UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Sede Amministrativa: Università degli studi di Padova
Dipartimento di Diritto comparato

SCUOLA DI DOTTORATO DI RICERCA IN: DIRITTO INTERNAZIONALE E DIRITTO PRIVATO E DEL LAVORO
INDIRIZZO: DIRITTO PRIVATO NELLA DIMENSIONE EUROPEA
CICLO XXII

I NUOVI SEGNI IDENTIFICATIVI DELLA PERSONA: PROBLEMI GIURIDICI DELLA BIOMETRIA

Direttore della Scuola: Ch.mo Prof. Paolo Zatti

Coordinatore d'indirizzo: Ch.mo Prof. Giorgio Cian

Supervisore: Ch.mo Prof. Paolo Zatti

Dottorando: Sabina Girotto

Al mio padre in spirito,
con gratitudine.

INDICE

CONSIDERAZIONI INTRODUTTIVE

SOMMARIO: 1. La biometria nel quadro della biopolitica. - 2. Il discorso giuridico intorno alla biometria: linee di ricerca.

1. La biometria nel quadro della biopolitica.

Scrive Francesco d'Agostino che il discorso intorno alla biometria va affrontato "con curiosità, con intelligenza aperta, e con saggia vigilanza"[1]. Il noto filosofo del diritto offre, in sostanza, a chi intende avvicinarsi a questo argomento, dei "suggerimenti metodologici" alquanto impegnativi. Eppure, l'approccio alla biometria sembra richiedere realmente questa capacità di combinare una curiosità vivace, essendo la riflessione su di essa, nelle diverse discipline che la avvicinano, ancora agli inizi; una intelligenza aperta, poiché la biometria appare come un mare che lambisce più terre; una saggia vigilanza, essendo una questione poliedrica e sfuggente per chi cerca di penetrarla.

Nelle indagini sociologiche e nel sentire comune questa scienza, che si basa sul riconoscimento dei soggetti a partire da elementi del loro stesso corpo, evoca l'immagine di un mondo su cui incombe una sorta di minaccia generalizzata, ingenerata in particolare dai tragici eventi dell'11 settembre 2001, dominato da un clima di sospetto, ove si impone l'esigenza di identificare le persone poiché, dietro ad ognuno, potrebbe nascondersi qualcuno di diverso e pericoloso: un potenziale terrorista, killer,

[1] Così F. D'AGOSTINO, *Individualità e biometria,* in *L'Arco di Giano*, n. 45, 2005, 7.

clandestino, ladro, imbroglione[2]. A ragione, pertanto, si è parlato di *guilty bodies*, di corpi colpevoli, poiché ogni corpo, e dunque ognuno, porta con sè il marchio di un sospetto di colpevolezza[3]. Tale fatto rappresenta un pericolo non solo per il singolo, minacciato nell'esercizio dei propri diritti e delle propria libertà fondamentali, ma altresì per la società nel suo insieme poiché, una volta che la comunità viene preventivamente liberata da un pericolo, e dunque *immunizzata*, essa si chiude al proprio interno, negandosi ogni possibilità di crescita e di sviluppo[4].

Tuttavia, si può osservare che il potenziamento delle misure di sorveglianza e sicurezza, a cui si è assistito recentemente, costituisce una evento affatto nuovo, piuttosto si tratta del punto culminante di un processo in atto da tempo[5].

Di tale processo, invero, si occupa la *biopolitica*, scienza che indaga il modo in cui la vita entra nella fitta rete del potere, e in cui il potere si prende carico della vita stessa, intesa nella sua dimensione biologica, ossia la *nuda vita*, il corpo umano[6]. È utile, a questo proposito, rivolgere l'attenzione al padre della biopolitica, Michel Foucault, secondo il quale "il corpo è anche direttamente immerso in un campo politico:

---

[2] Si vedano, *ex multis*, BEWLEY-TAYLOR D. R., *US concept wars, civil liberties and the technologies of fortification*, in 43 *Crime, Law & Social Change* (2005), 81-111; HOQUE S. M., *Government responses to terrorism: critical views of their impacts on people and public administration*, in 62 *Public Administration Review* (2002), 170-180; LYON D., *Technology vs. "Terrorism": circuits of city surveillance since September 11th*, in 27 *International Journal of Urban and Regional Research* (2003), 666-678.

[3] C. EPSTEIN, *Guilty Bodies, Productive Bodies, Destructive Bodies: Crossing the Biometric Borders*, in 1 *International Political Sociology* (2007), 149-164.

[4] Si veda R. ESPOSITO, *Bios. Biopolitica e filosofia*, Torino, Einaudi, 2004, 23. Quanto al concetto di *immunità*, scrive l'a. che è si tratta del "potere di conservazione della vita" (p. 41). L'immunizzazione è, cioè, una "protezione negativa della vita. Essa salva, assicura, conserva l'organismo, individuale o collettivo, cui inerisce – ma non in maniera diretta, immediata, frontale; sottoponendolo, al contrario, ad una condizione che contemporaneamente ne nega, o riduce, la potenza espansiva. Come la pratica medica della vaccinazione nei confronti del corpo individuale, anche l'immunizzazione del corpo politico funziona immettendo al suo interno un frammento della stessa sostanza patogena dalla quale vuole proteggerlo e che, dunque, ne blocca e contraddice lo sviluppo naturale" (p. 42).

[5] Così G. FROSIO, *Cosa resta della privacy? – diritto alla riservatezza dell'"uomo medio" dopo l'11 settembre*, in *Ciberspazio e diritto*, 2005, 223.

[6] La letteratura in tema di biopolitica è vasta, si veda, in particolare, R. ESPOSITO, *Bios. Biopolitica e filosofia*, cit., 23, che afferma: "Biopolitica non rimanda soltanto, o prevalentemente, al modo in cui da sempre la politica è presa –limitata, compressa, determinata- dalla vita, ma anche e soprattutto a quello in cui la vita è afferrata, sfidata, penetrata dalla politica".

i rapporti di potere operano su di lui una presa immediata, l'investono, lo marchiano, lo addestrano, lo suppliziano, lo costringono a certi lavori, l'obbligano a cerimonie, esigono da lui dei segni". L'assoggettamento del corpo al potere sovrano non rappresenta manifestamente un fatto nuovo e, se in passato poteva avvalersi soprattutto della violenza, si pensi solamente al potere di dare la morte, che peraltro non è ancora tramontato, oggi può realizzarsi attraverso una pluralità di mezzi: "esso può assai bene essere diretto, fisico, giocare della forza contro la forza, fissarsi su elementi materiali, e tuttavia non essere violento; può essere calcolato, organizzato, indirizzato tecnicamente, può essere sottile, non fare uso né di armi né del terrore, e tuttavia rimanere di ordine fisico"[7]. Il biopotere, inoltre, può agire tanto a livello del singolo corpo, che diviene un corpo-macchina, oggetto di strategie di controllo e sorveglianza, quanto a livello del corpo-specie, inteso nella sua appartenenza alla specie umana, base di processi biologici, quali la nascita, la morte, la riproduzione, la malattia, da controllare a livello globale[8].

Tra le possibili sottili forme di questo singolare governo sul *bios*, rientra precisamente l'uso delle tecnologie biometriche, impiegando il corpo umano come sorgente di informazioni di cui servirsi in una varietà di applicazioni. Si afferma, in questo modo, la pretesa del potere di sottrarre l'esistenza biologica umana dalla sua dimensione privata, per farle assumere un rilievo essenzialmente pubblico[9]. Infatti, i dati biometrici "sono usati per gli stessi scopi per cui sono impiegati i più convenzionali

[7] M. FOUCAULT, *Sorvegliare e punire. Nascita della prigionia*, Torino, Einaudi, 2005, 29.
[8] G. SADUN BORDONI, *Corpo e potere: biopolitica del totalitarismo*, in F. D'AGOSTINO (a cura di), *Corpo esibito, corpo violato, corpo venduto, corpo donato. Nuove forme di rilevanza giuridica del corpo umano*, Milano, Giuffrè, 2003, 122; G. BONACCHI, *Corpi di donna e scritture dell'uomo: spunti storici,* in *Democrazia e diritto*, 1996, 4.
[9] A questo proposito, si veda F. D'AGOSTINO, *Le prospettive della biopolitica*, Relazione tenuta il 20 ottobre 2007, presso il Centro Congressi dell'Università di Pisa, reperibile anche in *http://www.siti.chiesacattolica.it/siti/allegati/344/Relazione%20DAgostino.doc*, spec. p. 4.

modi di sorveglianza: per ordinare e classificare, per determinare la titolarità di diritti, per qualificare o squalificare, per includere e per escludere"[10].

Si potrebbe dire che nella biometria è pervasivo il modo in cui può realizzarsi il governo sulla vita, poiché il potere sul corpo passa attraverso il potere sull'informazione estratta dal corpo e, viceversa, il potere sull'informazione estratta dal corpo passa attraverso il potere sul corpo: sorvegliando il corpo si sorveglia l'informazione, e sorvegliando l'informazione si sorveglia il corpo stesso.

La biometria, dunque, provoca non solo un mutamento a livello sociale, ma altresì a livello antropologico, poiché l'uomo viene ridotto essenzialmente a fascio di informazioni.

In questo quadro, si intravede un rischio che non viene sufficientemente esaminato, così come dimostra la leggerezza con cui sovente vengono impiegati i sistemi biometrici, e la tacita disponibilità con cui gli utenti si lasciano da essi investigare. Ci si riferisce, precisamente, al pericolo di un appiattimento della coscienza individuale, per cui l'uomo moderno sembra non avere più nemmeno la percezione di essere utilizzato come un mezzo nelle mani di altri. È condivisibile dunque, quanto, a metà del secolo scorso, dichiarò un autorevole pensatore interrogandosi sul problema del potere e della sua gestione: "Con una disinvoltura sempre maggiore gli uomini sono trattati come oggetti, dalle innumerevoli forme di «conglobamento» statistico e amministrativo, sino alle inconcepibili violazioni dei singoli, dei gruppi e persino di interi popoli. E questo non solo nelle necessità e nei parossismi della guerra, ma come forma normale di governo e di amministrazione" [11].

---

[10] D. LYON, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano, Feltrinelli, 2001, 96.

[11] In altri termini, "il sentimento dell'uomo di avere un proprio essere e una propria sfera, quel sentimento che nel passato era la base di tutto il comportamento sociale, scompare sempre di più", R. GUARDINI, *La fine dell'epoca moderna. Il potere*, Brescia, Morcelliana, 2004, 62.

2. Il discorso giuridico intorno alla biometria: linee di ricerca.

Il discorso giuridico intorno alla biometria prende avvio da tali premesse che, *in nuce*, possono svelare già alcuni dei nodi problematici che il diritto è chiamato ad affrontare.

Si è accennato, anzitutto, alla carenza della riflessione sul tema che, pur assumendo una dimensione trasversale, tuttavia si rivela particolarmente acuta nell'ambito giuridico. In questo senso, non è agevole delineare, ad inizio della ricerca, uno *status questionis* poiché, al di là di qualche studio isolato, una indagine sistematica e approfondita sull'argomento e sulle sue ricadute giuridiche non è ancora stata svolta. Ciò nonostante, è opportuno soffermarsi brevemente sulle basilari fonti da cui può prendere avvio lo studio di questa tematica.

Anzitutto, come è in genere per ogni tecnologia emergente, la riflessione dottrinale più cospicua proviene dal mondo anglosassone.

Essenziale altresì il contributo dell'Unione europea, dove più enti si sono interessati ai problemi suscitati dal rapido diffondersi dei sistemi biometrici. Queste fonti per lo più non possono farsi rientrare nel diritto positivo, trattandosi principalmente di rapporti, raccomandazioni, linee guida. Esse, tuttavia, assumono valenza per il prestigio degli enti internazionali coinvolti, per l'apporto interdisciplinare di conoscenze fornito da una pluralità di esperti, e come base di partenza per una riflessione che coinvolga i singoli stati e governi, chiamati a dare risposte giuridiche di fronte al progresso tecnologico in corso.

A questo proposito si ricorda, anzitutto, il *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, relativo all'applicazione ai dati biometrici della Convenzione 108 del 1981 del Consiglio d'Europa sulla protezione degli individui riguardo al trattamento

automatizzato di dati personali[12]. Le biometrie sono state oggetto di particolare interesse, inoltre, da parte del *Joint Research Center*, organismo della Commissione europea che ha prodotto uno studio sul loro impatto etico e giuridico, dal titolo *Biometrics at the frontiers: assessing the impact on society*[13]. L'attività tuttavia più significativa nell'Unione a questo riguardo è stata svolta dal Gruppo per la tutela dei dati personali, istituito a norma dell'art. 29 della direttiva 95/46/CE. Si tratta dell'organo consultivo indipendente dell'Ue in tema di tutela dei dati e della vita privata, che ha elaborato un documento di riferimento nell'ambito in questione, il *Documento di lavoro sulla biometria*, stabilendo alcuni principi basilari per quanto riguarda la natura dei dati biometrici e definendone le modalità di trattamento[14].

---

[12] COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, in *http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/2Biometrics_2005_en.pdf*, February 2005. A questo proposito, si ricorda che la Convenzione 108 del 1981 - *Convention for the protection of individuals with regard to automatic processing of personal data*- dà attuazione all'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950, definendo principi per la tutela della vita privata della persone. Nel capitolo V della Convezione 108 è prevista l'istituzione di un Comitato Consultivo con il compito, tra gli altri, di dare opinioni sulla rilevanza della Convenzione circa aree specifiche. I principi enunciati, infatti, non danno risposte concrete su quali raccolte di dati siano permesse, ma si rende necessaria, di volta in volta, una "traslazione" di essi con riguardo alle concrete applicazioni. Pertanto, nel presente rapporto, che ha valore di guida e mira a "contribuire al dibattito circa la relazione tra i diritti umani e le biometrie", il Comitato intende studiare l'applicazione dei principi enunciati nella Convenzione 108 allo specifico caso del trattamento automatico dei dati biometrici sconosciuti all'epoca in cui essa fu stesa.

[13] EUROPEAN COMMISSION, *Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizen's Freedoms and Rights, Justice and Home Affaire (LIBE)*, rinvenibile in *http://ec.europa.eu/justice_home/doc_centre/freetravel/doc/biometrics_eur21585_en.pdf*, 2005. Il documento nasce da una iniziativa del LIBE (*Committee on Citizen's Freedoms and Rights, Justice and Home Affaire*) che nel giugno del 2004 fece richiesta al JRC (*Joint Research Center*) della Commissione di produrre uno studio sull'impatto futuro delle tecnologie biometriche.

[14] GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), Documento di lavoro sulla biometria, 1°agosto 2003, in *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp67_it.pdf*, 3. Il Documento di lavoro sulla biometria è stato adottato dal "Gruppo per la tutela dei dati personali (articolo 29)". Tale gruppo è stato istituito a norma dell'art. 29 della direttiva 95/46/CE. Si tratta dell'organo consultivo indipendente dell'UE in tema di tutela dei dati e della vita privata. I compiti del gruppo sono definiti dall'art. 30 della direttiva 95/46/CE e dell'art. 14 della direttiva 97/66/CE.

Uscendo dal contesto europeo, ma rimanendo nell'alveo sopranazionale, sono poi da menzionare il documento dell'OECD, *Biometrics-based technologies*[15], e l'attività svolta dall'ICAO relativamente all'elaborazione di documenti di viaggio[16].

Diversamente, la dottrina italiana sul punto è molto esigua, e si occupa per lo più dell'applicazione ai dati biometrici dei principi generali sul trattamento dei dati personali. Va segnalato il lavoro del Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA), che ha fornito in particolare delle *Linee guida per le tecnologie biometriche*[17]. Fondamentale è poi la copiosa attività del Garante per la protezione dei dati personali, che ha emanato, già a partire dal 2001, numerosi provvedimenti e pareri sul tema.

A partire dalle fonti suddette, sono individuabili due fondamentali linee di ricerca che, pur distinte, rappresentano un *continuum*: l'una considera l'impatto esercitato da tali nuove tecnologie sul corpo umano e sugli interessi riferibili alla corporeità; l'altra indaga il problema della natura e del trattamento dei dati biometrici. Prima di procedere lungo queste direttive, sarà indispensabile approfondire l'argomento anche dal punto di vista tecnico e terminologico.

Precisamente, in considerazione dell'impatto che le tecnologie biometriche esercitano sul corpo umano, prendendo le mosse dalla tradizionale configurazione

---

[15] OECD, WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometric-based technologies,* in *http://www.olis.oecd.org/olis/2003doc.nsf/LinkTo/NT000070D6/$FILE/JT00166988.PDF*, 30-Jun-2004.

[16] L'ICAO è un'agenzia specializzata dell'ONU, creata nel 1946. Essa promuove la salvaguardia e lo sviluppo dell'aviazione civile internazionale, definendo, a questo scopo, *standard* e norme, in particolare relativamente a passaporti e visti. L'ICAO ha promosso lo sviluppo dei c.d. MRTDs, *Machine Readable Travel Documents*, tra cui rientra anche il passaporto elettronico, *e-passport*, dotato di elementi biometrici. Si vedano in particolare ICAO, TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS (TAG-MRDT), Montréal, 23 March 2007, *Machine Readable Travel Documents (MRDTs): history, interoperability, and implementation,* in *http://www2.icao.int/en/MRTD/Downloads/Technical%20Report/ICAO_MRTD_History_of_Interoperability.pdf* e ICAO, *Biometric deployment of Machine Readable Travel Documents, ICAO TAG MRDT/NTWG, Technical Report,* in *http://www.policylaundering.org/archives/ICAO/Biometrics_Deployment_Version_2.0.pdf*, 21 May 2004.

[17] CNIPA, *Linee guida per le tecnologie biometriche,* in *www.cnipa.gov.it/site/_files/Linee%20guida%20tecnologie%20biometriche.pdf*, 8-10-2004.

giuridica di quest'ultimo, si intende effettuare una rilettura di alcuni fondamentali interessi riferibili alla corporeità, avendo di mira, come è stato autorevolmente affermato, una "ricostruzione dei singoli diritti fondamentali nel nuovo contesto sociale designato dalle tecnologie dell'informazione e della comunicazione"[18]. L'attenzione sarà rivolta soprattutto al diritto all'identità personale e al diritto all'integrità.

Si cercherà di capire, alla luce delle acquisizioni ottenute, se stiano emergendo nuove dimensione della corporeità, in altri termini, se il soggetto possa assumere anche una sussistenza virtuale, accanto a quella più propriamente biologica, ossia come flusso di dati o informazioni, al punto da rendere lecito parlare della nascita di un "nuovo corpo", il "corpo elettronico".

La possibilità che il corpo prenda tale ulteriore dimensione, apre l'indagine ad un principio, nuovo per la cultura giuridica europea, volto a garantire il *dominium* del soggetto sui propri dati. Si tratta dell'*habeas data*, il cui implicito riconoscimento si rinviene nell'art. 8 della *Carta dei diritti fondamentali dell'Unione europea*[19]. Tale Carta, che sancisce i diritti fondamentali del cittadino europeo, siglata a Nizza il 7 dicembre 2000, con la recente entrata in vigore del trattato di Lisbona il 1 dicembre 2009, ha assunto valore giuridico vincolante.

Invero, dal combinato disposto degli artt. 1 e 2 del Codice in materia di protezione dei dati personali, si può dedurre che il legislatore italiano stesso abbia inteso consacrare il nuovo diritto, laddove si dichiara che "ognuno ha diritto alla protezione dei dati personali che lo riguardano" (art. 1) e che il Codice "garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché

[18] S. RODOTÀ, *Tra diritti fondamentali ed elasticità normativa: il nuovo Codice sulla privacy*, in *Eur. e dir. priv.*, 2004, 4.
[19] Si deve essenzialmente a S. RODOTÀ la ripresa e l'enucleazione di tale principio all'interno della cultura giuridica italiana.

della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali" (art. 2).

Ci si propone, procedendo nella ricerca, di declinare nell'ambito della biometria le acquisizioni più generali ottenute nella prima parte del lavoro. Il capitolo terzo, in particolare, funge da cerniera tra i due fondamentali nuclei tematici della tesi. In esso, infatti, si intende approfondire il rapporto tra corpo e biometria, e tra identità e biometria, per giungere, infine, a delineare la relazione che intercorre tra informazione e biometria. Si inizierà ad indagare, pertanto, la natura giuridica del dato biometrico, per stabilire se sia possibile ascrivere l'informazione in questione all'ambito della disciplina sul trattamento dei dati personali.

La parte finale del lavoro sarà dedicata al problema del trattamento dei dati biometrici, con particolare attenzione ai principi generali sul trattamento dei dati personali e ai diritti dell'interessato.

Si prevede, per ultimo, di volgere l'attenzione alla dimensione europea, essendo le tecnologie biometriche impiegate in alcuni importanti ambiti dell'Unione. Accanto a ciò, sembra utile effettuare un raffronto con le esperienze di altre due nazioni, il Regno Unito e la Francia, ove il dibattito sul tema è particolarmente vivo, per comprendere quale approccio tali Stati abbiano adottato nei riguardi di questa scienza.

Lungo tutto il percorso, rimarrà aperto l'interrogativo se la soluzione giuridica offerta ai problemi posti dall'emergere delle tecnologie biometriche si possa considerare appropriata, se, in particolare, sia adeguato quell'approccio che colloca il problema quasi esclusivamente nell'ambito della disciplina sul trattamento dei dati personali, senza tener conto della specificità dell'informazione in questione, derivante dall'essere ricavata *dal* corpo e *sul* corpo.

CAPITOLO PRIMO

I TERMINI DELL'INDAGINE

SOMMARIO: 1. *Bio-metria*. Precisazioni terminologiche. - 2. Il processo biometrico: tra dato biometrico e *template*. – 3. (*Segue*) La fase del *matching*. - 4. Le tecnologie biometriche. Cenni. - 5. (*Segue*) Il DNA.

1- Bio-metria. Precisazioni terminologiche.

Non è possibile pensare di avviare un'analisi sulle problematiche giuridiche connesse alla biometria senza prima delimitarne il campo d'indagine attraverso, in primo luogo, una chiara comprensione del significato del termine. Questa operazione, di carattere più squisitamente descrittivo, non è affatto scontata, essendo il campo della biometria assai variegato e complesso.

Bio-metria significa "misurare la vita"[20]. Si tratta, come è suggerito dall'etimologia stessa, di una "disciplina che considera statisticamente i fenomeni biologico-vitali dal punto di vista quantitativo"[21]. Il campo di studio e di applicazione di questa scienza è, dunque, estremamente vasto, alludendo a tutto ciò che è legato ad una qualche misurazione della vita: esiste una biometria vegetale, che consente, per esempio, di stabilire l'età di un albero, una biometria animale, data dai sistemi di riconoscimento degli animali, e soprattutto una biometria medica, se si considera che la maggioranza degli esami medici hanno natura biometrica (non solo una TAC o una RMN, ma anche un semplice esame del sangue)[22]. Il termine biometria ha indicato così

[20] Dal greco ßίος (vita) e μέτρον (misura).
[21] A. GIULIANO, *Dieci e tutte diverse. Studio sui dermatoglifi umani*, Torino,Tirrenia Stampatori, 2004, 243.
[22] A. AGOSTINI, *Biometria e privacy: i presunti nemici a confronto*, Bologna, edis, 2006, 15.

per molto tempo lo studio e l'uso di metodi matematici e statistici applicati alle scienze della vita.

Non si tratterà, tuttavia, nel corso di questo lavoro, di biometria nelle accezioni sopra indicate. È necessario quindi ricavare una definizione che consenta di puntualizzare che cosa si voglia intendere d'ora innanzi con questa espressione.

L'accezione italiana del termine, utilizzato al singolare, corrisponde sostanzialmente all'inglese *biometrics* che, secondo la definizione dell'*International Biometric Group* (IBG)[23], fatta propria dal documento *Biometric-based technologies* dell'OECD, consiste nell'"uso automatizzato di caratteristiche fisiologiche o comportamentali per determinare o verificare l'identità"[24].

Lo stesso documento opera una distinzione tra *biometrics* e *biometric system*, dichiarando che "un sistema biometrico include tutti gli *hardware*, *software* associati, *firmware* e componenti di *network* necessari per portare a termine il processo biometrico di registrazione e di comparazione", ovvero, secondo l'autorevole definizione adottata dal Documento di lavoro sulla biometria, con l'espressione sistemi biometrici si vuole indicare "le applicazioni di tecnologie biometriche che permettono

[23] L'IBG è una società internazionale che offre servizi nel settore della biometria sia nell'ambito pubblico che nell'ambito privato.

[24] "*The automated use of physiological or behavioural characteristics to determine or verify identity*", INTERNATIONAL BIOMETRIC GROUP (IBG), *How is "Biometrics" Defined?*, in *http://www.biometricgroup.com/reports/public/reports/biometric_definition.html*; si veda poi OECD, WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometric-based technologies*, cit., 10-11. La definizione dell'OECD può considerarsi di riferimento poiché sinteticamente contiene tutti gli elementi essenziali per una corretta comprensione di cosa la biometria sia. In particolare, il documento sottolinea come il termine "*automated*", benché, si precisa, andrebbe sostituito con "*automated-assisted*", sia di cruciale importanza per la qualificazione di un sistema biometrico, poiché "per esempio, un sistema di documenti che usa immagini che sono confrontate manualmente da una persona non costituisce un sistema biometrico". *Biometric* al singolare, invece, precisa ancora il testo, indica "*one of the various technologies that utilise behavioural or physiological characteristics to determine or verify identity*". Si possono ricavare altre definizioni dai documenti in tema di biometria, benché concettualmente esse corrispondano. Per esempio, si veda il documento COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, cit., 8, "'*Biometrics' refers to systems that use measurable, physical or physiological characteristics or personal behaviour traits to recognise the identity, or verify the claimed identity of an individual*".

l'identificazione e/o l'autenticazione/verifica automatica di un individuo"[25]. Nonostante questa precisazione, *biometrics* e *biometric system* vengono sovente utilizzati indistintamente[26].

La definizione adottata va tuttavia presa in considerazione più attentamente. Essa infatti contiene in sé alcuni aspetti che sono di primaria importanza ai fini di una corretta comprensione del campo d'indagine.

Innanzitutto, si parla di caratteristiche di tipo fisico e fisiologico, e caratteristiche comportamentali[27]. Questa è la prima fondamentale distinzione, nonché l'elemento cruciale, che contraddistingue i sistemi di riconoscimento biometrico da tutti gli altri.

Tra le caratteristiche fisiche e fisiologiche rientrano la verifica delle impronte digitali, l'analisi dell'immagine delle dita, il riconoscimento dell'iride, l'analisi della retina, il riconoscimento del volto, la geometria della mano, il riconoscimento della forma dell'orecchio, il rilevamento dell'odore del corpo, il riconoscimento vocale, l'analisi dei pori della pelle, e altro ancora.

Le caratteristiche comportamentali, invece, valutano il "comportamento" di una persona, perciò possono comprendere, per esempio, la verifica della firma manoscritta, l'analisi della battitura su tastiera, l'analisi dell'andatura.

Allo stato attuale, pertanto, i modi attraverso cui un utente può essere riconosciuto sono generalmente tre. Il Documento di lavoro sulla biometria sottolinea chiaramente questa distinzione. Ci si può, infatti, basare su qualcosa che *l'utente conosce* (una password, un PIN), su qualcosa che *l'utente possiede* (un dispositivo di

[25] GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria,* cit., 3.
[26] A. AGOSTINI, *Biometria e privacy: i presunti nemici a confronto,* cit., 15, che afferma: "In inglese, lingua «ufficiale» per le tecnologie, i sistemi biometrici vengono riassunti nel termine plurale «Biometrics»…".
[27] GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria,* cit., 3-4.

autenticazione o *token*, una *smart card*), e infine su qualcosa che *è proprio dell'utente* (una caratteristica biometrica)[28]. Detto in altri termini, io conosco quindi accedo, io posseggo quindi accedo, e *io sono quindi accedo*[29].

La distinzione, così come espressa nei termini appena indicati, appare particolarmente significativa ed incisiva: porre infatti "l'essere" in relazione consequenziale con "l'accedere", significa identificare in qualche modo l'essere e l'accedere, l'essere e il riconoscere. Solo sulla base di se stessi, del proprio corpo, è possibile trovare riconoscimento da parte del sistema. Dunque, "la biometria si distingue tra tutte le tecnologie di *Automatic Identification and Data Capture* perché il riconoscimento non è più basato sul possesso di qualcosa che ci è stato dato o comunicato da un'autorità garante, ma su ciò che si è, sul proprio corpo"[30].

Benché ciò non rappresenti affatto una novità nella storia umana, non è possibile tuttavia pensare di equiparare questo fenomeno a quelli che lo hanno precorso, poiché oggi lo sviluppo della tecnica e i susseguenti sistemi di raccolta, gestione e utilizzazione dei dati, nella fattispecie di derivazione corporea, pongono problemi di nuova e delicata natura[31].

---

[28] GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria,* cit., 4. La distinzione è a sua volta ripresa in vari contributi, si vedano, per esempio, E. SANNA, *Le garanzie di sicurezza e autenticità delle informazioni in rete; in particolare del mandato informatico di pagamento,* in *Riv. giur. sarda,* 2001, fasc. 1, 311; S. BISI, *Il furto d'identità: panoramica attuale e prospettive giuridiche,* in *Ciberspazio e diritto*, 2004, 316; S. BISI, *Il corpo come password: alcune considerazioni in tema di sistemi di autenticazione biometrica*, in *Ciberspazio e diritto*, 2005, 9.

[29] A. GIULIANO, *Dieci e tutte diverse. Studio sui dermatoglifi umani,* cit., 244.

[30] E. MORDINI, C. OTTOLINI, *Implicazioni etiche e sociali della biometria*, in *L'Arco di Giano,* 2005, n. 45, 67.

[31] Nasce con l'uomo e con l'organizzazione della società umana l'esigenza di riconoscere i soggetti, e il corpo appare da principio il primo e più immediato veicolo di identificazione. Con l'evolversi della società, l'uso del corpo a fini identificativi è legato soprattutto a problemi di polizia, e di qui nascono scienze quali l'antropometria e la dattiloscopia. L'antropometria è un po' la madre della moderna biometria. Fu Alphonse Bertillon (1853-1914), un impiegato della prefettura della polizia di Parigi, che ideò il primo sistema di classificazione fondato su misure di parti del corpo, che venne definito metodo antropometrico o *bertillonage,* come lo battezzò un giornalista parigino. Il metodo si basava sullo studio antropometrico del capo (cefalometria e cefalosopia) e del corpo (somatometria e somatoscopia). L'avvento della dattiloscopia, i primi studi sulla quale possono farsi risalire intorno alla metà del 1700, basata sullo studio delle impronte digitali, segnò il superamento del sistema ideato da Bertillon. Di particolare interesse, sul piano della ricostruzione storica, A. GIULIANO, *Dieci e tutte diverse. Studio sui*

Una seconda fondamentale specificazione riguarda il fine che si propone la biometria, ossia determinare o verificare l'identità, in altri termini, l'identificazione o l'autenticazione/verifica di un individuo.

Autenticare significa "confrontare un campione biometrico presentato con il corrispondente dato biometrico registrato relativo ad una singola persona"[32], per accertare che la persona sia realmente chi dichiara di essere. Pertanto, i sistemi biometrici di autenticazione/verifica accertano la corrispondenza univoca, effettuando un raffronto di tipo "uno contro uno" (1-1) tra determinate caratteristiche, fisiche o comportamentali, di un individuo, e un *set* di valori precedentemente fornito dall'individuo stesso e registrato in un *database* o in un dispositivo mobile[33].

Se vi è una base di dati centralizzata, dove tutti i dati biometrici elaborati matematicamente e le corrispondenti identità sono registrati, l'identità richiesta è recuperata nella memoria del *database*. Se il soggetto, invece, si presenta al dispositivo di cattura del dato biometrico accompagnato da un supporto (una *smart card* o un *chip* integrato in un documento di identità), in cui sia archiviato il proprio dato biometrico, viene effettuato un confronto tra il dato rilevato in tempo reale e quello registrato nel supporto[34].

L'identificazione è, invece, un vero e proprio processo di attribuzione dell'identità, che si realizza attraverso il raffronto dei dati biometrici di un individuo con tutti quelli memorizzati in un *database* (il medesimo o altri connessi), effettuando così

---

dermatoglifi umani, cit., 1 ss., e A. BIASIOTTI, *Le tecnologie biometriche. Sicurezza, contrattualistica, privacy*, Roma, EPC LIBRI, 2002, 13 ss.

[32] COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, cit., 8, "*Verification means comparing a presented biometric sample with the corresponding enrolled biometric data pertaining to one single person*".

[33] S. BISI, *Il furto d'identità: panoramica attuale e prospettive giuridiche*, cit., 314; S. BISI, *Il corpo come password: alcune considerazioni in tema di sistemi di autenticazione biometrica*, cit., 6-7.

[34] EUROPEAN COMMISSION, *Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizen's Freedoms and Rights, Justice and Home Affaire (LIBE)*, cit., 38.

un confronto "uno contro molti" (1-n). Un sistema biometrico può operare in identificazione positiva o negativa, dichiarando l'individuo rispettivamente di appartenere o non appartenere al gruppo di utenti noti al sistema[35].

La scelta tra sistemi di autenticazione/verifica e sistemi di identificazioni dipende, naturalmente, dal fine che si intende perseguire.

Si distinguono, infatti, sistemi di accesso fisico, in cui il controllo biometrico viene effettuato per monitorare, limitare o permettere movimenti di persone all'ingresso di aree specifiche, come locali, edifici, zone ad accesso limitato, oppure per utilizzare determinate attrezzature o specifici oggetti, come, per esempio, aprire una cassaforte o azionare un'automobile, e sistemi di accesso logico, che riguardano la possibilità di accedere a dati o informazioni e quindi, più specificatamente, accertano la titolarità del soggetto ad usufruire di una determinata risorsa informatica. Esempi di accesso logico sono l'accesso ad un PC, ad una rete locale o aziendale, oppure l'accesso a servizi di *e-government*, *home banking*, commercio elettronico[36].

Proprio sulla base delle finalità perseguite, per l'accesso logico si utilizzano generalmente sistemi di autenticazione/verifica, mentre per l'accesso fisico sistemi di identificazione, benché, in quest'ultimo caso, sia frequente anche l'utilizzo di sistemi di autenticazione/verifica.

Vi sono inoltre distinti vantaggi pratici nell'utilizzo di un sistema piuttosto che di un altro, che in taluni casi ne orientano la scelta: i sistemi di autenticazione/verifica sono generalmente più rapidi e consentono un riconoscimento più preciso e accurato, mentre quelli di identificazione sono più lenti poiché richiedono un maggiore potere

---

[35] CNIPA, *Linee guida per le tecnologie biometriche,* cit., 12-13.

[36] S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world*, Wiley Computer Publishing, 2002, 14-15; CNIPA, *Linee guida per le tecnologie biometriche,* cit., 11. Per una trattazione completa dei sistemi di accesso fisico e di accesso logico, si veda CNIPA, *Linee guida per l'impiego delle tecnologie biometriche nelle pubbliche amministrazioni. Indicazioni operative*, in *www.cnipa.gov.it/site/_files/I%20Quaderni%2017.pdf*, settembre 2005, 43-74.

computazionale, dovendo effettuare una quantità talora molto elevata di confronti, ragion per cui sono più esposti alla possibilità di errore[37].

2- Il processo biometrico: tra dato biometrico e *template.*

Il processo di riconoscimento biometrico si apre con la fase di *enrollment*, ossia con la registrazione dell'utente, mediante la rilevazione della caratteristica biometrica da parte del sensore e l'acquisizione della stessa sotto forma di dato biometrico detto, più precisamente, "dato biometrico grezzo" o "campione biometrico", cui segue la conversione in un *template*[38].

Il dato biometrico è pertanto un'immagine (l'immagine dell'impronta digitale, l'immagine del volto, l'immagine dell'iride, e così via), una sorta di fotografia, della caratteristica biometrica.

Se di qualità soddisfacente, il campione viene trasformato in una rappresentazione matematica, cioè in una stringa di caratteri alfanumerici, il *template* o "modello biometrico"[39].

Si sostiene che i sistemi biometrici, in linea di massima, archivino e confrontino *template*, e non dati biometrici grezzi, i quali pertanto sono utilizzati per la creazione del

---

[37] S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world*, cit., 13-14.

[38] Si vedano: S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world*, cit., 17; A. BIASIOTTI, *Le tecnologie biometriche. Sicurezza, contrattualistica, privacy*, cit., 30; GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria*, cit., 4. Ai fini di una maggiore chiarezza, per indicare il dato biometrico si utilizza l'espressione "dato biometrico grezzo" o "campione biometrico". Tuttavia, solitamente l'espressione "dato biometrico", senza alcuna specificazione, viene utilizzata per indicare la stringa di dati numerici che costituisce il *template*.

[39] Traduzione del termine *template* adottata dal GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria*, cit., 4. Il processo automatizzato attraverso cui vengono individuate e codificate le distinte caratteristiche dei dati biometrici grezzi ai fini della creazione di un *template*, è chiamato processo di "estrazione delle caratteristiche", S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world*, cit., 18.

template e, in quasi ogni sistema, sono immediatamente cancellati[40]. Questo punto è estremamente critico.

È opportuno precisare che il concetto di *template*, così come quello di dato biometrico grezzo, benché allo stato attuale possa sembrare di poco conto ai fini dell'indagine giuridica, è centrale per la comprensione e lo studio dei problemi connessi alla protezione dei dati personali, di cui si tratterà. Infatti, a seconda che il dato venga memorizzato nell'una o nell'altra forma, potrebbe richiedersi una tutela differente, più o meno rafforzata.

Tuttavia, le informazioni che si raccolgo sul punto dalle diverse fonti sono alquanto laconiche. La maggior parte di esse asserisce che normalmente si conserva il solo *template*, lasciando poi intendere che in talune circostanze, peraltro non marginali se si va ad indagare sul piano applicativo, il campione biometrico stesso venga archiviato, a seconda dei sistemi utilizzati e delle finalità perseguite.

Lo stesso *Documento di lavoro sulla biometria* lascia aperte più possibilità, nel momento in cui dichiara: "È tale modello, presentato in forma digitale, ad essere archiviato e non l'elemento biometrico in se stesso. I dati biometrici inoltre possono essere elaborati come dati grezzi (un'immagine) in funzione del sistema biometrico utilizzato"[41], specificando, in nota, che il documento "si riferisce principalmente ai sistemi biometrici basati su modelli, ma può essere applicato anche in caso di dati grezzi" e che "la specificità dei dati grezzi tuttavia può rendere necessario l'adattamento delle prescrizioni in tema di tutela dei dati". L'apertura emerge anche in altri punti:

---

[40] Così S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world*, cit., 17, 18; GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria*, cit., 4.

[41] GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria*, cit., 4. Il punto è richiamato anche dalle Linee Guida della CNIPA, *Linee guida per le tecnologie biometriche*, cit., 14, "Talvolta, come può accadere ad esempio nel caso delle impronte digitali, il processo biometrico può fare riferimento alla immagine della caratteristica biometrica e non ad una estrazione di caratteristiche".

"L'identificazione invece è possibile solo memorizzando i dati di riferimento in una base di dati centralizzata dato che, per accertare l'identità della persona interessata, il sistema deve confrontare i suoi modelli o i suoi dati grezzi (immagine) con i modelli o i dati grezzi di tutte le persone i cui dati sono già registrati a livello centrale".

Esempio tipico di applicazione che prevede la memorizzazione dei dati grezzi è il c.d. *law enforcement*, ove è frequente l'uso del sistema AFIS, cui si accennerà nel corso della breve panoramica sulle tecnologie biometriche, e che comporta la registrazione delle immagini delle impronte digitali[42]. In alcuni Stati, si è utilizzato il sistema AFIS anche per evitare frodi nella distribuzioni di benefici assistenziali oppure nell'ambito della circolazione automobilistica, per assicurare la titolarità delle patenti di guida[43].

Un settore fondamentale in cui è necessaria la memorizzazione dei campioni biometrici è altresì quello dei passaporti, di cui meglio si dirà. Sul punto l'ICAO offre chiare indicazioni[44]. Essendo sostanzialmente i sistemi biometrici strutturati in maniera tale che il *template* creato da un sistema non possa essere letto da un sistema differente, l'ICAO richiede che l'intera immagine della caratteristica biometrica venga memorizzata, al fine di garantire l'interoperabilità[45]. Pertanto, è consigliato l'uso di tecniche specifiche di protezione e di criptazione dei dati, in particolare ricorrendo all'uso di chiavi pubbliche, che tuttavia non sono considerate garanzia assoluta di sicurezza[46].

---

[42] S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world*, cit., 262.
[43] *Ibidem*, 114 ss.
[44] Si veda ICAO, TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS (TAG-MRDT), Montréal, 23 March 2007, *Machine Readable Travel Documents (MRDTs): history, interoperability, and implementation*, cit.
[45] Così ICAO, *Biometric deployment of Machine Readable Travel Documents, ICAO TAG MRDT/NTWG, Technical Report*, 21 May 2004, cit., 31; ICAO, TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS (TAG-MRDT), Montréal, 20 to 22 March 2007, *Machine Readable Travel Documents (MRDTs): history, interoperability, and implementation*, cit., 16.
[46] GRUPPO DI LAVORO ARTICOLO 29, PROTEZIONE DATI, *Parere 3/2005 riguardante l'attuazione del regolamento (CE) n. 2252/2004 del Consiglio, del 13 dicembre 2004, relativo alle norme sulle*

Al di là delle applicazioni, è in ogni caso certo che, qualunque sia il sistema utilizzato, esso acquisisce pur sempre l'immagine della caratteristica biometrica, e il dato grezzo, seppur per breve o brevissimo tempo, è necessariamente "raccolto" fino al momento della sua cancellazione.

3. (*Segue*) La fase del *matching.*

Conclusa la fase di *enrollment*, si apre la procedura di comparazione dei *template* (o delle immagini), detta *matching*, per determinare il loro grado di somiglianza e di correlazione[47].

Il confronto avviene tra il *template* archiviato mediante il processo di *enrollment* (*enrollment template*), e il *template* creato quando l'utente fornisce il proprio dato biometrico al dispositivo di rilevazione del dato stesso (*verification template*), il quale, a differenza del primo, viene solitamente cancellato all'istante[48].

Al grado di somiglianza e correlazione viene assegnato un punteggio che, nella maggior parte dei sistemi, è valutato rispetto ad un numero predefinito che funge da soglia[49]. Se, dunque, il punteggio eccede la soglia, si avrà una combinazione dei

---

caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri, in *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp112_it.pdf*, 10, "I certificati a chiave pubblica contengono informazioni sul titolare e ognuno di essi rimanda unicamente alla persona alla quale è stato rilasciato […]. Tuttavia, i certificati digitali si prestano a un utilizzo indebito, inteso a negare al titolare del certificato l'accesso ai servizi. Inoltre, i dati generali dell'operazione svolta mediante certificati digitali può essere filtrata attraverso strumenti di sorveglianza ed essere trasmessa elettronicamente a terzi o alla polizia o altre autorità".

[47] S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world*, cit., 20 ss.

[48] Naturalmente, in un sistema di autenticazione/verifica entrambi i *template* sono del medesimo soggetto, in un sistema di identificazione il *template* ricavato sulla base dei dati forniti da un utente viene confrontato con i *template* archiviati di altri soggetti.

[49] Tale soglia è generalmente scelta dall'amministratore del sistema cosicché, a seconda del grado di sicurezza desiderato, è possibile optare per sistemi con soglie più o meno elevate, con una elasticità che non è contemplata nel caso di sistemi di sicurezza che si avvalgono, per esempio, di PIN o *password*.

template (*match*) e dunque il soggetto sarà riconosciuto, in caso contrario la combinazione fallirà e non avrà luogo alcun riconoscimento (*non match*).

Poiché ogni *template*, come si è già detto, è unico e irripetibile, le due stringhe di dati, quella archiviata e quella ottenuta "in tempo reale", saranno esse stesse diverse. Per questa ragione, il dispositivo di cattura deve essere governato da uno speciale algoritmo[50], il quale consente di confrontare i differenti modelli biometrici per verificarne il grado di correlazione, che in ogni caso non potrà mai essere totale, e determinare se esso ricade, in base al punteggio attribuito, al di sopra o al di sotto della soglia considerata accettabile[51].

Da quanto detto si può trarre un'importante deduzione: considerato che non è possibile, in nessun caso, raggiungere un grado di correlazione e somiglianza del cento per cento tra i *template* confrontati, evidentemente la risposta che il sistema biometrico può fornire ai fini del riconoscimento di un soggetto non può che essere, in un certo senso, approssimativa, benché ciò non vada inteso come limitata affidabilità e sicurezza. In altri termini, mentre un PIN o una password offrono risposte definite (si/no), i sistemi biometrici non sono in grado di fare altrettanto.

---

[50] I sistemi biometrici utilizzano algoritmi proprietari per esaminare i *template* e generare punteggi. Tali algoritmi manipolano i dati contenuti nel *template*, al fine di effettuare un valido confronto che tenga conto di numerosi fattori contingenti che variano di importanza a seconda del tipo di dispositivo di rilevazione, come rumori di sottofondo, illuminazione ambientale, corretto posizionamento dell'utente, livello di umidità o di temperatura, ecc., CNIPA, *Linee guida per l'impiego delle tecnologie biometriche nelle pubbliche amministrazioni. Indicazioni operative*, cit., 25 ss. Molti studi e sperimentazioni vengono condotti al fine di elaborare sempre nuovi e più efficaci algoritmi, in grado di migliorare il rendimento dei sistemi, si vedano, per esempio, gli studi raccolti in J. PEJAŚ, A. PIEGAT (edited by), *Enhanced methods in computer security, biometric and artificial intelligence systems*, Kluwer Academic Publishers, 2005, 143-251. Spesso, tuttavia, le compagnie valutano la precisione dei loro algoritmi utilizzando *template* statici o generati artificialmente, e non esaminando dati ricavati da un reale *enrollment*, S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world*, cit., 23.

[51] A. BIASIOTTI, *Le tecnologie biometriche. Sicurezza, contrattualistica, privacy*,cit., 30; S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world*, cit., 20. Non c'è una scala *standard* per il punteggio biometrico: alcuni sistemi utilizzano una scala che va da 1 a 100, altri da -1 a 1. Inoltre, i sistemi di punteggio variano non solo da tecnologia a tecnologia, ma anche da un venditore all'altro.

Vi è, pertanto, un problema di accuratezza, cioè di precisione ed esattezza, che viene calcolata utilizzando dei parametri ben definiti. Così, il parametro FMR (*false match rate*) indica la probabilità che il *template* di un utente sia abbinato al *template* di un utente differente, di modo che, per esempio, qualcuno potrebbe accedere ad un sistema pur non essendone titolato - FAR (*false acceptance rate*) -. Il parametro FNMR (*false non match rate*) indica, viceversa, la probabilità che il *template* dell'utente venga erroneamente giudicato dal sistema come inidoneo ad essere abbinato a quello archiviato e appartenente al medesimo utente, impedendo a qualcuno di accedere, pur essendone titolato - FRR (*false rejecton rate*) -. Infine, il parametro FTE (*failure to enroll*) indica la probabilità che un soggetto non sia in grado di essere registrato in un sistema biometrico[52].

È importante sottolineare che, da una parte, i sistemi biometrici non possono considerarsi affatto infallibili, dall'altra, per valutare la precisione del sistema, i tre parametri vanno applicati in maniera interdipendente.

