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.

svariate e inedite forme/rappresentazioni mediali (*habeas data*), che sempre più spesso si traducono in lesioni dei diritti e delle libertà fondamentali, con spazi per la discriminazione, la stigmatizzazione e la sopraffazione[179].
Nel mondo digitale (cyberspazio), vita privata, riservatezza e oblìo assumono una dimensione ampliata e dilatata, in cui la stessa funzione regolatrice del diritto è costretta a superare schemi predefiniti di tutela. Le informazioni private di ogni singolo individuo circolano quotidianamente in molteplici attività. Si pensi alla corrispondenza elettronica, ai pagamenti con carte di credito e di debito, agli accessi in *internet*, alle telefonate, solo per citare alcuni esempi; si tratta di azioni di *routine*, che tuttavia lasciano un'impronta digitale indelebile nelle banche dati e offrono un profilo permanente dei rapporti, degli spostamenti, delle scelte, dei gusti, delle preferenze, ma forniscono anche una traccia digitale di informazioni estremamente "sensibili" come quelle genetiche e biometriche[180].
Sul piano giuridico, si osserva che all'evoluzione tecnologica delle fattispecie distopiche, come ad esempio quelle criminose o terroristiche, debba corrispondere la definizione di nuovi livelli di tutela della persona.
I diritti che ridefiniscono l'integrità stessa della persona, comportano, pertanto, una riflessione finalizzata alla rivisitazione della distinzione tra diritto di *habeas corpus* delle Costituzioni più antiche e diritto di *habeas data* su cui si fondano le Costituzioni più giovani[181]. In questa direzione si colloca la valutazione in ambito politico dell'esistenza o meno di una corrispondenza delle regole costituzionali vigenti alle fattispecie giuridiche che emergono nell'era digitale. In altri termini, il problema che il legislatore deve affrontare è la dilatazione del concetto di libertà personale, intesa come "autonomia e disponibilità della propria persona" in virtù del fatto che la tutela del corpo fisico è, oggi, anche tutela delle informazioni personali che lo riguardano.
In Italia, così come in molti altri stati dell'Unione europea, i diritti della sfera individuale assumono valenza costituzionale con una "tecnica a spirale", che inizia con l'*habeas corpus* (art. 13 Cost., sulla libertà della persona fisica), ossia con la garanzia della persona e dei beni fisicamente connessi ad essa, estendendosi in maniera ricorsiva all'ambito spaziale immediatamente circostante. Ciò crea una continuità nella tutela della sfera individuale che porta la libertà personale a saldarsi con altri diritti sanciti dalla Costituzione[182], in tal modo, se da un lato si rafforza e si completa la garanzia complessiva dei diritti individuali dall'altro si assiste ad una variazione della tutela che tende a dilatarsi all'aumento della distanza dal punto di origine.
Ciò ha portato l'Autorità Garante per la privacy a richiedere interventi specifici per un rapido passaggio alla garanzia costituzionale di *habeas data*, in funzione della quale le persone hanno il diritto di pretendere che l'immagine che gli altri hanno di esse corrisponda all'esatta realtà[183].

---

[179] Cfr. S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, Laterza, 2004.
[180] G. Preite, *Cyberspazio e forme di autodeterminazione delle relazioni sociali. Un'analisi teorica*, in «Cosmopolis – Rivista di Filosofia e Teoria Politica», vol. XIV, n. 1-2/2017.
[181] La garanzia costituzionale di *habeas data* è presente nelle Carte costituzionali del Paesi africani, degli ex "Paesi satellite" dell'Europa dell'est e in particolare dell'America latina, che si caratterizzano per le più rilevanti novità in tema di garanzie costituzionali.
[182] R. Bin, G. Pitruzzella, *Diritto Costituzionale*, Torino, Giappichelli, 2001, p. 484.
[183] E.R. Acuña, *Habeas data costituzionale: nuova garanzia giurisdizionale del diritto pubblico latinoamericano* in «Diritto Pubblico comparato ed Europeo», n. 4/2002, p. 1928.

