Le ricerche compiute mediante l'utilizzo di dati genetici devono essere effettuate secondo le metodologie certificate per il trattamento.
Gli studi genetici condotti su popolazioni isolate devono essere preceduti da una formale attività di informazione volta ad illustrare alle comunità interessate le caratteristiche fondamentali della ricerca, gli eventuali rischi di discriminazione o stigmatizzazione che possono derivarne, nonché le azioni intraprese per ridurli al minimo[177].

7. Habeas data

Le questioni connesse all'autodeterminazione, all'identità biometrica, alla sicurezza pubblica e individuale assumono contorni altamente complessi quando interagiscono con le potenzialità dei servizi digitali, poiché è a questo livello che manifestano la complessità delle molteplici interconnessioni che possono derivare da scelte politiche e sociali[178].
I vantaggi di una maggiore partecipazione ai processi e alle interazioni sociali trovano, infatti, un limite nel rischio di pericolose invasioni della vita privata e persino della sfera intima, investendo non soltanto il corpo biologico (o corpo fisico) con le relative libertà (*habeas corpus*), ma anche il corpo digitale, nelle sue

[174] In ragione del loro *status*, della mancanza di un'autorità riconosciuta o della presunta inaffidabilità dei documenti rilasciati dall'autorità locale.
[175] È il caso dei *test* di paternità e/o maternità o cosiddetto *test* di consanguineità.
[176] È il caso del trattamento sugli *screening* genetici, rispetto ai quali va garantita l'informazione pubblica.
[177] Cfr. la *Relazione annuale sull'attività svolta dal Garante della privacy*, parte II, del 12 luglio 2007. Doc. n. 1423308.
[178] Cfr. J. Van Dijk, *Sociologia dei nuovi media*, trad. it., Bologna, Il Mulino, 2002.