4. Le tecnologie biometriche. Cenni.

Si accennerà brevemente ad alcune tra le più diffuse tecnologie biometriche in uso, al fine di una generica comprensione dei sistemi e degli strumenti utilizzati. La letteratura sul punto è alquanto vasta e dettagliata[53]. Non si ritiene tuttavia opportuno

[52] Altri due parametri, utili ai fini di una comparazione globale dei sistemi, sono EER (*equal error rate*), che indica il tasso di errore nel punto in cui le curve FAR e FRR si incrociano, e ATV (*ability to verify*), che è una combinazione di FTE e FNMR, e indica la percentuale di utenti che saranno in grado di utilizzare il sistema su base giornaliera. Per una trattazione completa sull'accuratezza dei sistemi biometrici, si consideri S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world*, cit., 23 ss..

[53] Si vedano: S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world*, cit., 43 ss.; CNIPA, *Linee guida per le tecnologie biometriche*, cit., 17 ss.; A. BIASIOTTI, *Le tecnologie biometriche. Sicurezza, contrattualistica, privacy*, cit., 39 ss.; EUROPEAN COMMISSION, *Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on*

soffermarsi con altrettanta scrupolosità su questo punto, sembrando piuttosto maggiormente utile, in relazione alle finalità che ci si propone, dare solo qualche generica informazione.

Si suole conferire ai dati biometrici degli attributi distintivi, che li rendono unici rispetto ad altri elementi identificativi. È necessario tuttavia precisare che non ogni caratteristica biometrica soddisfa in ugual misura tali requisitivi, pur dovendo essi essere presenti, se si intende ascrivere un determinato elemento alla categoria di dati in questione.

Questa valutazione avviene sulla base dei c.d. "sette pilastri"[54]. In altri termini, le caratteristiche biometriche devono soddisfare i requisiti dell'universalità, ossia essere presenti in tutte le persone, dell'unicità o diversità in ciascun soggetto, della permanenza nel tempo, inoltre, devono poter essere raccolte facilmente, avere un grado elevato di accuratezza nell'identificazione, essere accettate con favore dagli utenti, e infine garantire maggiore sicurezza rispetto ai tradizionali elementi identificativi.

Senza dubbio, tra le più note tecnologie biometriche rientra l'impronta digitale, ampliamente utilizzata nel mercato tanto per modalità di accesso fisico, quanto per modalità di accesso logico, grazie alla facilità di acquisizione, alla rapidità del riconoscimento, all'elevata accuratezza e al costo contenuto dei sistemi, nonché al buon grado di accettabilità[55].

Citizen's Freedoms and Rights, Justice and Home Affaire (LIBE), cit., 54 ss., 122 ss.; OECD, WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometric-based technologies*, cit., 21 ss.; J. D. WOODWARD, N. M. ORLANS, P. T. HIGGINGS, *Biometrics*, McGraw-Hill, 2003; P. REID, *Biometrics for network security*, Upper Saddle River, 2004; A. K. JAIN, R. BOLLE, S. PANKANTI (edited by), *Biometrics: personal identification in networked society*, Kluwer, 1999; D. D. ZHANG, *Automated biometrics. Technologies and systems*, Kluwer Academic Publishers, 2000.

[54] *Universality, distinctiveness, permanence, collectability, performance, acceptability, resistance to cirumvention*, EUROPEAN COMMISSION, *Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizen's Freedoms and Rights, Justice and Home Affaire (LIBE)*, cit., 37.

[55] Si tratta della riproduzione dell'epidermide di un polpastrello, che può avvenire oggigiorno in svariate forme (più frequentemente mediante sensori ottici, ad ultrasuoni, oppure utilizzando una piastrina di silicio). Il disegno dell'impronta è determinato dalle creste e dalle valli epidermiche del polpastrello, le quali si sviluppano nell'essere umano già a partire dalla vita prenatale, assumendo forme particolari in

Valutando questa tecnologia sulla base dei "sette pilastri", si potrebbe anzitutto rilevare che le impronte digitali non rispondono completamente ai requisiti né dell'universalità, né della permanenza, poiché in alcuni soggetti, come anziani o lavoratori, nei quali l'epidermide del polpastrello può essere stata in qualche modo compromessa con il passare del tempo, si riscontrano delle difficoltà di rilievo, senza contare le persone affette da qualche disabilità. Questa difficoltà può riguardare anche determinati gruppi etnici[56]. Quanto, invece, alla unicità dell'impronta digitale e quindi alla sua capacità di distinguere i soggetti, non sembrano sussistere dubbi: studi condotti sul campo rivelano che il carattere individuale è mantenuto persino nel caso di gemelli monozigoti[57].

Nell'ambito della rilevazione delle impronte digitali, un cenno merita anche quel diffuso sistema biometrico conosciuto come AFIS (*Automated Fingerprint Identification System*), che consente di effettuare ricerche su larga scala all'interno di *database* in cui siano archiviati sia *template* che campioni biometrici di impronte digitali. Per questa peculiarità, esso si distingue dagli altri sistemi, in cui l'archiviazione dei dati grezzi, come già detto, generalmente non avviene o non dovrebbe avvenire[58]. Pertanto, la tecnologia AFIS è interamente predisposta per identificare le persone a partire dalle immagini delle impronte digitali, soprattutto per finalità giudiziarie e di lotta alla criminalità ma, come si è visto, oggi trova applicazione anche nell'ambito civile.

---

ogni individuo, benché le caratteristiche più spesso utilizzate per il riconoscimento siano le minuzie, ossia le terminazioni o biforcazioni delle creste. Per una trattazione approfondita sul tema, si veda l'intera opera di A. GIULIANO, *Dieci e tutte diverse. Studio sui dermatoglifi umani*, cit.

[56] S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world*, cit., 59-60.

[57] A. GIULIANO, *Dieci e tutte diverse. Studio sui dermatoglifi umani*, cit., 259 s.

[58] S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world*, cit., 114 ss.

Molto utilizzato è altresì il sistema di riconoscimento del volto[59]. Questa caratteristica biometrica soddisfa i requisiti dell'universalità, dell'accettabilità, non essendo richiesto alcun contatto fisico con il sensore, della facilità di raccolta, cosicché è utilizzata di frequente, per esempio, nell'ambito di sistemi di sorveglianza o di controllo dei documenti.

Proprio la facilità di raccolta pone tuttavia seri interrogativi. Infatti, un sistema di riconoscimento del volto può operare senza alcuna collaborazione dell'utente, con una telecamera nascosta e collocata a una certa distanza, e pertanto all'insaputa del soggetto coinvolto, creando preoccupazioni per quanto riguarda il potere di intrusione nella sfera della vita privata e inoltre per l'emergere e il consolidarsi di una ipotetica, ma non troppo lontana, "società della sorveglianza".

Simile preoccupazione, che si estende peraltro ad altre tecnologie biometriche, è stata avvertita da Stefano Rodotà[60], secondo il quale "una cosa è il ricorso alle tecniche biometriche quando si tratta di verificare, ad esempio, l'identità di chi accede ad un'area protetta; altro sarebbe la loro adozione per finalità di identificazione di massa", e sottolineata dal *Documento di lavoro sulla biometria*: "L'aspetto problematico è rappresentato dal fatto che, da un lato, questa raccolta e questo trattamento di dati possono essere effettuati all'insaputa della persona interessata e, dall'altro, che indipendentemente dalla loro attuale affidabilità tali tecnologie biometriche si prestano

[59] Il riconoscimento biometrico del volto si basa sull'acquisizione delle caratteristiche del volto di un soggetto attraverso un dispositivo costituito da una telecamera, da cui le immagini vengono trasmesse a un PC. Il riconoscimento può essere di carattere statico o dinamico, a seconda che vengano confrontate immagini fisse o immagini in movimento. Si è anche sostenuto che un qualsiasi sistema di videosorveglianza con registrazione configura un sistema biometrico, con tutte le problematiche relative alla *privacy* che si applicano per questo tipo di dispositivi, sul punto v. A. BIASIOTTI, *Le tecnologie biometriche. Sicurezza, contrattualistica, privacy*, cit., 52-53.

[60] S. RODOTÀ, *Una scommessa impegnativa sul terreno dei muovi diritti*, Discorso del Garante per la protezione dei dati personali tenuto l'8 maggio 2001 alla presentazione della relazione del 2001, in *www.interlex.it/675/rodota6.htm.*

ad un uso generalizzato a causa del loro basso «livello di intrusività». È quindi necessario stabilire garanzie specifiche in materia"[61].

Inoltre, questa tecnologia si rivela molto sensibile a fattori esterni, come condizioni ambientali e variazioni della luminosità, e sono emerse altresì difficoltà di acquisizione del campione in taluni gruppi etnici, come nel caso di persone dal colore della pelle più scuro. Pertanto, si potrebbe sostenere che il grado di accuratezza non sia ottimale.

Infine, requisiti importanti come l'unicità e la stabilità nel tempo non vengono soddisfatti pienamente, poiché, evidentemente, tra volti si possono scorgere somiglianze e, per svariate cause, essi possono subire frequenti variazioni nel corso del tempo. Perciò, il sistema richiede che vengano raccolti molti campioni per effettuare un certo numero di confronti tra *template*, ottenendo sovente errori nel riconoscimento.

Ultimo esempio di tecnologia biometrica che si intende considerare, senza dubbio tra i più diffusi e interessanti, è il sistema di riconoscimento dell'iride[62].

È bene ricordare che solo una società fornisce questa tecnologia, pertanto non si pone il problema dell'interoperabilità così come negli altri sistemi, né si riscontrano differenze nella scansione dell'immagine o nella generazione dei *template* tra un sistema e un altro, benché, come controparte, si registra evidentemente una situazione di monopolio del mercato da parte dell'unico costruttore[63].

---

[61] GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria, 1°agosto 2003*, cit., 5.

[62] Il sistema si avvale di apparecchiature particolari, munite di video camere, che forniscono la necessaria illuminazione infrarossi. Tale tecnologia "consiste nell'analisi delle caratteristiche dell'anello colorato che circonda la pupilla e che rappresenta un identificatore biometrico particolarmente efficace. Le caratteristiche strutturali dell'iride umano sono molto complesse e comprendono uno strato epiteliale, non trasparente alla luce, alcuni muscoli che controllano l'apertura della pupilla, vasi sanguigni e uno strato di cellule pigmentali dette cromatofori, disposte in modo discontinuo secondo schemi diversi da individuo ad individuo, e diversi tra un occhio e l'altro anche per lo stesso individuo", CNIPA, *Linee guida per le tecnologie biometriche*, cit., 33.

[63] *Ibidem*, 34.

Questo sistema di riconoscimento, valutandolo sulla base dei parametri inizialmente considerati, è tra i più efficienti. È possibile, infatti, attribuire all'iride il carattere dell'universalità, eccezione fatta per i soggetti colpiti da particolari patologie, come l'"aniridia", cioè l'assenza dell'iride. Difficoltà si possono talora riscontrare anche per coloro che sono affetti da glaucoma o hanno subito una qualche operazione chirurgica importante. La peculiarità dell'iride consiste nel fatto che non varia nel corso della vita, ed è assolutamente unica e differente in ciascuna persona.

Questo sistema presenta, quindi, un elevato grado di accuratezza, benché tuttavia sia costoso, e non sia talvolta ben visto dagli utenti. Infatti, le biometrie suscitano sovente nel pubblico preoccupazioni, che attengono ai possibili danni al corpo e alla salute. Circa l'iride, data la delicatezza della parte del corpo coinvolta e l'utilizzo di radiazioni ad infrarossi, la preoccupazione pare essere accentuata, benché non ci siano dimostrazioni effettive di danni causati all'occhio a seguito dell'utilizzo di tale tecnologia[64].

Per quanto riguarda le implicazioni mediche indirette, invece, relative al timore di un uso secondario, ossia eccedente le finalità della raccolta, delle informazioni biometriche, si pongono maggiori problemi, che investono la sfera etico-giuridica, dei quali, pertanto, ci si occuperà in un secondo momento.

In particolare, tale preoccupazione si pone per il DNA.

[64] Le implicazioni mediche correlate all'utilizzo di tali tecnologie possono essere sia dirette (DMI, *Direct Medical Implications*), sia indirette (IMI, *Indirect Medical Implications*). Nell'ambito delle implicazioni dirette, l'occhio potrebbe soffrire un danno provocato da un'eccessiva esposizione ai raggi infrarossi, benché, per causare tale danno, sia necessaria una quantità di radiazioni molto maggiore rispetto a quella utilizzata nei sistemi in questione, EUROPEAN COMMISSION, *Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizen's Freedoms and Rights, Justice and Home Affaire (LIBE)*, cit., 50 ss.

5. (*Segue*) Il DNA.

Si discute se il DNA si possa considerare o meno una caratteristica biometrica. Ciò, naturalmente, è importante ai fini delle implicazioni normative.

Senza dubbio, il DNA non costituisce una caratteristica biometrica in senso stretto. Esso, infatti, richiede un campione fisico tangibile, mentre nelle comuni biometrie si ricava un'immagine, una registrazione, un'impronta di una caratteristica fisica o comportamentale. Inoltre, il confronto tra campioni di DNA non è effettuato in tempo reale, e non tutti gli stadi del confronto sono automatizzati, benché questo ostacolo con lo sviluppo tecnologico e scientifico si presume possa essere superato entro alcuni anni. Infine, l'uso del DNA a fini identificativi non comporta l'estrazione di caratteristiche e la susseguente costruzione del *template*[65].

È vero, tuttavia, che, eccetto i gemelli identici, il DNA di ciascuna persona è unico, pertanto si potrebbe considerare una modalità perfetta di riconoscimento, avendo inoltre un grado di accuratezza molto elevato, ragion per cui viene utilizzato prettamente nell'ambito di indagini investigative e a fini giudiziari[66].

---

[65] Si vedano S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world*, cit., 153 e OECD, WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometric-based technologies*, cit., 11, "*DNA requires an actual physical sample as opposed to an image, photograph or scan; DNA matching is done in real time and, for the most part, is not automated; DNA matching does not employ templates or feature extraction, but rather represents the comparison of actual samples*". Nello stesso senso anche P. JOHNSON, R. WILLIAMS, *European securitization and biometric identification: the uses of genetic profiling*, in 43 *Ann. ist. super. sanità* (2007), spec. p. 39 e pp. 40 ss.

[66] EUROPEAN COMMISSION, *Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizen's Freedoms and Rights, Justice and Home Affaire (LIBE)*, cit., 93. Le forze di polizia di numerosi paesi, compresi Canada, Germania, Stati Uniti, Regno Unito, hanno creato *database* nazionali che raccolgono campioni di DNA. Essi sono stati costituiti anche in Belgio a seguito dei reati di pedofilia, e si prevede un'espansione ulteriore del ricorso a campioni di DNA per finalità di polizia e preventive, P. DE HERT, *Biometrics: legal issues and implications*, in *http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf*, 2005, 7 ss. Inoltre, come sottolineato dalla recente raccomandazione COUNCIL OF EUROPE, *Rec(2007)1 of the Committee of Ministers to member States on Co-operation against terrorism between the Council of Europe and its member states, and the International Criminal Police Organization (ICPO-Interpol)*, in *http://www.coe.int/t/e/legal_affairs/legal_cooperation/fight_against_terrorism/2_Adopted_Texts/Rec_2007_1E%20Interpol.pdf*, l'Interpol possiede un *database* di DNA al quale 36 paesi hanno fornito all'incirca 65000 profili di DNA, in quanto la collaborazione internazionale nel campo della lotta alla criminalità e al

Pare, invero, che debba passare molto tempo ancora prima che il DNA possa diventare un vero e proprio identificatore biometrico[67], non essendo, nell'attuale contesto sociale e giuridico europeo, né accettabile né praticabile introdurlo come tale[68].

Tuttavia, malgrado molti documenti dichiarino la non possibilità del ricorso al DNA come modalità di riconoscimento biometrico, viene inserito ugualmente all'interno della categoria in esame.

Questa posizione è assunta, per esempio, dal *Documento di lavoro sulla biometria*[69] e dal documento del *Joint Research Center* della Commissione europea, che dichiara: "Tuttavia, a causa del livello di accuratezza del processo e poiché noi riteniamo che esso sia una possibile futura caratteristica biometrica, l'abbiamo analizzato in aggiunta alle tecnologie biometriche comuni"[70]. Il Documento dell'OECD, ancor più chiaramente, afferma che "in senso stretto, il confronto di DNA non è una biometria, nello stesso modo in cui l'esame tradizionale a fini giudiziari dell'impronte digitale non è una biometria. Senza tener conto di tale distinzione, noi riteniamo che le tecnologie basate sul DNA dovrebbero essere discusse a fianco di altre tecnologie biometriche poiché esse fanno uso di caratteristiche fisiologiche per verificare o determinare l'identità. Al di là della definizione, alla maggioranza degli osservatori il DNA appare, agisce e potrebbero essere utilizzato come le altre biometrie. Le ricadute

---

terrorismo è sentita come aspetto cruciale nell'ambito della tutela della sicurezza dei paesi membri dell'UE.

[67] Sul punto i pareri paiono unanimi, si veda EUROPEAN COMMISSION, *Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizen's Freedoms and Rights, Justice and Home Affaire (LIBE)*, cit., 93, 62; A. BIASIOTTI, *Le tecnologie biometriche. Sicurezza, contrattualistica, privacy*, cit., 47, "E' probabile che possano passare parecchi anni, e forse un decennio, prima che queste tecniche siano di relativa accessibilità"; GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria, 1°agosto 2003*, cit., nota p. 3, "Va detto comunque che attualmente non sembra possibile generare un profilo di DNA in tempo reale come strumento di autenticazione".

[68] P. DE HERT, *Biometrics: legal issues and implications*, cit., 7.

[69] GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria, 1°agosto 2003*, cit., 3.

[70] EUROPEAN COMMISSION, *Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizen's Freedoms and Rights, Justice and Home Affaire (LIBE)*, cit., 62.

politiche, mentre sono molto più serie per le tecnologie basate sul DNA, condividono alcuni attributi comuni con altre biometrie"[71].

Invero, il DNA potrebbe considerarsi una biometria in quanto si tratta dell'uso di una caratteristica fisica per verificare o determinare l'identità. Impiegato in campo giudiziario, per stabilire la colpevolezza o l'innocenza, esso può essere estremamente utile, tuttavia, i confronti tra campioni di DNA diffusi in ambiti più comuni potrebbero portare a un cattivo uso delle informazioni ricavate, e sarebbero, ragionevolmente, mal accetti da parte degli utenti.

Considerato quanto detto, in particolare tenendo conto degli elementi di differenziazione rispetto alle altre biometrie e della non utilizzabilità, allo stato attuale, del DNA come tecnica identificativa su larga scala, considerato altresì che il DNA solleva problemi giuridici specifici, che dilaterebbero eccessivamente il campo d'indagine che si intende esaminare, esso non verrà valutato in questo lavoro come una vera e propria caratteristica biometrica.

Si tornerà, tuttavia, sulla questione nel corso del lavoro, guardando però il problema da una prospettiva differente, ossia dal punto di vista dell'informazione veicolata.

[71] OECD, WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometric-based technologies*, cit., 11.

CAPITOLO SECONDO

IL NUOVO HABEAS CORPUS

SOMMARIO: 1. Il corpo tra l'*essere* e l'*avere*: l'ambiguità del corpo nella tradizione giuridica. – 2. (*Segue*) Corpo, parti staccate e appartenenza. – 3. Dal corpo all'informazione, attraverso l'identità. – 4. (*Segue*) La duplice anima del diritto all'identità personale. - 5. L'integrità e le integrità. - 6. Consenso, autodeterminazione, identità. – 7. (*Segue*) Inquadramento dell'istituto del consenso informato. – 8. (*Segue*) Il consenso: da implicito, a informato e libero. - 9. È nato un "nuovo corpo"? - 10. Dall'*habeas corpus* all'*habeas data*.

1. Il corpo tra l'*essere* e l'*avere*: l'ambiguità del corpo nella tradizione giuridica.

Al fine di indagare le molteplici dimensioni e sfaccettature della "corporeità giuridificata"[72], si ritiene opportuno, in primo luogo, comprendere quale possa essere una corretta qualificazione giuridica del corpo dell'uomo.

La parola "corpo" è usata dal legislatore italiano in maniera estremamente limitata. La disposizione centrale è l'art. 5 cod. civ., che tuttavia non ne offre alcuna definizione giuridica. Il corpo, infatti, viene racchiuso a fatica all'interno delle categorie concettuali proprie del diritto, tendendo, per sua natura, ad eccedere ogni categorizzazione. Non sorprende, pertanto, che esso sia stato poco indagato nell'ambito

[72] L'espressione allude alla mancanza di una concezione unitaria della corporeità nel diritto e alla varietà di interventi legislativi differenziati che investono il corpo, il quale può essere riguardato come "a) il corpo dell'uomo e quello della donna; b) il corpo vivo e il corpo morto; c) il corpo dei maggiori e dei minori d'età, dei capaci e degli incapaci, dei giovani e degli anziani; d) il corpo dei familiari e degli estranei; e) il corpo malato e il corpo sano, f) il corpo prima e dopo la nascita (una volta ammessa la possibilità di riferire la nozione di corpo al non nato), il corpo «potenziale» o «progettato» (embrione creato in vitro) e attuale; g) il corpo «terminale» e quello «recuperabile»; h) il corpo degli organi singoli o doppi; i) il corpo dei tessuti rigenerabili e non rigenerabili; l) il corpo dei tessuti fetali e non; m) il corpo delle cellule somatiche o germinali", S. RODOTÀ, *Ipotesi sul corpo "giuridificato"*, in *Riv. crit. dir. priv.*, 1994, 477-478.

della riflessione dottrinale privatistica[73], che rivela tutta la propria incertezza di fronte a tale oggetto di studio, a conferma della sua intrinseca complessità[74].

L'approccio giuridico alla corporeità appare così ultimamente orientato in negativo: il corpo è il "grande assente del codice civile"[75], un "puro accidente del complesso normativo"[76], un "servo muto"[77].

Si è osservato che la stessa matrice illuministica della teoria dei diritti dell'uomo, nel farsi promotrice di quell'ampia gamma di libertà che sono alla base degli ordinamenti democratici, ha lasciato nell'ombra la questione del corpo[78].

Emerge così l'esigenza, sollecitata dall'avvento della c.d. terza generazione dei diritti della persona, alla cui base si pone il principio di autodeterminazione[79], di

---

[73] "Il corpo umano, intero o peggio parti di esso, ha sempre avuto poco a che fare con le categorie giuridiche. Chi parla, da giurista, di organi da prelevare, sangue per trasfusione, ovociti da impiantare (per non parlare di mani rubate) esce dalle strade del diritto civile per incamminarsi in un percorso da dove è difficile ritornare", C. M. MAZZONI, *Avvertenza*, in J. P. BAUD, *Il caso della mano rubata. Una storia giuridica del corpo*, Milano, Giuffrè, 2003, IX.

[74] Riguardo alla complessità della dimensione corporea, e più propriamente alle diverse dimensioni che connotano la *persona*, è interessante lo studio condotto dal noto giurista P. SCHLESINGER, *La persona*, in *Riv. dir. civ.*, 2008, 379-393, ove l'a. prende in considerazione il complesso rapporto tra corpo, cervello, mente, coscienza, e finanche l'attributo della relazionalità. Si è detto, a fronte di tale complessità, che "la strada percorsa dalla cultura giuridica è stata sostanzialmente quella della «decisione di non decidere», ossia si è sempre evitato il problema trincerandosi dietro argomentazioni tecnico-formali, cui l'eredità del razionalismo kantiano non può certo dirsi estranea, preclusive di una soluzione sostanziale della questione", G. RESTA, *Proprietà, corpo e commodification nel dibattito nordamericano*, in *Riv. crit. dir. priv.*, 1995, 798.

[75] G. FERRANDO, *Diritto e scienze della vita. Cellule e tessuti nelle recenti direttive europee*, in *Familia*, 2005, 1158.

[76] S. AMATO, *Diritto e corpo: il soggetto «incarnato»*, in *Dem. e dir.*, 1988, 64.

[77] Così C. M. MAZZONI, *Il corpo e le sue immagini*, in *Riv. crit. dir. priv.*, 2005, 451. La suggestiva immagine è ripresa dall'antropologo Kamper. Al corpo vero e proprio, fatto di carne ed ossa, si sostituiscono le immagini, che funzionano come una "trappola", da cui il corpo chiede di liberarsi per affermarsi nella sua "realtà". L'a. parla altrove del "corpo nascosto dei giuristi", ad indicare come, essendo il mondo del giurista un mondo metafisico, fatto di rappresentazioni e figure, questi si trovi disorientato nell'approccio alla corporeità, C. M. MAZZONI, *Il corpo nascosto dei giuristi*, in *Riv. crit. dir. priv*, 2008, 339-346.

[78] F. D'AGOSTINO, *Riflessioni sui diritti della corporeità*, in *Rivista di teologia morale*, 1981, n. 50, 203-204.

[79] G. MARINI, *La giuridificazione della persona. Ideologie e tecniche nei diritti della personalità*, in *Riv. dir. civ.*, 2006, 366, ove l'a. individua una terza generazione dei diritti della persona, che si aggiunge alle due che l'hanno preceduta, "l'una statica, in cui si afferma come modello dominante il paradigma proprietario, l'altra dinamica il cui fulcro è costituito dal «pieno sviluppo della persona» realizzato attraverso la costruzione di relazioni sociali costitutive della propria identità". La terza generazione, che non si sostituisce necessariamente alle precedenti ma spesso convive con esse, si contraddistingue per il ruolo centrale assunto dal potere di autodeterminazione soggettiva, "come potere di controllare le modalità di costruzione della propria identità personale".

ridefinire in positivo il ruolo della corpo, poiché, come è stato efficacemente detto, "ogni giorno si rinnova per noi il compito di realizzare il nostro corpo"[80].

È utile, in primo luogo, rilevare che l'antica contrapposizione tra anima e corpo, su cui si fondava la visione dualistica dell'uomo che ha caratterizzato il pensiero filosofico a partire da Platone fino alla svolta fenomenologica[81], e che in tempi più recenti è stata espressa nella dicotomia tra l'essere un corpo e l'avere un corpo, è

[80] E. BIANCHI, *Corpo da rispettare anche nell'indegnità*, in *Avvenire*, sezione "Agorà", 23 settembre 2007, 4-5.

[81] Per comprendere l'approccio giuridico al corpo, è opportuno, in prima battuta, indagare il problema dal punto di vista della filosofia e, in particolare, della filosofia del diritto. Si veda, innanzitutto, l'essenziale contributo di M. M. MARZANO PARISOLI, *Norme e natura: una genealogia del corpo umano*, Napoli, Vivarium, 2001, 25-66, in cui l'a. arriva a proporre un nuovo statuto giuridico del corpo umano a partire dall'analisi del pensiero filosofico, soffermandosi sulla concezione dualistica dell'uomo in Platone, Cartesio e Descartes, per giungere al superamento della logica disgiuntiva, grazie al pensiero fenomenologico, con Husserl, Merleau-Ponty, Sartre. Significativo è altresì il contributo di F. MACIOCE, *Il corpo. Prospettive di filosofia del diritto*, Roma, Aracne, 2002, 23-72, in cui l'a. individua tre modelli fondamentali cui ricondurre, nella storia del pensiero e della cultura occidentale, il rapporto soggetto-corpo, ovvero 1. Il corpo e l'intenzionalità ontologica della persona, che vede nel corpo qualcosa di non oggettivabile, ma che dà senso all'alterità, per cui ciò che sta di fronte all'io corporeo riceve il suo senso proprio grazie a questo posizionamento (Rosmini, Husserl, Merleau-Ponty, Gabriel Marcel); 2. Il corpo come avere, in cui il soggetto si rapporta con il suo corpo pressoché allo stesso modo in cui si rapporta con il resto della realtà oggettuale, per cui il soggetto risulta essere disincarnato (Cartesio, Nietzsche); 3. Il soggetto incarnato e la dimensione della verticalità, in cui l'io è un io incarnato e dunque il soggetto è in una relazione con il proprio corpo non riconducibile alla categoria dell'avere, e tuttavia sussiste solo in una dimensione di verticalità, in rapporto cioè con la trascendenza di un Dio creatore (Emmanuel Lévinas, Bonhoeffer). Interessante è vedere come il dibattito tra l'essere e l'avere un corpo, tra corpo come persona e corpo come cosa, sia centrale anche nella riflessione teologica, I. FUČEK, S.I., *Prospettive teologiche ed etiche in tema di corporeità umana*, in *Medicina e Morale*, 1990, 933-948, in cui l'a. mostra come la dignità teologica del corpo umano risieda nell'unità e nell'integrità della persona intera (*Gaudium et Spes*, GS, n. 14: "*homo corpore et anima unus*"). Già nell'approccio veterotestamentario, le tre dimensioni *nephes* (psychè, anima), *basar* (sarx-soma, caro-corpo), *ruach* (pneuma, spirito) designavano tutta la persona umana. Nell'antropologia di S. Paolo, la *sarx* (carne, Körper) esprime sia la corporeità materiale, sia la persona umana dominata dalla schiavitù del peccato (Rm 7,14), mentre il *soma* (corpo, Lieb) è la persona stessa, "l'unico autentico modo di esistere della persona" ovvero "tutto il corpo umano è personalizzato" (p. 940). Su tali assunti si basa la riflessione della prospettiva metafisica personalista, secondo cui: "L'uomo «è» corpo, non «ha» il corpo. Il corpo è l'incarnazione e la manifestazione dell'io, il principio materiale-potenziale attualizzato dal principio formale spirituale (secondo il modello ilemorfico). Nell'uomo non sussiste la giustapposizione corpo/anima, bensì l'unità sostanziale della dimensione fisico-psichica e spirituale. Attraverso la corporeità si manifesta la persona non solo nella esteriorità, ma nella stessa struttura ontologica. Il corpo non è dunque un mero oggetto di cui l'uomo può disporre, bensì acquisisce un valore che partecipa della dignità dell'uomo stesso", E. SGRECCIA, *Corpo e persona*, in S. RODOTÀ (a cura di), *Questioni di bioetica*, Roma, Laterza, 1993, 114, si veda anche E. SGRECCIA, *La persona umana e il suo corpo*, in *Manuale di bioetica*, I, Milano, Vita e pensiero, 2003, 105-137. Interessante, al riguardo, è indagare anche il c.d. *mind-body problem*, il problema del rapporto corpo-mente, che è oggetto di studio da parte della filosofia della mente, per cui si tratta di stabilire "se il mentale sia (equivalga al) fisico, se sia in qualche senso riducibile ad esso, o se, invece, costituisca una categoria ontologicamente distinta", F. POGGI, *Tra anima e corpo. Il problema degli stati soggettivi nella filosofia della mente contemporanea*, in *Materiali per una nuova storia della cultura giuridica*, 2007, 162.

presente anche sul piano giuridico, ove si traduce nella distinzione tra il corpo come persona e il corpo come cosa ovvero il corpo come soggetto e il corpo come oggetto di diritti.

In particolare, è la riflessione dottrinale più risalente a incontrare l'*impasse* di tale contrapposizione.

Parte della dottrina considerava, infatti, il corpo umano come un bene ossia, ai sensi dell'art. 810 cod. civ., come "una cosa che può formare oggetto di diritti" [82], per cui al soggetto spettava anche la proprietà sul proprio corpo che, privato di ogni connotato "meta-fisico", poteva essere assimilato a qualunque altra *res*[83].

Tale teoria non pare essere del tutto tramontata, se si considera che recentemente il francese J. P. Baud ha sostenuto la tesi della "realtà" del corpo all'interno di una tanto accurata quanto discutibile ricostruzione storica sull'approccio giuridico alla corporeità, arrivando a concludere che, poiché non c'è una categoria intermedia tra le cose e le persone, "tutti i sistemi giuridici fondati sulla distinzione tra persone e cose dovranno riconoscere che il corpo di un uomo vivente è una cosa dal momento che il cadavere e le parti staccate del corpo sono delle cose"[84].

---

[82] Il legislatore non definisce le cose, che vanno intese nel significato comune di "porzione del mondo esterno percepibile con i sensi, di entità materiale". I beni, al contrario, sono definiti dal codice come cose idonee a soddisfare un bisogno del soggetto, entità materiali utilizzabili dall'uomo divenendo così oggetto di un diritto, M. COMPORTI, *Le cose, i beni, ed i diritti reali*, in *Istituzioni di diritto privato*, (a cura di) M. BESSONE, Torino, Giappichelli, 2005, 319.

[83] Si vedano, tra i più significativi, il contributo di F. CARNELUTTI, *Problema giuridico della trasfusione di sangue*, in *Foro it.*, IV, 1938, 94, il quale afferma, in riferimento agli uomini e alle cose: "Queste due specie di elementi sono l'una e l'altra, dei *beni*, cioè degli strumenti, che servono all'appagamento dei bisogni; anche gli uomini, non solo le cose, onde ciascuno di noi prima di tutto, *secum porta bona sua*", e di F. DEGNI, *Sulla trasfusione obbligatoria di sangue*, in *Foro it.*, IV, 1938, 129. Sulla base di tali premesse, ci si è interrogati "se la trasmissione ereditaria di quei «beni» possa individuarsi facendo appello alle norme sulla successione, legittima o testamentaria, considerandoli alla stregua di un bene mobile di cui il *de cuius* può disporre e che si rende disponibile al momento della morte", A. ZOPPINI, *Le "nuove proprietà" nella trasmissione ereditaria della ricchezza (note a margine della teoria dei beni)*, in *Riv. dir. civ.*, 2000, I, 243.

[84] J. P. BAUD, *Il caso della mano rubata. Una storia giuridica del corpo*, Milano, Giuffrè, 2003, 230. Il ricorso allo schema proprietario si giustifica, secondo l'a., proprio a partire dalla convinzione che esso sia il solo a poter conferire una tutela giuridica forte al corpo, garantendo il diritto all'integrità fisica, proteggendo il corpo dalla commerciabilità e, in ultima analisi, tutelando la dignità stessa dell'essere umano (pp. 238 ss.).

Questa concezione, che vuole restituire l'oggetto-corpo nelle mani del soggetto-proprietario secondo l'antica teoria dello *ius in se ipsum*[85], malgrado sia mossa dall'intento di garantire alla dimensione corporea una tutela forte, si rivela in realtà foriera di minacce, rischiando, paradossalmente, di limitare quella stessa libertà individuale che intendeva promuovere e tutelare[86].

Benché, infatti, la considerazione del corpo come un bene, legato al soggetto da un rapporto di tipo proprietario, non conduca necessariamente a collocarlo nell'orizzonte delle merci, essendo pur sempre possibile considerarlo una *res extra commercium*[87], tuttavia la sua oggettivazione ha portato spesso a paventare lo spettro del mercato[88].

---

[85] Secondo questa teoria, "a ciascun uomo spetterebbe la *proprietà del proprio corpo*; in questa prospettiva l'atto di disposizione del corpo altro non sarebbe che esplicazione di una delle facoltà insite nel diritto soggettivo che l'individuo vanta sul proprio essere fisico", C. M. D'ARRIGO, *Autonomia privata e integrità fisica*, Milano, Giuffrè, 1999, 128. Essa è stata successivamente ripresa e "aggiornata", "proponendosi di risolvere l'antinomia «uomo-soggetto uomo-oggetto» sostituendo alla parola «uomo» rispettivamente i concetti di «persona» e «corpo», cosicché l'uomo -in quanto persona- potrebbe essere considerato titolare di un diritto su se stesso -inteso, questa volta, come corpo, cioè come cosa", C. M. D'ARRIGO, *op.cit.*, 13. Si veda, al riguardo, anche G. CRISCUOLI, *L'acquisto delle parti staccate del proprio corpo e gli artt. 820 e 821 del c.c.*, in *Dir. fam. e pers.*, 1985, 267, ove si afferma che la persona, secondo tale teoria, "sarebbe «soltanto l'uomo come soggetto, vale a dire il suo spirito considerato in libertà di forma (o dal corpo, in altre parole)», il primo, o l'uomo, sarebbe combinazione del corpo e dello spirito e come tale entità oggettiva di rapporti giuridici, dei quali la «persona» sarebbe il primo titolare".

[86] Relativamente al c.d. *divided self* e al *self-owenership*, si è detto che l'idea della persona proprietaria di se stessa è una forte espressione di autonomia individuale, tuttavia "*if persons can objectify their selves they become susceptible to objectification by others*", cosicché "*property-in-self is a means of expressing human autonomy is, paradoxically, also to threaten liberty*", N. NAFFINE, *The Legal Structure of Self-Ownership: Or the Self-Possessed Man and the Woman Possessed*, in 25 *Journal of Law and Society* (1998), 200.

[87] Lo stesso Baud sostiene che il corpo umano, pur essendo una cosa, "è una cosa che non è una merce", J. P. BAUD, *op. cit.*, 230. Inoltre, si veda M. COMPORTI, *op. cit.*, 331, che include il corpo umano, il cadavere, il sangue, nella categoria in questione, pur sostenendo che tuttavia "si discute se possono essere considerati beni in senso giuridico".

[88] Si è detto che nel modello classico liberale la proprietà "con i suoi aspetti di controllo prettamente individualistico e alienabilità incondizionata, non è altro che un riflesso della società capitalistica di mercato, strutturata appunto sugli istituti della proprietà privata e del contratto", cosicché "non c'è spazio per «beni» che siano oggetti di proprietà senza nello stesso tempo divenire «merci», inevitabilmente inghiottiti dalla logica del mercato", G. RESTA, *Proprietà, corpo e commodification nel dibattito nordamericano*, cit., 800. Così come definita dal codice, che ne sottolinea l'aspetto dell'utilità, la nozione di bene è parsa assumere una "sfumatura «economica»", M. M. MARZANO PARISOLI, *Il corpo tra diritto e diritti*, in *Materiali per una nuova storia della cultura giuridica*, 1999, 533; "lo stesso concetto di bene giuridico è stato a lungo inficiato da una connotazione riduttivamente economicistica", M. TALLACCHINI, *Il corpo e le sue parti. L'allocazione giuridica dei materiali biologici umani*, in *Medicina e Morale*, 1998, 537. Il legame proprietà/commerciabilità viene poi a più riprese sollevato nell'ambito della riflessione bioetica, a proposito, in particolare, della donazione di organi: "E se c'è proprietà, se è possibile la

A questo riguardo, tanto la legislazione nazionale quanto le carte internazionali non lasciano adito a dubbi, negando qualunque possibilità di commercializzazione delle parti del corpo, in quanto lesiva dello stesso valore della dignità umana[89].

Inoltre, la scoperta da parte del diritto delle implicazioni sempre più strette tra identità personale e corporeità, di cui si dirà, non permette di assumere pacificamente tale approccio.

Altra parte della dottrina, invece, rigettando la tesi dualistica, escludeva la riduzione del corpo a bene, oggetto di diritto di proprietà, essendo la persona unità inscindibile di "sostanza materiale" e "sostanza immateriale", di corpo e spirito[90].

Tale concezione, se condivisibile opponendosi ad una gretta reificazione del corpo, incontrava tuttavia il limite giuridico della impossibilità di disporne, poiché l'uomo veniva ad essere, al tempo stesso, soggetto e oggetto di diritti[91].

---

donazione, può esservi anche vendita", G. BERLINGUER, *Il corpo come merce o come valore*, in S. RODOTÀ (a cura di), *Questioni di bioetica*, Roma, Laterza, 1993, 87; "Parlare di «mercato» in rapporto al corpo umano presuppone l'applicazione della categoria di «cosa», «oggetto», «proprietà»", in E. SGRECCIA, *Corpo e persona*, cit., 114; "[…] il diritto di donare, di per se stesso, sembrerebbe implicare una proprietà da parte del donatore; e se esiste tale proprietà perché non può conseguire la vendita?", M. LOCKWOOD, *La donazione non altruistica di organi in vita*, in S. RODOTÀ (a cura di), *Questioni di bioetica*, Roma, Laterza, 1993, 142.

[89] Relativamente alla disposizione a titolo gratuito di parti del corpo, per la legislazione nazionale si vedano la l. 26 giugno 1967, n. 458 – *Trapianto di rene tra persone viventi* (artt. 1, 6); l. 12 agosto 1993, n. 301 – *Norme in materia di prelievo ed innesti di cornea* (art. 1); l. 1 aprile 1999, n. 91 - *Disposizioni in materia di prelievi e trapianti di organi e tessuti* (artt. 19, 22); l. 16 dicembre 1999, n. 483 – *Norme per consentire il trapianto parziale di fegato* (art. 1); l. 6 marzo 2001, n. 52 – *Riconoscimento del Registro nazionale italiano dei donatori di midollo osseo* (art. 4); l. 21 ottobre 2005, n. 219 – *Nuova disciplina delle attività trasfusionali e della produzione nazionale degli emoderivati* (artt. 2, 3, 4, 11, 22). Per la legislazione internazionale, si ricorda, in particolare, l'art. 21 della *Convenzione per la protezione dei diritti dell'uomo e la dignità dell'essere umano riguardo alle applicazioni della biologia e della medicina*, nota come "Convenzione di Oviedo", aperta alla firma dal Consiglio d'Europa a Oviedo il 4 aprile 1997, e l'art. 3 della *Carta dei diritti fondamentali dell'Unione europea*, adottata dal Consiglio Europeo di Nizza il 7 dicembre 2000.

[90] F. SANTORO-PASSARELLI, *Dottrine generali del diritto civile*, Napoli, 1962, VII ed., 51, per il quale "non esiste e non è neppure concepibile, malgrado ogni sforzo dialettico, un diritto sulla propria persona o anche su se medesimo, o sul proprio corpo, stante l'unità della persona, per la quale può parlarsi soltanto di libertà, non di potere rispetto a se medesima; e neppure esiste, per il nostro ordinamento, un diritto sul corpo altrui…".

[91] M. PESANTE, voce «Corpo umano (Atti di disposizione)», in *Enc. del dir.*, X, Giuffrè, 1962, 655; M. M. MARZANO PARISOLI, *op. cit.*, 132-134.

Un'autorevole dottrina mirava, infine, a conciliare queste due opposte concezioni, elaborando una teoria intermedia che, concependo il corpo come un "modo di essere" della persona, come un "bene particolarmente prezioso", non esteriore al soggetto e ciò nonostante non identificabile con il soggetto stesso o con parte di esso, lo faceva rientrare nella categoria dell'essere piuttosto che dell'avere, vale a dire "il soggetto ha ciò che è in vari sembianti". Al corpo poteva essere così riconosciuta l'attitudine ad essere "indice di riferimento oggettivo di rapporti giuridici, poiché per essi il soggetto ha un interesse, ha, cioè, la possibilità di fruire della relativa utilità" [92]. Quest'ultimo approccio riprendeva, tuttavia, sotto diversi profili, la superata contrapposizione tra uomo-corpo e persona-spirito[93].

Sono numerose, pertanto, le ambiguità che sorgono nel momento in cui ci si avventura nella qualificazione del corpo umano, il quale rimane, anche per il diritto, un enigma, che "coincide e insieme non coincide con noi stessi"[94].

Oggi i più sono concordi nel guardare alla corporeità in termini di "«luogo» della nostra estrinsecazione"[95] oppure come "manifestazione esterna dell'individuo e del suo vissuto personale e sociale"[96]. Ancor più chiaramente, il corpo può considerarsi "strumento per la realizzazione della persona", ovvero "baluardo entro il quale è destinato a venire in contatto ogni processo di conformazione della persona ad opera del diritto"[97].

---

[92] M. PESANTE, voce «Corpo umano (Atti di disposizione)», cit., 655-656, per il quale: "Tali modi di essere, che quindi sono beni, hanno la caratteristica, a differenza degli altri beni, di appartenere, non alla categoria dell'avere, ma a quella dell'essere: si può dire che il soggetto ha ciò che esso stesso è in vari sembianti".
[93] M. C. VENUTI, *Gli atti di disposizione del corpo*, Milano, Giuffrè, 2002, 38.
[94] F. D'AGOSTINO, *Bioetica*, Torino, Giappichelli, 1998, 125 oppure F. D'AGOSTINO, *Introduzione*, in S. COTTA, A. C. AMATO MANGIAMELI, S. AMATO, A. LISITANO, V. VITALE, *Diritto e corporeità. Prospettive filosofiche e profili giuridici della disponibilità del corpo umano*, Milano, Jaca Book, 1987, 9.
[95] *Ibidem*, 208.
[96] M. C. VENUTI, *Integrità della persona e multietnicità*, in *Familia*, 2003, 613.
[97] G. MARINI, *La giuridificazione della persona. Ideologie e tecniche nei diritti della personalità*, cit., 366.

Sembra opportuno, tuttavia, riconoscere anche, senza tornare a inadeguati dualismi o, viceversa, identificazioni, che in esso "le due *polarità fondamentali* del soggetto e dell'oggetto" possono talora convivere oppure sovrapporsi[98].

In conclusione, solo partendo da una concezione di ampio respiro della corporeità, quale entità in grado di trascendere la dimensione meramente fisica e materiale, sarà possibile configurare più coerentemente gli interessi e i valori che ruotano intorno ad essa[99], e riconoscere che ogni scelta che incide sul corpo, inevitabilmente, si allarga, sino a toccare la persona nel suo complesso[100]. Solo individuando il *proprium* del corpo, in altri termini, sarà possibile rendergli il *suum*[101].

2. (*Segue*) Corpo, parti staccate e appartenenza.

La minaccia della reificazione si fa più forte quando l'analisi si sposta verso la considerazione del regime giuridico spettante alle parti del corpo. Invero, corpo e parti

[98] P. ZATTI, *Il corpo e la nebulosa dell'appartenenza*, in *Nuova giur. civ. comm.*, 2007, II, 12. Sul punto si veda anche M. TALLACCHINI, *Il corpo e le sue parti. L'allocazione giuridica dei materiali biologici umani*, cit., 506, ove l'a. dichiara: "Il primo paradosso del corpo consiste nel fatto che esso è sia il luogo e il mezzo della soggettività – il corpo-soggetto, in cui il «soggetto è il corpo» - sia l'oggetto di atti con sui il soggetto dispone di sé – il corpo-oggetto, in cui il «soggetto ha il corpo» -, e, come oggetto di sé, in tali atti il soggetto può disporre del proprio corpo come totalità di sé – della propria vita -, oppure può disporre quanto alle parti di esso". Così, il soggetto-corpo può disporre della totalità di sè prendendo decisioni in ordine alla propria salute, oppure "commercializzando la propria attività fisica o intellettuale, la propria immagine o talune altre facoltà (la voce)" (p. 507).

[99] Si veda, con riferimento al diritto alla salute, M. PICCINNI, *Il consenso al trattamento medico del minore*, Padova, CEDAM, 2007, 26, ove l'a. dichiara che "se la decisione sul corpo è una decisione su di sé, anche nella configurazione del diritto alla salute non potrà non tenersi conto […] della necessità di considerare il malato non solo come soggetto fisico, ma come individuo che occupa un preciso ruolo nella società e nelle formazioni sociali ove si esplica la sua personalità".

[100] G. FERRANDO, *Consenso informato del paziente e responsabilità del medico, principi, problemi e linee di tendenza*, in *Riv. crit. dir. priv*., 1998, 44, ove l'a. parla di "una diversa considerazione del corpo, che non può essere visto avulso dalla persona nel suo complesso e, nella sua fisicità, come «oggetto» di provvedimenti autoritativi alla stregua dei beni economici".

[101] Così F. D'AGOSTINO, *Riflessioni sui diritti della corporeità*, cit., 206.

sono tra loro strettamente intrecciati, benché sia differente la considerazione giuridica dell'uno e delle altre[102].

Tradizionalmente, infatti, la dottrina considera in modo pressoché unanime la parte staccata come ormai estranea al corpo, *res* tra le altre, per la quale può parlarsi di un vero e proprio diritto di carattere dominicale[103]. Non si dubita, dunque, della natura di oggetto dell'elemento corporeo separato, mentre divergenze si riscontrano relativamente al modo in cui sorge e si acquista tale diritto di proprietà[104].