Per il Garante, la tutela dei dati è un diritto fondamentale della persona, un elemento essenziale della nuova cittadinanza, come si evince dall'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea. Non vi è dubbio che il valore della *privacy* debba essere opportunamente controbilanciato con quello della sicurezza, ma è importante che le ragioni della sicurezza non prevalgano incondizionatamente sui diritti fondamentali. I Paesi europei (così evoluti in molti ambiti del sapere giuridico) hanno dunque Carte costituzionali arretrate, in cui non sono riconosciuti molti diritti ormai comuni nell'animo sociale, a differenza di alcuni Paesi extraeuropei li hanno costituzionalizzati.
Nell'era digitale il principio di autodeterminazione – informativa, informatica e, nel nostro caso, biometrica – subisce una mutazione socio-culturale trasformandosi da tensione di "affermazione" a sforzo di "negazione" della esclusività altrui[184]. Diviene cioè una manifestazione del tentativo infruttuoso di preservare ciò che di più caro rimane: il feticcio di una libera volontà. Non potendo "affermare se stesso"[185], il soggetto non può fare altro che "limitare" gli influssi esterni, non eliminandoli, ma riducendone la portata e la consistenza a un livello accettabile. A titolo esemplificativo, si pensi all'accesso ai servizi in rete, dove l'identificazione non è associata a dati anagrafici, ma a *username* e *password*, cioè a credenziali che consentono di soddisfare le richieste dell'individuo (in questo caso, utente), ma anche di creare archivi di memoria e dati e persino pacchetti statistici che beneficiano di un mercato per le transazioni.
A livello di *habeas data*, il concetto di identità e di riconoscimento, anche biometrico, porta con sé rinnovate esigenze di sicurezza per prevenire il furto dell'identità digitale, la sua compromissione e il suo abuso[186], tenuto conto che la sovrapposizione della vita sociale in rete a quella reale, diviene terreno fertile per lo sviluppo di crimini informatici e azioni di terrorismo digitale.
La disamina degli attacchi che hanno come obiettivo di fondo il furto dell'identità digitale, rileva una serie di fenomeni che riguardano in maniera diretta l'identità della persona nel suo rapporto con la rete, tra i più interessanti emerge l'appartenenza e la partecipazione ai *social network*, cioè reti sociali organizzate come comunità virtuali che connettono fra loro persone sulla base di legami tra i più svariati, quali vincoli di amicizia, parentela, lavoro e interessi di ogni tipo e che, attraverso la costruzione di un profilo digitale, si caratterizzano per la condivisione di informazioni private, spesso personali e intime. Quando una persona decide di partecipare allo spazio sociale in rete, si spoglia della sua fisicità e utilizza la sua identità digitale, spesso modellata sulla base delle informazioni che di sé ha scelto di mettere in gioco: viene così sciolto, o fortemente allentato, il vincolo tra nome, corpo e identità[187].
La questione più controversa e delicata è rappresentata dal fatto che, nella maggior parte dei casi, le informazioni personali pubblicate attraverso la partecipazione a *social network* sono frutto dell'iniziativa degli stessi utenti, ovvero trovano il loro consenso e la conseguente autorizzazione al trattamento dei dati immessi[188]. Una questione, quest'ultima, che è stata sollevata dal Gruppo di

[184] V. Frosini, *Contributi ad un diritto dell'informazione*, Napoli, Liguori Editore, 1991, p. 115.
[185] Ibidem.
[186] Cfr. A. Crescentini, *Elogio della sicurezza: aspetti multidisciplinari tra scienza e pratica*, Milano, Vita e Pensiero, 2007.
[187] S. Rodotà, *La vita e le regole: tra diritto e non diritto*, Milano, Feltrinelli, 2006, p. 76.
[188] Cfr. G. Preite, *Habeas data tra sicurezza e privacy: quale politica per i nuovi diritti?*, cit. p. 287-289.

lavoro internazionale sulla protezione dei dati nelle telecomunicazioni, che parla di una nuova generazione cresciuta con internet, che ha sviluppato approcci del tutto peculiari rispetto all'utilizzo dei servizi in rete e che, appartenendo di solito alla fascia adolescenziale, risulta maggiormente disposta a mettere a rischio la propria *privacy* rispetto alla fascia degli adulti, considerati "immigrati digitali"[189].

[189] In argomento cfr. il *Memorandum di Roma,* Rapporto e Linee-Guida in materia di *privacy* nei servizi di *social network*, adottato dal Gruppo di lavoro internazionale sulla protezione dei dati nelle comunicazioni, Roma, 3-4 marzo 2008.