---

[102] R. ROMBOLI, *Delle persone fisiche*, nel *Commentario Scialoja-Branca*, Zanichelli-Foro it., 1988, *sub* art. 5, 361, ove si afferma che "la loro caratteristica principale consiste nel fatto che il corpo umano è visto non più come elemento della persona, o come la persona stessa, ma come qualcosa di assolutamente distinto e separato, al seguito del verificarsi di certi fatti o di determinati avvenimenti"; più di recente, sulla complessa relazione esistente tra il tutto e le parti, si veda M. TALLACCHINI, *Il corpo e le sue parti. L'allocazione giuridica dei materiali biologici umani*, cit., 506 ss.; M. TALLACCHINI, *Bodyright. Corpo biotecnolgico e diritto*, in *Biblioteca della libertà*, 1998, 23 ss.; M. TALLACCHINI, *Habeas Corpus? Il corpo umano tra non-commerciabilità e brevettabilità*, in *Bioetica*, 1998, 537 ss.

[103] Si vedano G. ALPA, A. ANSALDO, *Le persone fisiche*, in *Commentario Schlesinger*, Giuffrè, *sub* artt. 1-10, 1996, 263; P. RESCIGNO (a cura di), *Codice Civile*, 5 ed., Milano, Giuffrè, 2003, *sub* art. 5, p. 31; M. PESANTE, *Corpo umano (Atti di disposizione)*, cit., 663; F. SANTORO PASSARELLI, *Dottrine generali del diritto civile*, cit., 52; A. DE CUPIS, voce «Corpo (Atti di disposizione del proprio)», nel *Noviss. Digesto it.*, IV, Utet, 1959, 854-855; G. DELL'OSSO, T. DE PALMA, *Il distacco di parti da soggetto vivente nei suoi riflessi medico-legali*, in *Riv. it. med. leg.*, 1983, 77; M. DOGLIOTTI, *Le persone fisiche*, nel *Trattato Rescigno*, 2, Utet, 1999, 111.

[104] Per una trattazione completa delle diverse teorie, si veda G. CRISCUOLI, *L'acquisto delle parti staccate del proprio corpo e gli artt. 820 e 821 del c.c.*, cit., 268 ss. e la replica di A. DE CUPIS, *Sull'equiparazione delle parti staccate del corpo umano ai frutti naturali*, in *Riv. trim. dir. e proc. civ.*, 1986, 137-138. Una prima teoria, detta del "prosieguo", affondando le proprie radici nella concezione dualistica dell'uomo, sostiene che il diritto di proprietà sul corpo si estende alle parti che se ne separano, secondo una soluzione di continuità, per cui esse, ininterrottamente, rimangono nella sfera patrimoniale del soggetto. Secondo la dottrina della "occupazione", invece, con la separazione la parte, non avendo in linea di massima più utilità per il soggetto, può considerarsi presumibilmente una cosa abbandonata e perciò *nullius*, dunque occupabile da chi ne abbia un qualche interesse. Una terza dottrina, definita del "distacco", sostiene che non ci sia continuità tra la situazione giuridica della parte prima e dopo il distacco, poiché solo a seguito del distacco la parte diviene esteriore al soggetto e in quanto tale acquisisce una natura reale, che prima non possedeva. Ciò nonostante, essa non passa mai per la fase intermedia della *res nullius*, così come sostenuto dall'approccio della occupazione, poiché "la coscienza giuridica non può ammettere che al diritto personale succeda, sia pure transitoriamente, l'assenza di qualsiasi diritto", A. DE CUPIS, *Il diritto sulle parti staccate del corpo umano e il diritto sul cadavere umano*, nel *Trattato Cicu-Messineo*, IV, Giuffrè, 1982, 160. L'orientamento della "fruttificazione", infine, equipara le parti del corpo ai frutti naturali secondo l'art. 820 c.c., presupponendo pertanto sempre una concezione dualistica dell'uomo, poiché "l'acquisto della proprietà dei frutti subentra a un già preesistente regime di proprietà, mentre ciò non si verifica per le parti staccate del corpo umano", A. DE CUPIS, *Sull'equiparazione delle parti staccate del corpo umano ai frutti naturali*, cit., 138.

Questo orientamento, tuttavia, lascia perplessi. Ci si può interrogare, viceversa, sulla analogia, per così dire, ontologica, tra la parte staccata e il corpo nel suo insieme, e sulla inscindibilità della relazione persona-corpo-parte.

J. P. Baud arrivò a concludere che, se la parte staccata è una cosa, allora il corpo stesso, da cui avviene il distacco, non può che essere una cosa[105]. La questione potrebbe essere capovolta: dal momento che il corpo non può essere considerato come una cosa, non si vedrebbe come le parti stesse, che di esso partecipano e da esso derivano, possa considerarsi come una cosa.

È pienamente condivisibile, dunque, quell'orientamento che contesta l'ascrizione delle parti del corpo alla categoria degli oggetti, considerando che "da una parte le possibilità di «isolamento» e separazione hanno invaso zone sempre più vicine al nucleo dell'identità corporea, e dall'altra è sopravvenuta l'evidenza, che la parte del corpo da separare o separata *non è mai (o quasi mai) solo oggetto*, né può essere oggetto di proprietà, ma è sempre, anche, luogo d'identità"[106].

Alla luce di ciò, si comprendono le proposte avanzate da più parti in ordine alla elaborazione di un modello giuridico che, cogliendo le molteplici sfumature

[105] "Tenuto conto del fatto che il cadavere è incontestabilmente una cosa, così come lo è un elemento separato del corpo, e che questi doni corporei, di cui la medicina avrà sempre più bisogno, riguardano ciò di cui si ha la proprietà prima dell'atto generoso, bisogna capire che in assenza di una nozione intermedia tra persona e cosa non si può far altro che classificare il corpo nella categoria delle cose", J. P. BAUD, *Il caso della mano rubata. Una storia giuridica del corpo*, cit., 225-226

[106] Così P. ZATTI, *Il corpo e la nebulosa dell'appartenenza*, cit., 9.

dell'appartenenza[107], riconosca al soggetto poteri di disposizione e di controllo sul proprio corpo e sulle sue parti di carattere non proprietario[108].

L'utilizzo di categorie alternative, tuttavia, a qualcuno non è parso segnare il superamento del diritto di proprietà *sul* proprio corpo né tantomeno della teoria dello *ius in se ipsum*, poiché le diverse qualificazioni sarebbero pur sempre accomunate dalla "accentuazione del dominio individuale sul proprio essere fisico" [109].

Invero, c'è anche chi ha negato qualunque forma di appartenenza, teorizzando il ricorso alla categoria delle *res communes omnium*. Quest'ultimo approccio si giustifica sulla base della convinzione che una tutela giuridica capace di sottrarre il corpo e le sue parti a una connotazione totalmente oggettiva e di manipolabilità ed eventualmente al mercato, di rafforzare inoltre la solidarietà, rispettando ad un tempo la volontà individuale, possa avvenire solamente sottolineandone la natura di bene comune e condiviso[110].

---

[107] Sul concetto di appartenenza e sulla pluralità delle forme di appartenenza, si veda P. ZATTI, *Verso un diritto per la bioetica: risorse e limiti del discorso giuridico*, in *Riv. dir. civ.*, 1995, I, 49, e *Il corpo e la nebulosa dell'appartenenza*, cit., 12, in cui l'a. dichiara: "La proprietà, che è una modalità dell'appartenenza, diviene il modello esaustivo dell'appartenenza; che invece, è enormemente più vasta e molteplice della proprietà"; inoltre, A. GAMBARO, *La proprietà*, nel *Trattato Iudica-Zatti*, Giuffrè, 1990, 12, secondo cui "[…] quando si parla di appartenenza si pensa istintivamente alla proprietà o al possesso di genere. Queste ultime, peraltro, sono le forme principali di appartenenza conosciute dalla nostra tradizione storica, ma, sul piano della progettazione razionale degli ordinamenti, sono solo alcune tra le forme di appartenenza pensabili nel novero delle quali si può scegliere".

[108] "Non stupisce che il rapporto dell'uomo col proprio corpo sia stato, in occasione dei primi approcci scientifici, conformato ai caratteri del diritto assoluto del proprietario: la proprietà rappresenta infatti il paradigma di diritto più pieno e completo, quindi il più adeguato per qualificare il diritto su se medesimo. Del resto è comprensibile che il giurista d'altri tempi, non stretto dalla necessità di dare risposte adeguate ai nuovi problemi posti dalle moderne tecniche, abbia preferito adagiarsi su una formula sicura e a lui consueta, sottraendosi all'onere d'inventare una più adeguata soluzione", C. M. D'ARRIGO, voce «Integrità fisica», in *Enc. del dir.*, Aggiornamento-IV, Giuffrè, 2000, 712, nota n. 4.

[109] C. M. D'ARRIGO, voce «Integrità fisica», cit., 713, ove l'a. sostiene che "diversa, invece, è la qualificazione giuridica della fonte di siffatta *potestas*: in alternativa alla proprietà in senso stretto vengono proposte le idee più sfumate di un rapporto di «appartenenza», di un dominio a contenuto non patrimoniale, ovvero di un diritto sul corpo *sui generis*, espressione di un più ampio diritto sulla persona".

[110] Si veda M. TALLACCHINI, *Il corpo e le sue parti. L'allocazione giuridica dei materiali biologici umani*, cit., 537 ss., che sostiene: "L'applicazione alla disciplina degli atti dispositivi e acquisitivi delle parti del corpo alla nozione di *res communes omnium* come "patrimonio umano", limitando i poteri soggettivi di disposizione e vincolando i modi e le finalità di quelli di acquisizione, consente di introdurre sia una maggior relazionalità nel rapporto tra soggetto e corpo sia una destinazione oggettiva del corpo ad usi qualificati" (p. 539).

La categoria, che dal diritto romano è stata traslata nel diritto internazionale[111], si ritiene tuttavia non sia la più appropriata per garantire una adeguata tutela giuridica della corporeità.

È sufficiente, infatti, effettuare una ricognizione, con gli opportuni accorgimenti, di tale concetto con riguardo ad alcune applicazioni nel diritto internazionale, per cogliere le difficoltà che insorgono se si intende applicarlo anche al corpo umano e alle sue parti, tanto che si è parlato, al riguardo, di *tragedy of the commons*[112].

Essendo le *res communes omnium* cose che sono in comunione tra tutti e di cui nessuno può vantare alcuna appartenenza specifica, si aggraverebbe infatti il rischio di uno sfruttamento indiscriminato e basato sulla legge del più forte, secondo la massima del *first come, first served* [113].

Concettualmente più adatto potrebbe essere, allora, l'istituto del *patrimonio comune humanitatis*, per avere un'accezione pienamente solidaristica[114].

---

[111] Nel mondo romano, certi beni (l'acqua fluente, l'aria, il mare), per loro intrinseca natura, non potevano divenire oggetto di dominio, erano pertanto *res nullius* o *res communes omnium*, perciò chiunque poteva farne uso ma nessuno poteva impedire ad altri di fare altrettanto. Il concetto fu poi, nel sec. XVII, traslato nel diritto internazionale pubblico con riferimento al mare. Negli anni fu poi esteso, per essere sostituito in alcuni casi da quello di patrimonio comune dell'umanità, ad altri beni (spazio, luna, corpi celesti). E. BACK IMPALLOMENI, *Il concetto di res communis omnium applicato allo spazio e ai corpi celesti,* in *Spazio cosmico e corpi celesti nell'ordinamento internazionale*, Padova, Cedam, 1983, cap. I, 28.

[112] A. GAMBARO, *La proprietà*, cit., 9. L'a. sostiene più specificatamente, con riguardo alle cellule, che la tesi di "adottare il solito regime delle *res communes omnium* con conseguente disconoscimento sia della appartenenza originaria all'individuo, sia, e soprattutto, del lavoro di ibridazione, immortalizzazione e coltivazione in vitro dei ceppi cellulari […] è parimenti assurda" (p. 44).

[113] È utile verificare cosa implichi nel diritto internazionale, e in particolare nel diritto spaziale ove è particolarmente impiegato, il ricorso a questa categoria. Il regime delle *res communes omnium* consente le operazioni militari o belliche, esclude qualunque forma di dominio o sovranità, ammette la libertà di utilizzo e sfruttamento della cosa nell'esclusivo interesse di chi la attua, secondo la massima "*first come, first served*", impone il rispetto del pari diritto altrui, E. BACK IMPALLOMENI, *Sfruttamento delle risorse della luna e patrimonio comune dell'umanità,* in G. CATALANO SGROSSO (a cura di), *Diritto dello spazio - Recenti sviluppi e prospettive*, Padova, Cedam, 1994, 229; E. BACK IMPALLOMENI, *I riflessi del Nuovo Ordine Economico Internazionale sul processo evolutivo del diritto spaziale,* in *Aspetti e problemi del Nuovo Ordine Economico Internazionale*, Padova, Cedam, 1987, 28.

[114] Sempre con riguardo al diritto internazionale, è interessante notare che il *patrimonio comune humanitatis* (che vige per la luna e gli altri corpi celesti, il fondo marino, il genoma umano) – o *common heritage of mankind* - è sovente considerato sinonimo dell'espressione *res communes omnium*. In realtà, "il patrimonio comune sta ad indicare un istituto giuridico che, seppure evolutosi dalle *res communes omnium*, tuttavia se ne diversifica", E. BACK IMPALLOMENI, *Il concetto di patrimonio comune dell'umanità applicato ai corpi celesti,* in *Spazio cosmico e corpi celesti nell'ordinamento internazionale*, Cedam, Padova, 1983, 62. Infatti, esso comporta l'esclusione delle attività dannose e di quelle che

Non si può escludere che, in specifici casi, questo concetto possa essere applicabile. Lo stesso genoma umano è stato definito, dalla Dichiarazione universale sul genoma umano e i diritti dell'uomo dell'UNESCO, patrimonio comune dell'umanità, seppure in senso simbolico[115]. Non sembra, tuttavia, proponibile come categoria generale cui assoggettare il regime giuridico della corporeità e delle parti staccate.

Si ritengono, quindi, maggiormente condivisibili quegli approcci che, non negando la speciale inerenza tra la persona e il suo corpo, riconoscono che esso, in qualche forma, le "*appartiene*".

Tra questi, c'è chi è giunto a sostenere l'impossibilità di una definizione in positivo della peculiare relazione intercorrente tra il soggetto, il proprio corpo e le sue parti, essendo possibile solamente la sua qualificazione in negativo, ovvero il ricorso a categorie "scarsamente formalizzabili", come quella di padronanza, quale *ius primordiale* sul proprio corpo[116].

Sono da rilevare, poi, i concetti di *dominium*[117] e il *principio di sovranità*[118].

---

dovessero risultare a beneficio di alcuni Stati soltanto con l'esclusione di altri, il rispetto dell'ambiente, la smilitarizzazione, la suddivisione dei vantaggi dello sfruttamento delle risorse tra tutti gli Stati, compresi quelli che non abbiano partecipato attivamente alle operazioni, la comunicazione dei risultati delle ricerche, E. BACK IMPALLOMENI, *Sfruttamento delle risorse della luna e patrimonio comune dell'umanità,* cit., 229.

[115] UNESCO, *Universal Declaration on the human genome and human rights*, 1997, art. 1 "*The human genome underlines the fundamental unity of all members of the human family, as well as the recognition of their inherent dignity and diversity. In a symbolic sense, it is the heritage of humanity*".

[116] Si vedano, ad esempio, le riflessioni di B. TRONCARELLI, *Il corpo nella prospettiva antiriduzionistica della complessità*, in F. D'AGOSTINO (a cura di), *Corpo esibito, corpo violato, corpo venduto, corpo donato. Nuove forme di rilevanza giuridica del corpo umano*, Milano, Giuffrè, 2003, 193-221. L'a. tratta del corpo sottolineandone "l'irriducibilità", "l'irripetibile eterogeneità", "l'inesaustività", "l'irripetibilità", "la strutturale incomparabilità" (p. 218), per cui dichiara: "Di fronte al corpo come sistema straordinariamente complesso, in quanto tale non suscettibile di un 'ordinario' inquadramento normativo, il concetto scarsamente 'formalizzabile' di padronanza può quindi aderire più di altri alla realtà del corpo stesso" (p. 220).

[117] M. M. MARZANO PARISOLI, *Norme e natura: una genealogia del corpo umano,* cit., 166-173; M. M. MARZANO PARISOLI, *Il corpo tra diritto e diritti*, cit., 548-552.

[118] P. ZATTI, *Il corpo e la nebulosa dell'appartenenza*, cit., 12 ss.; altri si sono espressi in termini di una "sovranità" sul proprio corpo, S. BARTOLOMMEI, *Corpo e cura di sé alla fine della vita: sulle "dichiarazioni anticipate di trattamento"*, in *L'Arco di Giano*, 2005, n. 44, 115, ove si afferma: "Individuare una modalità vincolante di espressione delle proprie volontà anche per questa estrema fase della vita consentirà di far valere il principio che ciascuno, indipendentemente dal suo grado di competenza attuale, è sovrano sul proprio corpo e non può essere sottoposto a terapie che implichino un trattamento che non intenda subire".

Il primo, che affonda le proprie radici nel mondo romano ed è stato ripreso dai teologi-giuristi medioevali[119], suggerisce l'idea di un "possesso limitato"[120], "capace di garantire e fondare l'indisponibilità del corpo umano, senza tuttavia negare possibili e limitate deroghe sulla base della pubblica utilità"[121].

Il secondo, invece, è un principio che nasce a partire dalla capacità che la persona ha di *governare* se stessa, indicando "ciò che il soggetto di un sistema di libertà e solidarietà ha diritto e dovere di fare appunto di *sé medesimo*"[122], benché, si precisa, ciò non significa che "il *solo* riferimento divenga la percezione soggettiva o il libero gioco di preferenze"[123].

3. Dal corpo all'informazione, attraverso l'identità.

Con accortezza, il giurista Paolo Pallaro ha affermato che sussiste un "valore giuridico fondamentale per la dignitosa esistenza delle persone consistente nel diritto a poter considerare le informazioni su di sé come parti di sé", specificando che si tratta di "beni giuridici assimilabili alle parti del corpo, quali pezzi di sé"[124] ovvero, secondo le

[119] Il termine designava, da un lato, quei rapporti che venivano protetti come se si trattasse di proprietà, pur non essendolo, e, dall'altro, veniva utilizzato dai teologi-giuristi (per lo più dalla scuola francescana) per indicare la particolare padronanza che l'uomo è chiamato ad esercitare sulla propria volontà.
[120] M. M. MARZANO PARISOLI, *Norme e natura: una genealogia del corpo umano,* cit., 170.
[121] M. M. MARZANO PARISOLI, *Norme e natura: una genealogia del corpo umano,* cit., 172. Alla nozione di proprietà si avvicina quella di amministrazione, H. KUHSE, *Il corpo come proprietà. Ragioni di scambio e valori etici*, in S. RODOTÀ (a cura di), *Questioni di bioetica*, Roma, Laterza, 1993, 65-73, benché, secondo M. M. MARZANO PARISOLI, l'amministrazione scivoli nel concetto di usufrutto piuttosto che in quello di *dominium*, che pure indica un particolare rapporto di amministrazione. Critica rispetto alla categoria del *dominium* è B. TRONCARELLI, *Il corpo nella prospettiva antiriduzionistica della complessità*, cit., 220, poiché "non risulta un concetto giuridico in grado di escludere la liceità della propensione 'possessoria' del soggetto sul proprio corpo, e in generale dell'uomo sulla corporeità. Il dominio permette, infatti, al suo titolare l'esercizio della propria signoria sulla cosa in oggetto, nel senso di un uso, se non di un 'abuso', di essa".
[122] P. ZATTI, *Il corpo e la nebulosa dell'appartenenza*, cit.,14.
[123] *Ibidem*,15.
[124] Così P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione Europea*, Milano, Giuffrè, 2002, 20-21.

parole di altra autorevole voce, il dato sulla persona è un "frammento che rinvia all'interezza del suo essere"[125].

Di là dal definire l'esatta natura giuridica del dato personale, si può rilevare che esso, di fatto, incontra difficoltà di qualificazione giuridica simili a quelle che investono la dimensione corporea e segue vicende analoghe a quelle del corpo e delle sue parti[126].

Anche in questo ambito, infatti, si rileva una contrapposizione tra fautori del modello proprietario, che nel dato colgono un nuovo bene immateriale, e sostenitori del modello dei diritti della personalità, secondo cui il diritto alla protezione dei dati personali rientrerebbe nell'alveo dei diritti della persona, con la prevalenza, dunque, di una concezione dinamica, relazionale e procedimentale, piuttosto che statica, del diritto in questione[127].

In particolare, gli assertori del modello proprietario sostengono che, a fronte della crescente mercificazione delle informazioni personali, una maggiore tutela si potrebbe concretizzare solamente riconoscendo il diritto di proprietà sui propri dati.

---

[125] Così A. PUNZI, *La persona nei dati. Ragioni e modelli di una regolamentazione*, in V. CUFFARO, R. D'ORAZIO , V. RICCIUTO (a cura di), *Il Codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 773.

[126] A tal proposito, si è detto: "*Several of the arguments mentioned in the debates on the appropriation of human body parts, as well as an individual's personality, will be encountered […] in the analysis of establishing a property right in a person's data*", C. PRINS, *When personal data, behaviour and virtual identities become a commodity: would a property rights approach matter?*, in 3 *SCRIPT-ed* (2006), 287. Queste difficoltà sono state, inoltre, chiaramente sottolineate da G. P. Cirillo, per il quale "[…] le informazioni personali non sono assimilabili alle cose del mondo fisico diverse dalla persona. Al tempo stesso non sono neppure una parte di questa, né sono un prodotto volontario e consapevole dell'ingegno umano o della capacità d'invenzione dell'uomo. Tuttavia prende in sé un po' di tutto questo, proiettandone così la nozione la disciplina e la tutela in un quadro particolarmente complesso", G. P. CIRILLO (a cura di), *Il Codice sulla protezione dei dati personali*, Milano, Giuffrè, 2004, 7.

[127] Per la natura relazionale del diritto alla protezione dei dati personali, si veda M. MESSINA, *I diritti dell'interessato*, in F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, Giuffrè, 2004, 71, ove l'a. precisa che il governo sulle proprie informazioni viene esercitato "alla luce delle ragioni di chi le tratta o ha bisogno di trattarle". In altri termini, il diritto al controllo dei propri dati non è assoluto, poiché va bilanciato con il contrapposto interesse di chi li tratta, che viene riconosciuto con maggiore o minore intensità a seconda del tipo di dato ovvero delle finalità perseguite, E. BARGELLI, Commento art. 7, in C. M. BIANCA, F. D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, I, Padova, Cedam, 2007, 138.

Questa posizione è stata criticata da più parti[128].

Anzitutto, prendendo le mosse dalla stessa nozione di proprietà che, non essendo una qualità intrinseca degli oggetti, quanto piuttosto una costruzione sociale, non può costituire una garanzia assoluta di tutela.

Un'altra rilevante obiezione nasce dalla considerazione che la prospettiva proprietaria risulterebbe eccessivamente gravosa, sotto il profilo economico nonché temporale, se applicata al campo delle informazioni.

Si porrebbe, invero, anche il problema di stabilire se tutti i dati personali siano suscettibili di ricadere nell'alveo del modello proprietario, o se, piuttosto, ve ne siano alcuni che, per le loro caratteristiche, vadano sottratti a determinate utilizzazioni.

Senza dimenticare, inoltre, che, per alcuni dati, sarebbe ben difficile designare un solo legittimo proprietario, come nel caso dei dati genetici, ove una pluralità di soggetti ha titolo per rivendicare tale diritto.

La prospettiva proprietaria rivela altresì la propria inadeguatezza se si considera che il dato personale, così come il corpo e le sue parti, appare sempre più destinato a

---

[128] Così C. PRINS, *When personal data, behaviour and virtual identities become a commodity: would a property rights approach matter?*, cit., spec. pp. 277-280 e 291-296.
Nell'ambito della dottrina italiana, per la più ampia questione del superamento della logica proprietaria, si veda G. RESTA, *Il diritto alla protezione dei dati personali*, in F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH (a cura di), *Il codice dei dati personali. Temi e problemi*, cit., 23. L'a. ritiene che "una lettura prettamente proprietaria del diritto alla protezione dei dati personali non riuscirebbe a spiegare numerose regole dettate nel testo unico. Basti soltanto osservare che uno dei corollari più rilavanti dell'impostazione dominicale è rappresentato dall'affermazione dell'alienabilità del diritto" (p. 21). Il Codice, in tema di dati sensibili (art. 26) e semisensibili (art. 17), pone al contrario la regola dell'inalienabilità, inoltre il soggetto può, per qualunque tipo di dato, interrompere il trattamento per motivi legittimi (art. 7), "così sconfessando uno dei postulati fondamentali della logica traslativa" (p. 22). Ancora, rigettando la lettura proprietaria, si può considerare che non si tratta di "una situazione di appartenenza esclusiva sui beni (immateriali), intangibile senza il consenso dell'interessato", poiché la regola del consenso incontra numerosi limiti (cfr. artt. 23, 26 e 75 del Codice); inoltre, alla base dell'intera disciplina vi è, come si vedrà, la regola del bilanciamento degli interessi, che "si distacca dalla logica della delimitazione *a priori* delle sfere dei soggetti coinvolti", E. BARGELLI, Commento art. 7, cit., 135-136. Per la contrapposizione tra i due modelli, si consideri anche G. P. CIRILLO (a cura di), *Il Codice sulla protezione dei dati personali*, cit., spec. pp. 4-7, ove, in particolare, si è negato che con il diritto alla protezione dei dati personali si intenda indicare un diritto dominicale sui dati personali, in quanto questa ipotesi sarebbe "riduttiva e non conforme al sistema generale, che invece tiene conto sia della peculiarità dell'«informazione personale», non assimilabile «tout court» agli altri beni suscettibili di appropriazione" e poiché "espressamente il legislatore colloca tale diritto tra i diritti fondamentali della persona, il che comporta una forma di tutela che è propria dei diritti della persona" (p. 4).

configurarsi come luogo e proiezione dell'identità, dunque legato, *per definizione*, all'identità stessa del soggetto [129].

In questo senso, si è espresso anche lo *European Group on Ethics in Science and New Technologies (EGE)*, dichiarando, in un rapporto sui diritti dei cittadini in relazione alle nuove tecnologie, che "*personal data are part of the identity of the individual*"[130].

4. (*Segue*) La duplice anima del diritto all'identità personale.

Si è più volte accennato al legame che intercorre tra corpo e identità, e tra dato personale e identità. Il diritto all'identità sembra, dunque, oscillare tra due poli, due cerchi distinti, ma che si intersecano tra di loro: quello dell'essere, legato al *soma*, e quello dell'apparire, che attiene, invece, alla proiezione esterna del sé, nella forma di dato o di informazione[131]. Questa duplice anima del diritto all'identità personale conferma, ad un tempo, l'irriducibilità sia del corpo che dell'informazione a semplice *res*, e la loro connessione.

---

[129] Per la qualificazione in termini identitari, si veda, anzitutto, il saggio di A. PUNZI, *La persona nei dati. Ragioni e modelli di una regolamentazione*, cit., 761-775, ove ricorre costantemente la concezione del dato come traccia, impronta, segno, che raccoglie un frammento dell'identità dell'interessato (spec. p. 765). Ancora, F. OLIVO, *Dati personali e situazioni giuridiche soggettive*, in *Giust. civ.*, 2002, II, spec. pp. 162-169, ove si rinviene l'immagine del dato come "proiezione dell'identità" (p. 162). La tesi è stata sostenuta anche da C. PRINS, *When personal data, behaviour and virtual identities become a commodity: would a property rights approach matter?*, cit., spec. pp. 299-302, per la quale il modello proprietario introdurrebbe nientemeno che una "*commodification of identities*".

[130] EGE, *Citizen rights and new technologies: a European challenge. Report of the European Group on Ethics in Science and New Technologies on the Charter on Fundamental Rights related to technological innovation as requested by President Prodi on February 3, 2000*, Brussels, May 23, 2000, in *http://ec.europa.eu/european_group_ethics/docs/prodi_en.pdf*, 26.

[131] Circa l'approccio giuridico all'identità, si è detto: "Specchio fedele di tutte le incertezze, delle difficoltà ma anche di tutte le possibili aperture, è l'esame del concetto giuridico del diritto all'identità personale, così come si è delineato nell'ordinamento italiano: esso riflette, infatti, le contraddizioni del tempo presente, esprimendo, per un verso, l'aspirazione a conferire sostanzialità alla tutela della persona e, per un altro verso, una qualche difficoltà ad enucleare il contenuto meritevole di tutela", A. DI GIANDOMENICO, *Identità e bioetica*, in T. SERRA (a cura di), *L'identità e le identità*, Torino, Giappichelli, 2003, 45.

La portata assunta dalla nozione di identità risulta, invero, destinata ad allargarsi sempre più[132], a fronte della cospicua invadenza dei processi tecnologici nella dimensione corporea e della raccolta sempre più vasta e pervasiva di informazioni sugli individui[133].

Può considerarsi specchio di tale processo, la recente *Universal Declaration on Bioethics and Human Rights*, ove si dichiara che l'identità personale è comprensiva della dimensione biologica, psicologica, sociale, culturale e spirituale[134].

Esito di questa rinnovata attenzione per le molteplici sfere costitutive della persona è, anzitutto, la valorizzazione della dialettica corpo-identità, che ha messo in luce come la corporeità sia un aspetto fondamentale dell'identità personale[135], tanto che

---

[132] Significativa la sintesi che P. Zatti offre delle molteplici dimensioni dell'identità: "identità genetica, somatica, personale", "identità e identificazione", "identità e salute", "identità e disposizione di sé", "identità e personalità", "identità e individuazione", "identità e differenze", "identità e creatività", "identità e «immagine» sociale", "identità e relazioni contrattuali", P. ZATTI, *Dimensioni ed aspetti dell'identità nel diritto privato attuale*, in *Nuova giur. civ. comm.*, supplemento fasc. 4/2007, 1-9. Interessante altresì il contributo offerto da S. Rodotà, il quale individua quattro paradigmi dell'identità: il paradigma Lepellettier o dell'identificazione; il paradigma Montaigne o della costruzione incessante; il paradigma Zelig o della moltiplicazione; il paradigma Auchan o della riduzione, S. RODOTÀ, *Quattro paradigmi per l'identità*, in *Nuova giur. civ. comm.*, supplemento fasc. 4/2007, pp. 21 ss.

[133] "[…] le forme oggi assunte dalla società dell'informazione chiedono una parziale riscrittura della semantica dell'umanesimo etico e giuridico", A. PUNZI, *La persona nei dati. Ragioni e modelli di una regolamentazione*, cit., 762. Interessanti, al riguardo, le riflessioni condotte dall'a., che parla di "perdita di senso della nozione di identità", di "eclissi dell'identità", che appare come "carattere tipico di quella che potrebbe definirsi società –meglio ancora, per le ragioni che verranno chiarite, comunità- «informazionale»" (p. 763). Di fronte a tale "eclissi", si avverte il rischio di due reazioni regressive, la prima delle quali viene definita "disperazione di voler essere disperatamente se stesso", ed è propria di "chi, alla messa in questione della sua identità indotta dalla comunità informazionale, reagisce con un'ostinata rivendicazione del proprio io-privato, con la pretesa di riscrivere forzosamente i confini del sé, elevando barriere che lo difendano dalla presenza invasiva del «comune»", per cui "ad un'identità privata incapsulata in se stessa, fa così da complemento un'identità pubblica compatta e sospettosa" (p. 765). La seconda, invece, è quella di colui che "rinuncia alla libera e critica formazione del proprio sé, fino addirittura a voler diventare altro-da-sé, trasformandosi in un'altra identità" (p. 766).

[134] UNESCO, *Universal Declaration on Bioethics and Human Rights, 19 October 2005*, secondo cui "*a person's identity includes biological, psychological, social, cultural and spiritual dimensions*".

[135] Si veda G. GAMBINO, *Il corpo de-formato tra cultura diagnostica e "geneticizzazione" della medicina*, in F. D'AGOSTINO (a cura di), *Il corpo deformato. Nuovi percorsi dell'identità personale*, Milano, Giuffrè, 2002, 45, in cui l'a. osserva che si assiste ad "uno spostamento dell'attenzione dai valori costitutivi dell'uomo, tra cui la consapevolezza di una corporeità come dimensione essenziale dell'identità personale, all'impatto psicologico e sociale delle qualità del corpo, che perde così la sua autonomia antropologica ed assiologica, l'in sé e per sé del proprio valore e della propria dignità, per farsi funzionale rispetto ai bisogni indotti dalla società produttiva ed efficientista del nostro tempo".

il corpo è stato definito "luogo biologico dell'espressione dell'identità personale"[136] e "principio d'identità"[137].

Non è un caso che la *Convenzione sui diritti dell'uomo e la biomedicina* abbia come finalità precipua, accanto alla protezione della dignità, la tutela dell'identità dell'essere umano, rivelando così la preoccupazione che gli interventi sul corpo non si traducano in una indebita violazione della dimensione identitaria personale[138].

Nello stesso senso va letto l'art. 3.1 della *Carta dei diritti fondamentali dell'Unione europea* che, nel sancire il diritto all'integrità fisica e psichica con riferimento alle applicazioni della biologia e della medicina, si propone indirettamente di tutelare anche l'identità della persona[139].

La stessa letteratura bioetica e biogiuridica offre numerosi esempi che attestano la centralità di questo legame[140].

---

[136] L. PALAZZANI, *Corpo e persona: i percorsi filosofici della bioetica e della biogiuridica*, in F. D'AGOSTINO (a cura di), *Il corpo de-formato, nuovi percorsi dell'identità personale*, cit., 145; si veda anche D. MESSINETTI, *Identità personale e processi regolativi della disposizione del corpo,* in *Riv. crit. dir. priv.*, 1995, 200, per il quale: "L'idea di identità mantiene un rapporto con il proprio essere, rappresentato dal corpo come unità degli elementi esistenziali".

[137] A. FILIPPONIO, *Il corpo: principio d'identità. Un'introduzione* in F. D'AGOSTINO (a cura di), *Il corpo de-formato, nuovi percorsi dell'identità personale*, cit., 97-100.

[138] "Le Parti di cui alla presente convenzione proteggono l'essere umano nella sua dignità e nella sua identità e garantiscono ad ogni persona, senza discriminazioni, il rispetto della sua integrità e dei suoi altri diritti e libertà fondamentali riguardo alle applicazioni della biologia e della medicina" (art. 1), CONSIGLIO D'EUROPA, *Convenzione per la protezione dei diritti dell'uomo e la dignità dell'essere umano riguardo alle applicazioni della biologia e della medicina*.

[139] Si è detto che "l'oggetto tutelato dall'articolo 3.1, finisce per coincidere con il diritto all'identità di ogni individuo, cioè la pretesa di ogni individuo a svolgere la propria identità diversa e unica senza danneggiare gli altri, e in ciò si conferma ulteriormente la sua innovatività rispetto ai tradizionali cataloghi di diritti fondamentali", R. BIFULCO, *Dignità umana e integrità genetica nella Carta dei diritti fondamentali dell'Unione Europea*, in *Bioetica*, 2003, 466.

[140] Si ricordano, a questo riguardo, il caso di allotrapianto di mano avvenuto a Lione nel settembre del 1998. Il paziente, che dichiarò: "*I've become mentally detached from it*" - D. DICKENSON, G. WIDDERSHOVEN, *Ethical Issues in Limb Transplants*, in 15 *Bioethics* (2001), 111 -, non accettò il nuovo arto e la mano, dopo tre anni, venne rimossa, proprio in ragione del peculiare legame con l'identità del soggetto, A. GRANELLI CASTIGLIONE, M. PAGANELLI, A. BRAIDOTTI, F. VENTURA, *Riflessioni bioetiche circa il trapianto di mano*, in *Medicina e Morale*, 2005, 790; significativi altresì i casi in cui il soggetto chiede una menomazione della propria integrità fisica per percepire una parte del proprio corpo come «sbagliata», soffrendo di disturbo dismorfico, a causa del quale sussiste uno scarto tra identità psicologica e identità corporea, P. FUNGHI, F. GIUNTA (a cura di), *Medicina, bioetica e diritto. I problemi e la loro dimensione normativa*, Pisa, Edizioni ETS, 2005, 132 ss.; T. BAYNE, N. LEVY, *Amputees by Choice: Body Integrity Identity Disorder and the Ethics of Amputation*, in 22 *J. Appl. Philos*. (2005), 75-86; in tema di mutilazioni genitali ricorre spesso il rapporto tra identità e corporeità, COMITATO NAZIONALE PER LA BIOETICA, *Problemi bioetici in una società multietnica. La circoncisione: profili bioetici*, 1998; A.

In verità, ancor prima del corpo, è il genoma a rappresentare il nucleo biologico fondamentale dell'identità umana, per cui si è affermato, grazie soprattutto alla produzione normativa di alcuni organismi internazionali[141], un vero e proprio diritto all'identità genetica, quale diritto a possedere un patrimonio genetico non alterato, riconosciuto in alcuni Stati anche a livello costituzionale[142].

Una particolare specie di violazione del diritto all'identità così inteso è rappresentata dalla clonazione umana, che "solleva problemi attinenti alla tutela dell'identità-diversità delle persone singole, e alla legittimità della sostituzione ad esse di un'identità-uguaglianza"[143].

Il diritto ad essere se stessi[144] rileva, in questo modo, sotto il primo profilo indicato, che può essere definito ontologico, ove l'identità si configura come "intrinseca qualità del soggetto"[145], cosicché ogni intervento sulla propria dimensione fisica incide sul libero sviluppo, sulla libera costruzione e sulla percezione della propria identità.

VITALONE, *Mutilazione genitale femminile e diritti umani*, in *Giur. merito*, 2001, spec. p. 870; anche i casi di interventi di chirurgia estetica volti a correggere specifiche malformazioni, come gli interventi correttivi nei minori Down, sono stati letti in chiave di alterazione dell'identità biopsichica del soggetto coinvolto, R. GADDINI, *Alterazioni, corpo e identità* in F. D'AGOSTINO (a cura di), *Il corpo de-formato, nuovi percorsi dell'identità personale*, cit., 101-111.

[141] Il diritto all'identità genetica trova espresso riconoscimento nell'art. 3 dell'*International Declaration on Human Genetic Data (16 October 2003)*, UNESCO INTERNATIONAL BIOETHICS COMMITTEE, e nell'art. 1 del *Working document on the applications of genetics for health purposes (7 February 2003)*, COUNCIL OF EUROPE, WORKING PARTY ON HUMAN GENETICS.

[142] Tale diritto viene esplicitamente riconosciuto dalla Costituzione portoghese, che all'art. 26, comma 2°, dispone: "La legge garantisce la dignità personale e l'identità genetica…", e dalla Costituzione greca, all'art. 5, comma 5°, ove si dichiara che "ognuno ha il diritto alla tutela della salute e dell'identità genetica", R. CRISCUOLI, *La biomedicina ed il principio di identità genetica nel diritto europeo*, in *Nuove Autonomie*, 2002, 675 ss.

[143] S. STAMMATI, *Costituzione, clonazione umana, identità genetica*, in *Giur. cost.*, 1999, 4083. Sul rapporto tra clonazione e diritto all'identità genetica, si vedano inoltre, *ex multis*, G. PAESANO, *Clonazione umana e diritto all'identità*, in *Dir. fam. e pers.*, 2004, spec. pp. 584 ss.; S. FILIPPI, *La clonazione umana e il diritto alla propria identità genetica*, in *Arch. giur.*, fasc. IV, 2001, spec. p. 520 s.; M. GALDI, *Profili costituzionali della clonazione umana*, in *Dir. e giur.*, 2001, 69-87; F. INTRONA, C. MAZZAROLO, *Manipolazione genetica, procreazione assistita, clonazione umana (ed altro ancora): il silenzio del legislatore italiano ed il codice penale spagnolo del 1995*, in *Riv. it. med. leg.*, 2001, 953-981; A. BOMPIANI, *La clonazione: considerazioni sulle normative internazionali*, in *Medicina e Morale*, 1998, 581-599.

[144] A. PIRAINO LETO, *Il diritto ad essere se stessi*, in *Dir. fam. e pers.*, 1990, 601-606.

[145] In questa accezione, "si ha riguardo esclusivo alla persona, in quanto tale, cioè individualmente considerata, e l'identità è rappresentata come un vero e proprio diritto personalissimo, il cui contenuto è delimitato appunto dall'avere il soggetto caratteri propri, che lo rendono diverso dagli altri ed identico

Invero, già nella sua accezione originaria, il concetto di identità personale esprime lo stretto rapporto che intercorre tra corpo e identità, benché in una prospettiva nettamente dissimile rispetto a quella sopra indicata. Nelle prime formulazioni, tale nozione indica infatti l'interesse, di carattere prettamente pubblicistico, che un soggetto sia individuabile, identificabile e distinguibile dagli altri, dal punto di vista anagrafico o fisico[146].

Nella seconda è più tradizionale accezione, invece, il diritto all'identità personale assume rilevanza non tanto sotto il profilo dell'"essere", quanto dell'"apparire", del "venire rappresentato", del "venire conosciuto"[147], affermandosi, secondo l'autorevole definizione della Corte di Cassazione, come interesse del soggetto ad "essere rappresentato, nella vita di relazione, con la sua vera identità, così come questa nella realtà sociale, generale o particolare, è conosciuta o poteva essere conosciuta", ossia come "interesse a non vedersi all'esterno alterato, travisato, offuscato, contestato il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale, ecc. quale si era estrinsecato od appariva, in base a circostanze concrete ed univoche, destinato ad estrinsecarsi nell'ambiente sociale", il cui fondamento viene individuato nell'art. 2 e nell'art. 3, comma 2, della Costituzione[148].

---

solamente a se stesso", V. BAVETTA, voce «Identità (diritto alla)», in *Enc. del dir.*, XIX, Giuffrè, 1970, 953.

[146] G. PINO, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, Il Mulino, 2003, 32-34; 43.

[147] Per una trattazione completa del diritto in questione nella sua accezione tradizionale, delle posizioni dottrinali e dell'evoluzione giurisprudenziale, si vedano, *ex multis*, G. PINO, *op. cit.*; V. ZENO-ZENCOVICH, voce «Identità personale», nel *Digesto IV ed., Disc. priv., sez. civ.*, IX, Utet, 1993, 294-303; A. CERRI, voce «Identità personale», in *Enc. giur. Treccani*, 1995, 1-8; G. CASSANO, *Il diritto all'identità personale*, in *Nuova giur. civ. comm.*, 1997, II, 351-370; M. DOGLIOTTI, *L'identità personale*, nel *Trattato Rescigno*, II, 1, Utet, 1999, 145-184.

[148] CASS., sez. I civ., 22.6.1985, n. 3769, in *Foro it.*, 1985, I, 2211, con nota di R. PARDOLESI. La sentenza del Supremo Collegio non fa altro che avvallare l'attività interpretativa della giurisprudenza che, a partire dalla prima metà degli anni '70, con la pronunzia della Pretura di Roma del 6 maggio 1974, in *Giur. it*, 1975, I, 2, 514-519, si era espressa nel senso della autonomia del diritto all'identità personale. Sono due ordinanze della Pretura di Roma del 2 giugno 1980 a individuare il fondamento del diritto in questione nell'art. 2 Cost., PRET. ROMA, ord. 2.6.1980 e ord. 30.5.1980, in *Foro it.*, 1980, I, 2047-2058, fondamento

L'esplicito riconoscimento legislativo avviene, tuttavia, molto tempo dopo la sua comparsa nel panorama giurisprudenziale, prima con la legge n. 675 del 1996, e successivamente con il Codice sul trattamento dei dati personali, il quale "garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali" (art. 2).

Il legame così istituito tra la tutela dei dati personali e il diritto all'identità è assai significativo poiché, sottolineando il valore dell'identità nella sua accezione di rappresentazione[149], evidenzia come esso si configuri sempre più nei termini di un potere di controllo da parte del soggetto sul dato o sull'informazione che lo riguarda[150], essendo "*cifra* che rinvia alla sua identità"[151].

In ragione di ciò, il legislatore ha fornito gli strumenti affinché l'individuo possa esercitare una "continua ripresa sul proprio sé"[152], come il diritto all'informazione e al

---

ribadito dalla citata sentenza della Corte di Cassazione, nonostante alcune incongruenze nella motivazione, per le quali si veda G. PINO, *op. cit.*, 86 ss. Sull'identità personale interviene con più pronunce anche la Corte Costituzionale, che conferma si tratta del "diritto ad essere se stesso, inteso come rispetto dell'immagine di partecipe della vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo", CORTE COST., 3.2.1994, n. 13, in *Foro it.*, 1994, I, 2, 1670. Di particolare rilievo, il problema dell'interpretazione dell'art. 2 Cost. quale norma a fattispecie aperta oppure chiusa, G. PINO, *op. cit.* 175 ss., G. CASSANO, *Il diritto all'identità personale*, cit., 355 ss.

[149] L'importanza del riconoscimento legislativo del diritto all'identità all'interno della normativa in tema di protezione dei dati personali è stata sottolineata da S. Rodotà, il quale indica tre aspetti significativi di tale scelta innovativa, che rappresenta "un consapevole ampliamento della disciplina, visto che il riferimento all'identità non è riproduttivo di quanto previsto dalla direttiva europea 95/46, di cui la legge del 1996 costituisce la trasposizione nell'ordine interno; come una collocazione dell'identità del quadro «dei diritti e delle libertà fondamentali (…) con particolare riferimento (…) all'identità personale» (art. 1 l. n. 675/1996; art. 2, comma 1°, d. legis. N. 196/2003); come criterio interpretativo della normativa sulla protezione dei dati personali nel suo complesso", concludendo: "Il rapporto stretto, che viene così istituito tra identità e tutela dei dati personali, fa emergere con nettezza l'identità come «rappresentazione»", S. RODOTÀ, *Quattro paradigmi per l'identità*, cit., 27.

[150] V. ZENO-ZENCOVICH, voce «Identità personale», cit., 301.

[151] A. PUNZI, *La persona nei dati. Ragioni e modelli di una regolamentazione*, cit., 768, ove l'a. evidenzia la natura del dato quale "segno che l'individuo, volontariamente o meno, imprime nello spazio materiale e immateriale e che altri abitanti del medesimo spazio possono raccogliere e utilizzare. Il dato, infatti, è come un'impronta lasciata dal cammino dell'individuo, una traccia che dice qualcosa del suo autore, senza, però, poterlo rappresentare nella sua integralità. E ciò non soltanto perché il dato riguarda un frammento della sua identità (un atto, un fatto, un detto, anziché l'interezza del suo agire, fare, dire)".

[152] *Ibidem*, 775.

consenso sulla raccolta e sul trattamento dei propri dati, il diritto di accedere ad essi, di chiederne la rettifica oppure la cancellazione[153].

Il diffondersi di banche dati ha determinato, tuttavia, una sorta di frammentazione dell'immagine unitaria della persona, e conseguentemente della sua identità, che viene dislocata in una pluralità di luoghi, facendone una realtà dispersa e inconoscibile[154].

Ciò avviene non solo da un punto di vista diacronico, bensì anche sincronico[155], cosicché l'identità non può più considerarsi come dato costante e immutabile nello spazio e nel tempo, bensì appare "come *processo*, costantemente in atto, aperto ad una pluralità di esiti e continuamente esposto all'interferenza, capillare e pervasiva, delle varie forme di potere sociale"[156].

---

[153] In altri termini: "L'io dev'essere riconosciuto dall'altro per ciò che effettivamente è e nel modo in cui si dà al mondo, deve poi potersi ritrovare nei dati che lo riguardano. Il che presuppone anche che sia posto in condizione di sapere quali frammenti della sua identità sono stati raccolti ed eventualmente registrati (art. 7.1), come sono stati ricavati e quale uso se ne vuole fare (art. 7.2), così da poter verificare l'adeguatezza e la pertinenza nel rapporto tra dati raccolti e obiettivi perseguiti ed eventualmente valutare l'opportunità di ritirare il consenso già espresso di trattamento dei dati medesimi (diritto di uscita)", A. PUNZI, *La persona nei dati. Ragioni e modelli di una regolamentazione*, cit., 773.

[154] S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, ove l'a. dichiara: "Nelle diverse banche dati, infatti, si hanno rappresentazioni della persona perfettamente funzionali alle finalità di ciascuna raccolta, ma che possono dare un'immagine profondamente distorta della persona se, ad esempio, questa viene unicamente presentata per le sue propensioni al consumo o per il suo traffico telefonico o per i siti frequentati in internet, e via dicendo" (p. 605), cosicché "è il fatto che quei dati rappresentano una parte soltanto dell'individualità complessiva di un soggetto a determinare una decontestualizzazione rispetto all'integralità della persona" (p. 606). Riguardo al concetto di "identità dispersa", si veda ancora S. RODOTÀ, *La privacy secondo l'Europa*, in *Le Scienze*, novembre 2008, n. 483, 65.

[155] Il problema dell'"unità" è centrale in tema di identità: "L'assunzione di molteplici identità non è possibile solo nella dimensione *diacronica*, nel corso dei diversi momenti della giornata, ricoprendo diversi ruoli, corrispondenti a diverse funzioni. Ora le diverse identità possono essere assunte anche *sincronicamente*, manifestarsi tutte nello stesso istante grazie all'ubiqua presenza in luoghi diversi della rete", S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma, Laterza, 1997, 143. Sullo stesso punto si veda anche L. LOMBARDI VALLAURI, *Identità, Identificazioni*, in *Nuova giur. civ. comm.*, supplemento fasc. 4/2007, il quale afferma: "[…] io ero cattolico, carnivoro, europeo adesso sono non cattolico, vegetariano, uomo dell'intersezione Oriente-Occidente; chi era costui, quel Luigi di quarant'anni fa? Quale dei due Luigi sono io?" (p. 14). Diversamente, l'unità sincronica comporta che "in uno stesso istante tutte queste strane componenti, queste schegge impazzite, sono unificate dall'attrattore strano detto io, che tutte se le attribuisce e che di tutte dice mio".

[156] Così G. RESTA, *Identità personale, identità digitale*, in *Dir. inf.*, 2007, 524.

Dal tradizionale diritto all'identità personale come potere di esigere una *corretta rappresentazione* di sé, si perviene così ad una nuova e più attuale specificazione, volta a tutelare la *rappresentazione integrale* della propria identità e, ad un tempo, a contrastare la riduzione della persona alle sole informazioni che la riguardano trattate in forme automatizzate[157].

5. L'integrità e le integrità.

Il concetto di integrità, così come quello di identità, è estremamente complesso e merita un'attenta rilettura[158], benché la scienza giuridica lo abbia considerato per lungo tempo nella sola accezione anatomico-funzionale, ovvero come interezza o conservazione della sfera corporea e capacità di svolgere tutte le funzioni ad essa correlate[159].

All'interno di questa univoca concezione, tale nozione risentiva dell'influsso interpretativo di diverse correnti filosofiche e ideologiche, con immediate ricadute sul piano della disponibilità stessa da parte del soggetto del bene in questione.

---

[157] S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali,* cit., 606. Ugualmente, A. PUNZI sottolinea il diritto inviolabile di ciascuno sia "a non essere ridotto a (conosciuto come) materiale informazionale liberamente disponibile", sia "ad essere rispettato nella sua integralità *attraverso* l'uso del dato", A. PUNZI, *La persona nei dati. Ragioni e modelli di una regolamentazione*, cit., 773. Di fronte a questo quadro di disintegrazione dell'io e dell'identità, potrebbe cogliersi tuttavia una sorta di appello rivolto all'uomo moderno a radicarsi in se stesso, a ritrovare e ricostituire in sé quel nucleo di unità di cui la realtà minaccia costantemente di privarlo. In questo senso, si veda ancora A. PUNZI: "Il *proprium*, infatti, non è un luogo definito da confini, ma innanzitutto un rapporto: è la capacità dell'io di ritrovare se stesso muovendo dall'essersi dato al mondo, di ritornare al nucleo più intimo (indiviso) della propria individualità attraverso e oltre il proprio essersi diviso in frammenti distribuiti nel mondo" (p. 769).

[158] Si è osservato come l'art. 5 cod. civ., che di tale concetto fa menzione, sia una delle disposizioni "più controverse e tormentate" del Codice, tanto che "l'unica cosa certa è l'incertezza che regna", R. ROMBOLI, *Delle persone fisiche*, cit., 225.

[159] Secondo questa prima e più comune concezione, "l'integrità fisica consiste nella disponibilità di tutti gli organi, e nello svolgimento di tutte le funzioni", G. GEMMA, voce «Integrità fisica», nel *Digesto pubbl.*, VIII, Utet, 1993, 451, ovvero come "assenza di malattie o di menomazioni fisiche", R. ROMBOLI, *op. ult. cit.*, 230.

Tra le più note, si ricordano, anzitutto, la dottrina, oramai superata, autoritario-collettivistica, che considera l'integrità dell'individuo come funzionale agli interessi dello Stato, il quale può arrogarsi il diritto di disporne a fini sociali, limitando massimamente l'autodeterminazione del singolo; il personalismo protettivo che, malgrado non intenda l'individuo come strumentale all'interesse pubblico, ritiene tuttavia opportuno, in limitate ipotesi, l'intervento dello Stato, al fine di impedire un "cattivo uso del corpo che abbia conseguenze gravi di ordine fisico o morale per l'interessato"; un'ultima corrente, infine, è il personalismo liberale, che considera lecite le restrizioni alla libertà individuale sulla propria sfera fisica esclusivamente in nome della tutela di interessi di terzi[160].

È il superamento della visione dualistica dell'uomo a consentire al bene dell'integrità di uscire dalla strette maglie della dimensione materiale, per includere la sfera psichica dell'uomo, favorendo l'emergere del concetto di integrità psicofisica, come "modo di essere fisico dell'individuo umano, consistente nell'integrità del suo organismo naturale, considerato nel suo aspetto così anatomico come fisiologico e altresì psichico"[161]. Sembra chiaro, infatti, che l'approccio all'integrità può risultare più

[160] G. GEMMA, voce «Integrità fisica», cit., 454-455. Al riguardo, si veda anche R. ROMBOLI, *op. ult. cit.*, 241, per il quale, nell'ipotesi di contrasto tra i due principi costituzionalmente tutelati di integrità fisica e di libertà di autodeterminarsi in ordine a scelte che riguardano il proprio corpo, si deve "dare la prevalenza alla libertà, in quanto la soluzione opposta, allorché gli effetti dell'atto si esauriscono nella sfera soggettiva dell'agente, senza quindi toccare gli altri componenti la comunità, potrebbe essere giustificata solamente in un ordinamento che avesse accolto il principio utilitaristico o quanto meno quello di uno Stato paternalistico, in base ai quali l'integrità fisica è comunque indisponibile perché condizione per il godimento di beni ancorché rifiutati dall'interessato e per lo svolgimento di attività e di funzioni di interesse pubblico e la persona è quindi vista come necessariamente soggetta agli interessi superiori dello Stato".

[161] A. DE CUPIS, voce «Integrità fisica (diritto alla)», in *Enc. giur. Treccani*, XVII, Ed. Enc. it., 1989, 1, ove l'a. afferma che "anche la sanità psichica è un elemento dell'integrità dell'organismo naturale umano: supporto del corpo umano è la psiche che lo dirige e lo controlla, talchè l'alterazione peggiorativa della psiche compromette l'equilibrio complessivo dell'essere fisico dell'uomo". Si veda, a questo riguardo, il significativo contributo di P. PERLINGIERI, *La tutela giuridica della «integrità psichica» (a proposito delle psicoterapie),* in *Riv. trim. dir. e proc. civ.*, 1972, 2, 764, ove l'a. sostiene che è tempo di "non limitarsi a considerare il bene dell'«integrità fisica», ma a sottolineare l'importanza e la sacertà del valore umano, socio-culturale, esistenziale dell'«integrità psichica»". Di avviso contrario è G. GEMMA, voce «Integrità fisica», cit., 451-452, per il quale: "Pur sussistendo nessi stretti fra la componente fisica e quella psichica, non sembra dubbio che si tratti di nozioni diverse nel senso comune. Basti pensare che, mentre l'integrità fisica è menomata da fattori, che pur manifestandosi di frequente, sono purtuttavia

o meno restrittivo a seconda della nozione di corpo assunta, per cui quanto più essa è ampia e comprensiva, tanto più variegata sarà la configurazione del diritto in questione[162].

L'art. 5 cod. civ., pertanto, si rivela norma posta a tutela non solo della dimensione fisica dell'uomo, bensì della persona nel suo complesso, e dunque si mostra "espressione di un principio generale, operante anche in tema d'integrità psichica"[163]. La stessa *Carta dei diritti fondamentali dell'Unione europea*, come si è più volte ricordato, sancisce espressamente il "diritto alla propria integrità fisica e psichica" (art. 3.1)[164], e lo include nel più ampio "diritto all'integrità della persona", stabilendo il rispetto di quattro principi ad esso correlati: consenso libero e informato, divieto di pratiche eugenetiche, divieto di fare del corpo umano oggetto di lucro, divieto di clonazione riproduttiva.

A ben vedere, tuttavia, la lettura del concetto di integrità come sola intangibilità della sfera psicofisica non pare più sufficiente. In particolare, alla luce della riflessione in atto sui principi etico-giuridici che sono alla base della bioetica e del biodiritto nel

---

eccezionali, l'integrità psichica è un parametro ideale, in quanto essa è menomata da tante contrarietà quotidiane e la sua sussistenza costituisce, a ben vedere, non la norma, ma l'eccezione nel tempo di vita del complesso degli individui".

[162] A questo proposito, una innovativa e interessante teoria in tema di integrità è la c.d. *human information integrity*, per cui l'integrità consiste nell'unitarietà dei "sistemi di informazione naturali" di cui l'essere umano è costituito: il sistema di informazione genetico, sensoriale, percettivo e mentale, YU. M. SERDYUKOV, *Human information integrity*, in 77 *Herald of the Russian Academy of Sciences* (2007), 475.

[163] P. PERLINGIERI, *La tutela giuridica della «integrità psichica» (a proposito delle psicoterapie)*, cit., 768, ove l'a. dichiara: "L'integrità della persona fisica ha invero una sua unitarietà problematica, in quanto unico è il bene e l'interesse protetto: la persona umana. Sia il profilo fisico sia quello psichico costituiscono componenti indivisibili di una struttura umana. Il che comporta che la tutela giuridica di uno di questi profili si traduce nella tutela della persona umana nel suo complesso e che la disciplina in cui consiste la tutela della persona umana è di regola utilizzabile per la tutela di uno dei suoi aspetti. Precisazioni queste che consentono di utilizzare non solo la normativa specifica all'integrità fisica ma anche quella che, prevista a difesa dell'integrità fisica, sia pur sempre ispirata a tutela della persona umana nella sua nozione unitaria".

[164] Commentando questo articolo, si è detto che esso "ha come oggetto precipuo la tutela della integrità fisica e psichica sia nella sua fase di formazione che in quella successiva in cui l'individuo, inteso come unione di fattori fisici e psichici, si è ormai costituito (lo si potrebbe definire «diritto al corpo»)", R. BIFULCO, *Dignità umana e integrità genetica nella Carta dei diritti fondamentali dell'Unione Europea*, cit., 466.

contesto internazionale[165], è possibile cogliere ben cinque diverse declinazioni che tale nozione può assumere[166].

Una prima declinazione, *the health view of integrity*, partendo dal tradizionale concetto di integrità fisica e psichica, identifica il bene integrità con il bene salute, questione dibattuta nell'ambito della dottrina italiana stessa[167]. Una seconda accezione, definita *the integrated-self view of integrity*, vede nel rispetto dell'integrità il rispetto per la persona intesa come un tutto, armonioso e indiviso. Una terza possibile declinazione, *the identity view of integrity*, assume come centrale la nozione di identità, per cui l'integrità di una persona non è altro che l'identità, fisica, mentale, e finanche sociale, in cui si esprime. Un quarto approccio, *the rights view of integrity*, considera il diritto all'integrità come il diritto a che la propria sfera privata sia protetta da intrusioni, identificando così integrità e *privacy*. Infine, in base ad un'ultima accezione, *the human dignity view of integrity* , è teorizzata la coincidenza tra integrità e dignità.

Vi è, pertanto, una pluralità di valori e interessi che si raccolgono sotto il manto del diritto all'integrità fisica, per lo più riconosciuti a livello costituzionale, dalla salute, allo svolgimento e alla realizzazione unitaria della propria persona, dall'identità, nelle sue diverse manifestazioni[168], al rispetto per la sfera privata, alla dignità.

---

[165] Per una trattazione sintetica dei principi, si veda J. D. RENDTORFF, *Basic Ethical Principles in European Bioethics and Biolaw: Autonomy, Dignity, Integrity and Vulnerability – Towards a Foundation of Bioethics and Biolaw*, in 5 *Medicine, Health Care and Philosophy* (2002), 235-244, ove vengono presentati in sintesi i principi etici basilari della bioetica e del biodiritto europei, così come emersi dal BIOMED II *project* "*Basic Ethical Principles in European Bioethics and Biolaw*". Lo scopo del progetto è identificare i principi di rispetto per l'autonomia, la dignità, l'integrità e la vulnerabilità come quattro valori portanti della bioetica e del biodiritto europei.

[166] Così R. FJELLSTROM, *Respect for Persons, Respect for Integrity*, in 8 *Medicine, Health Care and Philosophy* (2005), 233-236.

[167] Sul rapporto tra integrità fisica e salute, si vedano, *ex multis*, per la tesi della distinzione tra le due nozioni, C. M. D'ARRIGO, *Autonomia privata e integrità fisica*, cit., 119 ss., mentre per la tesi della loro assimilazione, A. DE CUPIS, voce «Integrità fisica (diritto alla)», cit., 1-2.

[168] Per quanto riguarda il legame che intercorre tra identità e integrità fisica, un caso emblematico è quello che riguarda atti volti a incidere, spesso irreversibilmente, sul corpo, operati da determinati gruppi etnici o religiosi, con l'intento di affermare la propria identità etnico-religiosa e personale, VENUTI M. C., *Integrità della persona e multietnicità*, cit., ove l'a. afferma: "La consapevole sottoposizione ad un intervento (modificativo, additivo, riduttivo) sul proprio corpo può avere il significato, per la persona che

A ragione, dunque, si è parlato di "«frantumazione» del concetto di integrità fisica"[169], che appare come "formula sintetica e riassuntiva", in cui "ciascun interesse giuridico riferibile all'integrità fisica costituisce un «punto di vista» dal quale il corpo umano viene preso in considerazione dal diritto. E questi «punti di vista» si moltiplicheranno man mano che il soggetto evidenzierà – con atti di autonomia privata - nuovi interessi verso la propria integrità fisica"[170]. È il corpo vivente, come sostrato organico, ad essere la base e il presupposto per realizzare gli interessi che afferiscono alle "sfere superiori" della persona[171].

Tuttavia, a fronte dell'incessante progresso tecnologico che mina sempre più radicalmente le frontiere naturali della corporeità, e contestualmente sta conducendo ad un ripensamento della stessa idea di corpo[172], la nozione di integrità non può più

---

effettua una simile scelta, di (ri)costituire e/o (ri)affermare la propria unità e coesione con il gruppo (etnico/religioso) di appartenenza e di definire in questo modo la propria identità personale" (p. 614).

[169] Si veda C. M. D'ARRIGO, voce «Integrità fisica», cit., 723, che afferma: "La rassegna di valori, in maggior parte dotati di riscontro costituzionale, che possono trovare svolgimento sul piano dell'integrità fisica - e questo catalogo, che già oggi potrebbe non essere esaustivo, è comunque destinato a rinnovarsi ed ampliarsi con il progresso delle tecniche biomediche - deve convincere dell'inesattezza della prospettiva che rimanda ad un unico ed indistinto diritto all'integrità fisica. Si assiste, piuttosto, alla «frantumazione» giuridica del concetto di integrità fisica". In altri termini: "Ciascun interesse giuridico riferibile all'integrità fisica costituisce un «punto di vista» dal quale il corpo umano viene preso in considerazione dal diritto. E questi «punti di vista» si moltiplicheranno man mano che il soggetto evidenzierà –con atti di autonomia privata- nuovi interessi verso la propria integrità fisica" (p. 725). Questa concezione "frantumata" di integrità si rinviene anche in M. C. VENUTI, *Integrità della persona e multietnicità*, cit., 608, ove, riferendosi al problema del rapporto tra integrità fisica e multietnicità, alla luce dell'art. 3 della *Carta dei diritti fondamentali dell'Unione europea*, si sottolinea come "[…] la considerazione del diritto all'integrità della persona e in particolare del potere di autodeterminazione dei singoli in ordine al proprio corpo come esplicazione della personalità di ciascuno, richiede che si coniughi l'analisi dell'art. 3 con altre disposizioni della Carta: in primo luogo con quelle in materia di dignità umana (art. 1), di protezione dei dati di carattere personale (art. 8), di libertà di pensiero, coscienza e religione (art. 10), di non discriminazione (art. 21), di diversità culturale, religiosa e linguistica (art. 22). Tutte infatti sono collegate al profilo dello svolgimento della personalità che può avere incidenza nella sfera fisica (transessualismo, sterilizzazione, orientamenti sessuali), dei criteri in forza dei quali si attribuisce rilevanza ai corrispondenti atti nell'ordinamento europeo (e interno)".

[170] C. M. D'ARRIGO, voce «Integrità fisica», cit., 725, ove l'a. conclude che l'integrità fisica "non deve essere intesa come un concetto statico -nel senso che l'opzione preferibile è quella che tenda solamente alla sua conservazione- bensì come un fenomeno dinamico, che non soltanto deve essere preservato dagli eventi lesivi o peggiorativi ma anche «gestito» per promuovere e per assecondare la realizzazione ed il contemperamento di ogni altro valore direttamente condizionato" (p. 727).

[171] "L'integrità fisica è, quindi, il presupposto organico dei fenomeni delle sfere superiori e, in particolare, di quelli scrivibili al livello tipicamente umano della spiritualità. Tale assetto determina che ogni avvenimento che interessa direttamente l'integrità fisica non può essere privo di ripercussioni –dirette o indirette- anche sui fenomeni afferenti alle classi superiori", *Ibidem*, 726.

[172] Si veda il paragrafo 9 di questo capitolo.

considerarsi "chiusa nei confini dell'antica sua fisicità, al cui rispetto sono state fin'ora riferite le stesse garanzie costituzionali"[173].

Il riferimento è alla raccolta e conservazione di dati e informazioni sugli individui, ad un nuovo corpo che si delinea in maniera sempre meno incarnata e sempre più virtuale, la cui integrità va ugualmente tutelata[174]. Si è detto, pertanto, che, così come avviene per il corpo, anche nel caso dei dati personali, una loro menomazione può incidere sulla sfera dell'integrità psichica e della coscienza, andando a colpire le dimensioni più personali ed intime del soggetto interessato[175].

Accogliendo dunque quella concezione ampia e frammentata di integrità di cui si è detto, inscindibile in particolar modo dai valori della dignità, dell'identità, della riservatezza, l'art. 2.1 del Codice sul trattamento dei dati personali, nel garantire "che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali", pare consacrare anche il diritto all'integrità della "proiezione informazionale" dell'individuo, vale a dire dell'insieme di informazioni che lo riguardano.

6. Consenso, autodeterminazione, identità.

Il principale strumento con cui il soggetto compie delle scelte in ordine alla propria integrità personale è il consenso informato. Non a caso, la *Carta dei diritti*

[173] S. RODOTÀ, *Trasformazioni del corpo*, in *Pol. dir.*, 2006, 22.
[174] "Il riconoscimento della rilevanza della persona, tuttavia, sarebbe incompleto se si limitasse a ribadire, e a collocare nel contesto determinato dall'innovazione scientifica e tecnologica, l'inscindibilità tra corpo e mente, trascurando la dimensione del «corpo elettronico»", S. RODOTÀ, *Dal soggetto alla persona*, Napoli, Editoriale Scientifica, 2007, 35.
[175] Così P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione Europea*, cit., 21.

fondamentali dell'Unione europea, dopo aver enunciato il diritto all'integrità fisica e psichica, pone il consenso al primo posto tra i principi correlati a tale diritto (art. 3.1).

Per comprendere il valore del consenso e dell'autodeterminazione sulla propria persona[176], è necessario, ancora una volta, partire da quella concezione ampia di corporeità di cui si è detto inizialmente, ove cioè il corpo non può essere concepito separatamente dalla persona considerata nel suo complesso[177]. Non si vedrebbe, infatti, alcun motivo per cui il soggetto possa divenire attore, benché non onnipotente[178], in ordine alle scelte che riguardano la propria integrità personale, se non per il fatto che essa non è estranea alla sua stessa dimensione interiore[179].

Contestualmente, appare chiaro che non si può parlare di consenso prescindendo dalla nozione di identità. Il rapporto tra consenso e identità risulta, infatti, a tal punto stringente, che a un autorevole giurista non è sembrato eccessivo affermare che "consentire equivale ad essere"[180].

Tale stretto legame si evince, in primo luogo, nell'ambito delle riflessioni dottrinali e giurisprudenziali in tema di consenso al trattamento diagnostico o terapeutico[181] - quale momento distinto dal consenso al contratto di cura[182] - , ove il

---

[176] M. PICCINNI, *Il consenso al trattamento medico del minore*, cit., 25-26, ove l'a. dichiara che, valorizzando il rapporto corpo-identità, è più corretto parlare di "autodeterminazione *sulla propria persona* oppure di diritto all'autodeterminazione *attraverso le scelte sul proprio corpo*".

[177] "Il carattere unitario della persona e della tutela che ad essa spetta sulla base, appunto, del principio personalistico fa sì che la questione dell'autodeterminazione vada correttamente impostata non in termini di potere di disporre del corpo, ma invece di libertà di decidere, di autodeterminarsi in relazione a scelte che coinvolgono la persona anche nella sua dimensione fisica", G. FERRANDO, *Consenso informato del paziente e responsabilità del medico, principi, problemi e linee di tendenza*, cit., 44.

[178] Come sottolinea M. TALLACCHINI: "Autodeterminazione non significa che gli individui siano esenti da condizionamenti nelle proprie scelte, o che queste non abbiano un carattere contestuale e non siano suscettibili di ulteriori modificazioni; si tratta invece di affermare che le scelte sono espressione di valori e scopi personali che fanno di ogni essere umano un'entità peculiare, e che tale libertà deve essere anche istituzionalmente sostenuta e promossa, poiché incorpora un ideale etico di essere umano", M. TALLACCHINI, *Biotecnologie e consenso informato. Un inizio…*, in *Notizie di Politeia*, 1999, n. 54, 5.

[179] "[…] la persona umana e il corpo che non ne è avulso", CORTE COST., 22.10.1990, n. 471, in *Foro it.*, 1991, I, 15 ss., con nota di, R. ROMBOLI, *I limiti alla libertà di disporre del proprio corpo nel suo aspetto«attivo» e in quello «passivo»*.

[180] S. RODOTÀ, *Dal soggetto alla persona*, cit., 45.

[181] Per quanto riguarda il rapporto tra il consenso informato in ambito medico e la nozione di identità, si vedano, in particolare, le riflessioni di P. ZATTI, per il quale, stante il passaggio della concezione di salute "da standard a vissuto", la questione del consenso diviene evidentemente una questione di identità. L'a.

paziente, nel valutare la proposta del medico, non fa altro che esercitare "una libertà che attiene alla configurazione della propria identità"[183].

Lo stesso può dirsi per quanto riguarda il trattamento dei dati personali[184], dal momento che l'interessato, attraverso il dispositivo del consenso, esercita quello che è stato definito come il potere di autodeterminazione informativa, ovvero il "diritto di

---

afferma così: "Alla radice del problema del consenso sta il nucleo del diritto fondamentale - o piuttosto il viluppo dei diritti fondamentali libertà-identità-salute - che si enuncia nella sua più nitida interezza formulando il principio secondo cui la valutazione del rapporto tra la proposta terapeutica, i relativi benefici e rischi, il benessere possibile, spetta esclusivamente all'interessato come esercizio, non comprimibile né fungibile, della percezione di sé e di una libertà che attiene alla configurazione della propria identità", P. ZATTI, *Il diritto a scegliere la propria salute (in margine al caso S. Raffaele)*, in *Nuova giur. civ. comm.*, II, 2000, 6. Dello stesso avviso E. PALMERINI che, mettendo in luce le molteplici dimensioni e sfumature del consenso, evidenzia come esso possa fungere da "momento propositivo e di scelta in ordine alla cura", "atto impegnativo, fonte di responsabilità per le conseguenze giuridiche che vi si connettono", e "strumento, infine, di affermazione della propria identità", E. PALMERINI, *Le scelte sul corpo: i confini della libertà di decidere*, Consiglio Superiore della Magistratura – Roma, 9-10 giugno 2005, in *http://appinter.csm.it/incontri/relaz/11876.pdf*, 6-7. Infine, in tal senso si esprime anche S. VICIANI, *L'autodeterminazione «informata» del soggetto*, in *Rass. dir. civ.*, 1996, 272-308, che sottolinea l'esigenza del consenso al trattamento medico come condizione perché l'intervento sul soggetto non leda la sua identità (spec. p. 278 e p. 294); infatti, "il riferimento del comportamento del medico ad una finalità informativa è destinato a garantire al soggetto la massima esplicazione della propria identità, attraverso l'affermazione del proprio essere" (p. 290). Nell'ambito della giurisprudenza, invece, un riferimento a tal proposito si rinviene anche nella recente sentenza del Trib. Roma del 15.12.2006 (caso Welby), laddove, in tema di consenso informato, si dichiara: "Il quadro di riferimento dei principi generali si rinviene innanzitutto negli artt. 2, 13 e 32 Cost., ed abbraccia la tutela e promozione dei diritti fondamentali della persona della sua dignità ed identità, della libertà personale e della salute".

[182] Sulla distinzione tra consenso al trattamento e consenso al contratto, si veda, *ex multis*, S. TOMMASI, *Consenso informato e disciplina dell'attività medica*, in *Riv. crit. dir. priv.*, 2003, 556 ss., ove l'a. in particolare sottolinea come "il paziente ha diritto di autodeterminarsi e di esprimere un valido consenso, anche laddove il rapporto professionale con il medico non derivi dal contratto" (p. 557) e come il consenso non venga prestato una volta per tutte, ma possa essere continuamente rinnovato.

[183] P. ZATTI, *Il diritto a scegliere la propria salute (in margine al caso S. Raffaele)*, cit., 6.

[184] "Sotto tale profilo, è evidente la natura autorizzativi del consenso, incidente su ambiti propri del diritto alla personalità individuale, *sub specie* di autodeterminazione informativa come capacità di determinare il destino delle informazioni relative alla propria identità personale. In tal senso, esso costituisce senz'altro atto di esercizio del diritto alla personalità, in quanto, come è stato rilevato, la negazione del consenso costituisce da parte dell'interessato esercizio del diritto di costruire la propria identità personale come identità riservata; viceversa, la prestazione del consenso da parte dell'interessato determina il passaggio da una identità riservata a una identità controllata, nel senso che mediante la predisposizione di condizioni e limiti al trattamento egli è posto in grado di controllare il modo in cui gli altri identificheranno la sua identità. Secondo tale impostazione, la *natura giuridica* di autorizzazione, propria del consenso, deriva – indipendentemente dalla funzione assolta – dalla sua capacità di permettere un'azione (il trattamento) altrimenti vietata in sua assenza, integrando in pieno la figura del consenso dell'avente diritto. Tale natura è altresì confermata da una interpretazione della disciplina vigente", G. P. CIRILLO (a cura di), *Il Codice sulla protezione dei dati personali*, cit., 134. Si consideri attentamente anche la ricca analisi di D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, 339-407, ove ricorre costantemente il rapporto dati personali-identità-consenso, essendo quest'ultimo, nella sua natura autorizzativa, "presupposto e al tempo stesso espressione giuridica del passaggio alla identità controllata" (p. 350).

autodeterminarsi sulle proprie informazioni"[185], il "potere di determinare il circuito informativo"[186], la "decisione selettiva sui flussi delle informazioni"[187], mantenendo un controllo su di esse e definendone il destino, decidendo, in particolare, il se, il quando, il come ed il *quantum* della circolazione dell'informazione. In questo modo, "il consenso ha la funzione di rimuovere il carattere di riservatezza sull'identità personale, permettendo all'interessato di conformare la circolazione delle informazioni in modo da tutelare la propria identità rivelata"[188].

A partire dalla centralità del consenso come facoltà per l'esercizio di un *dominium* della persona su sè medesima oppure sulle proprie informazioni, finalizzato alla costruzione della propria identità personale, la relazione tra il medico e il paziente è stata paragonata alla relazione che intercorre tra l'interessato e colui che tratta i suoi dati, tanto che, in entrambi i casi, si è parlato di "nascita di un «nuovo soggetto morale»", non più soggiogato al potere altrui, ma capace di autodeterminarsi[189].

---

[185] L. STILO, *Il diritto all'autodeterminazione informativa: genesi storica di un diritto fondamentale dell' "HOMO TECNOLOGICUS"*, in *Nuovo dir.*, 2002, 7-8, 23.
[186] S. VICIANI, *L'autodeterminazione «informata» del soggetto*, cit., 278.
[187] R. MESSINETTI, *Pluralità dei circuiti comunicativi e autodeterminazione informativa della persona*, nota a TRIB. PERUGIA, 31.5.2006, n. 709, in *Danno e resp.*, 2007, 695.
[188] G. P. CIRILLO (a cura di), *Il Codice sulla protezione dei dati personali*, cit., 134. Proprio perché atto di natura autorizzativa diretto alla costruzione della propria dimensione identitaria personale, si è detto che il consenso così espresso esula dalla logica negoziale. Si, veda in particolare, D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, cit., 353-354, ove l'a. afferma: "In quanto il fine che l'esercizio del potere tende a realizzare è costituito dalla costruzione della propria sfera personale di identità, si dovrà convenire che, dal punto di vista degli effetti che esso esplica, l'atto non ha natura negoziale. Il soggetto è arbitro degli effetti che interessano e conformano il modo di essere della propria persona in se stessa e, di riflesso, nelle relazioni sociali. Mancando, pertanto, ogni aspetto di relazionalità, è chiaro che non sussiste il presupposto che è necessario perché si possa riconoscere ai comportamenti soggettivi un contenuto dispositivo di carattere negoziale". Sul punto, in rapporto al consenso al trattamento medico, si consideri anche M. GORGONI, *La «stagione» del consenso e dell'informazione: strumenti di realizzazione del diritto alla salute e di quello all'autodeterminazione*, in *Resp. civ. e prev.*, 1999, 496. In realtà, questa teoria è ancora dibattuta tanto nel settore medico, quanto in quello della tutela dei dati personali, ove alcuni considerano il consenso come atto giuridico e altri, invece, appoggiano l'ipotesi negoziale; al riguardo si veda, per i dati personali, S. M. MELONI, *Il trattamento dei dati da parte di soggetti privati: la disciplina del consenso*, 201, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il Codice del trattamento dei dati personali*, cit. A ragione, dunque, si è parlato della sussistenza, nei due ambiti, "del medesimo tormento teorico e della medesima difficoltà di inquadramento sistematico", M. GORGONI, *La «stagione» del consenso e dell'informazione: strumenti di realizzazione del diritto alla salute e di quello all'autodeterminazione*, cit., 497.
[189] S. RODOTÀ, *Dal soggetto alla persona*, cit., 45.

Il legame tra i due diversi settori di rilevanza del consenso appare chiaro se si considera inoltre che la *privacy*, quale ambito "degli atti con cui l'individuo dispone di sé tanto in senso fisico e materiale, quanto in senso simbolico e informazionale", è stato il primo settore ove "si è *naturalmente* esteso" il consenso informato sviluppatosi in campo medico[190], per cui la successiva disciplina legislativa in tema di consenso al trattamento dei dati personali (contenuta prima nella l. 675/1996, poi nel Codice in materia di protezione dei dati personali del 2003) ha concorso a tracciare i caratteri anche del consenso al trattamento medico[191].

7. (*Segue*) Inquadramento dell'istituto del consenso informato.

Per delineare il quadro normativo di riferimento, si dovrà dunque valutare l'evoluzione dell'istituto così come è avvenuta all'interno del rapporto terapeutico, tenendo conto altresì delle interazioni con il settore del trattamento dei dati personali.

Considerato il ruolo di primaria rilevanza assunto dalla *Carta dei diritti fondamentali dell'Unione europea*, è opportuno prendere le mosse da questo testo.

Nella Carta, come già ricordato, è essenziale il richiamo operato dall'art. 3.2, secondo cui nell'ambito biologico e medico merita particolare rispetto "il consenso

[190] M. TALLACHINI, *Biotecnologie e consenso informato. Un inizio…*, cit., 5, c.vo agg.

[191] Si è detto che "nuovo impulso al vecchio ed abusato tema del consenso informato viene, non a caso, proprio dallo studio di settori diversi, rispetto a quello medico, in cui molto si è investito sulla sua portata. Si allude, ad esempio, al trattamento dei dati personali, in cui informazione e consenso dell'interessato (o della persona presso cui i dati sono acquisiti) assumono un ruolo centrale anche se non esaustivo, né enfatizzabile, nella tutela dei diritti fondamentali della persona cui i dati si riferiscono", M. GORGONI, *La «stagione» del consenso e dell'informazione: strumenti di realizzazione del diritto alla salute e di quello all'autodeterminazione*, cit., 495-496. Similmente, G. FERRANDO, *Consenso informato del paziente e responsabilità del medico, principi, problemi e linee di tendenza*, cit., spec. pp. 44-45, che riscontra la "tendenza in atto all'espansione dell'area del consenso ben oltre i suoi confini tradizionali" e la "necessità di una nuova lettura che dalla tradizione prenda le mosse per vagliare tuttavia di questo nuovo fenomeno quei profili che la tradizione non è in grado di abbracciare e governare" (p. 59 nota n. 57). A tal proposito, si vedano, ancora, V. COLONNA, *Il danno da lesione della privacy*, in *Danno e resp.*, 1999, nota 64, p. 33 e M. GORGONI, *La «stagione» del consenso e dell'informazione: strumenti di realizzazione del diritto alla salute e di quello all'autodeterminazione*, cit., 498.

libero e informato della persona interessata, secondo le modalità definite dalla legge"[192]. Oltre a trovare un forte ed esplicito riconoscimento giuridico, il principio viene collocato in una posizione affatto indifferente, dato il collegamento che si viene a stabilire con il diritto all'integrità della persona e con il valore della dignità, di cui il consenso costituisce una significativa concretizzazione[193].

In realtà, ancor prima, è stata la *Convenzione sui diritti dell'uomo e la biomedicina* ad aver solennemente affermato che "un intervento nel campo della salute non può essere effettuato se non dopo che la persona interessata abbia dato consenso libero e informato" (art. 5)[194], malgrado si debba registrare la situazione, indefinibilmente protrattasi, di ritardo in merito all'entrata in vigore della stessa nell'ordinamento giuridico italiano[195].

[192] L'art. 3 tutela il diritto all'integrità della persona, ed è inserito nel capo I, dedicato alla dignità.

[193] Si è detto, relativamente all'art. 3, che "è evidente la sua diretta derivabilità dal valore della dignità e, nel merito, la sua superiorità rispetto agli altri valori espressi dalla Carta. Il rapporto tra art. 3 e art. 1 sulla dignità umana va sottolineato con enfasi perché è in grado di dare vita a un modello costituzionale di bioetica alternativo rispetto a quello nordamericano", R. BIFULCO, *Dignità umana e integrità genetica nella Carta dei diritti fondamentali dell'Unione Europea*, cit., 465.

[194] L'articolo prosegue dichiarando: "Questa persona riceve innanzitutto una informazione adeguata sullo scopo e sulla natura dell'intervento e sulle sue conseguenze e i suoi rischi. La persona interessata può, in qualsiasi momento, liberamente ritirare il proprio consenso". Le norme successive regolano altri aspetti specifici della disciplina del consenso, dalla "Protezione delle persone che non hanno la capacità di dare consenso" (art. 6), alla "Tutela delle persone che soffrono di un disturbo mentale" (art. 7), alle "Situazioni d'urgenza" (art. 8), al caso dei "Desideri precedentemente espressi" (art. 9). È altresì interessante considerare il rapporto tra la Convenzione di Oviedo e la Carta di Nizza, R. BIFULCO, *Dignità umana e integrità genetica nella Carta dei diritti fondamentali dell'Unione Europea*, cit., spec. pp. 454 ss.

[195] Nonostante l'adozione della l. 28.3.2001, n. 145, di ratifica ed esecuzione della Convenzione e nonostante il suo indubbio valore politico e morale, per cui ne è frequente il richiamo all'interno di pronunce giurisprudenziali in tema di trattamenti sanitari – si veda, a titolo di esempio, il richiamo alla Convenzione effettuato nella recente sent. del Trib. Roma, 15.12.2006 (caso Welby) -, il mancato deposito del documento di ratifica presso il Consiglio d'Europa da parte del Governo italiano ha fatto sì che la stessa non sia ancora entrata in vigore per l'Italia, C. CASONATO, *Introduzione al biodiritto. La bioetica nel diritto costituzionale comparato*, Quaderni del Dipartimento di Scienze Giuridiche dell'Università di Trento, n. 57, 2006, 174-175. Per una breve e accurata analisi del problema, si veda anche S. PENASA, *Alla ricerca dell'anello mancante: il deposito dello strumento di ratifica della Convenzione di Oviedo*, in *http://www.forumcostituzionale.it*, ove l'a. dichiara che "la giurisprudenza della Corte costituzionale italiana sembra condividere la necessarietà dell'elemento del deposito dello strumento di ratifica, riconoscendo come, in assenza del deposito a livello di diritto internazionale (andamento 'out→in'), la correlata legge contenente l'ordine di esecuzione deve considerarsi inefficace (andamento 'in →out')".

Significativo, inoltre, il richiamo che si ritrova in numerose carte e raccomandazioni di organismi internazionali, soprattutto nell'ambito della bioetica[196], nonché nel Codice italiano di deontologia medica, ove il consenso informato ha assunto sempre maggiore rilevanza, mettendo in chiara luce il processo di maturazione storica e sociale della relazione tra medico e paziente[197].

A partire dalla l. 23 dicembre 1978, n. 833, istitutiva del Servizio sanitario nazionale, il carattere della volontarietà dei trattamenti sanitari inizia ad essere affermato dallo stesso legislatore italiano[198], per poi divenire principio di riferimento di tutti quegli atti che incidono sulla dimensione corporea individuale, venendo dunque enunciato in numerose leggi speciali relative al corpo[199].

---

[196] Si vedano, *ex multis*, la *Universal declaration on bioethics and human rights*, cit., artt. 5, 6, 7; la *Universal declaration on the human genome and human rights*, UNESCO, 1997, artt. 5, 9; il *Working document on the applications of genetics for health purposes (7 February 2003)*, cit., artt. 6, 7, 8; l' *International declaration on human genetic data*, cit., artt. 8, 9, 10; la *Recommendation 1418 (1999) on the protection of the human rights and dignity of the terminally ill and dying*, COUNCIL OF EUROPE, art. 9.

[197] "Il medico non deve intraprendere attività diagnostica e/o terapeutica senza l'acquisizione del consenso esplicito e informato del paziente" (art. 35, CDM 2006). L'aggiunta dell'aggettivo "esplicito" costituisce una novità rispetto alla precedente versione del 1998, che si limitava a richiedere il carattere "informato". Questa scelta integrativa avvalora l'importanza attribuita all'acquisizione del consenso, che va manifestato in maniera espressa ed evidente. È da rilevare che, mentre le prime versioni del Codice del 1978 e del 1989 avevano una connotazione fortemente paternalistica, nel prevedere il ricorso al consenso solo nei casi in cui l'attività medica comportasse un rischio per il paziente, i successivi Codici del 1995, del 1998, e, per ultimo, il Codice del 2006, hanno ridefinito il ruolo del consenso, attribuendo ad esso notevole importanza (artt. 33-38, CDM del 2006; artt. 30-35, CDM del 1998), G. FACCI, *Il dovere di informazione del sanitario*, in *Nuova giur. civ. comm.*, 2006, II, 558-559. È opportuno altresì precisare che le fonti deontologiche, benché non rientrino nel rango delle tradizionali fonti del diritto, assumono tuttavia un valore non trascurabile, "sia quali elementi di integrazione extranormativa dei concetti di diligenza professionale (e quindi di colpa) e delle clausole generali di correttezza e buona fede, sia quali strumenti ermeneutici idonei alla precisazione di principi generali, come quelli dell'adeguatezza dell'informazione, della libertà del consenso, e in ultima analisi del principio di rispetto dell'autodeterminazione", P. ZATTI, *Il diritto a scegliere la propria salute (in margine al caso S. Raffaele)*, cit., 10.

[198] L'art. 33 prevede anzitutto il requisito della volontarietà per gli accertamenti e trattamenti sanitari, tranne il caso in cui lo Stato possa, a norma dell'art. 32 Cost., intervenire coattivamente. Tuttavia, per i trattamenti sanitari obbligatori, è in ogni caso previsto l'impegno da parte dei sanitari a garantire la partecipazione e il consenso dell'interessato. Si veda, inoltre, la precedente l. 13 maggio 1978 (*Accertamenti e trattamenti sanitari volontari e obbligatori*).

[199] G. FERRANDO, *Consenso informato del paziente e responsabilità del medico, principi, problemi e linee di tendenza*, cit., 39. Si ricordano, *ex multis*, la l. 26.6.1967, n. 458 – *Trapianto di rene tra persone viventi* (art. 2) e la l. 22.5.1978, n. 194 – *Norme per la tutela sociale della maternità e sull'interruzione volontaria di gravidanza* (artt. 2, 14).

Il principio di autodeterminazione trova, nonostante qualche voce dissonante[200], il suo più alto e radicato riconoscimento nella Carta costituzionale, come si evince dal combinato disposto dell'art. 2 Cost., posto a garanzia dei diritti inviolabili dell'uomo[201], dell'art. 13 Cost., che sancisce il diritto alla libertà dell'individuo[202], e dell'art. 32, comma 2°, Cost., laddove, oltre al diniego dei trattamenti sanitari obbligatori al di fuori dei casi previsti dalla legge, si proclama il limite invalicabile del "rispetto della persona umana"[203], che costituisce, come si è osservato, una delle più forti enunciazioni della nostra Costituzione[204].

8. (*Segue*) Il consenso: da implicito a informato e libero.

Senz'altro centrale, sia che si tratti di trattamento medico, sia che si tratti di trattamento di dati personali, è il passaggio del consenso dalla forma implicita, a quella

[200] Di avviso contrario è A. DONATI il quale, per quanto riguarda l'art. 13 Cost., considera eccessivo il richiamo a tale norma, poiché essa sarebbe volta alla tutela del rapporto che intercorre tra lo Stato e i cittadini; in secondo luogo, essendo il codice civile il "codice della libertà", si imporrebbe, prima di ricorrere all'art. 13 Cost., di dimostrare l'impossibilità della tutela civilistica del paziente; infine la libertà personale, se inviolabile, sarebbe indisponibile tanto da parte del titolare, quanto da parte di terzi. Circa l'art. 32, l'a. ritiene che senz'altro "il «diritto al consenso informato» si collochi nell'ampio quadro del «diritto alla salute», ma nulla ha a che vedere con il significato che questa espressione assume nel più ristretto ambito dell'art. 32". Nulla sembra ostare, infine, a derivare la libertà di autodeterminarsi dall'art. 2 Cost., interpretato come norma aperta. Tuttavia, a ben vedere, il consenso informato non possiede i caratteri propri dei diritti fondamentali della persona umana (originarietà, assolutezza, indisponibilità, imprescrittibilità), perciò non può essere ancorato neppure ad esso, A. DONATI, *Consenso informato e responsabilità da prestazione medica*, in *Rass. dir. civ.*, 2000, 1-5.

[201] G. FERRANDO, *Consenso informato del paziente e responsabilità del medico, principi, problemi e linee di tendenza*, cit., 45, "La libertà di autodeterminarsi nelle scelte inerenti alla dimensione fisica della persona discende perciò in primo luogo dal riconoscimento dei diritti inviolabili della persona contenuto nell'art. 2 della Costituzione. La tutela integrale della persona umana che in esso si esprime implica la sua inviolabilità fisica e, ad un tempo, la sua libertà nelle scelte personali".

[202] La stessa Corte Costituzionale ha riconosciuto il "[…] valore costituzionale della inviolabilità della persona costruito, nel precetto di cui all'art. 13, primo comma, della Costituzione, come <libertà>, nella quale è postulata la sfera di esplicazione del potere della persona di disporre del proprio corpo", CORTE COST., 22.10.1990, n. 471, cit.

[203] "Questo potere di autodeterminazione, pur non essendo previsto espressamente dalla Costituzione, troverebbe ugualmente garanzia e previsione nel 2° co. dell'art. 32, laddove per i trattamenti sanitari obbligatori da un lato chiede il rispetto (positivo) della «dignità umana» e, dall'altro, impone i trattamenti sanitari solo nei casi particolari previsti dalla legge a garanzia della salute collettiva", A. SIMONCINI, E. LONGO, nel *Commentario alla Costituzione*, I, Utet, 2006, *sub*. art. 32, 665.

[204] Così S. RODOTÀ, *Dal soggetto alla persona*, cit., 33.

informata, creando le condizioni perché si esplichi l'autodeterminazione del soggetto e, conseguentemente, si affermi la sua identità[205].

L'informazione, a sua volta, rendendo il soggetto consapevole, è presupposto, necessario, ma non sufficiente[206], perché si realizzi il requisito della libertà[207]. Sembrerebbe, dunque, logicamente più corretto il sintagma "consenso informato e libero", benché tanto nelle summenzionate *Carta dei diritti fondamentali dell'Unione europea* (art. 3.2) e *Convenzione sui diritti dell'uomo e la biomedicina* (art. 5), quanto nel Codice sul trattamento dei dati personali (art. 23), l'elemento della libertà preceda, nell'enunciazione, quello dell'informazione[208].

Per quanto riguarda il momento informativo, esso può perseguire finalità diversificate. In base al profilo teleologico, possono essere definiti distinti *standards*, che attengono al contenuto, alla quantità delle informazioni ovvero alla modalità di comunicazione[209]. In ogni caso, essendo la manifestazione del consenso del tutto personale, proprio la "persona interessata" sarà il parametro di riferimento ultimo, in

---

[205] S. RODOTÀ, *Protezione dei dati e circolazione delle informazioni*, in *Riv. crit. dir. priv.*, 1984, 755, ove l'a. evidenzia il passaggio dall'*implied consent* all'*informed consent*.

[206] Come è stato detto, "un consenso può essere molto «informato» e finanche consapevole (e molto spesso, in realtà, a dispetto di ogni previsione e obbligo di legge continua a essere poco o comunque non sufficientemente «informato») e poco libero", L. BOZZI, *Le regole generali per il trattamento dei dati*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il Codice del trattamento dei dati personali*, cit., 92.

[207] La persona va posta nella condizione di "fare scelte libere perché consapevoli, tanto più libere in quanto consapevoli, tanto più consapevoli in quanto compiutamente informate", G. TOSCANO, *Informazione, consenso e responsabilità sanitaria*, Milano, Giuffrè, 2006, 69. In tal senso si veda G. GEMMA, voce «Integrità fisica», cit., 461, per il quale "il consenso, per essere veramente libero, dev'essere consapevole e per essere tale deve avvenire sulla base di adeguate informazioni. Tale configurazione del consenso consapevole, previa informazione, è, a ben vedere, una proiezione di quella teorica della libertà morale del soggetto, che è stata elaborata in altri settori ove si sono verificate manipolazioni a scopo politico o commerciale". Si veda anche E. CALÒ, *Sulla libertà del consenso informato*, in *Riv. trim. dir. e proc. civ.*, 1999, 230.

[208] Così S. PATTI, Commento art. 23, in C. M. BIANCA, F. D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, cit., 551.

[209] Si è osservato infatti come "la finalizzazione dell'informazione in vista della protezione della salute enuclei *standards* «informativi» (categorie di informazioni, modalità di informazioni, ecc.) che possono essere diversi rispetto a quelli in base ai quali si realizza l'identità della persona nell'aspetto suo più peculiare e cioè come manifestazione della libertà decisionale", S. VICIANI, *Brevi osservazioni sul trattamento dei dati inerenti la salute e la vita sessuale in ambito sanitario*, in *Riv. crit. dir. priv.*, 2007, 320.

quanto destinataria di atti che possono coinvolgere, più o meno invasivamente, il proprio corpo o i dati ad esso relativi, e dunque, più in generale, la propria persona[210].

Il paziente, anzitutto, viene informato in vista della protezione della salute[211]. Come si rinviene nello stesso *Codice di deontologia medica*[212], l'informazione che il medico fornisce non deve essere di carattere manualistico, dovendo egli, al contrario, sempre misurarsi sulla persona che gli sta innanzi. Può accadere così che non sia necessaria una *full disclosure*, ovvero un'informazione del tutto completa e dettagliata[213], la quale, paradossalmente, potrebbe nuocere al soggetto e non permettergli di prendere una decisione realmente libera[214]. È possibile tuttavia individuare, partendo dalla stessa giurisprudenza in materia, alcuni criteri informativi valevoli in linea di massima, cui il medico possa riferirsi per consentire alla persona di esprimere il proprio "informato consenso"[215].

---

[210] Il riferimento alla "persona interessata", anziché al "paziente", adottato nella versione definitiva della Carta di Nizza al già citato art. 3.2, va sottolineato in quanto individua una categoria ampia di destinatari della norma: tale è, infatti, "ogni persona che deve decidere se il rischio sia accettabile in relazione a possibili complicanze o esiti alternativi più o meno apprezzabili secondo una propria personale visione della qualità della vita", G. TOSCANO, *Informazione, consenso e responsabilità sanitaria*, cit., 71.

[211] S. VICIANI, *L'autodeterminazione «informata» del soggetto*, cit., 286-289.

[212] Molto significativo è l'art. 33 del CDM del 2006: "Il medico deve fornire la più idonea informazione sulla diagnosi, sulla prognosi, sulle prospettive e le eventuali alternative diagnostico-terapeutiche e sulle prevedibili conseguenze delle scelte operate. Il medico dovrà comunicare con il soggetto tenendo conto delle sue capacità di comprensione, al fine di promuovere la massima partecipazione alle scelte decisionali e l'adesione alle proposte diagnostico-terapeutiche. Ogni ulteriore richiesta di informazione da parte del paziente deve essere soddisfatta. Il medico deve, altresì, soddisfare le richieste di informazioni del cittadino in tema di prevenzione. Le informazioni riguardanti prognosi gravi o infauste o tali da poter procurare preoccupazione e sofferenza alla persona, devono essere fornite con prudenza, usando terminologie non traumatizzanti e senza escludere gli elementi di speranza. La documentata volontà della persona assistita di non essere informata o di delegare ad altro soggetto l'informazione deve essere rispettata".

[213] Per quanto riguarda invece la scienza e, più specificatamente, il settore biotecnolgico, le modalità e i contenuti dell'informazione saranno tesi ad una *full disclosure*, dovendosi considerare il bene non del tanto e non solo del singolo, bensì della società intera, M. TALLACCHINI, *Biotecnologie e consenso informato. Un inizio…*, cit., 9.

[214] Si veda, S. CACACE, *Il consenso informato del paziente al trattamento sanitario*, in *Danno e resp.*, 2007, 285, ove l'a. sottolinea il rischio che l'informazione fornita, seppur completa, possa divenire anche dis-umana se "sprovvista di una qualsiasi attenzione e/o preoccupazione all'indirizzo del destinatario".

[215] Con riferimento ad alcune recenti pronunce giurisprudenziali, è stato tracciato un "esalogo" dei doveri informativi del medico, il quale non può non informare il paziente riguardo: 1. La natura dell'intervento chirurgico cui andrà a sottoporsi; 2. La portata e l'estensione dei risultati ottenibili; 3. La possibilità e probabilità dei risultati conseguibili; 4. I rischi prevedibili; 5. La situazione concreta della struttura ospedaliera; 6. I rischi specifici connessi a possibili scelte alternative, S. CACACE, *Il consenso informato del paziente al trattamento sanitario*, cit., 286.

Diversamente, nell'ambito del trattamento dei dati personali, il momento informativo si propone di garantire al soggetto di esercitare un controllo sulla circolazione delle informazioni che lo riguardano, ovvero la finalità risiede nella "protezione" dell'informazione, pertanto, quanto più "peso" assumerà quest'ultima, tanto più la preoccupazione di controllo e protezione dei dati sarà intensa. A questo proposito, si deve considerare l'art. 23 del Codice in materia di protezione dei dati personali, che definisce i caratteri del consenso, individuando, tra gli altri, i requisiti della libertà e dell'"informatezza"[216]. Esso non può essere letto indipendentemente dall'art. 13, cui rinvia, che più specificatamente tratta della previa informazione da dare alla persona interessata[217].

A metà strada, potrebbe collocarsi il caso di particolari trattamenti diagnostici, come i *test* genetici o i *test* HIV, ove vengono in gioco non solo e non tanto il bene-salute e il bene-informazione, bensì il valore della libertà autodeterminativa in sé e per sé considerata, come possibilità di scegliere e configurare le proprie scelte di vita esistenziali oppure patrimoniali e i propri modi di essere[218].

Nonostante, in ultima analisi, siano differenti i beni tutelati dal consenso a seconda delle macroaree in cui rileva, non pare tuttavia sempre possibile tracciare una netta linea di demarcazione tra gli interessi protetti nell'un caso o nell'altro. Per esempio, l'informazione su una grave patologia che non può in alcun modo nuocere ad

[216] Art. 23, Consenso, 1. Il trattamento dei dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato. 2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso. 3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13. 4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

[217] E. BASSOLI, *Regole ulteriori per privato ed enti pubblici economici*, in G. CASSANO, S. FADDA (a cura di), *Codice in materia di protezione dei dati personali*, Milano, Ipsoa, 2004, 164.

[218] Si pensi solo alle scelte procreative, nel caso di test genetici, oppure alla possibilità di prevenzione del contagio della malattia, nel caso di persona informata della propria sieropositività. Si deve, quindi, tenere presente che in questi casi "l'informazione comporta una libertà autodeterminativa del soggetto (e tende alla tutela di tale valore) nel senso che il soggetto, benché informato del vizio genetico, non resta vincolato alla predeterminazione di taluni comportamenti, che potremo definire necessari, piuttosto che altri", S. VICIANI, *L'autodeterminazione «informata» del soggetto,* cit., 289.

altri soggetti o non incide direttamente su scelte procreative, se volta principalmente a tutelare la salute, tuttavia consente che il soggetto eserciti contemporaneamente un controllo sull'informazione ricevuta, quale ambito di autodeterminazione informativa e di riservatezza, e in ogni caso influenzerà e guiderà importanti scelte esistenziali o patrimoniali dello stesso.

Per quanto riguarda, invece, il secondo e correlato requisito, non pare semplice enucleare il pieno significato che può assumere la parola "libertà" nell'ambito della formazione del consenso, benché il problema della libera manifestazione di volontà da parte di un soggetto passivo di un'attività sia un problema affatto nuovo per il diritto[219]. L'intensa riflessione sull'attività terapeutica degli ultimi anni, ma anche quella relativa al trattamento dei dati personali, ha portato ad una nuova attenzione per tale requisito.

Quanto più l'intervento sul corpo si profila rischioso per la persona coinvolta, come può essere nel caso estremo della sperimentazione, tanto più si esige che il consenso venga liberamente prestato, ponendosi la necessità di "massima garanzia della volontà, che non sarebbe adeguatamente tutelata attraverso la normativa sui vizi della volontà del contratto"[220].

Lo stesso può dirsi riguardo al trattamento di dati personali[221], ove in determinati contesti e circostanze si è nientemeno costretti a riconoscere l'impossibilità del formarsi

[219] G. GEMMA, voce «Integrità fisica», cit., 460.
[220] A. BELLELLI, *Aspetti civilistici della sperimentazione umana*, Padova, Cedam, 1983, 56. Nello stesso senso, S. PATTI, Commento art. 23, cit., 547, per il quale, nella disciplina in questione, "il consenso può considerarsi non prestato «liberamente» anche in fattispecie che non permetterebbero di configurare un vizio del volere secondo la regolamentazione codicistica dettata con riferimento ai contratti".
[221] Con riferimento al trattamento dei dati personali, E. CALÒ, *Sulla libertà del consenso informato*, cit., 232: "[…] se da una parte appare riduttivo ipotizzare che il legislatore abbia sentito il bisogno di chiarire che il consenso non dev'essere viziato, dall'altra il preciso concetto di libertà del consenso non sembra sovrapponibile alla previsione codicistica del consenso dato per errore, estorto con violenza o carpito con dolo"; S. M. MELONI, *Il trattamento dei dati da parte di soggetti privati: la disciplina del consenso*, cit., 198: "Tale requisito […] non si mostra particolarmente efficace se letto alla luce della più generale disciplina relativa agli obblighi di informazione, soprattutto a garanzia del contraente più debole […]". Così anche S. PATTI, Commento art. 23, cit., 547, per il quale, nella disciplina in questione, "il consenso può considerarsi non prestato «liberamente» anche in fattispecie che non permetterebbero di configurare un vizio del volere secondo la regolamentazione codicistica dettata con riferimento ai contratti".

di una vera e propria libertà di scelta[222]. Si pensi solamente a quanto sarebbe limitata la possibilità di godere di determinati servizi, per lo più essenziali allo svolgersi delle attività della vita quotidiana, se l'utente rifiutasse di fornire il proprio consenso alla raccolta e al trattamento di informazioni sulla propria persona[223].

9. È nato un "nuovo corpo"?

Dall'indagine svolta fino a questo momento, sono emersi alcuni dati costanti: la complessità della dimensione corporea, quale portatrice di significati eccedenti la sfera fisica; l'interdipendenza tra la qualificazione del corpo e la configurazione dei diritti ad esso relativi, con particolare attenzione al diritto all'integrità e al diritto all'identità personale; l'interazione tra corpo e informazione, che conduce ad un progressivo estendersi all'ambito della tutela dei dati personali di interessi e garanzie che sono proprie del corpo fisico.

Si tratta, pertanto, di cogliere se realmente il progresso tecnologico abbia tracciato un nuovo ritratto della corporeità, e quali siano alcuni dei suoi aspetti o delle sue manifestazioni più evidenti.

Naturalmente, questo "nuovo corpo" non potrebbe in alcun modo sostituire l'unicità di quel "corpo naturale" che ognuno è. Si deve, però, prendere atto del

[222] Così S. RODOTÀ, *Protezione dei dati e circolazione delle informazioni*, cit., 756, che parla di "contesti in cui esistono condizionamenti tali da escludere una reale possibilità di scelta", e inoltre S. M. MELONI, *Il trattamento dei dati da parte di soggetti privati: la disciplina del consenso*, cit., 199: "Si verificano, infatti, nel mercato, situazioni in cui dare il proprio consenso diviene condizione indispensabile per poter usufruire di determinate prestazioni contrattuali, ed in tal caso il presupposto della libertà perde rilevanza di fronte all'esigenza di ottenere, ad esempio, un certo servizio".

[223] Si veda, ancora, S. RODOTÀ, *Protezione dei dati e circolazione delle informazioni*, cit., 756, il quale afferma che, nell'ambito dei "nuovi *media* interattivi", "i gestori, per evidenti ragioni d'ordine economico, sono in condizione di esercitare forti pressioni sugli utenti perché autorizzino l'elaborazione (e l'eventuale trasmissione a terzi), di 'profili' personali o familiari sulla base delle informazioni raccolte in occasione della fornitura dei servizi".

delinearsi di nuove forme di espressione della persona, ove cioè la persona può, sebbene parzialmente, prendere forma e aspetto indipendentemente dalla sua presenza incarnata, e accanto ad essa.

È lecito, dunque, chiedersi se "si può ancora dire che l'entità biologico naturale individuale, che è l'essere umano, costituisca una delimitazione *sicura* della persona fisica *giuridica*", ovvero se "l'espressione linguistica *persona fisica naturale* abbia un non equivoco corrispondente *naturale*"[224].

Il corpo è parso oggetto giuridico nuovo già quando ci si è resi conto della possibilità di una sua scomposizione e di un utilizzo delle sue parti al fine di realizzare interessi fondamentali all'interno della comunità umana, come il diritto alla salute. Un tempo si parlava di capelli, unghie, latte materno, oggi di sangue, organi, tessuti, gameti, DNA. La metafora dell'uomo come macchina vivente ha preso così forma sempre più concreta[225], portando ad una concezione del corpo come insieme di parti tra loro separate ed intercambiabili, a una maggiore standardizzazione dell'essere umano, e infine all'alienazione della persona dal suo proprio corpo fisico[226], espressione di quella frammentazione dell'individuo che il progresso scientifico ha via determinato.

La rivoluzione biotecnologica, ponendo il problema della creazione di prodotti elaborati a partire da materiali biologici umani, ha modificato ulteriormente la

---

[224] A. SANTOSUOSSO, *Persone fisiche e confini biologici: chi determina chi*, in *Pol. dir.*, 2002, 543.

[225] La metafora della macchina vivente può essere intesa sia "come espressione dell'idea che *l'uomo non è altro che una macchina*", sia "come affermazione della possibilità di *realizzare una macchina che diventa uomo*", G. ISRAEL, *La macchina vivente. Contro le visioni meccanicistiche dell'uomo*, Torino, Bollati Boringhieri, 2004, 10-11.

[226] J. A. MARCUM, *Biomechanical and Phenomenological Models of the Body. The Meaning of Illness and Quality of Care*, in 7 *Medicine, Health Care and Philosophy* (2004), 313, ove l'a. presenta il modello del corpo-macchina, detto anche biomeccanico, come il modello che per lungo tempo è stato predominante nella cultura occidentale. In particolare, l'assunzione di tale prospettiva all'interno della medicina ha avuto pesanti ricadute nell'ambito della relazione medico-paziente, ove il medico diviene "*an authority figure with the technical knowledge, power, and expertise to save the patient's body or body part*" (p. 314). Ad esso, si contrappone il modello fenomenologico, ove il corpo non è un qualcosa che la persona possiede come un oggetto, bensì "*a lived, integrated unity that is not readily divisible into a body on the one hand and mind (or self) on the other*" (p. 315).

percezione del corpo[227], che può divenire "corpo artificiale", oscillante tra scoperta e invenzione[228]. Ancor più di recente, i c.d. *ICT implants* e le nanotecnologie, hanno portato ad un ulteriore attenzione per i processi di trasformazione cui il corpo è, suo malgrado, soggetto[229]. Frammentato e modificato, esso rimane invero ancora un'entità materiale.

Accanto a questo processo, si assiste oggi anche alla dematerializzazione o disincarnazione della persona indotta dalle tecnologie informatiche, cosicché essa prende forma attraverso un corpo che è stato definito "corpo elettronico" o "corpo digitale"[230].

---

[227] "Con l'espressione «biotecnologie moderne» o «avanzate», si designano tutte le applicazioni, a uso effettivamente o potenzialmente commerciale o industriale, di tecniche che permettono di modificare o manipolare il patrimonio genetico di organismi viventi unicellulari (microrganismi) o pluricellulari (esseri umani, piante o animali). A tal fine, si utilizza il materiale genetico –essenzialmente i geni, frammenti ereditari del DNA che codificano le proteine- proveniente da altri organismi, non necessariamente appartenenti alla stessa specie dell'organismo modificato. Queste tecniche consentono sia la modificazione di organismi mediante procedimenti di «ingegneria genetica o del DNA ricombinante», sia la creazione *ex novo* di forme di vita geneticamente identiche a organismi preesistenti («clonazione»)". È da precisare che esse vanno tenute distinte dalle "biotecnologie tradizionali", che riguardano processi utilizzati in campo vegetale e agroalimentare, pertanto non aventi ad oggetto gli esseri umani, dalla biomedicina, che è un fenomeno più ampio, e dalle tecniche di riproduzione assistita, di cui le biotecnologie possono rappresentare solo una fase tecnica, R. PAVONI, voce «Biotecnologie», in *Diritti umani, cultura dei diritti e dignità della persona nell'epoca della globalizzazione. Dizionario*, I, Utet, 2007, 90-91.

[228] Il problema che si pone, è quello di stabilire se i materiali biologici umani modificati attraverso processi biotecnologici siano oggetti artificiali, da considerarsi come invenzioni, oppure semplici scoperte, e in quanto tali, non brevettabili, M. TALLACCHINI, *Il corpo e le sue parti. L'allocazione giuridica dei materiali biologici umani*, cit., 519 ss.

[229] Si vedano, a questo proposito, COMITATO NAZIONALE PER LA BIOETICA, *Nanoscienza e Nanotecnologie*, 9 giugno 2006, in *http://www.governo.it/bioetica/testi/Nanoscienze_Nanotecnologie.pdf*; A. G. SPAGNOLO, V. DALOISO, *Outlining ethical issues in nanotechnologies*, in *Bioethics*, 2008, 1 ss.; COMITÉ CONSULTATIF NATIONAL D'ETHIQUE POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ, CCNE, Avis n° 96, *Questions éthiques posées par les nanosciences, les nanotechnologies et la santé* (Paris, le 1er février 2007), in *http://www.ccne-ethique.fr/docs/fr/avis096.pdf*; EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES (EGE), *Opinion on the ethical aspects of nanomedicine*, N° 21, 17 January 2007, in *http://ec.europa.eu/european_group_ethics/activities/docs/opinion_21_nano_en.pdf*, 50, ove si afferma che "*nano-scale implants and devices may have an impact on autonomy, integrity, self identity and freedom*".

[230] Il primo e principale teorizzatore del "corpo elettronico" nel panorama giuridico italiano è S. RODOTÀ, *Dal soggetto alla persona*, cit., 35-36; si veda anche M. G. GIANNICHEDDA, voce «Corpo», in *Diritti umani, cultura dei diritti e dignità della persona nell'epoca della globalizzazione. Dizionario*, I, Utet, 2007, 207.

La tecnica, nel suo potere di "*somatopoiesis*"[231], mette dunque il corpo umano in una posizione sempre più critica, tanto che il soggetto può collocarsi nel mondo anche solamente come flusso di informazioni o simboli, per cui, a ragione, si è parlato di "persona nei dati"[232]. Si registra in questo modo il passaggio dal paradigma meccanicistico, al paradigma della simbolizzazione, ove il corpo come entità biologica, in un certo senso, si offusca, sostituto da una rete di dati, simboli, misure[233]. Il dualismo *corpo* (*the body itself*) - *dati personali* (*personal data*), appare destinato ad essere superato, cosicché si dubita della stessa ragionevolezza di una netta separazione tra i due elementi, atteso che sempre più il corpo si manifesta in termini di informazione[234].

Non più, dunque, identificabile attraverso il solo naturale confine circoscritto dalla pelle, non più percepibile nella sua, seppur modificata, fisicità, un corpo che si fa *data* vive la duplice dimensione della pervasività e dell'assenza[235]: benché i due termini

[231] Può definirsi "*somatopoiesis* tecnologica" il modo in cui la tecnologia investe il corpo e lo crea, S. GIARDINA, V. MELE, *Biotecnologie e "somatopoiesi": inquietudini del corpo e dilemmi bioetici nella letteratura,* in *Medicina e Morale*, 2006, 303-325.

[232] Efficacemente si è osservato che l'individuo postmoderno "avverte l'inquietante sensazione di essersi trasformato in un flusso di informazioni che concernono il suo stato di salute, il suo reddito, le sue relazioni materiali e immateriali, il suo rapporto con le istituzioni, finanche le sue preferenze culturali e politiche. La personalità sembra frammentarsi in un insieme di dati raccolti e registrati in archivi pubblici e privati e il cui trattamento tendenzialmente sfugge al controllo dell'interessato. Caduto in disgrazia persino il motto «*my home is my kingdom*», l'individuo si trova, suo malgrado, soggetto ad una continua scansione in uno spazio pubblico permanente e soprattutto trasparente", A. PUNZI, *La persona nei dati. Ragioni e modelli di una regolamentazione*, cit., 764.

[233] Con riferimento alla videosorveglianza, si è detto: "[…] *the visible, physical features of the body are transformed into digital (often textual) codes and reduced to a virtual, symbolic form*", L. DUBBELD, *Observing Bodies. Camera Surveillance and the Significance of the Body*, in 5 *Ethics and Information Technology* (2003), 152. Si può ben sostenere, allora, che "*the true body as such –homo natura- is absent; the body as it is perceived by us, is interpretation rather than text*", H. ZWART, *Medicine, Symbolization and the "Real" Body – Lacan's Understanding of Medical Science*, in 1 *Medicine, Health Care and Philosophy* (1998), 116.

[234] Si veda I. VAN DER PLOEG, *Genetics, biometrics, and the informatization of the body*, in 43 *Ann. Ist. Super. Sanità* (2007), 46-47, ove l'a. riporta una lista di celebri dicotomie: *reality* ↔ *language*; *referent* ↔ *representation*; *material* ↔ *immaterial*; *biological* ↔ *social*; *"the body itself"*↔ *"personal data"*; *anatomy* ↔ *registration/data search*; *inside/outside* ↔ *public/private*; *integrity* ↔ *privacy*.

[235] G. AZZONI, *L'arbitrarietà del corpo umano*, in F. D'AGOSTINO (a cura di), *Corpo esibito, corpo violato, corpo venduto, corpo donato. Nuove forme di rilevanza giuridica del corpo umano*, cit., 66-67.

siano l'uno l'opposto dell'altro, si riscontra come, quanto più diviene pervasivo, tanto più esso risulta anche assente, e dunque estraneo al soggetto stesso cui appartiene[236].

Il delinearsi della "corporeità elettronica" come dimensione fondamentale della persona accanto a quella fisica e psichica, non è estraneo al diritto, emergendo nella stessa *Carta dei diritti fondamentali dell'Unione europea*, laddove il "diritto alla protezione dei dati personali" (art. 8) si pone come diritto fondamentale autonomo, distinto dal correlato diritto "al rispetto della propria vita privata e familiare" (art. 7), che sempre l'aveva inglobato[237].

Come efficacemente osservato da S. Rodotà, emerge "il problema di quale debba essere il rapporto ordinario di ciascuno con la realtà di un corpo ormai istituzionalmente distribuito. Nella dimensione sociale, questa nuova condizione ordinaria implica una vera e propria cogestione di questo corpo tra il soggetto al quale si riferiscono le informazioni, e che conserva il diritto di controllarle ovunque esse si trovino, e i soggetti che gestiscono le informazioni stesse. Nella dimensione individuale, le domande possono porsi in modo ancor più radicale. Riesco davvero a «conoscere me stesso» quando possono essermi ignoti i luoghi in cui sono presente con le mie informazioni ?"[238].

---

[236] Il corpo "è passato dall'essere luogo dell'espressione dell'io a non-luogo, ossia da contrassegno fedele della propria soggettività a partner pronto al tradimento e dunque bisognoso di costante sorveglianza", M. T. RUSSO, *Dal corpo proprio al corpo estraneo: cultura post moderna e immagini del corpo*, in F. D'AGOSTINO (a cura di), in *Corpo esibito, corpo violato, corpo venduto, corpo donato. Nuove forme di rilevanza giuridica del corpo umano,* cit., 105. Un corpo non più proprio diviene dunque un "luogo pubblico" (pp. 116 ss.).

[237] "Il riconoscimento della protezione dei dati come diritto fondamentale realizza proprio l'obiettivo di mantenere il rapporto tra la persona e il suo corpo, non più racchiuso nei confini della fisicità e nel segreto della psiche, ma davvero sconfinato, affidato alle infinite banche dati che dicono al mondo chi siamo", S. RODOTÀ, *Dal soggetto alla persona,* cit., 36.

[238] Si veda, ancora, S. RODOTÀ, *La vita e le regole*, Milano, Feltrinelli, 2006, 81.

10. Dall'*habeas corpus* all'*habeas data*.

A partire dal riconoscimento della corporeità elettronica come dimensione essenziale della persona umana accanto a quella fisica e, conseguentemente, della rilevanza autonoma assunta dal diritto alla protezione dei dati personali, si perviene all'identificazione di un principio, nuovo per la cultura giuridica europea, volto a garantire il *dominium* del soggetto sui propri dati: l'*habeas data*[239].

Per comprenderne la portata, è opportuno, da una parte, considerare quello che può ritenersi il suo antecedente storico, il principio dell'*habeas corpus* e, dall'altra, esaminare la sua origine ed evoluzione all'interno della cultura giuridica latino americana, laddove ha trovato la sua prima formulazione.

Tradizionalmente, si ritiene che il *writ* di *habeas corpus* rinvenga il proprio fondamento nella *Magna Charta* inglese del 1215 ove, all'art. 29, si afferma: "Nessun uomo libero dovrà essere arrestato, imprigionato, spossessato della sua dipendenza, della sua libertà o libere usanze, messo fuori legge, esiliato, molestato in alcun modo, *né noi metteremo mano o faremo mettere mano su di lui*, se non in virtù di un giudizio legale, dei suoi pari e secondo la legge del Paese"[240].

Con tale principio si fa abitualmente riferimento a quell'atto con cui il giudice ingiunge all'autorità di polizia che detiene una persona in arresto di portarla innanzi a lui per controllare e giustificare la legalità della custodia[241], ovvero, più in generale,

---

[239] Si deve essenzialmente a S. Rodotà la ripresa e l'enucleazione di tale principio all'interno della cultura giuridica italiana, S. RODOTÀ, *Una scommessa impegnativa sul terreno dei nuovi diritti. Discorso del presidente del Garante per la protezione dei dati personali tenuto l'8 maggio 2001 alla presentazione della Relazione per il 2001*, in *http://www.interlex.it/675/rodota6.htm*; S. RODOTÀ, *Trasformazioni del corpo,* cit., 10-11; S. RODOTÀ, *Avventure del corpo*, in *Notizie di Politeia*, 2006, n. 84, 53. Esso è stato poi ripreso da altri autori, tra cui si veda D. VACCARO, *Il corpo controllato tra nuove tecnologie e tutela della dignità,* in *http://www.computerlaw.it/public/Vaccaro%20il%20corpo%20controllato%201.pdf*, I parte, 3.

[240] A. M. DE CESARIS, voce «Habeas corpus», in *Enc. giur. Treccani*, XV, Ed. Enc. it, 1989, 1, (c.vo agg.).

[241] G. R. MUSSO, voce «Habeas corpus», nel *Digesto pen*., VI, 1992, 59.

funge da strumento di garanzia della libertà individuale, con particolare riguardo al pericolo di arresti arbitrari.

La minaccia terroristica degli ultimi anni sembra aver attentato, ancor prima che alla vita di molte persone, alla loro stessa libertà, limitata da misure talora eccessive di controllo e prevenzione esercitate sui "corpi". Si è parlato così di "fine dell'*habeas corpus*" quando in Gran Bretagna è stata emanata la legge *The Prevention of Terrorism Bill*, dell'11 marzo 2005, in base alla quale il ministro dell'interno può autorizzare misure limitative della libertà personale (di cittadini e stranieri), tra cui gli arresti domiciliari, sulla base di fondati sospetti circa il coinvolgimento di un individuo in un'azione terroristica, senza che vi sia una formale imputazione e si svolga un regolare processo[242].

Nel tempo, l'*habeas corpus* è stato impiegato in un'accezione ancor più ampia, per indicare cioè il "diritto di disporre della propria persona o diritto alla protezione della libertà personale contro atti arbitrari o illegittimi da parte delle autorità o dei privati"[243], non solo in riferimento alla dimensione fisica, ma anche alla sfera morale (*habeas mentem*), in quanto, nell'un caso come nell'altro, è il rispetto della dignità umana ad essere in gioco[244].

Stabilendo dunque che nessuna coercizione possa essere effettuata senza il consenso della persona interessata[245], si riconosce che quest'ultima esercita un

[242] J. C. PAYE, *Gran Bretagna: fine dell'habeas corpus*, in *Dem. e dir.*, 2005, 211-216.
[243] E. ROZO ACUÑA, voce «Habeas corpus (America Latina)», nel *Digesto IV ed., Disc. pen.*, Aggiornamento I, Utet, 2005, 669.
[244] "La libertà personale viene intesa, almeno inizialmente, come pretesa di non vedere illegittimamente esercitata alcuna «potestà coercitiva personale», che gravi sui singoli, indipendentemente dal loro previo consenso o dalla loro spontanea collaborazione, per poi trascendere questo limitato ambito, come si evince dall'affermazione per cui «la garanzia dell'*habeas corpus* non deve essere intesa soltanto in rapporto alla coercizione fisica delle persone, ma anche alla menomazione della libertà morale, quando tale menomazione implichi un assoggettamento totale della persona all'altrui potere (sentenza n. 30 del 1962)»", M. RUOTOLO, voce «Habeas corpus», in *Diritti umani, cultura dei diritti e dignità della persona nell'epoca della globalizzazione. Dizionario*, II, Utet, 2007, 698.
[245] "Più in generale, la libera determinazione del consenso, non soggetto ad alcun condizionamento esterno né in contrasto con altri principi costituzionali, permetterebbe di porre in relazione la libertà personale con la disposizione del proprio corpo, essendo quest'ultimo inteso non come oggetto autonomo

dominium sul proprio corpo, in virtù della relazione di appartenenza che ad esso lo lega[246].

Tuttavia, a fronte del delinearsi della dimensione elettronica della corporeità accanto a quella fisica, anche la protezione dei dati personali diviene un aspetto essenziale della libertà personale, cosicché quel "*né metteremo mano o faremo mettere mano su di lui*" esige di essere interpretato anche come "*né metteremo mano o faremo mettere mano sui suoi dati*", sancendo il passaggio dall'*habeas corpus* all'*habeas data*: è "l'avanzamento di una nuova frontiera della libertà umana verso la società futura" [247].

L'*habeas data* nasce, pertanto, per fronteggiare il cosiddetto "potere informatico", un quarto potere che può essere attribuito allo Stato liberale e affiancarsi ai tre tradizionalmente conosciuti, sviluppatosi a seguito dell'incremento dei mezzi di informazione di massa, dell'informatica, delle raccolte elettroniche di dati personali e dell'interconnessione di banche dati[248].

---

e separato dalla persona ma come elemento costitutivo della stessa", M. RUOTOLO, nel *Commentario alla Costituzione*, I, Utet, 2006, sub. art 13, nota p. 323; si veda anche M. RUOTOLO, voce «Habeas corpus», cit., 698.

[246] E. ROZO ACUÑA, voce «Habeas corpus (America Latina)», cit., 669.

[247] Così T. M. FROSINI, *Tecnologie e libertà costituzionali*, in *Dir. Inf.*, 2003, 489. Il saggio di Frosini è particolarmente interessante a proposito della rilettura della tradizionale concezione di libertà personale alla luce del progresso tecnologico e delle esigenze imposte dalla società (spec. pp. 490 e 496 ss). Spostando la questione sul versante socio-politico, si può dire che l'avvento della libertà informatica porta alla nascita di una nuova democrazia, che è stata definita come: «elettronica», «virtuale», «continua», «di massa» (p. 502). In tema di libertà informatica, si veda anche E. GIANNANTONIO, *Il nuovo disegno di legge sulle banche di dati* personali, in *Dir. inf.*, 1991, 74 ss., ove si parla di "libertà di adoperare senza vincoli ingiustificati i mezzi informatici per le proprie personali esigenze" (p. 77). Per la tesi dell'evoluzione del diritto alla libertà personale, si veda anche S. Rodotà, che in più parti ribadisce questo orientamento: S. RODOTÀ, *Trasformazioni del corpo,* cit., 10, e *Avventure del corpo,* cit., 53, ove l'a. dichiara che la promessa della *Magna Charta* "sopravvive ai mutamenti tecnologici", ovvero "svolge la funzione di garantire l'*habeas data* reso necessario dalle mutate circostanze, divenendo in tal senso una componente irrinunciabile di civiltà come lo è stato l'*habeas corpus*".

[248] Esso è stato definito come "la possibilità di memorizzare e trattare una grande quantità di dati personali secondo le nuove tecnologie in modo da acquistare un nuovo potere di dominio sociale sull'individuo", E. GIANNANTONIO, voce «Dati personali (tutela dei)», in *Enc. del dir.*, Aggiornamento III, Giuffrè, 1999, spec. pp. 483. Si vedano anche, *ex multis*, E. ROZO ACUÑA, *Habeas Data costituzionale: nuova garanzia giurisdizionale del diritto pubblico latinoamericano*, in *Dir. pub. comp. ed eur.*, 2002, IV, 1926 e M. PETRONE, *Banche di dati e tutela della "privacy". Riflessi penalistici*, in *Dir. Inf.*, 1988, 82-83.

Pur riguardando tale fenomeno essenzialmente la società occidentale, laddove il progresso tecnologico ha consentito un uso sempre più diffuso e affinato di queste tecniche, è interessante rilevare che solo in alcuni paesi dell'Americana latina tale principio ha trovato esplicito riconoscimento, già da alcuni anni e all'interno delle Carte costituzionali stesse[249].

Prendendo le mosse dall'esperienza degli Stati latino americani, si può allora enucleare con precisione il contenuto del diritto all'*habeas data*, il quale si configura come l'insieme delle "garanzie, azioni, ricorsi e giudizi idonei ad assicurare: 1) il *diritto di protezione dei dati*, come tutela dei diversi diritti della persona che possono essere lesi da «gestori» di dati personali; 2) il *diritto alla protezione dei dati*, come potere delle persone ad ottenere dalle pubbliche autorità la difesa di quei diritti violati o minacciati dall'accesso, registro o trasmissione a terzi dei loro dati personali; 3) la *libertà d'informazione*, intesa in senso ristretto come diritto all'autodeterminazione informativa, vale a dire, come diritto delle persone, gruppi e istituzioni a determinare il quando, il come ed il *quantum* dell'informazione personale oggetto di comunicazione ai terzi; 4) la *libertà informatica*, come garanzia personale a conoscere e accedere alle informazioni personali esistenti nelle *banche dati*, a controllare il loro contenuto e quindi a poterle modificare in caso d'inesattezza o indebita archiviazione o trattamento, nonché a decidere sulla loro circolazione o trasmissione"[250].

---

[249] Si ricordano, tra le Costituzioni che hanno sancito l'*habeas data* in forma diretta e completa: la Costituzione del Guatemala del 1985, modificata nel 1993; la Costituzione brasiliana del 1988 ("Su tali presupposti la Costituzione garantisce a tutti l'azione di *habeas data* per assicurare la conoscenza d'ogni informazione relativa alla persona che risulti da registri o banche-dati di enti governativi o di carattere pubblico"); la Costituzione colombiana del 1991; la Costituzione del Paraguay del 1992; la Costituzione del Perù, riformata nel 1993; la Costituzione dell'Ecuador, modificata nel 1996; la Costituzione argentina, secondo la riforma del 1994; la Costituzione del Venezuela, modificata nel 1999. I paesi che garantiscono l'*habeas data* solo a livello legislativo o in forma indiretta attraverso l'*amparo* costituzionale sono invece la Repubblica del Cile, il Costa Rica, la Bolivia, il Nicaragua, l'Honduras. Altre esperienze che prevedono una tutela indiretta dell'*habeas data* sono quelle delle Repubbliche di Panama, Messico, Uruguay, El Salvador, E. ROZO ACUÑA, *Habeas Data costituzionale: nuova garanzia giurisdizionale del diritto pubblico latinoamericano*, cit., 1928 ss.
[250] *Ibidem*, 1923.

Per quanto riguarda l'Europa, invece, il principio, malgrado non sia espressamente sancito, ha trovato di recente, come si è detto, il proprio riconoscimento nell'art. 8 della *Carta dei diritti fondamentali dell'Unione europea*, che è inserito precisamente nel capo II, dedicato alla "libertà". In particolare, esso prescrive il diritto di ogni individuo alla protezione dei dati personali che lo riguardano, il loro trattamento secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata, o a un altro fondamento legittimo previsto dalla legge, nonché il diritto di accedere ai dati raccolti e di ottenerne la rettifica[251].

[251] *Ibidem*, 1927.

CAPITOLO TERZO

CORPO, IDENTITÁ, INFORMAZIONE BIOMETRICA

SOMMARIO: 1. Acquisizione della caratteristica biometrica e *habeas corpus.* – 2. (*Segue*) L'identificazione attraverso l'elemento biometrico: il corpo come *password*. – 3. Una nuova identità. Identità digitale e identificazione. – 4. (*Segue*) Frode d'identità. – 5. Dal diritto alla riservatezza al diritto alla protezione dei dati personali: l'affermazione dell'*habeas data*. − 6. La complessa qualificazione giuridica dei dati biometrici. I dati biometrici come dati personali. − 7. (*Segue*) Il problema dell'anonimia. − 8. Dati biometrici come categoria *sui generis* distinta da altri dati personali. − 9. Dati biometrici come dati sensibili. − 10. (*Segue*) Informazione genetica *vs.* informazione biometrica: stesso *genus*?

1. Acquisizione della caratteristica biometrica e *habeas corpus*.

Prima di procedere all'approfondimento della relazione che intercorre tra identità e biometria, e tra informazione e biometria, si rende necessario considerare, seppur brevemente, un aspetto che può dirsi preliminare, e che si inserisce in quel delicato passaggio che conduce dalla caratteristica al dato biometrico, ovvero dall'*habeas corpus* all'*habeas data*.

Il dato, infatti, per poter essere trattato, deve anzitutto essere stato legittimamente acquisito. L'atto del prelievo potrebbe sollevare questioni di legittimità

costituzionale, con particolare riguardo al principio della libertà personale, di cui all'art. 13 Cost., ossia al menzionato principio dell'*habeas corpus*[252].

Invero, qualcuno ha sostenuto che, essendo alquanto agevole il reperimento di taluni dati biometrici, le operazioni identificative sono "scarsamente o affatto invasive", in ragione del fatto che "nella maggior parte dei casi il prelievo dei dati biometrici con le tecniche rese attualmente disponibili dalla scienza risultino intervenire sul solo aspetto esteriore e perciò stesso essere del tutto rispettose della libertà personale"[253]. Tali tecniche, si dichiara inoltre applicando alla questione in esame una celebre pronuncia della Corte Costituzionale in tema di rilievi segnaletici, "rappresenterebbero «soltanto una forma di prestazione imposta, al fine della prevenzione dei reati, a certi individui che si trovino in determinate condizioni previste dalla legge»"[254].

Questa posizione va considerata più accuratamente e con maggiore attenzione al "fenomeno biometria".

Anzitutto, è opportuno precisare che misure come i rilievi dattiloscopici, fotografici e antropometrici e altri accertamenti ai fini della identificazione della persona, rientrano nei c.d. provvedimenti di polizia giudiziaria, e mirano precisamente ad identificare persone nei confronti delle quali vengono svolte indagini penali (art. 349, comma 2°, c.p.p.), in vista della tutela dell'ordine e della sicurezza pubblica e del sistema processuale penale. Si tratta, dunque, di misure affatto comuni, che ricadono nel novero dell'art. 13 Cost., in quanto restrittive della libertà personale[255], e per le quali, fatte salve le prescrizioni della legge, si rende necessaria la collaborazione del soggetto

[252] Si veda L. BOCCHI, *Libertà personale e vista di leva: il rilevamento dattiloscopico*, in *Riv. trim. dir. pubbl.*, 1992, 134-157.
[253] L. TRUCCO, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Torino, Giappichelli, 2004, 48-49.
[254] *Ibidem*, 49. Il riferimento è a CORTE COST., 27.3.1962, n. 30, in *Giur. cost.*, 1962, 240-242.
[255] Così M. RUOTOLO, nel *Commentario alla Costituzione*, cit., p. 329.

ai fini dell'acquisizione, non essendo permesso, in linea di principio, procedere ad atti di acquisizione coattiva, senza che sia stato cioè prestato consenso libero e informato[256].

Le parole sopra citate della Corte non sembrano dunque *in toto* riferibili al caso concreto dell'acquisizione delle caratteristiche biometriche, operazione che, come si è già avuto modo di osservare, non coinvolge solo "certi individui che si trovino in determinate condizioni previste dalla legge", bensì spesso *qualunque individuo* e in *qualunque condizione* questi si trovi.

Invero, benché sembra non si possa nemmeno escludere che, a fronte di un pericolo per la collettività, sia legittimo procedere ad un prelievo generalizzato di alcune caratteristiche biometriche in vista di un intervento preventivo[257], rimane pur sempre "doveroso per uno Stato di diritto non utilizzare mezzi restrittivi della libertà di tutti coloro che formano la sua popolazione, al fine di colpire un numero proporzionalmente molto piccolo di devianti con maggior facilità di quanto si possa fare utilizzando strade più garantiste"[258].

La compressione delle sfere soggettive individuali, in nome di un interesse pubblico, esige dunque non solo un corretto bilanciamento degli interessi, ma altresì di accertare con dovizia di che natura sia il rischio paventato, trattandosi spesso di un "pericolo tutt'altro che certo e comprovato, anzi spesso evanescente e per nulla accertato"[259]. Come è stato efficacemente detto: "Ritenere che, *sempre*, in presenza di un pericolo per un interesse pubblico (solo astrattamente configurabile), il diritto soggettivo possa essere compresso significa fornire giustificazione ad un abuso dell'esercizio delle pubbliche potestà. In assenza dei concreti presupposti per l'adozione

[256] CNIPA, *Linee guida per le tecnologie biometriche*, cit., 55.
[257] L. BOCCHI, *Libertà personale e vista di leva: il rilevamento dattiloscopico*, cit., 150, ove l'a. dichiara: "Si può ipotizzare un utilizzo a fini sociali anche del rilevamento delle impronte digitali"
[258] Così L. BOCCHI, *Libertà personale e vista di leva: il rilevamento dattiloscopico*, cit., 151.
[259] P. GALLO, *Il dopo 11 settembre: un nuovo concetto giuridico di «pericolo». Tra libertà individuale ed esigenze di tutela della sicurezza collettiva*, in *Jus*, 2007, 434.

di misure emergenziali, fissati dalla legge, dovrà perciò ritenersi illegittima la compressione dei diritti individuali"[260].

In secondo luogo, pare riduttivo ritenere che, per il fatto di non essere, in linea di principio, fortemente invasive della sfera corporea, tali tecniche possano automaticamente considerarsi rispettose del principio di libertà personale costituzionalmente sancito. Non convince, in altri termini, l'idea che la limitazione della libertà personale sia direttamente proporzionale al solo grado di invasività materiale dell'atto compiuto, per cui, quanto più esso si configura come invasivo, tanto più il soggetto risulterà menomato nella sua libertà. Infatti, è opinabile lo stesso concetto di "invasività", dal momento che vi sono atti fortemente invasivi, pur non coinvolgendo la persona nel suo solo "aspetto esteriore", come si approfondirà di seguito.

2. (*Segue*) L'identificazione attraverso l'elemento biometrico: il corpo come *password*.

L'utilizzo del corpo e delle sue parti a fini identificativi, implica che uno degli aspetti più significativi che attengono alla biometria sia il nuovo e singolare paradigma entro cui la corporeità umana viene sospinta[261].

Si è già trattato di come l'attuale progresso tecnologico abbia portato alla nascita di un nuovo concetto di corpo, un corpo che si va definendo sempre più nella forma di dato, informazione, simbolo.

L'avvento dei sistemi di identificazione biometrica si inserisce pienamente in questo processo di ridefinizione della corporeità, da una parte radicalizzandolo,

[260] *Ibidem*, 435.
[261] In questo senso, F. MACIOCE, *Il corpo digitale. Profili etici dei rilievi biometrici: il caso della carta di identità elettronica*, in *L'Arco di Giano*, n. 45, 2005, 33-41. Si veda anche Rodotà, secondo il quale siamo in presenza di "mutamenti che toccano l'antropologia stessa delle persone", in S. RODOTÀ, *La vita e le regole*, cit., 89, e in S. RODOTÀ, *Trasformazioni del corpo*, cit., 8.

dall'altra ponendosi come crocevia tra antiche e nuove forme di utilizzo e determinazione del corpo: la fisicità torna ad essere elemento centrale, ma ad un tempo lo diviene attraverso il dato, giacché il campione viene convertito in una stringa numerica[262].

La filosofa olandese Irma Van Der Ploeg porta l'attenzione sulla già citata dicotomia tra "identità incarnata" e informazioni riguardo alle persone e alle loro caratteristiche fisiche, tra "*the body itself*" e la sua "*digital representation*", sottolineando come i dati biometrici non siano semplici informazioni ma, attraverso il "trasferimento" di elementi fisici in un codice digitale, determinino un cambiamento a livello ontologico, anziché di mera rappresentazione[263]. Efficacemente, pertanto, si è affermato che la biometria apre la strada alla definizione del corpo umano in termini di *password*, ovvero di macchina-leggibile, di carta d'identità universale, che permette l'identificazione e la classificazione delle persone[264].

Invero, si può ben riscontrare una differenza tra i tradizionali sistemi di riconoscimento delle persone, come il documento d'identità dotato di nome e fotografia dell'interessato, e gli identificatori biometrici, differenza che, come si è detto, attiene ad una sorta di spazio che si frappone tra la persona e l'identificatore, difficile da

---

[262] Si veda, in particolare, E. MORDINI, C. OTTOLINI, *Implicazioni etiche e sociali della biometria*, cit., 69, per il quale "la biometria appartiene interamente alla tarda modernità: nel suo essere radicata sul corpo e nel suo basarsi sulla corporeità. Il corpo è il luogo in cui si incrociano le scommesse più ardite e più pericolose della contemporaneità. La tecnologia infatti sembra poter ridisegnare una soggettività mutante, una corporeità programmata, clonata, replicata. A questo proposito si parla di superamento dell'esser biologico, di una nuova carne sintetica, di un corpo postorganico. Il corpo sembra poter diventare una superficie informatizzata, un corpo-segno totalmente formalizzato, come viene in qualche modo preannunciato nella top model o nel body-builder".

[263] Così I. VAN DER PLOEG, *Biometrics, and the body as information: normative issues of the socio-technical coding of the body*, in *http://www.bmg.eur.nl/smw/publications/vdp_02.pdf* , 3-4. In questo senso, si veda anche E. MORDINI, S. MASSARI, *Body, biometrics and identity*, in 22 *Bioethics* (2008), 494 ss., ove si dichiara che "*digital representations always imply a certain degree of simplification, which modifies the nature of the represented object*" e E. MORDINI, C. OTTOLINI, *Body identification, biometrics and medicine: ethical and social considerations*, in 43 *Ann. ist. super. sanità* (2007), 54.

[264] L'immagine del "corpo come *password*" ricorre soprattutto in S. RODOTÀ, del quale si vedano, in particolare, *Trasformazioni del corpo*, cit., 8 e *Avventure del corpo*, cit., 48; si consideri poi S. BISI, *Il corpo come password: alcune considerazioni in tema di sistemi di autenticazione biometrica*, cit., 9.

caratterizzare, ma che riguarda un fondamentale tipo di libertà, ovvero la distribuzione del potere tra lo Stato e gli individui, "uno spazio che scompare interamente con gli identificatori biometrici, come se la carta d'identità fosse incollata al tuo corpo"[265].

Ci si può chiedere, a questo proposito, che rilevanza assuma l'interesse all'integrità fisica in un corpo che si fa *password*. In altri termini, la domanda che ci si pone è la seguente: "Come possiamo assicurare l'integrità dei corpi una volta che questi assumono una esistenza estesa, come informazioni?"[266].

Normalmente, quando si parla di produzione e di conservazione di rappresentazioni digitali di caratteristiche corporee individuali, si corre il rischio di attribuire a tale concetto una valenza molto ristretta, ossia limitatamente al momento in cui si verifica un materiale contatto tra la parte del corpo interessata e i sensori che rilevano l'informazione[267]. Pertanto, se l'integrità attiene ai confini, ricorrendo al tradizionale criterio di delimitazione del corpo umano definito dalla pelle, di integrità potrebbe parlarsi solo per ciò che riguarda tale confine. Vi sono però delle zone grigie, nelle quali non è agevole stabilire in che modo quest'ultimo sia implicato[268].

Si consideri, per esempio, il caso dei raggi X, i quali generano un contatto *sui generis*, apparentemente inesistente, eppure caratterizzato da un alto grado di invasività, sia perché, in modo singolare, attraversano la superficie corporea, sia perché l'immagine che permettono di ricavare è una vera e propria rappresentazione della costituzione interna del corpo.

---

[265] I. VAN DER PLOEG, *The illegal body: 'Eurodac' and the politics of biometric identification*, in 1 *Ethics and Information Technology* (1999), 301.
[266] Così I. VAN DER PLOEG, *Genetics, biometrics, and the informatization of the body*, cit., 48.
[267] Si veda I. VAN DER PLOEG, *Biometrics, and the body as information: normative issues of the socio-technical coding of the body*, cit., 18. Sul problema del grado di invasività materiale dello strumento biometrico sul corpo umano e conseguentemente della violazione dell'integrità corporea, si veda anche A. HAREL, *Biometrics, Identification and Practical Ethics*, in *http://www.europeanbiometrics.info/resources/index.php?Id_folder_tx=10#10*, 2001, 9.
[268] Così I. VAN DER PLOEG, *Biometric identification technologies: ethical implications of the informatization of the body*, in *http://www.biteproject.org/documents/policy_paper_1_july_version.pdf*, 12.

Un altro esempio è rappresentato dal DNA: vi sono modi di ottenere campioni di DNA non molto invasivi sul piano strettamente tecnico-materiale, eppure il prelievo può dar luogo ad una grave violazione dell'integrità, permettendo di ricavare informazioni circa l'identità della persona.

È dunque, da una parte, lo scopo a fare la differenza: è lo scopo a rendere alcuni atti di raccolta di informazioni sul corpo lesivi dell'integrità fisica, anche se di fatto meno invasivi di altri sul piano strettamente materiale.

Dall'altra, secondo quanto precedentemente argomentato[269], il concetto di integrità non può essere più considerato meramente sotto il profilo della intangibilità della sfera psicofisica della persona, ma è destinato ad espandersi, in corrispondenza della virtuale espansione dei confini del corpo stesso e, segnatamente, del passaggio dalla dimensione materiale alla dimensione immateriale, dal corpo fisico al corpo elettronico[270].

Si può convenire, pertanto, che, nella maggior parte delle tecnologie biometriche, il problema del diritto all'integrità del corpo e della persona nel suo complesso è implicato[271].

In primo luogo, poiché si verifica in ogni caso un contatto, il cui grado di invasività varia da caratteristica a caratteristica, nel momento in cui l'informazione viene prelevata, tanto che tale atto sarebbe, in linea di massima, considerato illegittimo se realizzato contro la volontà della persona.

---

[269] Si veda il cap. II, paragrafo 5.

[270] I. VAN DER PLOEG, *Biometrics, and the body as information: normative issues of the socio-technical coding of the body*, cit., 22-24 e I. VAN DER PLOEG, *Genetics, biometrics, and the informatization of the body*, cit., 48., ove si dichiara: "*It is not the generation of the body data per se, but the information about the body thus gathered, and all the analyses, processing, and knowledge about the person this information makes possible, that is of concern*". In questo senso, si è espresso altresì D. LYON, *Biometrics, identification and surveillance*, in 22 *Bioethics* (2008), 506, il quale afferma: "*The informatized body requires new ways of thinking about integrity, equal to the shift from anatomical to data-based definition of the body*".

[271] I. VAN DER PLOEG, *Biometric identification technologies: ethical implications of the informatization of the body*, cit., 14-15.

In secondo luogo, e principalmente, poiché questa informazione è un frammento di quel "corpo elettronico" la cui integrità, nell'ampia accezione considerata, va tutelata, conferendo a coloro che l'acquisiscono notevoli poteri di controllo sull'interessato.

Come è stato efficacemente detto, la biometria "realizza l'antico sogno pitagorico-platonico di rappresentare il reale per tramite di relazioni geometriche. Ma questo processo non rende il corpo più degno di onori, piuttosto lo trasforma, definitivamente, in un cadavere. *Soma, sema*; corpo, tomba: mai fu più vero l'antico gioco di parole"[272].

3. Una nuova identità. Identità digitale e identificazione.

Appare chiaro, a questo punto, che la biometria è radicata in una sorta di trinomio, i cui termini principali sono corpo, identità, informazione.

Il corpo come *password*, infatti, è finalizzato alla costruzione e gestione dell'identità del soggetto, rendendo possibili atti di inclusione o esclusione dello stesso nei diversi contesti pubblici e privati. A ragione, pertanto, si è affermato che, attraverso le tecnologie biometriche, "il problema della gestione dell'identità diviene quello di corpi *(dis)qualified*", di corpi, per così dire, "squalificati"[273].

A tal proposito, vale la pena soffermarsi sull'interessante documento *Biométrie, données identifiantes et droits de l'homme*, emanato in Francia dal *Comité Consultatif National d'Ethique pour les Sciences de la Vie et de la Santé* (CCNE), ove si pone il

[272] Così E. MORDINI, C. OTTOLINI, *Implicazioni etiche e sociali della biometria*, cit., 70.

[273] Così B. J. MULLER, *(Dis)Qualified bodies: securitization, citizenship and 'identity management'*, in 8 *Citizenship Studies* (2004), 288. In particolare, l'a. solleva il problema del rapporto tra biometrie e cittadinanza, sostenendo che le tecnologie biometriche e l'uso del corpo come *password* sono alla base del passaggio "*from citizenship to identity management*". Il problema delle cittadinanza, in altri termini, si sta concretizzando sempre più come un problema di sicurezza e dunque di accertamento e gestione dell'identità. Di qui l'interrogativo: "*What's left of citizenship?*".

problema se i dati biometrici possano delineare la vera identità di un individuo, ovvero provochino l'inevitabile e grave pericolo di una "*instrumentalisation du corps et en quelque sorte à une déshumanisation, en réduisant une personne à quelques mesures biométriques*", conducendo così ad una deformazione della persona, che neghi la sua vera identità ed essenza[274].

Significativo il richiamo operato nel documento al filosofo Paul Ricoeur, secondo il quale, nell'ambito della nozione di identità, sussiste una distinzione tra *ipséité* e *mêmeté*[275].

Il concetto di *mêmeté* riguarda l'oggettività del corpo e sta ad indicare che, attraverso lo spazio e il tempo, il corpo rimane sostanzialmente lo stesso, al di là di qualunque segno che possa incidere su di esso.

L'*ipséité*, al contrario, attiene al vissuto di un essere umano senziente e cosciente, e concerne il corpo come soggetto, così come viene sperimentato nelle dimensioni più intime della persona: si tratta del "*maintien de soi de l'individu à travers les aléas événementiels qui construisent son histoire*".

Riguardo ai dati biometrici, ci si può chiedere allora se "*respectent-elles toujours l'«ipséité», qui est au fondement de sa liberté*". Infatti, quando tali dati sono diffusi, ovvero quando sono connessi ad altri, la sfera stessa dell'identità, in quanto *ipséité* e non meramente *mêmeté*, può essere coinvolta.

Nell'affrontare la questione, è bene, anzitutto, soffermarsi su alcune nozioni di carattere preliminare, le quali, pur distinte, sono tra loro correlate.

Ci si è già addentrati, nel corso di questo lavoro, nella complessa qualificazione del diritto all'identità personale, del quale sono state colte le più significative sfumature.

---

[274] COMITÉ CONSULTATIF NATIONAL D'ETHIQUE POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ, CCNE, Avis n° 98, *Biométrie, données identifiantes et droits de l'homme*, I – *Une approche transformée de l'identité de l'homme*, 26 avril 2007, p. 6.
[275] *Ibidem*, 7-8.

Si tratta ora di approfondire i concetti di identità digitale e di identificazione, utili a comprendere in che modo le tecnologie biometriche intreccino il problema dell'identità lungo tutta la sua estensione.

La nozione di "identità digitale", invero, non trova specifici riferimenti legislativi all'interno del panorama giuridico italiano, né vi è una definizione universalmente riconosciuta o sufficientemente completa di essa[276], tuttavia è possibile metterne in luce le due maggiori accezioni[277].

Essa allude alla c.d. identità "in rete" o "virtuale", e può affiancarsi alla nozione di "identità informatica", indicando "la rappresentazione virtuale dell'identità reale che può essere usata durante interazioni elettroniche con persone o macchine". In questa definizione sono compresi, quali elementi costitutivi dell'identità digitale, anche le credenziali, ossia gli elementi che permettono la verifica dell'identità (autenticazione), gli attributi, vale a dire le informazioni aggiuntive legate all'identità (il profilo), e talvolta la reputazione elettronica, ovvero l'immagine che la persona dà di se medesima interagendo nel mondo virtuale[278].

In altri termini, l'identità digitale può essere complessivamente definita come "l'insieme delle informazioni e delle risorse concesse da un sistema informatico ad un particolare utilizzatore del suddetto. Queste informazioni sono di norma protette da un sistema di autenticazione. L'autenticazione può essere effettuata tramite parola chiave (*password*), caratteristiche biologiche (iride, impronta digitale, impronta vocale, riconoscimento del volto, ecc.) o attraverso un particolare oggetto (tessera magnetica, *smart card*, ecc.)"[279].

---

[276] ASSOSECURITY, *La gestione dell'identità digitale*, 2006, 6.
[277] G. RESTA, *Identità personale, identità digitale,* cit., 513-515.
[278] Così ASSOSECURITY, *La gestione dell'identità digitale*, cit., 6.
[279] G. RESTA, *Identità personale, identità digitale,* cit., 515, che propone la definizione offerta da *Wikipedia.*

Grazie a tale "nuova identità", distinta da quella tradizionalmente intesa, di cui poteva parlarsi prima dell'epoca dell'*Information Technology,* il soggetto può assumere facilmente più di una identità, oppure può rappresentarsi attraverso una identità parziale, celando la sua identità complessiva, oppure può far propria l'identità altrui, usando una falsa identità, parziale o completa che sia[280].

Infatti, l'identità digitale prende forma nel c.d. "cyberspazio", un mondo che non ha una sussistenza fisica vera e propria, perché fatto di informazioni, che tuttavia possiedono una propria consistenza e producono reali conseguenze, uno spazio elettronico ove ogni individuo può vivere quotidianamente[281].

Il processo di acquisizione di una pluralità di identità, o di false identità, che verrà approfondito in seguito, può rivelarsi particolarmente significativo nel caso delle tecnologie biometriche: una persona che abbia registrate più caratteristiche biometriche in un sistema, risulterà avere più identità, una per ciascuna caratteristica. Oppure, un utente che venga riconosciuto sotto falsa identità, continuerà ad avere questa stessa falsa identità verificata positivamente in ogni confronto biometrico cui si sottopone[282].

---

[280] Si veda il documento di N. MITCHISON, M. WILIKENS, L. BREITENBACH, R. URRY, S. PORTESI, *Identity Theft. A Discussion Paper*, European Commission, Joint Research Centre, 2004, spec. pp. 9-10. La possibilità di avere più identità è legata in modo particolare al c.d. *nym* (lett. nomignolo), con il quale si intende lo *username* o un nome simile, un numero di telefono o di conto, che conferisce una identità o delle credenziali per l'accesso ad un sistema elettronico, ivi inclusi alcuni privilegi o, viceversa, delle restrizioni (p. 8, nota n. 3).

[281] Così G. I. ZEKOS, *State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction*, in 15 *International Journal of Law and Information Technology* (2007), 2, ove il cyberspazio è definito come "*an amorphous space that does not occupy a set physical or geographic location*" (p. 1). Il cyberspazio può divenire campo di battaglia anche per attacchi economici, politici e in genere per ogni sorta di frode informatica, sia per mano di privati che di enti pubblici, tanto che si parla di "cyberguerra" e "cyberterrorismo", W. DIFFIE, S. LANDAU, *Il selvaggio mondo delle intercettazioni*, in *Le Scienze*, novembre 2008, n. 483, 72-73.

[282] S. NANAVATI, M. THIEME, R. NANAVATI, *Biometrics. Identity verification in a networked world*, cit., 10-11.

La nozione di "identificazione", a sua volta, è chiamata in causa dallo stesso concetto di identità digitale, e verrà intesa nell'accezione più concreta, ossia come "associazione di dati ad uno specifico essere umano"[283].

Si paventa, in particolare, la possibilità, in alcuni paesi già in atto, che si pervenga alla creazione di un sistema di identificazione nazionale (*NIDS*, *National Identification System*), ovvero di un unico *database*, che faciliti la gestione completa ed immediata delle informazioni sul conto di ogni cittadino[284]. Ciò potrebbe verificarsi mediante l'integrazione di singole banche dati settoriali, contenenti dati riguardo ai principali ambiti in cui si svolge l'attività del soggetto, da quello amministrativo a quello, in particolare, relativo ai rapporti con la giustizia.

Naturalmente, i dati biometrici verrebbero chiamati immediatamente in causa nella costruzione di un *NIDS*.

Efficacemente, si è detto che un tale sistema generalizzato di identificazione rimuove e trasferisce l'identità di una persona in tessere, numeri, e banche dati, cosicché "*identity exists in a document rather than in a person, as people become paper, plastic, or electronic subjects*"[285]. In questo modo, la propria identità può essere accidentalmente smarrita, o dolosamente sottratta.

Un *National ID* presenta, invero, innumerevoli altri punti di debolezza[286].

Anzitutto, crea, ma ad un tempo nega, le identità dei soggetti, di modo che lo Stato può espandere il proprio potere arbitrariamente. La vita, in altre parole, viene

[283] Anche di "identificazione" potrebbero darsi più definizioni, tuttavia, è opportuno considerare che nel mondo dell'*Information Technology*, l'identificazione assume finalità concrete, cioè è utilizzata per collegare ad una persona una serie di dati, e dunque è utile evitare le determinazioni di significato più astratte, R. CLARKE, *Human identification in information systems: management challenges and public policy issues*, in 7 *Information Technology & People* (1994), 7-8.
[284] Si veda l'interessante contributo di R. SOBEL, con riferimento all'esperienza statunitense, *The Demeaning of Identity and personhood in National Identification Systems*, in 15 *Harvard Journal of Law & Technology* (2002), 373.
[285] *Ibidem*, 373.
[286] Per la critica al NIDS, si consideri sempre il contributo di R. SOBEL, op. cit., pp. 362 ss.

compenetrata dal potere, entra nei suoi giochi, nella ricerca spasmodica e ossessiva della sicurezza, cosicché la libertà viene imprigionata sempre più nel circuito dell'autoconservazione[287]. Si parla, a questo proposito, come è già stato approfondito, di biopolitica, ovvero di quella scienza che "non rimanda soltanto, o prevalentemente, al modo in cui da sempre la politica è presa - limitata, compressa, determinata - dalla vita, ma anche e soprattutto a quello in cui la vita è afferrata, sfidata, penetrata dalla politica"[288].

In secondo luogo, e con particolare riferimento ai dati in questione, l'accumulo di informazioni sui soggetti espone al rischio della creazione di profili individuali, capovolgendo così il principio della presunzione di innocenza e rendendo ogni persona, in via preventiva, sospettata: è il *guilty body*, il corpo colpevole[289].

La creazione di profili individuali espone altresì ad indebite classificazioni e discriminazioni, violando il fondamentale principio di uguaglianza (art. 3 Cost.)[290].

Infine, si può agevolmente rilevare che, nei paesi in cui è stato sperimentato un sistema di identificazione nazionale, come nello Stato d'Israele, non è stato risolto il problema della sicurezza né è stata eliminata la piaga del terrorismo.

4. (*Segue*) Frode d'identità.

Uno dei fondamentali problemi connessi alla creazione di una identità digitale è, come si è accennato, la possibilità che essa venga sottratta all'interessato, per venire

[287] R. ESPOSITO, *Bios. Biopolitica e filosofia*, cit., 72.
[288] *Ibidem*, 23.
[289] *Ibidem*.
[290] Sul rapporto tra identificazione e discriminazione, G. ALPA, *Identità e discriminazioni*, in *Nuova giur. civ. comm.*, suppl. fasc. 4/2007, 33-35. Si veda, inoltre, I. VAN DER PLOEG, *The Politics of Biometric Identification. Normative aspects of automated social categorization*, in *www.biteproject.org/documents/politics_of_biometric_identity%20.pdf*, spec. pp. 6 ss.

illecitamente utilizzata, concretizzando l'ipotesi del c.d. "furto d'identità" (*identity theft*).

Tale fenomeno, pur essendo molto diffuso, è poco noto nella sua estensione e gravità e, al fine di favorirne la prevenzione, sarebbe auspicabile che gli enti e le istituzioni maggiormente implicati, quali ad esempio le istituzioni finanziarie, denunciassero pubblicamente la portata del problema, indicando il numero di casi rilevati, le tipologie di frodi, l'ammontare di perdite subite[291].

Di furto d'identità o, più opportunamente, di "frode d'identità" (*identity fraud*)[292], si parla generalmente quando un soggetto, con finalità criminose, intenzionalmente crea la copia di una identità che non gli appartiene, utilizzando l'identità di un diverso soggetto ovvero di una persona inesistente[293].

La frode d'identità apre la strada alla commissione di innumerevoli altri reati. Una volta, infatti, che una persona si sia appropriata dell'identità altrui, venendo con successo riconosciuta dal sistema che intende raggirare, può servirsi di tale privilegio

---

[291] A questo proposito, vale la pena ricordare l'interessate studio condotto da C. J. HOOFNAGLE, *Identity Theft: Making the Known Unknowns Known*, in 21 *Harvard Journal of Law & Technology* (2007), 98, ove l'a. efficacemente dichiara che il furto d'identità rientra nelle "*known unknowns*", ovvero nelle cose che "si sa di non conoscere", di cui è necessario invero venire a conoscenza. Si illustrano, pertanto, le sfide e i benefici che la soluzione della "pubblica conoscenza" produrrebbe. Si veda altresì S. L. GARFINKEL, *Informazioni del mondo, unitevi!*, in *Le Scienze*, novembre 2008, n. 483, 98.

[292] Si tratta dei c.d. *ID-related crime*, ovvero dei reati connessi all'identità. Comunemente, *identity theft* e *identity fraud* vengono utilizzati come sinonimi. Nel panorama giuridico italiano ricorre solitamente l'espressione "furto d'identità", e non "truffa (o frode) d'identità", tuttavia si è precisato che sussiste una distinzione, tale che è preferibile utilizzare, con riguardo a quanto si intende qui trattare, la seconda. Infatti, se il reato di furto è ipotizzabile in riferimento a beni materiali, di furto d'identità non potrebbe parlarsi in questo caso, stante, per così dire, l'immaterialità dell'oggetto considerato. Inoltre, marcare l'accezione del "furto" sposta l'attenzione quasi esclusivamente all'ambito penale, senza tener conto che l'uso dell'identità altrui potrebbe giustificare in ambito civile la richiesta da parte della vittima di risarcimento del danno. Per la distinzione tracciata, si veda FIDIS, *ID-related Crime: Towards a Common Ground for Interdisciplinary Research*, in *http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp5-del5.2b.ID-related_crime.pdf*, 05 May 2006**,** 12-13.

[293] Questa la definizione di J. Grijpink: "*ID fraud is when someone with malicious intent consciously creates the semblance of an identity that does not belong to him, using the identity of someone else or of a non existing person*". Secondo il Ministero della giustizia tedesco, invece, "*identity fraud concerns forms of misuse or fraud with respect to identity and identity data, with which a person or a group of persons intends to unlawfully claim government services, or to otherwise unlawfully benefit himself*". Si veda, al riguardo, FIDIS, *ID-related Crime: Towards a Common Ground for Interdisciplinary Research*, cit., 10-12.

per il perseguimento di più finalità illecite. Si pensi solo alle frodi negli ambiti delle carte di credito, dei conti bancari e degli assegni, del commercio, dell'immigrazione clandestina, della pubblica sicurezza oppure dei benefici assistenziali[294].

Invero, i sistemi di identificazione biometrica si collocano in modo ambivalente lungo lo scenario dell'*identity fraud*: essi, infatti, possono essere riguardati come strumenti atti a contrastare tale fenomeno ma, ad un tempo, possono divenire essi stessi oggetto di incriminazione, potendo essere facilmente contraffatti[295].

Per quanto riguarda quest'ultima ipotesi, sono prospettabili, sul piano prettamente tecnico, diversi scenari[296], che si collocano all'interno di distinte tipologie di attacchi perpetrabili contro i sistemi di identificazione biometrica[297].

Una prima tipologia di interventi fraudolenti si verifica per lo più in fase di raccolta delle informazioni.

Tra questi, sono alquanto diffusi i tentativi di truffa aventi ad oggetto la caratteristica fisiologica o comportamentale stessa. Per frodare un sistema biometrico di riconoscimento del volto, assumendo falsa identità, una persona potrebbe travestirsi

---

[294] Così J. GRIJPINK, *Biometrics and identity fraud protection. Two barriers to realizing the benefits of biometrics – A chain perspective on biometrics, and identity fraud – Part II*, in 21 *Computer Law & Security Report* (2005), 253. Si veda anche N. MITCHISON, M. WILIKENS, L. BREITENBACH, R. URRY, S. PORTESI, *Identity Theft. A Discussion Paper*, cit., 21-22, ove viene indicata la tipica sequenza che porta alla commissione della frode d'identità, e che consiste nei seguenti passaggi: 1. *Fishing for data*; 2. *Misappropriation*; 3. *Misuse*; 4. *Criminal Action*.

[295] Si è detto, circa la possibilità di raggirare i sistemi di identificazione biometrica: "*The current biometric devices are easy to mislead and the current biometric techniques cannot be organised as to resist fraud if used on a wide scale. With patient observation the identity fraudster can discover weak spots in an identity checking process and come up with a method that guarantees his success. New technology thus unintentionally yields the opposite of what is expected of it: instead of better identity verification, more identity fraud!*", J. GRIJPINK, *Identity fraud as a challenge to the constitutional state*, in 20 *Computer Law & Security Report* (2004), 32.

[296] A questo proposito, gli scenari descritti sono riportati nel documento FIDIS, *ID-related Crime: Towards a Common Ground for Interdisciplinary Research*, cit., 85-94. Sulla questione si veda anche M. G. P. FLORA, *Biometria e clonazione delle impronte digitali*, in *Dir. Internet*, 2006, 627-629, che offre chiare indicazioni su come la frode d'identità possa essere facilmente praticata nell'ambito delle biometrie. Questi riporta, tra gli altri, il celebre studio di Matsumoto & Matsumoto che, con la copia di un dito creato utilizzando una sostanza gommosa, riuscirono ad ingannare 8 dispositivi su 10 di rilevazione dell'impronta digitale (p. 629). Ancora, un chiaro schema sulle modalità di frode si rinviene in V. LEE, *Biometrics and identity fraud*, in *Biometric Technology Today* (February 2008), 9.

[297] Così V. LEE, *Biometrics and identity fraud*, cit., 9.

oppure utilizzare una fotografia da collocare di fronte alla telecamera. Immagini fotografiche potrebbero essere utilizzate anche nel caso di riconoscimento dell'iride, così come protesi dell'occhio o lenti a contatto colorate. Per quanto riguarda l'impronta digitale, studi condotti sul campo rivelano come essa possa essere agevolmente riprodotta rilevando le tracce lasciate involontariamente da un soggetto su una superficie. Si riportano altresì casi, ancor più drammatici, di vero e proprio furto, attraverso la mutilazione del dito della persona da frodare o persino di un cadavere. Senza arrivare a tanto, è stato considerato sufficiente che il dispositivo ove viene appoggiato il dito per la rilevazione non sia ben pulito, perché con le impronte residue possa verificarsi un accesso non autorizzato, coprendo la propria mano con un velo di materiale plastico come un sottile guanto di lattice[298]. La stessa tecnica di riconoscimento vocale può essere facilmente raggirata mediante la registrazione della voce.

Una seconda modalità di frode colpisce il sistema tecnologico stesso, agendo in fase di riconoscimento, per esempio alterando la qualità della caratteristica biometrica.

Infine, una terza via consiste nel danneggiare il sensore, al fine di interferire sulla sua capacità di operare una corretta identificazione, riducendone la precisione e l'accuratezza.

Sono poi da considerare gli attacchi che possono essere effettuati in fase di elaborazione e trattamento, agendo sulla funzionalità del sistema. Rientrano in questa categoria le modifiche apportate all'algoritmo di riconoscimento, le riproduzioni dei campioni, gli accessi non autorizzati, oppure il furto dei dati nel corso della comunicazione.

[298] L'esempio è riportato da M. G. P. FLORA, *Biometria e clonazione delle impronte digitali*, cit., 629.

Vanno ricordati, per ultimi, gli interventi fraudolenti nel campo della conservazione del dati.

Alla luce di quanto detto, non pare possibile concordare con quell'opinione per cui le tecnologie biometriche sarebbero più sicure, per venire più difficilmente sottratte, riprodotte e contraffatte, di una semplice *password* o di un PIN[299]. Al contrario, esse sembrano maggiormente esposte alla circonvenzione rispetto ai tradizionali sistemi di identificazione, giustificando così l'adozione di contromisure[300]. Maggiori garanzie potrebbero essere fornite, per esempio, dalla combinazione di più sistemi di autenticazione (una caratteristica biometrica e un PIN oppure una *password*); installando, nel caso di riconoscimento del volto, più telecamere; infine, adottando o potenziando le tecnologie in grado di distinguere tra caratteristiche biometriche reali e fittizie, come protesi o immagini.

Dal punto di vista legislativo, per quanto riguarda il contesto europeo, il fenomeno non è stato regolamentato in via diretta. Invero, il problema in questione si colloca a metà strada tra due ambiti, quello relativo alla protezione dei dati personali e quello che riguarda i reati informatici in genere[301].

Relativamente al primo, si può sostenere che alcune forme di frode d'identità si configurano come una violazione della Direttiva 95/46/CE sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati, con particolare riferimento alla necessità che il soggetto presti il proprio consenso libero e informato per legittimare ogni operazione che abbia ad oggetto i propri dati (art.

---

[299] Grande fiducia sulla sicurezza dei sistemi biometrici, è stata espresso dai ricercatori A. K. JAIN e S. PANKANTI, *Oltre le impronte digitali*, in *Le Scienze*, novembre 2008, n. 483, 76. Si vedano inoltre V. LEE, *Biometrics and identity fraud*, cit., 8 e P. JONES, P. WILLIAMS, D. HILLIER, D. COMFORT, *Biometrics in retailing*, in 35 *International Journal of Retail & Distribution Management* (2007), 219-220.

[300] Così, in particolare, FIDIS, *ID-related Crime: Towards a Common Ground for Interdisciplinary Research*, cit., 102 ss.

[301] Si veda, nuovamente, il documento FIDIS, *ID-related Crime: Towards a Common Ground for Interdisciplinary Research*, cit., 26 ss.

7), e al principio per cui il trattamento deve essere effettuato lecitamente e lealmente, nonché per finalità determinate, esplicite e legittime (art. 6, comma 1°, lett. a e lett. b). Pertanto, per quanto riguarda il nostro Paese, una regolamentazione indiretta della questione si rinviene nello stesso Codice in materia di protezione dei dati personali, come meglio si vedrà in seguito.

Quanto al secondo ambito, il più importante testo europeo in tema di reati informatici è la *Convention on Cybercrime*, adottata a Budapest il 23 novembre del 2001, entrata in vigore il primo luglio del 2004, e ratificata allo stato attuale da 26 Stati, tra i quali è compresa l'Italia, e altresì alcuni paesi extraeuropei, come gli Stati Uniti[302].

È proprio negli Stati Uniti che il fenomeno si è diffuso, portando nel 1998 alla emanazione di una specifica legge, l'*Identity Theft and Assumption Deterrence Act*, ove è considerato responsabile di tale reato chiunque "consapevolmente trasmette o utilizza, senza diritto, un mezzo di identificazione di un'altra persona con l'intenzione di commettere, agevolare o favorire una qualunque attività illecita che costituisca una violazione della legge federale o che rappresenti un crimine per le leggi statali o locali"[303].

Così come nella Direttiva 95/46/CE, nella stessa Convenzione sul *cybercrime* non sono contenuti riferimenti diretti all'*identity fraud*, tuttavia vengono definiti alcuni reati che sono ad essa strettamente connessi: si tratta dell'accesso illegale (art. 2), dell'intercettazione illegale (art. 3), della contraffazione informatica (art. 7), e della frode informatica (art. 8).

---

[302] COUNCIL OF EUROPE, *The Convention on Cybercrime*, in *http://www.coe.int/*. Lo stato delle ratifiche è riferito al 19.11.2009. Il 5 giugno 2008 l'Italia ha ratificato la Convenzione, che è entrata in vigore il primo ottobre del medesimo anno.

[303] "*knowing transfer or use, without lawful authority, of a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law*" (§ 003). Tale legge ha riformato il Capitolo 47 del Titolo 18 del Codice Penale statunitense, sul tema delle frodi e attività connesse. Essa è reperibile in *http://www.ftc.gov/os/statutes/itada/itadact.htm.*

Esplicito richiamo si ritrova, infine, nell'*Explanatory Memorandum* del documento emanato dall'Assemblea parlamentare del Consiglio d'Europa il 6 aprile 2001, dal titolo: "*Europe's fight against economic and transnational organized crime: progress or retreat?*", ove il furto d'identità a fini di truffa viene considerato il crimine in più rapida crescita del nostro tempo[304].

5. Dal diritto alla riservatezza al diritto alla protezione dei dati personali: l'affermazione dell'*habeas data*.

Una volta delineata la relazione corpo-biometria e identità-biometria, rimane da definire il rapporto tra informazione e biometria. In altri termini, è necessario indagare la natura giuridica del dato biometrico, al fine di ascrivere l'informazione in questione all'ambito della disciplina sul trattamento dei dati personali.

Pare tuttavia opportuno, prima di procedere in tale direzione, approfondire il problema più volte sollevato dell'esistenza di un autonomo diritto alla protezione dei propri dati, come facoltà del soggetto di mantenere il controllo sulla circolazione delle informazioni che lo riguardano e di determinare liberamente le modalità di costruzione della propria sfera privata.

Tale diritto si afferma come elemento costitutivo del nuovo *habeas data*, di cui raccoglie tutte le dimensioni, e il cui fondamento si rinviene nell'art. 8 della *Carta dei diritti fondamentali dell'Unione europea*.

In particolare, esso si è separato, quasi per una naturale spinta indotta dal progresso tecnologico, dal diritto alla *privacy*, inteso invece come "diritto al rispetto

[304] PARLIAMENTARY ASSEMBLY, COUNCIL OF EUROPE, EXPLANATORY MEMORANDUM BY THE RAPPORTEUR, *Europe's fight against economic and transnational organized crime: progress or retreat?*, 6 April 2001, in *http://assembly.coe.int/documents/workingdocs/doc01/edoc9018.htm*, n. 54.

della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni" (*Carta dei diritti fondamentali dell'Unione europea*, art. 7), per dare vita ad un nuovo diritto fondamentale della persona[305].

Se si considerano i caratteri propri dei due diritti, si comprende perché assumano portata diversificata, benché taluni abbiano scorto, piuttosto che la nascita di un autonomo diritto, una sorta di ramificazione del diritto alla riservatezza, come se la *privacy* avesse due anime che convivono, l'una volta alla protezione della persona da invasioni della sfera privata, l'altra, invece, tesa a conferire al soggetto poteri di controllo sulla raccolta e circolazione delle informazioni[306].

Oppure, c'è chi ha lasciato intendere che il diritto alla *privacy* si sia evoluto verso la dimensione della protezione dei dati personali, segnando il definitivo tramonto della originaria sfera del segreto, dell'esclusione, del "*right to be let alone*"[307].

---

[305] Nell'ambito della dottrina italiana, per la tesi dell'autonomia del diritto alla protezione dei dati personali rispetto al diritto alla *privacy*, si vedano: G. RESTA, *Il diritto alla protezione dei dati personali*, cit., 11-63; E. GIANNANTONIO, voce «Dati personali (tutela dei)», cit., spec. pp. 483-487; UGO DE SIERVO, *Tutela dei dati personali e riservatezza*, in AA.VV., *Diritti, nuove tecnologie, trasformazioni sociali. Scritti in memoria di Paolo Barile*, Padova, Cedam, 2003, spec. pp. 307 e 308; S. RODOTÀ, *Tra diritti fondamentali ed elasticità normativa: il nuovo Codice sulla privacy*, cit., spec. pp. 2 e 3; S. RODOTÀ, *Prefazione*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, I, Milano, Giuffrè, 2006, spec. pp. VIII-X; S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, Cedam, 2006, spec. pp. 62-79. In particolare, G. Mirabelli ha sostenuto che "un mero inquadramento di questo interesse nella figura del diritto alla tutela della vita privata o del diritto alla riservatezza non sembra offrire quel particolare soddisfacimento che consiste nell'evitare il conglobamento di informazioni per scopi non desiderati o non previsti. Anche se si accetta una nozione di diritto alla riservatezza che sia la più ampia possibile e si ammette che in questo vanno annoverate non soltanto le ipotesi di diritto soggettivo specificatamente previste dalle norme di legge, ma anche una ampia considerazione della posizione sociale del soggetto nell'ambito della collettività, si deve riconoscere che la tutela che l'ordinamento offre alla riservatezza è una tutela repressiva e sanzionatoria, successiva al verificarsi della lesione. L'interesse di cui si tratta richiede, invece, una tutela preventiva, diretta ad evitare la stessa possibilità di lesione", G. MIRABELLI, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Dir. inf.*, 1993, 317, e, ancor più esplicitamente, si vedano pp. 323 e 326.

[306] Così, in particolare, R. PARDOLESI, Dalla *riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003, spec. pp. 6, 8, 14, 16. Per la non univocità della nozione di riservatezza, si veda C. COSSU, *Il diritto alla riservatezza nel nuovo diritto delle banche dati*, in *Giur. it.*, 1997, IV, 367-368. Nello stesso senso anche A. ALTERMAN, *"A piece of yourself": ethical issues in biometric identification*, in 5 *Ethics and Information Technology* (2003), 139-150.

[307] In questo senso pare orientato G. Resta, che altrove tuttavia aveva affermato l'autonomia dei due diritti (cfr. nota n. 307). Egli, infatti, dichiara che la *privacy* "non è più sinonimica di una sfera protetta ed inaccessibile a terzi, ma significa ormai controllo sulla circolazione delle proprie informazioni, tanto in privato quanto in «pubblico»", G. RESTA, *Privacy e processo civile: il problema della litigation*

A sostegno della tesi delle separazione delle due posizioni giuridiche si può osservare, anzitutto, che la tutela della riservatezza risponde alle esigenze di una società liberale, che intende fornire ai cittadini "strumenti di opacità" (*opacity tools*) contro gli interventi dello Stato oppure di attori privati, garantendo l'autonomia dei soggetti, proteggendo da interferenze e contrastando la diffusione di informazioni personali[308].

In particolare, questa sfera di non-accesso può riguardare tanto la dimensione spaziale, fisica o psicologica, quanto la sfera informazionale, vale a dire il patrimonio di informazioni sulla propria persona. In qualunque forma si presenti, dunque, la *privacy* si configura come "*a state of separateness from others*", e si connota di una valenza principalmente negativa, definendo un ambito di esclusione e proibizione, piuttosto che di libertà[309].

Esempio di tale tensione è l'art. 8 della *Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali* (1950), laddove, dopo aver proclamato il diritto al rispetto della vita privata, si dichiara che non è permessa l'ingerenza di una autorità pubblica nell'esercizio di tale diritto, salvo non sia una legge

---

«anonima», in *Dir. inf.*, 2005, 684. Così anche A. Bellavista, che parla di *emblematica trasformazione* "della definizione della *privacy* da «diritto ad essere lasciato solo» a «diritto a controllare l'uso che altri facciano delle informazioni che mi riguardano»", A. BELLAVISTA, *Quale legge per le banche dati?*, in *Riv. crit. dir. priv.*, 1991, 684-685.

[308] Particolarmente interessante la distinzione tra *opacity tools* e *transparency tools*, per la quale si consideri anzitutto P. DE HERT, S. GUTWIRTH, *Making sense of privacy and data protection: a prospective overview in the light of the future of identity, location-based services and virtual residence*, in EUROPEAN COMMISSION, JRC, IPTS, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A prospective Overview*, in *http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20STUDY/20823-ExeSummEN.pdf*, 138-146. Significativo altresì il saggio di S. GUTWIRTH, *Biometrics between opacity and transparency*, in 43 *Ann. ist. super. sanità* (2007), 61-65, ove l'a. dichiara: "*Opacity tools are legal tools/measures that protect individuals and their liberty/autonomy against state interventions and against private actors: they guarantee the non-interference in individual matters, they work as shields or bulwarks*" (p. 61). A questo proposito, si veda inoltre P. DE HERT, *Biometrics: legal issues and implications*, cit., 19. Pur non ricorrendo alla distinzione tra strumenti di opacità e strumenti di trasparenza, l'idea dell'opacità e della trasparenza e la loro contrapposizione è stata sviluppata anche da E. GIANNANTONIO, voce «Dati personali (tutela dei)», cit., 483.

[309] Sulla distinzione tra *spatial privacy* e *informational privacy* e sulla configurazione di tale diritto come "uno stato di separazione dagli altri", si veda G. LAURIE, *Genetic privacy. A challenge to medico-legal norm*, Cambridge University press, 2002, 6.

a prescriverlo oppure non costituisca una misura necessaria all'interno di una società democratica[310].

Tuttavia, il diritto alla riservatezza non segna necessariamente un'insanabile separazione tra ambito privato e ambito pubblico, ponendoli in conflitto. In realtà, l'esercizio di tale potere, mentre limita, ad un tempo consente l'inserimento del singolo nei diversi contesti sociali e civili, assumendo in questo modo anche una valenza positiva[311].

Al contrario, il diritto alla protezione dei dati personali si iscrive negli "strumenti di trasparenza" (*transparency tools*), dal momento che consente di regolare, incanalare, controllare l'esercizio del potere da parte di soggetti pubblici e privati, rispondendo pertanto all'ideale di una società democratica, basata sulla reciproca conoscenza da parte dei consociati. Esso si realizza nella possibilità di conoscere e gestire le informazioni raccolte sul proprio conto, indipendentemente dalla loro diffusione, mediante, per esempio, il potere di accedere ad esse o di consentire al loro utilizzo[312].

---

[310] CONSIGLIO D'EUROPA, *Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali* (1950), art. 8, "1. Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui".

[311] Sul "*positive role of privacy*", si veda il saggio di P. DE HERT, S. GUTWIRTH, *Making sense of privacy and data protection: a prospective overview in the light of the future of identity, location-based services and virtual residence*, cit., 139-40. Gli a., in particolare, sottolineano il ruolo della *privacy* quale quintessenza dello Stato democratico, il quale "*is precisily based upon the idea that its legitimacy can only result from a maximal respect of each person's individual liberty*" (p. 139). Così anche S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, cit., 590, ove tuttavia non è chiara ancora la linea di demarcazione tra diritto alla protezione dei dati personali e diritto alla *privacy* informazionale. Si veda, infine, S. GUTWIRTH, *Biometrics between opacity and transparency*, cit., 62, per la quale gli *opacity tools* "[…] *on the one hand they work as shields against interferences in individual matters, but on the other, and simultaneously, they provide the solid ground for a successful a public sphere in which the democratic political life can take form*".

[312] Si considerino ancora: P. DE HERT, S. GUTWIRTH, *Making sense of privacy and data protection: a prospective overview in the light of the future of identity, location-based services and virtual residence*, cit., 144-146; S. GUTWIRTH, *Biometrics between opacity and transparency*, cit., 62, che conclude: "*In other words, transparency tools tend to make the powerful transparent and accountable*"; infine, E. GIANNANTONIO, voce «Dati personali (tutela dei)», cit., 483.

Anche i mezzi di tutela sono dunque diversificati, prevalendo, nel caso della riservatezza, gli strumenti di carattere risarcitorio, mentre, nel caso della tutela dei dati personali, quelli di natura inibitoria[313].

Infine, un ulteriore elemento di distinzione, si rinviene considerando che, mentre il diritto alla riservatezza non ha per oggetto un bene esterno alla persona, ma trova nella persona il suo punto di riferimento oggettivo, il diritto alla protezione dei dati personali ha per oggetto un bene esterno ad essa, il dato, che tuttavia, come si è detto, veicola l'identità e dunque si pone in stretta correlazione con la persona stessa[314].

Dal combinato disposto degli artt. 1 e 2 del Codice in materia di protezione dei dati personali, si coglie come il legislatore italiano stesso abbia inteso allargare l'ambito di trasparenza dei poteri, consacrando il nuovo diritto all'*habeas data*, laddove si dichiara il diritto di ognuno alla protezione dei dati personali che lo riguardano (art. 1) e che il Codice "garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali" (art. 2) [315].

Potrebbe sembrare che le disposizioni in esame abbiano una portata meramente declamatoria, tuttavia, a fronte dell'innegabile e sempre più pervasiva raccolta di informazioni sugli individui all'interno di banche dati, sollecitata dallo sviluppo del potere informatico[316], tenuto conto dei documenti giuridici di portata sopranazionale,

---

[313] E. GIANNANTONIO, voce «Dati personali (tutela dei)», cit., 483-484.
[314] *Ibidem*, 484-485.
[315] Si veda G. RESTA, *Il diritto alla protezione dei dati personali*, cit., 41, che parla di "apertura del catalogo dei diritti fondamentali riconosciuti nell'ordinamento italiano ad una 'nuova' posizione soggettiva di rango primario", e aggiunge: "Gli artt. 1 e 2 del *Codice* si iscrivono così all'interno di quel processo di universalizzazione e integrazione su base transnazionale del sistema dei diritti, tipico dell'attuale esperienza di 'costituzionalismo cooperativo' o *multilevel*, di cui rappresentano un chiaro ed importante riflesso". Così anche T. M. FROSINI, *Tecnologie e libertà costituzionali*, cit., 490, per il quale, già a partire dalla l. n. 675 del 1996, il diritto alla libertà informatica trova riconoscimento nell'ordinamento giuridico.
[316] Si veda il cap. II.

appare chiaro l'intento dei primi due articoli del Codice, che è quello di "immergere più profondamente il diritto alla protezione dei dati personali nella dimensione dei diritti fondamentali, confermandone e rafforzandone la rilevanza"[317].

Invero, benché la distinzione vada mantenuta sotto più profili, è opportuno segnalare che tra i due diritti non sussiste totale incompatibilità[318]: essi vivono in un rapporto di complementarietà, presupponendosi l'un l'altro in un delicato bilanciamento, in cui l'ordinamento è chiamato ad intervenire "senza elevare l'autodeterminazione informativa a dogma aprioristicamente sottratto a controllo, ma altresì senza sacrificare in nome di un astratto principio di trasparenza reali esigenze di protezione delle persone coinvolte"[319].

Tale equilibrio va ricercato ancor più attentamente quando si parla di sistemi biometrici, avendo cura di distinguere caso per caso dove l'ago della bilancia debba pendere, poiché non esiste una soluzione univoca, ma variabile da contesto a contesto e da applicazione ad applicazione[320].

---

[317] Così S. RODOTÀ, *Tra diritti fondamentali ed elasticità normativa: il nuovo Codice sulla privacy*, cit., 3. Si veda, inoltre, il commento alle disposizioni generali del Codice di G. P. Cirillo, in G. P. CIRILLO (a cura di), *Il Codice sulla protezione dei dati personali*, cit., 3, ove l'a. dichiara: "La diretta derivazione della norma dalla Carta dei diritti del cittadino europeo viene riconosciuta dalla stessa relazione al «Codice», che, pur nella sua estrema sinteticità, chiarisce anche l'autonomia del diritto contemplato nell'art. 1 rispetto al diritto alla riservatezza nonché il fatto che esso vada collocato tra i diritti fondamentali della persona". Dello stesso avviso anche C. Filippi, commento ai principi generali, art. 1, in G. P. CIRILLO (a cura di), *ult. op. cit.*, 11-12.

[318] E. GIANNANTONIO, voce «Dati personali (tutela dei)», cit., 483; S. GUTWIRTH, *Biometrics between opacity and transparency*, cit., 63; P. DE HERT, *Biometrics: legal issues and implications*, cit., 19.

[319] Si consideri, in particolare, G. RESTA, *Privacy e processo civile: il problema della litigation «anonima»*, cit., 684. Così anche M. G. LOSANO, *Un progetto di legge sulla protezione dei dati personali*, in *Dir. inf.*, 1987, 469-470, ove l'a. parla del "difficile equilibrio" tra trasparenza e riservatezza. L'ordinamento, pertanto, è chiamato a interrogarsi di volta in volta sugli strumenti a cui ricorrere e sulla loro concreta applicabilità: " […] *how much of what tool is necessary and when? When will opacity (privacy) be called upon, when will transparency (data protection) apply? How to combine the tools appropriately, especially when faced with new challenges, such as today's insistence of various government initiatives on security or the development of new technologies?*", S. GUTWIRTH, *Biometrics between opacity and transparency*, cit., 64.

[320] Così S. GUTWIRTH, *Biometrics between opacity and transparency*, cit., 64-65.

6. La complessa qualificazione giuridica dei dati biometrici. I dati biometrici come dati personali.

Non è presente, nell'attuale panorama giuridico italiano, una definizione di dato biometrico, benché il termine biometria, a partire dal 1997, abbia fatto la sua comparsa in diversi corpi normativi.

Il primo riferimento si rinviene negli artt. 1, comma 1°, lett. g, e 3, comma 3°, del d.p.r. 513/97, sulla trasmissione con strumenti informatici e telematici di documenti nell'ambito della pubblica amministrazione, ove si richiama il concetto di chiave biometrica, di cui viene offerta una chiara definizione[321].

Successivamente, il d.p.c.m. 437/1999, in tema di carta d'identità e documento d'identità elettronico, contiene un ulteriore richiamo alla chiave biometrica, dichiarando che la carta di identità elettronica può contenere non solo le informazioni e applicazioni necessarie per la firma digitale, ma anche tutti gli elementi necessari per generare la chiave biometrica (art. 4)[322].

Invero, la prima vera e propria menzione di dato biometrico, compare nel d. lgs. 443/2000, ove si dichiara che la carta d'identità e i documenti elettronici possono

[321] Decreto del Presidente della Repubblica 10 novembre 1997, n. 513, *Regolamento contente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'art. 15, comma 2, della legge 15 marzo 1997, n. 59*, in G.U. 13 marzo 1998, serie generale, n. 60. In particolare, l'art. 1, comma 1°, lett. g, dispone che per chiave biometrica deve intendersi "la sequenza di codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità basati su specifiche caratteristiche fisiche dell'utente". A questo proposito, si vedano i contributi *Firma digitale o garanzie biometriche*?, in *Riv. giur. sarda*, 2001, fasc. 1, 293 ss.: G. DUNI, *L'autenticità degli atti in forma elettronica*, 295-298; M. C. SIDDI, *Chiavi biometriche e impatto sulla pubblica amministrazione*, 298-303; G. GERRA, *Alcune tecniche di identificazione biometrica di pratica attuabilità*, 303-306; P. GIACALONE, *Il riconoscimento biometrico e l'utilizzo della firma digitale*, sarda, 307-309; E. SANNA, *Le garanzie di sicurezza e autenticità delle informazioni in rete*; *in particolare del mandato informatico di pagamento*, cit., 310-315; G. DUNI, *Conclusioni: cosa chiedono i giuristi ai tecnici?*, 315-320.

[322] Decreto del Presidente del Consiglio dei Ministri 22 ottobre 1999, n. 437, *Regolamento recante caratteristiche e modalità per il rilascio della carta d'identità elettronica e del documento di identità elettronico, a norma dell'art. 2, comma 10, della legge 15 maggio 1997, n. 127, come modificato dall'art. 2, comma 4, della legge 16 giugno 1998, n. 191*, in G.U. 25 novembre 1999, n. 277.

contenere dati biometrici, purché non si tratti di DNA (art. 36, comma 3°, lett. c)[323]. Disposizione analoga si rinviene nel d.p.r. 117/2004, in tema di carta nazionale dei servizi[324].

Infine, si ricordano due Decreti del Ministro degli Affari Esteri relativi al passaporto elettronico, l'uno del 29 novembre 2005, l'altro del 31 marzo 2006. In particolare, essi disciplinano la modalità di raccolta e conservazione dei dati in questione, disponendo che i dati biometrici saranno utilizzati solo nell'ambito di sistemi di verifica dell'identità e pertanto non saranno conservati in banche di dati[325].

---

[323] Decreto Legislativo 28 dicembre 2000, n. 443, *Disposizioni legislative in materia di documentazione amministrativa (Testo B)*, in G.U. n. 42, 20 febbraio 2001, suppl. ordinario n. 30. Il decreto, contiene anche, alla lettera e) del medesimo articolo, un riferimento alla chiave biometrica.

[324] Decreto del Presidente della Repubblica, *Regolamento concernente la diffusione della carta nazionale dei servizi, a norma dell'art. 27, comma 8, lett. b), della legge 16 gennaio 2003, n. 3*, art. 36, comma 3°, lett. c), in G.U. n. 105, 6 maggio 2004.

[325] Ministero degli Affari Esteri, *Decreto 29 novembre 2005 relativo al passaporto elettronico*, in G.U. n. 13 del 17 gennaio 2006, art. 2: "Nella revisione dei processi di emissione del passaporto ordinario e degli sviluppi tecnologici è previsto l'inserimento del microprocessore RF/ID di prossimità (chip) nella copertina del passaporto, conforme alla direttiva ISO 1443, alle specifiche ICAO OS/LDS con capacità minima di 64Kb e curabilità di almeno 10 anni. Nel chip verranno memorizzate, in formato interoperativo, l'immagine del volto e le impronte digitali del dito indice di ogni mano. Ove, in una mano, l'impronta del dito indice non fosse disponibile si utilizzerà per la stessa, procedendo in successione, la prima impronta disponibile nelle dita medio, anulare e pollice. Nel chip verranno altresì memorizzate le informazioni già presenti sul supporto cartaceo relative al passaporto ed al titolare, nonché i codici informatici per la protezione ed inalterabilità dei dati e quelle necessarie per renderne possibile la lettura agli organi di controllo. Gli elementi biometrici contenuti nel chip potranno essere utilizzati solo al fine di verificare l'autenticità del documento e l'identità del titolare attraverso elementi comparativi direttamente disponibili quando la legge preveda che siano necessari il passaporto o altro documento di viaggio. I dati biometrici raccolti ai fini del rilascio del passaporto non saranno conservati in banche di dati. La presente disposizione si applica anche alla normativa sui passaporti diplomatici e di servizio".
Il riferimento ai dati biometrici, si rinviene, poi, nel *Decreto 31 marzo 2006 sul passaporto elettronico* del Ministero degli Affari Esteri, in G.U. n. 88 del 14 aprile 2006, art. 2, art. 5, art. 6, art. 8, art. 10. In particolare, l'art. 6 dispone: "1. Il passaporto elettronico assume come dati biometrici, in coerenza con quanto specificato nell'art. 1, comma 2, del Regolamento del Consiglio dell'Unione europea n. 2252/2004, l'immagine del volto e le impronte digitali in formato interoperativo. 2. Le caratteristiche relative al tipo, formato, qualità e disposizioni di memorizzazione di tali elementi biometrici, devono essere conformi alle decisioni della Commissione europea riguardanti le specifiche tecniche relative alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio. 3. In particolare gli elementi biometrici devono soddisfare le prescrizioni indicate nella decisione della Commissione europea C(2005) 409 del 28 febbraio 2005". Importante anche l'art. 8, ove si dichiara che, nella «banca dati passaporti» istituita presso il Dipartimento della pubblica sicurezza del Ministro dell'interno, "non sono registrate le impronte digitali e dati biometrici", e inoltre: "Gli elementi e i dati biometrici possono essere utilizzati solo per finalità di verifica dell'identità del titolare del passaporto".

Per procedere all'ascrizione del dato biometrico, tanto nella forma di dato grezzo, quanto in quella di *template*, nell'alveo della disciplina sul trattamento dei dati personali, si rende necessario, in prima battuta, accertarsi che si tratti di "dato personale", nel senso indicato dal Codice in materia di protezione dei dati personali.

Secondo l'art. 4, comma 1°, lett. b, del Codice, che riprende la più dettagliata disposizione della Direttiva 95/46/CE sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[326], si definisce dato personale "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale". È utile, a questo proposito, il più specifico riferimento che si rinviene nell'art. 2 della Direttiva 95/46/CE, ove, in particolare, si accenna a "un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale"[327].

Tenendo conto delle caratteristiche proprie del dato biometrico[328], per prima cosa si può rilevare che esso costituisce senz'altro un'informazione concernente una persona fisica[329].

---

[326] L'articolo citato riprende l'art. 2, lett. a), della 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*, il quale, più dettagliatamente, definisce il "dato personale" come "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". Più sintetica la definizione dell'art. 2 della *Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108)*, Council of Europe, Strasbourg, 28.I.1981, "*personal data means any information relating to an identified or identifiable individual*".

[327] C.vo agg.

[328] Si veda cap. I.

[329] GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria*, cit., 5, per cui: "I dati biometrici possono sempre essere considerati come «informazione concernente una persona fisica» in quanto sono dati che, per loro stessa natura, forniscono informazioni su una determinata persona".

Qualche dubbio si scorge, invece, per quanto riguarda il requisito della identificabilità, che riguarda soggetti in partenza non identificati, i quali tuttavia possono in un successivo momento divenire tali mediante interventi intermedi, come attraverso altre informazioni ricollegabili in via indiretta ai dati trattati ovvero ricorrendo ad operazioni di decodificazione[330].

Questo concetto si presenta, dunque, molto ampio, essendo possibile individuare categorie di dati che possono condurre ad identificare una persona, pur non avendo spesso, in apparenza, tale proprietà[331].

A tal proposito, per stabilire se una persona sia o meno identificabile, la Direttiva 95/46/CE dispone che "è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare la persona"[332], ove il criterio della ragionevolezza allude sostanzialmente all'uso di mezzi proporzionati, per cui risalire al soggetto interessato non richiede un dispendio eccessivo di risorse[333]. Oltre questo confine, si giunge, perlomeno sul piano teorico, nel terreno dell'anonimia, di cui si dirà. È sufficiente, inoltre, che il solo responsabile del trattamento sia in grado di identificare il soggetto interessato perché quest'ultimo possa considerarsi identificabile[334].

---

[330] M. ATELLI, M. MAZZEO, *Le definizioni del Codice dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il Codice del trattamento dei dati personali*, cit., 34.

[331] P. DE HERT, *Biometrics: legal issues and implications*, cit., 13-14. Si veda anche M. ATELLI, M. MAZZEO, *Le definizioni del Codice dei dati personali*, cit., 34.

[332] Si veda la considerazione preliminare n. 26 della Direttiva 95/46/CE.

[333] M. ATELLI, M. MAZZEO, *Le definizioni del Codice dei dati personali*, cit., 35. Dello stesso avviso P. M. VECCHI, *Commento art. 4, 1°comma, lett. b*, in C. M. BIANCA, F. D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, cit., 54-55.

[334] P. DE HERT, *Biometrics: legal issues and implications*, cit., 13-14, ove l'a. aggiunge: "*The definition of 'identifiable' is so broad that data data can be considered personal as long as the controller himself is still able to identify the persons behind the data*". È stata opportunamente valutata anche l'ipotesi in cui l'interessato possa essere individuato dal responsabile correlando i dati oggetto del trattamento con informazioni oggetto di trattamento da parte di altro responsabile. Non è sembrato opportuno considerare, in questo caso, il soggetto come identificabile, poiché sarebbe astrattamente possibile che ogni trattamento di dati, anche in forma anonima, si configuri come trattamento di dati personali, essendo astrattamente possibile che in qualunque contesto siano raccolti dati suscettibili di identificare gli interessati. Il Garante, tuttavia, è parso giungere a conclusioni diverse quando, in uno dei provvedimenti

Alla luce delle considerazioni svolte, tendendo conto altresì dell'orientamento pressoché unanime della dottrina italiana e internazionale[335], si può ben sostenere che, in linea di principio, i dati biometrici rientrano nella categoria dei dati personali.

Tale soluzione trova conferma nei dati normativi di cui si dispone.

Anzitutto, il fondamentale Documento di lavoro sulla biometria, dichiara che "le misure di identificazione biometrica o la loro traduzione in un modello sono, nella maggior parte dei casi, dati a carattere personale"[336].

È questa anche la posizione del legislatore italiano, stante l'espressa menzione di dato biometrico all'interno del Codice in materia di protezione dei dati personali, che dispone, all'art. 37, l'obbligo di notifica di trattamento dei dati personali da parte del titolare "solo se il trattamento riguarda: a) dati genetici, biometrici […]" e, all'art. 55, fa

---

in tema di videosorveglianza, ha menzionato la possibilità di collegare, ai fini della identificabilità, i dati in possesso del responsabile con quelli contenuti in archivi di polizia, G. CASSANO, S. FADDA (a cura di), *Codice in materia di protezione dei dati personali*, cit., 55.

[335] Per la dottrina in ambito internazionale, si vedano: P. DE HERT, *Biometrics: legal issues and implications*, cit., 14, per il quale: "*All biometrical technologies are covered by the Directive, with or without recording of the 'raw image' or with our without use of templates*"; P. DE HERT, W. SCHREURS, E. BROUWER, *Machine-Readable Identity Documents with Biometric Data in the EU – Part II*, in 22 *Keesing Journal of Documents & Identity* (2007), 23: "*Biometric data (fingerprints, photos) and alphanumerical data related to persons (age, sex, name, address, etc.) are considered personal data. It is expressly recognized in all Regulations that the Directive 95/46 applies to Eurodac, VIS and the European Passport*"; Y. LIU, *Identifying Legal Concerns in the Biometric Context*, in 3 *Journal of International Commercial Law and Technology* (2008), 46, ove l'a. supporta la tesi sostenuta da De Hert, condividendone le argomentazioni, per cui sostiene: "[...] *the starting point of our discussion is biometric data including raw image and templates, should be regarded as personal data covered by the Data Protection Directive*"; V. ZORKADIS, P. DONOS, *On Biometrics-Based Authentication and Identification from a Privacy-Protection Perspective. Deriving Privacy-Enhancing Requirements*, in 12 *Information Management & Computer Security* (2004), 130: "*Every biometric system has to comply with the principles of data protection legislation because the information being processed can be characterized as personal data*".

Per la dottrina italiana, si vedano: S. BISI, *Il corpo come password: alcune considerazioni in tema di sistemi di autenticazione biometrica*, cit., 14, secondo cui il dato biometrico "rientra nell'ampio alveo dei dati personali"; A. PIERUCCI, *Videosorveglianza e biometria*, in *Libera circolazione e protezione dei dati personali*, in R. PANETTA (a cura di), II, Milano, Giuffrè, 2006, 1662, per la quale questo assunto appare fuori discussione; A. BIASIOTTI, *Le tecnologie biometriche. Sicurezza, contrattualistica, privacy*, cit., 165: "Non vi è alcun dubbio che l'acquisizione di un dato biometrico rappresenti l'acquisizione di un dato personale, anzi personalissimo, perché in pratica unico al mondo"; V. D'ANTONIO, *I dati genetici*, in F. CARDARELLI, S. SICA, V. ZENO ZENCOVICH, *Il codice dei dati personali. Temi e problemi*, Milano, Giuffrè, 2004, 378, il quale si spinge oltre, sostenendo la tesi, che verrà in seguito verificata, di configurare i dati biometrici come *species* del *genus* dati genetici.

[336] GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria*, cit., 5. L'affermazione viene ribadita in sede di conclusioni: "Il gruppo ritiene che la maggior parte dei dati biometrici comporti il trattamento di dati personali", p. 12.

riferimento al "trattamento di dati personali che implica maggiori rischi di un danno all'interessato, con particolare riguardo a banche di dati genetici o biometrici […]".

La giurisprudenza dello stesso Garante per la protezione dei dati personali porta a concludere che i dati biometrici "sono senza dubbio dati personali"[337]. Tale considerazione trova conferma in tutti i provvedimenti in tema di biometria[338].

In particolare, il Garante afferma che "sia le impronte dattiloscopiche, ancorché raccolte in modo parziale e solo ai fini del completamento della fase dell'*enrollment*, sia i codici numerici successivamente utilizzati per le descritte operazioni di confronto, in quanto informazioni riferibili ai singoli lavoratori, sono dati personali (art. 4, comma 1, lett. *b*), del Codice). Ne discende, pertanto, l'applicazione della disciplina contenuta nel Codice, così nella fase dell'*enrollment*, come pure in relazione alle successive operazioni di confronto (con il correlato tracciamento degli orari di ingresso/uscita dal luogo di lavoro)"[339].

---

[337] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Videosorveglianza e biometria – Trattamento dati personali mediante utilizzo di impronte digitali*, 19 novembre 1999, doc. web n. 42058, in *www.garanteprivacy.it*.

[338] La prima affermazione in tal senso compare, come si è detto, nel provvedimento *Videosorveglianza e biometria – Trattamento dati personali mediante utilizzo di impronte digitali*, 19 novembre 1999, doc. web n. 42058, cit. Si vedano, di seguito, i provvedimenti *Videosorveglianza - Impronte digitali per l'accesso in banca - 11 dicembre 2000*, doc. web n. 30903; *Videosorveglianza - Raccolta di impronte digitali associate ad immagini per l'accesso a banche – 7 marzo 2001*, doc. web n. 30947; *Videosorveglianza e dati biometrici - Rilevazioni biometriche presso istituti di credito - 28 settembre 2001*, doc. web n. 39704; *Compiti del Garante - Uso delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro - 21 luglio 2005*, doc. web n. 1150679; *Istituti di credito - Rilevazione di impronte digitali ed immagini: limiti e garanzie - 27 ottobre 2005*, doc. web n. 1246675; *Accesso ad aree riservate di particolari aziende: uso proporzionato di impronte digitali - 23 novembre 2005*, doc. web n. 1202254; *Dati biometrici e Rfid nelle banche - 23 febbraio 2006*, doc. web n. 1251535; *Uso della biometria per identificazione del personale nelle banche - 15 giugno 2006***,** doc. web n. 1306098; *Trattamento di dati biometrici con finalità di verifica della presenza dei dipendenti e di accesso a particolari aree produttive - 15 giugno 2006*, doc. web n. 1306551; *Sicurezza merci e controllo delle presenze presso aeroporti - 26 luglio 2006*, doc. web n. 1318582; *Trattamento di dati personali biometrici per l'accesso a un complesso polifunzionale - 1 febbraio 2007*, doc. web n. 1381983; *Sicurezza siti archeologici e uso dei dati biometrici - 8 novembre 2007*, doc. web n. 1461908; *Trattamento di dati biometrici presso Cariprato S.p.A. - 23 gennaio 2008*, doc. web n. 1490382; *Trattamento di dati biometrici presso Banca San Paolo Imi S.p.A. - 23 gennaio 2008*, doc. web n. 1490533; *Provvedimento del 23 gennaio 2008*, doc. web n. 1487903; *Trattamento dei dati biometrici di dipendenti per garantire la salute pubblica - 15 febbraio 2008*, doc. web n. 1497675; *Riconoscimento vocale e gestione di sistemi informatici - 28 febbraio 2008*, doc. web n. 1501094.

[339] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Compiti del Garante - Uso delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro – 21 luglio 2005*, doc. web. n. 1150679,

Infine, il *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data* dichiara che i dati biometrici sono dati personali. In particolare, il documento sottolinea come, a sostegno di questa tesi, in dottrina emergano diverse argomentazioni: da una parte, l'argomento della intrinseca natura identificativa, per cui i dati biometrici, per loro stessa natura, rendono necessariamente una persona identificabile; dall'altra, la tesi per cui essi, solo in determinate circostanze, possiedono questa proprietà[340]. Il Rapporto, tuttavia, conclude sottolineando il carattere sostanzialmente superfluo del dibattito suddetto poiché, dal momento in cui i dati sono raccolti in vista di un trattamento automatico, c'è la possibilità che siano collegati ad una persona identificata o identificabile[341].

7. (*Segue*) Il problema dell'anonimia.

È opportuno segnalare che le conclusioni raggiunte potrebbero rivelarsi inadeguate qualora il dato biometrico non sia salvato all'interno di una base dati

---

cit. Il caso riguardava un'industria di coperture in fibrocemento e metalliche che aveva presentato una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, per il trattamento di dati biometrici dei dipendenti finalizzato ad accertarne la presenza sul luogo di lavoro e commisurare la retribuzione da corrispondere. L'Autorità reputò non lecito il trattamento, sulla base della valutazione principio di proporzionalità. Altro esempio significativo, in proposito, si rinviene nel provvedimento *Accesso ad aree riservate di particolari aziende: uso proporzionato di impronte digitali - 23 novembre 2005*, doc. web n. 1202254, cit., relativo ad un'azienda fornitrice di tecnologie per la difesa nel settore avionico ed elettronico, per il trattamento di dati biometrici di un numero ristretto di dipendenti non superiore a quindici unità, finalizzato a controllarne gli accessi in un'area aziendale circoscritta. Ivi analogamente si dispone: "Sia le impronte digitali, sia i dati da esse ricavati successivamente utilizzati per verifiche e raffronti nelle procedure di autenticazione o di identificazione sono informazioni personali riconducibili ai singoli interessati (art. 4, comma 1, lett. b), del Codice), alle quali trova applicazione la disciplina contenuta nel Codice".

[340] COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, cit., 15-16, punti n. 51-52.

[341] *Ibidem*, punto n. 52: "*The Committee finds it unnecessary to decide whether biometric data are personal data in themselves or whether this is only the case under certain circumstances. It is of the opinion that as soon as biometric data are collected with a view to automatic processing there is the possibility that these data can be related to an identified or identifiable individual. In those cases the Convention applies*".

computerizzata, ove normalmente viene collegato con altre informazioni relative alla persona, rendendola perciò identificabile, bensì in un dispositivo portatile in possesso dell'interessato[342].

In questo caso, infatti, non si renderebbe necessario collegare il dato in questione con altre informazioni relative al soggetto, dal momento che non si tratterebbe di attribuire l'identità (identificazione), bensì di verificare se la persona sia chi realmente dichiara di essere (verifica o autenticazione). Il dato, in altri termini, potrebbe essere salvato come anonimo. Se si propendesse, tuttavia, per la tesi della intrinseca natura identificativa dei dati biometrici, neppure nella ipotesi sopraindicata si potrebbe parlare di anonimia[343].

Di là dal riconoscimento di un'eventuale natura identificativa propria dei dati biometrici, cosa che pare in ogni caso difficile da sostenere[344], è certo che il problema della c.d. "anonimia" o "anonimizzazione", vale a dire la possibilità di salvare le informazioni senza che vengano ricollegate alla persona da cui sono estratte, di modo che non sia più applicabile la disciplina sul trattamento dei dati personali, è tutt'altro che secondario.

---

[342] Si veda C. PRINS, *Making Our Body Identify for Us: Legal Implications of Biometric Technologies*, in 14 *Computer Law & Security Report* (1998), 160 e 163. In questo senso, si può allora sostenere: "*Not all biometrical data and not all means of storing biometrical data are subject to the laws regarding the protection of personal data*", C. PRINS, *Body ID*, in 3 *The EDI Law Review* (1997), 160. L'a. sottolinea come il desiderio che si raggiunga l'anonimato è cresciuto drammaticamente nella società attuale, dove lo scambio di dati personali aumenta in modo incontrollato (p. 163).

[343] Si è detto: "[…] *with regard to biometric data the option of making the data anonymous is not available as biometric data by their very nature, form an instrument to identify individuals, particularly when they are automatically processed*", Y. LIU, *Identifying Legal Concerns in the Biometric Context*, cit., 48.

[344] "*A biometric personal characteristic is therefore by definition person-related, but is not necessarily a personal detail. The decisive factor regarding the legal position of a biometric detail is therefore whether it can be traced back to the right person, if necessary making a good deal of effort*". Se il dato biometrico all'interno di una certa applicazione è realmente anonimo, allora: "*There are no legal obstacles to the use of anonymous biometrics*", J. GRIJPINK, *Biometrics and Privacy*, in 17 *Computer Law & Security Report* (2001), 156.

Il Codice dispone, all'art. 4, comma 1°, lett. n, che per dato anonimo deve intendersi quello che "in origine, o *a seguito di trattamento*, non può essere associato ad un interessato identificato o identificabile"[345].

Dunque, a differenza del dato personale identificabile, deve sussistere un'assoluta impossibilità di risalire all'interessato, che permanga anche a fronte di operazioni di collegamento con altri dati[346].

La definizione pone, invero, alcuni problemi, se si considera il riferimento all'anonimizzazione derivante da successivo procedimento.

Da più parti si ritiene, infatti, che il concetto di anonimia si configuri come un concetto relativo, tale che un dato può essere anonimo per qualcuno e non per qualcun altro, in determinate circostanze e non in altre, per certi scopi e non per altri[347]. Si è parlato, pertanto, di "retorica dell'anonimia", poiché "la opacizzazione dell'identità è perlopiù un fenomeno parziale, temporaneo, valido per taluni soggetti che accedono alle informazioni, ma non per chi possiede le chiavi di decodifica"[348].

Si può sostenere, allora, che non esiste una *full anonymity*, che un dato personale non può essere anonimo in assoluto[349], a meno che non lo sia da principio, come

---

[345] C.vo agg. La rilevanza del dato anonimo si rinviene anche nella direttiva 95/46/CE che, al considerando n. 26, dichiara: "[…] i principi della tutela non si applicano a dati resi anonimi in modo tale che la persona interessata non è più identificabile".

[346] Si rimanda a M. ATELLI, M. MAZZEO, *Le definizioni del Codice dei dati personali*, cit., 41.

[347] Sulla relatività del concetto di anonimato, si vedano sia Y. LIU, *Identifying Legal Concerns in the Biometric Context*, cit., 48, sia C. PRINS, *Making Our Body Identify for Us: Legal Implications of Biometric Technologies*, cit., 164, ove l' a. sostiene che l'anonimizzazione può variare da situazione a situazione. Dello stesso avviso G. FINOCCHIARO, *Alcune riflessioni sul trattamento dei dati personali*, in *Contr. e impr.*, 2006, 1427.

[348] Si veda M. TALLACCHINI, *Retorica dell'anonimia e proprietà dei materiali biologici umani*, in F. D'AGOSTINO (a cura di), *Corpo esibito, corpo violato, corpo venduto, corpo donato. Nuove forme di rilevanza giuridica del corpo umano*, cit., 181. Le riflessioni condotte dall'a. con riferimento ai materiali biologici umani (*Human Biological Materials*, HBMs), possono essere riferite anche al caso dei dati biometrici, benché per essi non si pratichi alcun prelievo di materiale.

[349] Per la distinzione tra *full anonymity* e *relative anonymity*, per cui, in base alla prima accezione, in nessun caso è possibile tracciare l'identità, in base alla seconda, invece, solo in determinate circostanze, si veda C. PRINS, *Making Our Body Identify for Us: Legal Implications of Biometric Technologies*, cit., 164. Il principio per cui il dato non è in assoluto anonimo è ribadito più volte da G. FINOCCHIARO, *Alcune riflessioni sul trattamento dei dati personali*, cit., spec. p. 1431.

nell'ipotesi dell'impronta digitale lasciata da un cliente in un ristorante sul bicchiere con il quale ha bevuto (perché naturalmente le sue impronte non siano già conservate in una qualche banca dati)[350], mentre, se è stato reso "anonimo" solo in un secondo momento, esiste sempre la ragionevole possibilità che venga ricondotto al soggetto interessato[351].

A ragione, dunque, si è detto che il procedimento di anonimizzazione "è una costruzione giuridica più che tecnico-scientifica, nel senso che il riferimento che le norme giuridiche fanno ai criteri tecnici tende ad assumere questi - *iuris et de iure* – come più certi di quanto essi non pretendano. Il «dato anonimo» rappresenta così non tanto il recepimento giuridico di un'informazione de-soggettivata, ma il frutto di una costruzione e presunzione giuridica, che tende a cancellare ogni residuo interesse del soggetto-dei-dati nei confronti dei materiali biologici"[352].

Non va confuso, dunque, il dato cifrato o munito di un codice di riferimento, con il dato potenzialmente anonimo, configurandosi il primo come un qualsiasi altro dato identificato o identificabile, fintanto che sia collegato o sia collegabile ad un soggetto determinato. Lo stesso processo di estrazione del *template* dall'immagine non può considerarsi un processo di anonimizzazione. Si può ritenere, piuttosto, che l'impiego del *template* sia una modalità di trattamento dei dati *privacy enhancing*, in grado

---

[350] L'esempio è riportato da J. GRIJPINK, *Biometrics and Privacy*, cit., 156, il quale correttamente osserva: "*This could explain why we don't concern ourselves too much with this glassware in practice*".

[351] M. TALLACCHINI, *Retorica dell'anonimia e proprietà dei materiali biologici umani*, cit., 181, ove l'a. sostiene, con riferimento ai materiali biologici, che essi "sono, fin dall'inizio, o identificati o anonimi, e che solo gli esemplari nati come anonimi continuano a godere di tale statuto una volta destinati alla ricerca (*unidentified samples*)". A proposito della possibilità di risalire all'identità del soggetto cui il dato "anonimo" si riferisce, si veda anche W. W. LOWRANCE, *Learning from Experience. Privacy and the Secondary Use of Data in Health Research*, in *http://www.nuffieldtrust.org.uk/ecomm/files/161202learning.pdf*, 29, ove l'a. dichiara che, con le interconnessioni di banche dati e con le tecniche di cui si dispone, il processo di re-identificazione è relativamente semplice, per cui quanto si può chiedere in tema di anonimizzazione è un "*«acceptable degree» of anonymisation with identifiers and code-keys not accesible by researchers who have access to the anonymised data*". Considerazioni analoghe si rinvengono in M. ATELLI, M. MAZZEO, *Le definizioni del Codice dei dati personali*, cit., 41.

[352] Così M. TALLACCHINI, *Retorica dell'anonimia e proprietà dei materiali biologici umani*, cit., 176.

semplicemente di assicurare una maggiore garanzia sul piano della non immediata accessibilità alle informazioni[353].

8. Dati biometrici come categoria *sui generis* distinta da altri dati personali.

Si tratta ora di definire se i dati biometrici si possano considerare alla stregua di qualsiasi altro dato di natura personale, ovvero se rientrino in una categoria particolare, in virtù del loro carattere, per così dire, personalissimo, non essendo semplicemente "dati sul corpo", bensì, in qualche modo, "il corpo stesso".

I caratteri di specialità dei dati in questione sono principalmente l'universalità, l'unicità, la permanenza e la stabilità nel tempo, benché, come si è detto, simili proprietà non debbano essere intese in senso assoluto[354]. Altro aspetto peculiare, è il fatto che tali informazioni possono essere tanto "stabili" quanto "comportamentali dinamiche". Infine, alcuni dati biometrici si contraddistinguono per poter essere raccolti anche all'insaputa dell'interessato[355].

Un primo riconoscimento significativo nella direzione della specialità viene offerto dal Documento di lavoro sulla biometria, ove, dopo aver espresso preoccupazione in relazione alla tutela dei diritti e delle libertà fondamentali degli individui, si dichiara che "si tratta di dati di carattere speciale in quanto riguardano le

[353] "[…] *we have to agree, that this kind of application mentioned by Grijpink is somewhat privacy enhancing, and it managed to make the biometric information not so directly identifiable. But whether it amounts to the anonymous level that can be excluded from the data protection constraint is still controversial*", Y. LIU, *Identifying Legal Concerns in the Biometric Context*, cit., 48-49. Tuttavia, come si è visto, questa opinione non trova appoggio nei documenti in tema di biometria.
[354] Si veda cap. I, par. 4.
[355] A. PIERUCCI, *Videosorveglianza e biometria*, cit., 1663.

caratteristiche comportamentali e fisiologiche di un individuo e sono tali da consentire l'identificazione univoca" [356].

Un altro contributo, in senso analogo, è costituto dal *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data.*

Nella parte conclusiva del Rapporto, al punto n. 107, si dichiara: "I dati biometrici devono essere considerati come una categoria specifica di dati poiché essi sono presi dal corpo umano, rimangono inalterati nei diversi sistemi e sono in via di principio inalterabili nel corso della vita". Il requisito dell'inalterabilità, vale tuttavia, come appena detto, "in via di principio". Si supponga, per esempio, si tratti di un sistema biometrico di identificazione o di verifica basato sul riconoscimento del volto: l'invecchiamento, talune malattie, determinati interventi chirurgici o incidenti, potrebbero alterare le caratteristiche del volto e il sistema non sarebbe più in grado di riconoscere il soggetto in questione.

Altro elemento specifico dei dati biometrici, così come indicato dal punto n. 63, è "la possibilità che essi contengano più dati di quelli necessari allo scopo di verificare o identificare gli individui": per esempio, dalla scansione dell'iride si potrebbero ricavare informazioni circa una malattia da cui la persona è affetta.

Il legislatore italiano riconosce che ai dati biometrici va riservata speciale attenzione, stante l'applicazione ad essi, su espresso rinvio dell'art. 55, dell'art. 17 del Codice in materia di protezione dei dati personali, che riguarda "il trattamento di dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà

[356] GRUPPO PER LA TUTELA DEI DATI PERSONALI (articolo 29), *Documento di lavoro sulla biometria,* cit., 2.

fondamentali, nonché per la dignità dell'interessato". Il riferimento è ai dati c.d. "semisensibili", tra i quali pertanto rientrano anche i dati biometrici[357].

La particolarità dei dati biometrici è stata riconosciuta più volte dallo stesso Garante per la protezione dei dati personali[358]. Nelle Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati (deliberazione n. 53 del 23 novembre 2006), si dichiara infatti: "Tali dati, per la loro peculiare natura, richiedono l'adozione di elevate cautele per prevenire possibili pregiudizi a danno degli interessati, con particolare riguardo a condotte illecite che determinino l'abusiva «ricostruzione » dell'impronta, partendo dal modello di riferimento, e sua ulteriore «utilizzazione» a loro insaputa"[359].

9. Dati biometrici come dati sensibili.

Una volta identificati i dati biometrici come dati di carattere personale, si pone il problema se essi siano suscettibili di essere considerati come dati di natura sensibile. La questione si presenta particolarmente complessa, data l'incertezza delle conoscenze

[357] G. P. CIRILLO, *Il Codice sulla protezione dei dati personali*, cit., 80. Oltre ai dati biometrici, dati "semisensibili" sono anche quelli che ledono il diritto all'immagine, i nominativi presenti nelle centrali rischi utilizzate nel settore creditizio, le liste dei sospettati, i provvedimenti disciplinari, i dati raccolti per assistenza sociale e per effettuare sondaggi di opinione.

[358] In particolare, nel discorso tenuto da S. Rodotà alla presentazione della Relazione del 2001, il Presidente ha affermato: "Per valutare questa nuova dimensione del trattamento dei dati personali, è indispensabile considerare anzitutto le particolarità dei dati biometrici, che «catturano» la personalità di ciascuno anche in forme che esigono un rigoroso rispetto del criterio di proporzionalità e del principio di dignità, riferimento per noi sempre obbligato […]", S. RODOTÀ, *Una scommessa impegnativa sul terreno dei muovi diritti*, cit.

[359] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati (deliberazione n. 53 del 23 novembre 2006)*, in *www.garanteprivacy.it*, 7. Lo scopo delle linee guida è indicato nella premessa, ove si dichiara che esse sono adottate al fine di "fornire indicazioni e raccomandazioni con riguardo alle operazioni di trattamento effettuate con dati personali (anche sensibili) di lavoratori operanti alle dipendenze di datori di lavoro privati". Ai dati biometrici è dedicato l'intero punto 4.

scientifiche di cui si dispone e non essendo possibile pervenire a soluzioni generalizzate. Da una parte, infatti, le caratteristiche biometriche sono molteplici ed eterogenee, dall'altra, ciascuna può essere utilizzata in applicazioni diversificate.

Prima di procedere ad una più puntuale trattazione, è opportuno soffermarsi sulla definizione di dato sensibile, prendendo le mosse, ancora una volta, dal Codice in materia di protezione dei dati personali, che definisce i dati in questione come "dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute" (art. 4, 1° comma, lett. d)[360].

Evidentemente, i dati biometrici che potrebbero essere considerati di natura delicata, sono quelli idonei a rivelare l'origine razziale ed etnica, ovvero lo stato di salute del soggetto. È opportuno distinguere poi tra dati biometrici grezzi, ossia immagini, e *templates*, poiché, mentre per il dato grezzo c'è generale accordo in dottrina sul fatto che possa, in determinate ipotesi, essere ascritto alla categoria dei dati sensibili[361], lo stesso non può dirsi per il *template*.

Considerando le immagini, esse potrebbero facilmente svelare l'origine razziale o etnica, come nel caso palese del riconoscimento del volto. Simili informazioni si potrebbero ricavare mediante altre caratteristiche fisiologiche, come attraverso il rilevamento dell'odore del corpo o il riconoscimento vocale[362]. Il rischio maggiore, a

[360] Si veda la Direttiva 95/46/CE, art. 8, 1°comma, "Gli stati membri vietano il trattamento di dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale".

[361] Si vedano: Y. LIU, *Identifying Legal Concerns in the Biometric Context*, cit., 46; P. DE HERT, *Biometrics: legal issues and implications*, cit., 17; P. DE HERT, W. SCHREURS, E. BROUWER, *Machine-readable identity documents with biometric data in the EU – part III*, in 23 *Keesing Journal of Documents & Identity* (2007), 28; V. ZORKADIS, P. DONOS, *On Biometrics-Based Authentication and Identification from a Privacy-Protection Perspective. Deriving Privacy-Enhancing Requirements*, cit., 133; CNIPA, *Linee guida per l'impiego delle tecnologie biometriche nelle pubbliche amministrazioni. Indicazioni operative*, cit., 61.

[362] P. DE HERT, *Biometrics: legal issues and implications*, cit., 17, ove si afferma che il riconoscimento della voce "*could as well give information relating to racial or ethnic origin or health*".

questo riguardo, è quello del c.d. "*ethnic profiling*" o "*racial profiling*", che consiste nell'utilizzo della razza, del colore, della lingua, della religione, della nazionalità o dell'origine nazionale o etnica come criterio determinante nell'ambito delle politiche di sicurezza, ossia in attività di controllo, di sorveglianza, o investigative, di modo che una persona viene sospettata di una condotta pregiudizievole solo sulla base di elementi legati alla razza o all'etnia di appartenenza. Ciò, evidentemente, conduce a possibili gravi forme di discriminazioni, con la conseguente violazione della stessa legislazione europea posta a garanzia dei diritti dell'uomo, di cui si ricorda, in particolare, la recente raccomandazione n. 11 della Commissione europea sulla lotta al razzismo e all'intolleranza, del 29 giugno 2007[363].

Sembra altresì sussistere una stretta correlazione tra biometria e medicina. Le immagini biometriche sono suscettibili infatti di fornire, in più ipotesi, informazioni riguardanti lo stato di salute del soggetto[364]. In primo luogo, ferite o variazioni dello stato di salute possono impedire che una persona venga registrata o riconosciuta dal sistema biometrico. In secondo luogo, informazioni di carattere medico possono essere desunte confrontando il dato catturato durante il processo di *enrollment* e i successivi confronti effettuati in tempi differenti. In terzo luogo, i dati biometrici possono rivelare direttamente informazioni sullo stato di salute: l'immagine del volto può indicare la presenza di una qualche sindrome o malattia, si pensi ad un soggetto affetto da sindrome di Down[365]; il riconoscimento dell'iride, e ancor più della retina, può facilmente svelare

[363] "*The use by the police, with no objective and reasonable justification, of grounds such as race, colour, language, religion, nationality or national or ethnic origin in control, surveillance or investigation activities*" (par. 1), COUNCIL OF EUROPE, EUROPEAN COMMISSION AGAINST RACISM AND INTOLERANCE (ECRI), *Recommendation n. 11 on combating racism and racial discrimination in policing*, in *http://www.coe.int/t/dghl/monitoring/ecri/activities/gpr/en/recommendation_n11/e-RPG%2011%20-%20A4.pdf*. Si veda, inoltre, il contributo di O. DE SCHUTTER, J. RINGELHEIM, *Ethnic Profiling: A Rising Challenge for European Human Rights Law*, in 71 *The Modern Law Review* (2008), spec. pp. 372 ss., ove l'a. sottolinea come, nell'ambito della lotta al terrorismo, i servizi di *intelligence* ricorrano sempre più a dati personali concernenti l'origine razziale o etnica conservati all'interno di *databases*.

[364] Così E. MORDINI, S. MASSARI, *Body, biometrics and identity*, cit., 491.

[365] P. DE HERT, W. SCHREURS, E. BROUWER, *Machine-readable identity documents with biometric data in the EU – part III*, cit., 29.

informazioni di natura medica delicate[366]; sono state altresì individuate delle correlazioni tra il disegno dell'impronta digitale e la presenza di particolari patologie[367]; infine, un ulteriore esempio, può essere rappresentato dai dati biometrici di carattere comportamentale, per i quali, attraverso l'analisi dell'andatura o verificando la firma manoscritta, è possibile ricavare informazioni sullo stato di salute del soggetto.

Un problema che non ha ricevuto sufficiente attenzione è, invece, se anche i *templates* debbano essere considerati, in talune ipotesi, come dati sensibili.

A questo proposito, sono due le modalità con cui da questa stringa alfanumerica si potrebbero ricavare informazioni di tale natura: ricostruendo, a partire dal *template*, l'immagine o parte di essa, ovvero ottenendo direttamente dal *template* l'informazione sensibile[368].

Mentre la prima ipotesi sembra sia stata provata[369], la seconda è dubbia, cosicché la questione è destinata a rimanere, allo stato attuale, controversa[370].

---

[366] *Ibidem*, 28-29, ove si sostiene:"*Biometric data of disabled people may relate to their medical condition and correlations could, for example, be drawn between papillary patterns and diseases such as leukaemia and breast cancer*".

[367] Y. LIU, *Identifying Legal Concerns in the Biometric Context*, cit., 46. L'a. riporta il caso di una malattia chiamata CIP, che determina un disegno raro dell'impronta digitale. È stato individuato, inoltre, un legame tra il disegno dell'impronta digitale e l'omosessualità. Anche altre informazioni (randotipica, comportamentale, o i segni immutabili) possono essere rilevanti nel dare indicazioni sull'origine razziale, etnica o sullo stato di salute.

[368] Questa interessante argomentazione è stata proposta, ancora una volta, da Y. LIU, *Identifying Legal Concerns in the Biometric Context*, cit., 46.

[369] Di tale avviso è Y. LIU, *Identifying Legal Concerns in the Biometric Context*, cit., 46, benchè altri si siano espressi in senso diametralmente opposto. Si vedano, per la tesi della impossibilità di configuarare il *template* come dato sensibile, E. MORDINI, S. MASSARI, *Body, biometrics and identity*, cit., 492; C. PRINS, *Making Our Body Identify for Us: Legal Implications of Biometric Technologies*, cit., per la quale "*the template representing this information does not qualify as sensitive personal data because, as mentioned above, this digital data of the template cannot be translated back into the biometrical information (the sensitive information of a person's skin cannot be traced on the basis of a template). This means that a template as such never constitutes sensitive data*" (p. 162), e ancora:"[...] *whereas the 'raw data' can be translated into the set of numbers of the template, the numbers cannot be translated back into the 'raw data'. In other words, an individual's fingerprint cannot be traced on the basis of a template"* (p. 160); inoltre, J. GRIJPINK, *Biometrics and Privacy*, cit., 157, che afferma: "[…] *it is not possible to retrospectively calculate the original image of the fingerprint from the biometric number (template)*".

[370] Circa il carattere sensibile o meno di dati biometrici conservati sotto forma di *template*, dubbi sono stati espressi anche da P. DE HERT, *Biometrics: legal issues and implications*, cit., 17 e P. DE HERT, SCHREURS W., BROUWER E., *Machine-readable identity documents with biometric data in the EU – part III*, cit., 29, ove si afferma che "*it is unclear whether the algorithms and machine-readble templates that contain the information are always to be treated as sensitive personal data*".

Pur nell'incertezza che regna, pare lecito riconoscere che i dati biometrici si distinguono da altre categorie di dati proprio per la loro attitudine ad essere "*key data*", in grado cioè, anche quando non sono sensibili, di derivare il carattere della sensibilità dall'informazione a cui si può avere accesso attraverso la "chiave" [371]. In altri termini, vi sono "dati che, di per se stessi insuscettibili di essere immediatamente ascritti alla categoria dei dati particolari, possono però, sulla base di un procedimento logico induttivo o deduttivo, condurre a rivelare informazioni di un certo tipo, in relazione al particolare contesto in cui avviene il trattamento"[372].

Ci si può allora interrogare se è sufficiente proteggere i dati biometrici come dati sensibili solo quando in modo evidente rivelano informazioni sullo stato di salute o sull'origine etnica o razziale, come può essere nel caso di alcuni dati grezzi, oppure se non è preferibile considerarli come una nuova categoria di informazioni sensibili, o ancora se la lista presente nell'art. 8 della Direttiva 95/46/CE dovrebbe essere estesa, o se invece dovrebbe essere adottato un approccio alternativo[373].

Lo stesso Documento di lavoro sulla biometria si rivela nebuloso e non offre soluzioni incontrovertibili, asserendo: "Stabilire se un trattamento comprende dati di natura delicata è una questione di valutazione legata alle caratteristiche biometriche specifiche utilizzate nonché all'applicazione biometrica stessa. È maggiormente probabile che sia il caso quando vengono trattati dati biometrici sotto forma di immagini

[371] Y. LIU, *Identifying Legal Concerns in the Biometric Context*, cit., 47.
[372] E. PELLECCHIA, Commento art. 26, in BIANCA C. M., BUSNELLI F. D. (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, cit., 620, nota n. 9, ove opportunamente l'a. osserva che "qualsiasi classificazione delle informazioni personali non può mai risolversi nella definitiva assegnazione di un dato ad una categoria che ne definisca una volta per tutte le modalità della protezione".
[373] Y. LIU, *Identifying Legal Concerns in the Biometric Context*, cit., 47-48. Secondo l'a., la lista di dati personali sensibili dovrebbe diventare una lista aperta, non esaustiva, così da poter aggiungere i dati biometrici o altri dati che con il progresso tecnologico si rivelano sensibili. In conclusione: "*Based on the fact that various kinds of sensitive information can not be technically excluded from the biometric authentication process, biometric template and biometric image in general should be regarded as sensitive personal data in the legal sense*" (p. 53).

dato che in linea di massima i dati grezzi non possono essere ricostruiti a partire dal modello"[374].

Il gruppo dei Garanti europei, dunque, lascia ampia discrezionalità all'interprete, non escludendo categoricamente che il *template* stesso, seppur con minore probabilità, sia qualificabile come dato sensibile, ma negando che i dati biometrici costituiscano, anche quando conservati come immagini, una categoria generale di dati di natura delicata, poiché cioè dipende pur sempre dalla caratteristica in gioco e dall'applicazione utilizzata.

Generica anche la posizione del *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, per il quale i dati biometrici potrebbero rivelare uno stato di malattia oppure l'origine razziale, implicando "*the unavoidable processing of unnecessary data*"[375].

I dati biometrici potrebbero considerarsi, infine, anche dal punto di vista della normativa italiana, dati personali sensibili, stante l'accostamento che viene effettuato con i dati genetici nel Codice in materia di protezione dei dati personali (artt. 37 e 55).

Il Codice, invero, non offre alcuna indicazione specifica, tuttavia, questa scelta del legislatore lascia intendere non si tratti genericamente di dati personali, bensì di dati aventi una forma peculiare e assimilabile, quando vi siano le circostanze, a quella dei dati di natura delicata.

---

[374] GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria,* cit., 11.

[375] COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data,* cit., 19-20, n. 74. Questa ipotesi è destinata a consolidarsi con lo sviluppo tecnologico, che apre la strada a strumenti più precisi e sofisticati, per cui il Rapporto si appella al principio di precauzione: "*The precautionary principle demands that where new techniques may uncover unexpected new information one should be reticent to start with systems where there can be reasonable doubt that in the long run unwanted and possibly irreversible side effects may appear*" (p. 20).

Altro problema è verificare se, come è stato sostenuto, i dati biometrici possano nientemeno essere ritenuti una *species* del *genus* dati genetici.

10. (*Segue*) Informazione genetica *vs.* informazione biometrica: stesso *genus*?

Nell'ambito della dottrina italiana, si è sostenuto che per «dato biometrico» "deve intendersi una particolare categoria di informazioni, all'interno del *genus* dei dati genetici, caratterizzata dalla assoluta singolarità e dalla conseguente diretta riferibilità ad un unico e solo individuo"[376]. Conseguentemente, il trattamento di dati biometrici si configurerà come un trattamento di dati genetici, anche quando si presentano in forma di *template*, poiché, secondo il suddetto orientamento, "attraverso esso è sempre possibile risalire ad una persona fisica «identificata o identificabile»"[377].

Alla luce delle considerazioni svolte in precedenza, questa teoria appare problematica, e pertanto merita una più puntuale trattazione[378]. In particolare, si ritiene opportuno mettere a confronto le due categorie di dati, per verificarne le analogie e il grado di correlazione.

Da tempo si sostiene la particolare natura dei dati genetici rispetto agli altri tipi di informazioni concernenti l'individuo, per cui si parla di "eccezionalità genetica"[379]. Tale eccezionalità si radica sulle caratteristiche proprie dei dati in questione, i quali

---

[376] Questo orientamento è stato proposto solo nell'ambito della dottrina italiana, da parte di V. D'ANTONIO, *I dati genetici*, cit., 375.
[377] *Ibidem*, 378.
[378] In particolare, come si è detto, non trova riscontro l'opinione per cui dal *template* sia *sempre* possibile risalire all'interessato.
[379] Si vedano, *ex multis*, S. GAINOTTI, A. G. SPAGNOLO, *Test genetici: a che punto siamo in Europa? A margine del Rapporto e delle Raccomandazioni della Commissione Europea sugli aspetti etici, giuridici e sociali dei test genetici*, in *Medicina e Morale*, 2004, n. 4, 750-751; L. PICOTTI, *Trattamento dei dati genetici, violazione della privacy e tutela dei diritti fondamentali nel processo penale*, in *Dir. inf.*, 2003, 691; G. LAURIE, *Genetic privacy. A challenge to medico-legal norms*, cit., 104; S. RODOTÀ, *Tra diritto e società. Informazione genetica e tecniche di tutela*, in *Riv. crit. dir. priv.*, 2000, 584.

possiedono *attitudini fortemente predittive* sullo stato futuro di salute, anche se nel momento in cui l'informazione viene raccolta l'individuo non presenta i sintomi di una malattia; si caratterizzano per una particolare *stabilità*, poiché sono inalterabili lungo l'arco della vita; definiscono la *specificità e l'unicità della persona*, rendendo possibile una identificazione sempre più analitica delle sue caratteristiche, in un processo di differenziazione rispetto a tutte le altre; *riguardano la famiglia biologica e i membri di una comunità*, non solo gli individui singoli, pertanto sono strutturalmente condivisi con tutti gli appartenenti ad un medesimo gruppo biologico, cioè il gruppo dei consanguinei; possono fornire *informazioni inaspettate.*

Invero, questa tesi è stata messa in discussione da più parti, in particolare nell'ambito della Commissione europea che, nel Documento *"25 raccomandazioni concernenti le implicazioni etiche, giuridiche e sociali dei test genetici"*[380], ha invitato ad "evitare l'«eccezionalità genetica» a livello internazionale, a livello UE e nei singoli Stati membri" (Raccomandazione n. 3, lett. a)[381].

---

[380] COMMISSIONE EUROPEA, DIREZIONE GENERALE RICERCA, *25 raccomandazioni concernenti le implicazioni etiche, giuridiche e sociali dei test genetici*, in *http://europa.ue.int*. Tale Gruppo, formato da esperti in varie discipline, è stato incaricato di discutere sulle implicazioni etiche, giuridiche e sociali dei test genetici, portando così alla elaborazione di un documento che consta di 25 raccomandazioni, discusso a Bruxelles il 6 e 7 maggio 2004. Le 25 raccomandazioni sono suddivise in tre capitoli (quadro generale; svolgimento di test genetici nei sistemi sanitari; test genetici in quanto strumento di ricerca) e rappresentano un documento di *soft law*, essendo da una parte "codice di buona condotta" per chi opera nel settore, dall'altra "piano d'azione per i test genetici" che i responsabili politici dovrebbero attuare in futuro (p. 6). Si veda, a questo proposito, S. GAINOTTI, A. G. SPAGNOLO, *Test genetici: a che punto siamo in Europa? A margine del Rapporto e delle Raccomandazioni della Commissione Europea sugli aspetti etici, giuridici e sociali dei test genetici*, cit., 750-753. La critica al principio dell' "eccezionalità genetica" è stata espressa anche da G. LAURIE, *Genetic privacy. A challenge to medico-legal norms*, cit., 104-113.

[381] COMMISSIONE EUROPEA, DIREZIONE GENERALE RICERCA, *25 raccomandazioni concernenti le implicazioni etiche, giuridiche e sociali dei test genetici*, Raccomandazione n. 3: "Si raccomanda: a. di evitare l'«eccezionalità» genetica a livello internazionale, a livello UE e nei singoli Stati membri. Tuttavia la percezione diffusa della diversità dei test genetici dovrebbe essere riconosciuta e considerata; b. che tutti i dati medici, ivi compresi i dati genetici, siano conformi a norme rigorose in termini di qualità e riservatezza; c. per monitorare l'evoluzione della percezione del pubblico per quanto riguarda i test genetici ed individuare i temi futuri di dibattito: • di svolgere ulteriori ricerche sugli aspetti etici e sociali dei test genetici che devono essere promosse dalla Commissione europea e da enti nazionali; • di inserire le questioni concernenti i test in indagini su scala quali l'Eurobarometro".
In particolare, più critiche sono state mosse alla tesi dell'eccezionalità: fattori non genetici possono essere altamente predittivi, come l'esposizione a radiazioni o a certe infezioni; certe fattori ambientali come i raggi ultravioletti o l'inquinamento possono influenzare i livelli di rischio per certe malattie in maniera

Il documento non può tuttavia esimersi dal riconoscere, in altri punti, il carattere peculiare dei dati in questione[382].

La maggior parte dei testi giuridici internazionali in tema di dati genetici pare comprovare la tesi dell'eccezionalità. Il recente *Working document on genetic data* dichiara che i dati genetici presentano caratteristiche del tutto singolari rispetto agli altri dati personali relativi alla salute, caratteristiche che vengono minuziosamente elencate e grazie alle quali si ritiene che essi meritino speciale protezione[383]. Il *Working document*

---

irreversibile, come nel caso del tumore alla pelle o l'asma, per cui l'insorgere di una malattia è determinato anche da fattori ambientali o dallo stile di vita; anche le impronte digitali o altri dati personali identificano l'individuo in modo unico; fattori non genetici, come infezioni contagiose quali la tubercolosi, possono fornire informazioni sulla famiglia; una qualsiasi visita medica potrebbe diagnosticare una malattia inaspettata, S. GAINOTTI, A. G. SPAGNOLO, *Test genetici: a che punto siamo in Europa? A margine del Rapporto e delle Raccomandazioni della Commissione Europea sugli aspetti etici, giuridici e sociali dei test genetici*, cit., 750-753.
Inoltre, l'idea dell'eccezionalità nascerebbe da ragioni di ordine logico e storico. In primo luogo, fino ad oggi i test genetici sono stati adottati soprattutto per studiare malattie collegate a un solo gene (monogenetiche), ad esempio la Corea di Huntington, o per alcune forme ereditarie di tumore al seno o al colon, anche se attualmente si stanno identificando i geni coinvolti nelle malattie più comuni, e la maggior parte dei test genetici (come i test per determinare il gruppo sanguigno) non hanno nulla di "eccezionale". Inoltre, la percezione dell'eccezionalità è alimentata dal fatto che non esistano cure per la maggior parte delle malattie monogenetiche. Altri fattori decisivi nello sviluppo di tale percezione sono la perdita di controllo sui campioni e l'idea che le informazioni genetiche possano arrecare particolari danni se svelate impropriamente, per cui renderle una classe a parte comporterebbe anche una riduzione di tale potenziale danno. Si osserva da parte del Gruppo che, di fronte alle paure dei cittadini e del pubblico, i singoli governi e la comunità internazionale hanno mirato a creare documenti, raccomandazioni, leggi, che applicano regole specifiche ai dati genetici, considerati appunto "eccezionali". "Tuttavia queste attività sono accettabili solo in quanto tappa intermedia verso un inquadramento giuridico e regolamentare più globale e strutturale che comprenda tutti i dati e test medici, e che rispecchi i progressi effettuati nella fornitura delle cure sanitarie" (nota introduttiva alla Raccomdazioni n. 3). Concludendo, l'informazione genetica non dovrebbe essere considerata diversamente dagli altri dati medici, ma andrebbe trattata allo stesso modo. In caso contrario, sarebbero agevolati gli abusi e aumenterebbe il rischio di discriminazioni, COMMISSIONE EUROPEA, DIREZIONE GENERALE RICERCA, *25 raccomandazioni concernenti le implicazioni etiche, giuridiche e sociali dei test genetici*, cit.; S. GAINOTTI, A. G. SPAGNOLO, *Test genetici: a che punto siamo in Europa? A margine del Rapporto e delle Raccomandazioni della Commissione Europea sugli aspetti etici, giuridici e sociali dei test genetici*, cit., 750-753.

[382] Si veda, per esempio, la Raccomandazione n. 10, lett. c., che prevede "[…] sia riconosciuto al paziente sia il diritto di essere informato che il diritto di non sapere e siano previsti meccanismi nella pratica medica che rispettino entrambi i diritti. Nell'ambito dei test genetici, si raccomanda di istituire, a tal fine, oltre alle pratiche riguardanti la trasmissione delle informazioni, il *counselling*, le procedure di consenso informato e la comunicazione dei risultati dei test, anche procedure specifiche a tal fine".

[383] "*Genetic data show in themselves characteristics which make them singular, in particular compared to health data. They provide or are likely to provide, in the future, scientific, medical and personal information relevant throughout the life of an individual. This information can also have a significant incidence on the family of the data subject, over several generations and in certain cases on the whole group to which the data subject belongs. The identification by the genetic print also presents a unique nature. Indeed, genetic data are likely to reveal information on several people while making it possible to identify only one of them. They reveal the uniqueness of the data subject. As a result of these specificities,*

on the applications of genetics for health purposes[384], mira a creare un quadro normativo che permetta di controllare i rapidi sviluppi delle tecniche e della conoscenze nel campo della genetica, sancendo implicitamente lo speciale *status* di questi dati. Nell'ambito dell'UNESCO, l'*International declaration on human genetic data*, riconosce apertamente il principio dell'eccezionalità genetica già nel preambolo e in seguito all'art. 4[385].

A questo punto, è necessario chiedersi in che misura i dati biometrici siano equiparabili ai dati genetici e se ne condividano realmente il carattere di specialità.

Come è noto, anche i dati biometrici sono tendenzialmente in grado di definire la *specificità* e l'*unicità* della persona e si contraddistinguono per una certa, seppur inferiore, *stabilità* nel tempo. Tuttavia, eccetto il caso del DNA utilizzato con finalità

---

the processing of genetic data requires and justifies a particular legal protection. Such is the object pursued by the working paper on genetic data. But, mankind should not be reduced to its genetic characteristics only, to its sole genetic cartography, which in any case does not constitute the ultimate universal explanation of human life. One of the first guarantee conditioning the use of genetic data should therefore be to avoid attributing to these data a universal explanatory value. Genetic data thus present a number of characteristics which can be summarised as follows: - while genetic information is unique and distinguishes an individual from other individuals it may also at the same time reveal information about and have implications for that individual's blood relatives (biological family) including those in succeeding and preceding generations. Furthermore, genetic data can characterise a group of persons (e.g. ethnic communities); genetic data can reveal parentage and family links; - genetic information is often unknown to the bearer him/herself and does not depend on the bearer's individual will since genetic data are non modifiable; - genetic data can be easily obtained or be extracted from raw material although this data may at times be of dubious quality;- taking into account the developments in research, genetic data may reveal more information in the future and be used by an ever increasing number of agencies for various purposes", DATA PROTECTION WORKING PARTY, *Working document on genetic data*, 17 March 2004, in *www.europa.eu.int*, 4-5.

[384] COUNCIL OF EUROPE, WORKING PARTY ON HUMAN GENETICS, *Working document on the applications of genetics for health* purposes, 7 February 2003, in *http://www.coe.int*.

[385] UNESCO, INTERNATIONAL BIOETHICS COMMITTEE, *International Declaration on Human Genetic Data*, 16 October 2003, in *http://www.unesco.org*, ove nel preambolo si dichiara: "*Also recognizing that human genetic data have a special status on account of their sensitive nature since they can be predictive of genetic predispositions concerning individuals and that the power of predictability can be stronger than assessed at the time of deriving data; they may have a significant impact on the family, including offspring, extending over generations, and in some instances on the whole group; they may contain information the significance of which is not necessarily known at the time of the collection of biological samples; and they may have cultural significance for persons or groups*". L'art. 4, intitolato "*special status*", enuncia per punti e ancor più chiaramente il carattere di eccezionalità già esplicitato nel preambolo: essi potrebbero avere funzione predittiva, un impatto significativo sulla famiglia nonché sull'intero gruppo cui la persona appartiene, contenere informazioni il cui significato non è necessariamente conosciuto al tempo in cui sono raccolti i campioni biologici, avere un significato culturale per le persone o i gruppi.

identificative, non condividono due dei caratteri fondamentali propri dei dati genetici: non hanno attitudini predittive e non sono strutturalmente condivisi con tutti gli altri appartenenti al medesimo gruppo biologico.

Va da sé che la tesi per cui "il trattamento di dati biometrici è un trattamento di dati genetici" deve essere quantomeno attentamente vagliata[386].

A parere di chi scrive, infatti, non sembra possibile considerare *sic et simpliciter* il dato biometrico, ivi compresa la sua traduzione in un *template*, alla stregua del dato genetico[387].

Questa posizione trova conferma nello stesso dato normativo, anzitutto considerando che i documenti giuridici internazionali in tema di biometria non fanno alcun riferimento alla possibilità di estendere analogicamente la disciplina sul trattamento dei dati genetici al trattamento dei dati biometrici.

In secondo luogo, lo stesso legislatore italiano, pur non dando alcuna indicazione a questo proposito, riserva l'art. 90 del Codice in materia di protezione dei dati personali ai soli dati genetici, e non ha esteso la recente Autorizzazione Generale sul trattamento di tali dati ad altre categorie di informazioni. Invero, nel documento sopraccitato, si trova un cenno ai dati biometrici, ma per disporre che l'accesso ai locali ove sono custoditi i dati genetici "è controllato mediante incaricati della vigilanza o strumenti elettronici che prevedano specifiche procedure di identificazione anche mediante dispositivi biometrici"[388].

---

[386] V. D'ANTONIO, *I dati genetici*, cit., 375.

[387] Conclusioni analoghe sembrano essere state raggiunte da L. Trucco, la quale dichiara, dopo un breve elenco delle caratteristiche biometriche, che "anche il DNA rientrerebbe in tale categoria, ma, come suggerito dalla stessa sistematica del codice della *privacy*, è opportuno analizzarlo separatamente a motivo delle sue spiccate peculiarità", L. TRUCCO, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, cit., 47-48.

[388] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Autorizzazione al trattamento dei dati genetici – 22 febbraio 2007*, G. U. n. 65 del 19 marzo 2007, in *www.garanteprivacy.it*, doc. web n. 1389918, punto 4.3 (Misure di sicurezza).

Sembra più coerente allora dedurre che, in mancanza di norme specifiche, per i dati biometrici che possono considerarsi sensibili ovvero data l'elevata probabilità della loro sensibilità, si applicheranno le disposizioni che riguardano i dati di natura delicata e, nel caso in cui si tratti di dati sensibili in grado di rivelare lo stato di salute del soggetto, troveranno applicazione le disposizioni che attengono al trattamento dei dati sanitari in genere. Nelle altre circostanze, pare corretto considerarli come dati c.d. "semisensibili", ovvero che presentano particolari rischi per l'interessato, ma non alla stregua dei dati genetici.

CAPITOLO QUARTO

IL TRATTAMENTO DEI DATI BIOMETRICI

SOMMARIO: 1. Dati biometrici e principi generali sul trattamento dei dati personali. Il principio di necessità. − 2. (*Segue*) I principi di liceità, correttezza, finalità e proporzionalità. - 3. (*Segue*) Il problema della conservazione: *database vs. smart card*. − 4. I diritti dell'interessato come fulcro dell'*habeas data*. In particolare, il diritto di accesso. − 5. Informazione, libertà, consenso. − 6. (*Segue*) Consenso informato e dati biometrici sensibili. - 7. Altri aspetti significativi in tema di trattamento dei dati biometrici: dati biometrici semi sensibili, controllo preliminare e notificazione dei sistemi. - 8. (*Segue*) Misure di sicurezza. Cenni. - 9. Cittadinanza europea e biometria: lo *European passport*. – 10. (*Segue*) L'*Eurodac*. – 11. Uno sguardo comparato. Il Regno Unito: *Identity Cards Act* e *UK Borders Act*. – 12. (*Segue*) La Francia e l'attività del CNIL.

1. Dati biometrici e principi generali sul trattamento dei dati personali. Il principio di necessità.

Alla base della disciplina sul trattamento dei dati personali, e dunque anche biometrici, si pongono alcuni principi di carattere generale, che assumono un ruolo di fondamentale rilevanza al fine di armonizzare l'intero apparato normativo del Codice, bilanciando i diversi interessi e le diverse sfere di libertà chiamate in causa da ogni attività che abbia ad oggetto i dati in questione[389].

[389] Così P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, cit., spec. p. 405; E. NAVARRETTA, Commento art. 11, in C. M. BIANCA, F. D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, cit., 244, ove l'a., più specificatamente, dichiara che "l'art. 11, comma 1°, riveste una duplice fondamentale funzione:

Anzitutto, posto a monte dell'intera legislazione, si colloca il principio di necessità, di cui all'art. 3 del Codice, che non era contemplato nella legge n. 675/1996[390].

Esso introduce un "criterio minimalista", mirando precisamente ad evitare l'avvio di un trattamento di dati personali allorché ciò non risponda a reale occorrenza, anche qualora avvenga nel rispetto degli altri principi posti a garanzia dell'intera disciplina[391].

Pertanto, tale nuovo principio testimonia la crescente preoccupazione riguardo alle potenzialità sempre più sofisticate delle tecnologie di raccolta e conservazioni di dati, tra cui può essere senza dubbio annoverato anche l'uso delle tecniche biometriche[392].

Benché, come si è detto, conduca ad un sindacato preliminare, il principio di necessità interagisce anche con gli altri principi generali del Codice, in particolare si

---

coordinare e governare le regole di condotta dettate per il trattamento dei dati personali e introdurre una disciplina che operi quale ponte fra il piano degli interessi protetti e il terreno dei rimedi".

[390] Art. 3, comma 1°, "I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità". È da rilevare che, benché si parli di sistemi informativi, si vede ritenere che il principio vada applicato anche in caso di trattamenti non automatizzati di dati. Tale disposizione, inoltre, si rivolge genericamente a tutti coloro che trattano dati personali, ivi inclusi gli operatori, come i produttori di *hardware* e *software*. Si veda, a questo riguardo, G. BUTTARELLI, Commento art. 3, in C. M. BIANCA, F. D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, cit., 34-35.

[391] L'obbiettivo è, in altri termini, quello di "minimizzare il ricorso a dati personali ed identificativi prevedendo l'utilizzo degli stessi solo quando si rivelino indispensabili per il raggiungimento delle finalità consentite, e non anche quando i medesimi scopi possano essere raggiunti mediante l'uso, rispettivamente, di dati anonimi o di opportune modalità che permettano di identificare l'interessato solo in caso di necessità", S. KIRSCHEN, *Il codice della privacy, fra tradizione ed innovazione*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, cit., 68. Per il "criterio minimalista" o "principio di minimalizzazione", si considerino R. D'ORAZIO, *Il principio di necessità nel trattamento dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il Codice del trattamento dei dati personali*, cit., 20; G. BUTTARELLI, *Profili generali del trattamento dei dati personali*, in G. SANTANIELLO (a cura di), *La protezione dei dati personali*, nel *Trattato di diritto amministrativo*, diretto da G. SANTANIELLO, XXXVI, Cedam, 2005, 77; G. BUTTARELLI, Commento art. 3, cit., 34.

[392] Così G. BUTTARELLI, Commento art. 3, 32-33 e S. RODOTÀ, *Tra diritti fondamentali ed elasticità normativa: il nuovo Codice sulla privacy*, cit., 6, ove l'a. sottolinea l'importanza del principio poiché, per suo mezzo, viene contrastata "la tendenza (la deriva?) ad utilizzare qualsiasi innovazione tecnologica per trattare dati personali".

pone in rapporto con il sindacato di proporzionalità, di cui rappresenta un complemento[393].

Le considerazioni appena svolte trovano riscontro nella giurisprudenza del Garante in tema di biometria, laddove i principi generali vengono costantemente richiamati, orientando in maniera determinante le decisioni dell'Autorità.

In particolare, quest'ultima ha ritenuto contrario al principio di necessità il ricorso alle tecnologie biometriche quando potessero rivelarsi ugualmente efficaci, in relazione alle finalità perseguite, strumenti di verifica dell'identità alternativi, ma decisamente "meno invasivi della sfera personale, della libertà individuale e che non coinvolgono il corpo […]"[394].

È il caso, per esempio, della rilevazione delle impronte digitali effettuata da parte del Consiglio dell'Ordine degli avvocati di Santa Maria Capua Vetere per verificare le presenze dei praticanti avvocati ai corsi di formazione forense ove, nel divieto imposto dal Garante al trattamento dei dati in questione, si evince chiaramente l'interazione tra il principio di necessità e quello di proporzionalità, essendo possibile

[393] Ci si è interrogati sul rapporto tra il principio in questione e gli altri principi generali sul trattamento dei dati personali, se cioè sia rispetto ad essi sovraordinato, complementare ovvero integrativo. È innegabile il carattere preventivo e nel contempo generale assunto da questo principio che, da una parte, consente di valutare l'opportunità del trattamento prima che esso abbia avvio, dall'altra "riguarda più l'approccio globale di tale attività, ovvero la correlazione tra una classe di dati, una pluralità di interessi e una generale finalità", G. BUTTARELLI, *Profili generali del trattamento dei dati personali*, cit., 80. Analogamente, G. BUTTARELLI, Commento art. 3, cit., 32-40, ove l'a. precisa che con il principio di necessità "il legislatore ha in sostanza codificato nella protezione dei dati il principio di precauzione che affaccia in altri contesti normativi" (p. 33). Ciò nonostante, una lettura che porti a "polarizzare" il principio in esame, è parsa eccessiva. Si veda, in quest'ultimo senso, R. D'ORAZIO, *Il principio di necessità nel trattamento dei dati personali*, cit., 22 e, in particolare, G. RESTA, *Il diritto alla protezione dei dati personali*, cit., 48, per il quale il sindacato sulla necessità rappresenta il secondo gradino dello scrutinio di proporzionalità, e pertanto si tratta di "una specifica concretizzazione di un principio più generale, in ragione del quale la limitazione del diritto alla protezione dei dati personali, per non incorrere nella declaratoria di illiceità, deve rispondere a canoni di ragionevolezza e non eccessività".

[394] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Compiti del Garante - Uso delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro - 21 luglio 2005*, cit.

l'adozione di sistemi alternativi di controllo, maggiormente proporzionati rispetto allo scopo perseguito[395].

Viceversa, altrove, il ricorso ai sistemi in questione si è rivelato strettamente necessario, come nella recente decisione relativa all'uso di dati biometrici nelle operazioni di trasfusione, ove il Garante ha autorizzato l'azienda ospedaliera civile Maria Paternò Arezzo di Ragusa ad introdurre un sistema di sicurezza trasfusionale basato sul rilevamento biometrico delle impronte digitali, per prevenire errori di identificazione di pazienti o delle unità di sangue in sede di trasfusione, poiché è stato ritenuto "non esente da rischi assicurare con sistemi tradizionali l'autenticazione certa ed univoca dei pazienti e degli operatori sanitari, nonché la verifica dei prodotti ematici in fase di trasfusione"[396], o comunque ogniqualvolta fossero richiesti "*standard* di sicurezza specifici ed elevati, nonché un quadro di certezza riguardo all'identificazione dei soggetti […]"[397].

---

[395] Così GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento del 23 gennaio 2008*, doc. web n. 1487903, in *www.garanteprivacy.it*.

[396] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati biometrici nelle operazioni di trasfusione – 19 giugno 2008*, doc. web n. 1532480, in *www.garanteprivacy.it*, punto 6.2. Vale la pena ricordare che l'utilizzo della biometria in ambito sanitario è diffuso in particolar modo negli Stati Uniti. Infatti, essa consente sia di controllare l'accesso logico agli archivi che contengono informazioni fortemente sensibili sui pazienti, sia di limitare l'accesso fisico ad aree particolari delle aziende ospedaliere, sia di identificare i pazienti con maggiore certezza. Uno dei reati connessi all'utilizzo indebito di informazioni mediche, è il c.d. *medical identity theft*, che si verifica allorquando un soggetto utilizza il nome di una persona o altri elementi della sua identità, senza averne ottenuto il previo consenso, al fine di ricavare particolari benefici o servizi in ambito sanitario. La vittima potrebbe così ricevere un trattamento medico sbagliato, oppure subire furti nella propria assicurazione sanitaria. L'uso dei sistemi biometrici è parso scongiurare il pericolo di tale reato, tuttavia ad un tempo solleva altre problematiche di natura etica e giuridica. A questo proposito, si veda E. MORDINI, C. OTTOLINI, *Body identification, biometrics and medicine: ethical and social considerations*, cit., spec. pp. 55 ss.

[397] In tal senso si è sempre pronunciata l'Autorità qualora si trattasse, per esempio, di attività lavorative ove si imponesse l'esigenza di accertamenti particolarmente rigorosi, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Accesso ad aree riservate di particolari aziende: uso proporzionato di impronte digitali - 23 novembre 2005*, cit., punto n. 2, oppure si veda anche il recente provvedimento sul *Trattamento dei dati biometrici di dipendenti per garantire la salute pubblica – 15 febbraio 2008*, doc. web n. 1497675, punto n. 2.2, ove la Società risorse idriche calabresi, gestore di servizi idrici calabresi, ha richiesto l'autorizzazione all'uso di strumenti biometrici per il controllo degli accessi a impianti di potabilizzazione.

2. (*Segue*) I principi di liceità, correttezza, finalità e proporzionalità.

In secondo luogo, il trattamento deve svolgersi "in modo lecito e secondo correttezza" (art. 11, comma 1°, lett. a)[398].

Per quanto riguarda la liceità, tale requisito non si limita ad indicare la non contrarierà alle norme imperative, all'ordine pubblico e al buon costume, ma svolge il ruolo di "selezionare i trattamenti ammessi dall'ordinamento in ragione del fatto che, per le modalità in cui sono realizzati, essi ledano o meno alcuni particolari interessi meritevoli di tutela"[399]. Non basta, in altri termini, per limitare l'autonomia dei singoli nel trattamento dei dati, la non conformità al precetto giuridico, ma è necessaria la lesione di un interesse meritevole di *particolare* tutela che l'ordinamento ha già individuato come rilevante. Il principio di liceità opera, dunque, *ex ante*.

Il principio di correttezza, invece, "indica all'agente un canone generale cui deve attenersi la sua condotta, che rimane fondamentalmente libera, ma nel rispetto della clausola generale che colora tale autonomia di una connotazione discrezionale"[400]. La correttezza, dunque, si configura come un giudizio *ex post*, che si inserisce all'interno di una dinamica relazionale, i cui attori sono l'interessato e il titolare del trattamento, stabilendo un limite al perseguimento dell'interesse dell'uno in rapporto a quello dell'atro. Si evince, dunque, l'esistenza di uno stretto legame tra il criterio di correttezza e altre regole e principi che governano il trattamento dei dati personali: dall'obbligo di informazione, al consenso, alla facoltà di opposizione[401].

---

[398] Si veda, per quanto riguarda i principi di liceità e correttezza, P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., 408-419, spec. p. 415, e 419-427.
[399] *Ibidem*, 415.
[400] E. NAVARRETTA, Commento art. 11, cit., 251.
[401] P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., 427-435. In altri termini, "la regola di correttezza è imposta *a priori*, ma le specifiche regole di condotta che concretizzano il canone generale sono affidate alla discrezionalità dell'agente e sono suscettibili, pertanto, di una valutazione in termini di conformità o difformità al diritto solo *a posteriori*", E. NAVARRETTA, Commento art. 11, cit., 251.

Particolarmente importante, nella disciplina in esame, è il principio di finalità, che stabilisce un vincolo tra il trattamento dei dati e il perseguimento di un determinato fine[402].

Esso rinviene il proprio fondamento nell'art. 11, comma 1°, del Codice, ove si stabilisce che i dati devono essere "raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni di trattamento in termini compatibili con tali scopi" (lett. b), e si indicano, come ulteriori corollari di tale principio, i requisiti della pertinenza, completezza e non eccedenza rispetto alle finalità della raccolta e del successivo trattamento (lett. d), nonché il principio per cui essi siano "conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati" (lett. e).

Appare chiaro che il rispetto del principio di finalità costituisce il parametro principale per valutare in concreto anche il requisito della liceità, ovvero il trattamento sarà lecito nella misura in cui viene rispettato lo scopo per cui i dati sono raccolti, benché non si debba escludere nemmeno lo speciale legame esistente con il principio di correttezza[403]. Infatti, considerato che il titolare del trattamento può scegliere dall'inizio, all'interno dei confini della legittimità dello scopo stabiliti aprioristicamente dal legislatore, il fine specifico che intende perseguire, appare centrale la dinamica relazionale intercorrente tra interessato e titolare, cosicché il principio di finalità si

[402] Si veda P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., 436, per la quale il principio di finalità "si presenta come uno strumento di controllo della circolazione dell'informazione che lega il dato personale e il trattamento, di cui quello è oggetto, ad un determinato fine".

[403] Sul legame tra principio di liceità e di finalità, si veda E. NAVARRETTA, Commento art. 11, cit., 264-265 e G. CASSANO, S. FADDA (a cura di), *Codice in materia di protezione dei dati personali*, cit., 88. Di parere in parte diverso, P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., 436, che colloca il principio in esame principalmente sul piano della correttezza, per quanto non vengano esclusi legami anche con il principio di liceità. In quest'ultimo senso, infatti, l'a. rileva che, essendo la finalità uno dei principi fondamentali del trattamento, il sindacato sulla liceità non può non considerare l'aspetto dei fini; in secondo luogo, la "legittimità", cui l'articolo fa riferimento, e la "liceità", possono considerarsi sinonimi.

rivela legato inscindibilmente anche al principio di correttezza, tendendo a "regolare l'esercizio di questo potere decisionale", ovvero "riducendo il rischio di comportamenti opportunistici da parte dei soggetti"[404].

Il principio di finalità si specifica in più aspetti. In primo luogo, nello stabilire che la raccolta e la registrazione dei dati debba avvenire per scopi determinati, espliciti, e legittimi, il legislatore ha inteso garantire la trasparenza nella circolazione delle informazione, in stretta connessione anche con gli obblighi di notificazioni e informazione. Esso trova attuazione nel corso dell'intero trattamento e va rispettato anche a fronte della determinazione di una eventuale nuova finalità, assicurando così al soggetto il potere di esercitare il proprio diritto all'*habeas data*[405].

In secondo luogo, il principio in esame viene precisato attraverso la definizione di alcuni attributi che i dati debbono possedere. Laddove la pertinenza attiene alla dimensione qualitativa, quale "indice oggettivo del principio di finalità riferito alla natura dell'informazione", i requisiti della completezza e della non eccedenza attengono, invece, alla dimensione quantitativa. Da una parte, infatti, se i dati si rivelano incompleti, non si persegue lo scopo e si può violare il vincolo della verità (l'art. 11, comma 1°, lett. c, definisce il "criterio della verità", per cui i dati devono essere "esatti e, se necessario, aggiornati"). Dall'altra, se hanno un contenuto informativo superiore a quello necessario per il raggiungimento del fine preposto, insorgono seri rischi per

[404] Così, ancora, P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., 438, ove, in relazione al nesso finalità-correttezza, si è osservato come il principio operi in modo diverso a seconda della relazione che sussiste tra interessato e titolare in rapporto alla circolazione delle informazioni. Infatti, se non si richiede il consenso (c.d. circolazione libera), il principio di finalità dovrà essere applicato in modo particolarmente attento, diversamente da come accadrebbe nel caso in cui il consenso fosse richiesto (c.d. circolazione controllata).

[405] Si veda E. NAVARRETTA, Commento art. 11, cit., 266 e P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., 441-443, ove, in particolare, si dichiara: "La trasparenza è fondamentale ai fini dell'esercizio dei poteri di intervento da parte dell'interessato, soprattutto nei casi in cui questi non partecipa alla definizione delle finalità attraverso la prestazione del consenso" (p. 443).

l'interessato, che altri cioè vengano a conoscenza di informazioni di natura anche delicata[406].

Si è sostenuto, inoltre, che i tre caratteri della pertinenza, completezza e non eccedenza, concorrono a definire il fondamentale principio di proporzionalità, che mette in relazione i mezzi utilizzati, ovvero la tipologia di dati raccolti e le modalità di trattamento e conservazione, e i fini perseguiti[407].

In particolare, tale criterio è stato fondamentale nel guidare le decisioni del Garante in tema di biometria.

L'Autorità ha più volte disposto che non è sufficiente vi sia "una esigenza generica di sicurezza, non accompagnata da elementi che evidenzino una concreta situazione di rischio" per installare un sistema biometrico, in quanto ciò si traduce in un "sacrificio sproporzionato della sfera di libertà di tutte le persone interessate che possono legittimamente lamentare anche una considerazione non adeguata e un rilevante pregiudizio della propria dignità personale"[408], precisando altrove che questo comporta altresì "pericolo di abusi in relazione a dati a sé riferibili particolarmente delicati"[409].

---

[406] P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., 444-445.

[407] E. NAVARRETTA, Commento art. 11, cit., 267; la questione è ripresa anche da P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., 441-443, 446.

[408] Così i primi provvedimenti del GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Videosorveglianza - Impronte digitali per l'accesso in banca - 11 dicembre 2000*, doc. web n. 30903, cit., e *Videosorveglianza - Raccolta di impronte digitali associate ad immagini per l'accesso a banche – 7 marzo 2001*, cit., relativi all'installazione di sistemi di rilevazione delle immagini del volto e delle impronte digitali presso banche. Le considerazioni svolte vengono riprese anche in alcune recenti pronunce, relative ancora ad istituti di credito, ove, per esempio, vengono reputati elementi concreti di rischio il fatto che la banca sia collocata in una zona pericolosa, ovvero che la banca stessa sia stata già oggetto di rapine, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati biometrici presso Banca San Paolo Imi S.p.A. – 23 gennaio 2008*, doc. web n. 1490533, e *Trattamento di dati biometrici presso Cariprato S.p.A. – 23 gennaio 2008*, doc. web n. 1490382, in *www.garanteprivacy.it*. Così anche C. PRINS, *Making Our Body Identify for Us: Legal Implications of Biometric Technologies*, cit., 161, per la quale "*fundamental rights are likely to be violated in case biometrics is used for applications merely requiring a low level of security. In the end organizations and government agencies must demonstrate that there is a compelling interest in using biometric technology and that, e.g. an obligatory fngerprint requirement is reasonably related to the objective it is required for*".

[409] Si veda il provvedimento GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Istituti di credito - Rilevazione di impronte digitali ed immagini: limiti e garanzie - 27 ottobre 2005*, cit., punto n. 2, relativo alla richiesta di installazione di sistemi di lettura di impronte digitali in alcuni istituti di credito.

Diversamente, è stato ritenuta proporzionata la rilevazione delle caratteristiche geometriche della mano per l'accesso ad aree particolari, in quanto "possono non garantire l'identificazione univoca e certa di una persona, ma sono, comunque, sufficientemente descrittive per essere impiegate in circoscritti ambiti ai fini della verifica di identità"[410].

Il principio di proporzionalità rileva altresì in rapporto alle modalità di conservazione dei dati, di cui si dirà.

In terzo luogo, il principio di finalità si specifica in rapporto alla durata del trattamento e della conservazione dei dati (lett. e), di modo che il soggetto ha "diritto «*ad essere dimenticato*»" una volta che, in relazione agli scopi perseguiti, non sia più necessario conservare le informazioni[411]. Si parla, a questo proposito, di "diritto all'oblio" che, mirando a rimuovere l'elemento della identificabilità del soggetto cui il dato appartiene, si affianca al diritto all'anonimato, di cui si è detto[412].

Anche a questo proposito, l'Autorità ribadisce costantemente l'esigenza di conservare i dati biometrici, nella forma di *template*, per un tempo limitato, generalmente non superiore ai sette giorni, con meccanismi di cancellazione automatica delle informazioni allo scadere dei termini indicati, "evitando ogni prolungamento surrettizio dei tempi di conservazione attraverso la creazione di copie di sicurezza"[413]. Altrove, si precisa che, durante il predetto periodo di conservazione, vi è la possibilità

---

[410] Così GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sicurezza di siti archeologici e uso di dei dati biometrici – 8 novembre* 2007, doc. web n. 1461908, in *www.garanteprivacy.it*, punto n. 1. Il provvedimento riguarda la rilevazione della geometria della mano per l'accesso ad un'area particolare di un sito archeologico, in relazione ad un numero ristretto di dipendenti. Ugualmente si è espressa l'Autorità in relazione alla lettura della geometria della mano per l'accesso a un complesso polifunzionale, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati personali biometrici per l'accesso a un complesso polifunzionale - 1 febbraio 2007*, cit., punto n. 2.2.

[411] G. CASSANO, S. FADDA (a cura di), *Codice in materia di protezione dei dati personali*, cit., 92.

[412] Per il diritto all'oblio, si vedano: G. B. FERRI, *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ.*, 1990, I, 801-823; G. CASSANO, S. FADDA (a cura di), *Codice in materia di protezione dei dati personali*, 92-94; P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., 450;

[413] Per tutti, si veda il provvedimento sul *Trattamento dei dati biometrici di dipendenti per garantire la salute pubblica – 15 febbraio 2008*, cit., punto n. 2.5.

per gli organi giudiziari o di polizia di acquisire i dati[414] ed è altresì ammessa, sempre per ragioni di giustizia, la conservazione per un periodo di tempo superiore a quello previsto[415].

Diversamente, il dato grezzo necessario per realizzare il *template*, non può essere conservato per un tempo superiore a quello necessario ad effettuare la fase di iscrizione del soggetto nel sistema (*enrollment*), e dunque per una periodo molto breve[416].

Se il principio di finalità assume un ruolo di centrale rilevanza, non si può tuttavia ignorare come esso stia subendo una sorta di erosione, con l'affermarsi del contrapposto criterio della multifunzionalità, di modo che i dati raccolti per un fine sono sovente resi disponibili per un altro, oppure utilizzati da più soggetti non autorizzati. L'interesse alla tutela delle informazioni personali soccombe dunque facilmente di fronte all'interesse alla pubblica sicurezza, alla lotta alla criminalità, alla maggiore efficienza del sistema amministrativo, al risparmio economico[417].

---

[414] Si veda il provvedimento GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Videosorveglianza e dati biometrici - Rilevazioni biometriche presso istituti di credito - 28 settembre 2001*, doc. web n. 39704, cit., punto n. 4, lett. c) e d).

[415] Così la pronuncia sul *Trattamento di dati personali biometrici per l'accesso a un complesso polifunzionale - 1 febbraio 2007*, cit., punto n. 4.

[416] Si vedano, *ex multis*, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Uso della biometria per identificazione del personale nelle banche - 15 giugno 2006*, cit., punto n. 5; GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sicurezza merci e controllo delle presenze presso aeroporti - 26 luglio 2006*, cit., punto n. 4; GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati biometrici con finalità di verifica della presenza dei dipendenti e di accesso a particolari aree produttive - 15 giugno 2006*, cit., punto n. 4.

[417] Si veda S. RODOTÀ, *La privacy secondo l'Europa*, cit., 64, ove l'a. dichiara che, in questo modo, "non solo si possono contraddire principi essenziali per la protezione dei dati, ma si rompe il patto con i cittadini in una materia sempre più decisiva per la tutela effettiva delle loro libertà".

3. (*Segue*) Il problema della conservazione: *database vs. smart card*.

Come si è accennato, il sindacato di proporzionalità si lega strettamente alle modalità di conservazione dei dati in questione. I dati biometrici, infatti, possono essere conservati principalmente in una banca dati centralizzata, ovvero in un piccolo supporto portatile (*token* o *smart card*).

Anzitutto, si deve rilevare che per banca dati deve intendersi "qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti" (Codice in materia di protezione dei dati personali, art. 4, comma 1°, lett. p), benché la locuzione possa essere analizzata in maniera più articolata.

Più precisamente, tre elementi possono considerarsi fondamentali nella ricostruzione della nozione in esame: il primo "contempla la presenza di un insieme o complesso di elementi informativi di base, ciascuno dotato di propria autonomia"; il secondo, è relativo al metodo di organizzazione dei dati, di modo che "ciò che rileva è che gli elementi informativi di base rispondano ad un sistema organizzato, funzionale alla facile reperibilità dell'informazione"; il terzo elemento, riguarda l'accesso alle informazioni contenute nella banca, il quale deve essere "realizzabile rapidamente, ovvero più rapidamente o facilmente di quanto sia realizzabile un accesso ad identico «archivio» tradizionale". Infine, si potrebbe aggiungere l'elemento della tutela legislativa delle informazioni[418].

È sul finire degli anni sessanta che si assiste alla proliferazione dei *database*, indotta principalmente dalla diffusione degli elaboratori elettronici, dalla volontà politica di controllo degli avversari e in genere dei comportamenti dei cittadini, dalla

[418] Si veda, per questa approfondita definizione di banca dati, l'analisi condotta da F. CARDARELLI, *Le banche dati pubbliche*, in *Dir. inf.*, 2002, 321-326.

possibilità di meglio ripartire le risorse nell'ambito della pubblica amministrazione, dal valore di merce di scambio attribuito alle informazioni[419].

Tale modalità di trattamento pone numerosi problemi relativamente alla sicurezza delle informazioni, rispetto a quelli che nascono, piuttosto, nel caso in cui il dato venga salvato in un dispositivo mobile[420].

In particolare, ha ingenerato un diffuso allarme la questione della c.d. interoperabilità dei sistemi che, se per talune applicazioni si rivela necessaria e di pubblica utilità, molto spesso è invece superflua ed estremamente rischiosa, stante la possibilità di connettere le informazioni raccolte nei diversi *database* così da creare profili individuali dei soggetti[421].

Infatti, lo sviluppo delle tecnologie informatiche consente in breve tempo "la congiunzione di informazioni inserite in memorie e programmi diversi, in modo da presentare, intorno ad un medesimo soggetto, un rilevante complesso di informazioni, fino ad un massimo, di difficile verificazione ma pur sempre ipotizzabile, della fornitura di tutte le informazioni concernenti un soggetto che in qualsiasi luogo ed in qualsiasi tempo siano state raccolte ed inserite in memorie elettroniche"[422].

---

[419] A. BELLAVISTA, *Quale legge per le banche dati?*, cit., 677-678.

[420] In questo senso, J. GRIJPINK, *Biometrics and Privacy*, cit., 157, per il quale: "*The distinction between central/decentralized is of legal importance because central storage involves more social risks*"; P. DE HERT, *Biometrics: legal issues and implications*, cit., pp. 9, 10, 26; Y. LIU, *Identifying Legal Concerns in the Biometric Context*, cit., 49.

[421] L'interoperabilità è stata definita come "*the ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge*", COMMISSION OF THE EUROPEAN COMMUNITIES, *Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs*, Brussels, 24.11.2005, punto n. 2.2, p. 3, in *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0597:FIN:EN:PDF*.

[422] Così G. MIRABELLI, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, cit., 314, ove si precisa che l'allarme nasce poiché chi può disporre dei mezzi elettronici capaci di collegare una notevole molteplicità di informazioni intorno ad un soggetto, esercita nei riguardi di quest'ultimo un notevole potere, "vuoi con l'utilizzazione delle informazioni per propria utilità, vuoi con la minaccia di propagare le informazioni in modo da presentare un profilo del soggetto comunque suscettibile di valutazione negativa". Tutto ciò fa temere il consolidarsi di dittature poliziesche che, come a ragione si afferma, sono "in parte scomparse da non molto tempo ed in parte ancora esistenti". A questo proposito, si vedano anche G. GUNASEKARA, *The 'final' privacy frontier? Regulating trans-border data flows*, in 15 *International Journal of Law and Information Technology* (2007), spec. pp. 362-366 e P. H. O'NEIL, *Complexity and Counterterrorism: Thinking about Biometrics*, in 28 *Studies in Conflict & Terrorism*

Il Documento di lavoro sulla biometria esprime disappunto rispetto all'archiviazione centralizzata di dati biometrici, a fronte del "rischio che tali dati vengano utilizzati come chiave per collegare basi di dati distinte ed ottenere così profili dettagliati delle abitudini della persona interessata tanto nel settore pubblico quanto in quello privato"[423].

Tale posizione è ripresa dal Garante italiano per la protezione dei dati personali, ribadendo più volte che la modalità centralizzata "risulta di regola sproporzionata e non necessaria", per cui appare sufficiente ricorrere ad un "supporto posto nell'esclusiva disponibilità dell'interessato (una *smart card* o un dispositivo analogo) e privo di indicazioni nominative riferibili a quest'ultimo (essendo sufficiente attribuire a ciascun dipendente un codice individuale)"[424].

Altrove, l'Autorità ha ritenuto proporzionata l'archiviazione all'interno di una base di dati, piuttosto che in un dispositivo portatile, alla luce delle particolari finalità perseguite e delle garanzie di sicurezza fornite per lo specifico sistema esaminato, ovvero del tipo di caratteristica implicata[425].

(2005), ove l'a., nel confutare la capacità dei sistemi biometrici di accrescere la sicurezza, ipotizzando al contrario che essa possa essere pericolosamente ridotta, sottolinea come la conservazione di tali dati, soprattutto se avviene all'interno di una base dati, "*could give governments an unprecedent level of surveillance over the public, limiting privacy*" (p. 548).

[423] GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria*, cit., punto n. 3.2, ove si accenna anche al problema della interoperabilità.

[424] Così GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati (deliberazione n. 53 del 23 novembre 2006)*, cit., punto n. 4.2. Si vedano poi, *ex multis*, i seguenti provvedimenti dell'Autorità: *Compiti del Garante - Uso delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro - 21 luglio 2005*, doc. web n. 1150679, cit., punto n. 4; *Sicurezza merci e controllo delle presenze presso aeroporti - 26 luglio 2006*, doc. web n. 1318582, cit., punto n. 2; *Uso della biometria per identificazione del personale nelle banche - 15 giugno 2006***,** doc. web n. 1306098, cit., punto n. 2; GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Dati biometrici e Rfid nelle banche - 23 febbraio 2006*, doc. web n. 1251535, cit., punto n. 2.

[425] Si veda il citato provvedimento GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati biometrici nelle operazioni di trasfusione – 19 giugno 2008*, doc. web n. 1532480, ove si dichiara, al punto n. 6.2, che la conservazione in un terminale appare proporzionata a fronte delle caratteristiche dell'apparecchiatura utilizzata (priva di accessi fisici), delle garanzie di sicurezza previste, della mancanza di indicazioni nominative e della difficoltà di produrre per i pazienti singoli badge. La centralizzazione è stata ritenuta lecita altresì nel provvedimento GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Riconoscimento vocale e gestione di sistemi informatici - 28 febbraio 2008*, cit., punto n. 2.2, essendo in gioco una caratteristica biometrica come l'impronta vocale, che "non rappresenterebbe un dato

Il Comitato Consultivo Nazionale Etico francese (CCNE) stesso, nel citato documento *Biométrie, données identifiantes et droits de l'homme*, manifesta preoccupazione per la raccolta massiccia di dati biometrici in banche dati e per la loro trasmissione, poiché ciò costituisce una minaccia per le libertà individuali, cosicché si prevede che venga stabilita una "*interdiction de l'interconnexion des fichiers présentant des identifiants communs mais destinés à des finalités différentes*"[426].

La questione dell'interoperabilità si rivela oggi centrale, con i suoi pregi ma anche con i suoi innumerevoli limiti, nell'ambito dell'Unione europea, ove si è affermato, a partire dal 2004, il c.d. *principle of availability*. Sancito nell'ambito del *Hague Programme* sul rafforzamento della libertà, della sicurezza e della giustizia nell'Unione[427], il principio riguarda lo scambio di informazioni tra Stati membri, disponendo che i dati utilizzabili dalle autorità che operano nell'ambito della sicurezza di uno Stato debbano essere accessibili anche alle corrispondenti autorità di altri Membri[428]. Grazie ad esso, si è assistito a numerose iniziative volte ad incrementare il

---

biometrico suscettibile di essere in concreto utilizzato per finalità diverse da quella perseguita dal titolare del trattamento".

[426] CCNE, Avis n° 98, *Biométrie, données identifiantes et droits de l'homme*, cit., IV-Reccomandations, p. 19. Si veda inoltre il punto III (*Vie privée et altérité*).

[427] COUNCIL OF EUROPE, *The Hague Progamme: Strengthening Freedom, Security and Justice in the European Union*, Brussels, 13 December 2004, in *http://ec.europa.eu/justice_home/doc_centre/doc/hague_programme_en.pdf*, punto 2.1, pp. 18-19, secondo cui il "*principle of availability*" stabilisce che "*throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in that State*". Ai fini dell'implementazione di tale principio, vengono individuate alcune condizioni: "*the exchange may only take place in order that legal tasks may be performed; the integrity of the data to be exchanged must be guaranteed; the need to protect sources of information and to secure the confidentiality of the data at all stages of the exchange, and subsequently; common standards for access to the data and common technical standards must be applied; supervision of respect for data protection, and appropriate control prior to and after the exchange must be ensured; individuals must be protected from abuse of data and have the right to seek correction of incorrect data*". Il documento prosegue dichiarando che, per lo scambio di dati, si potrà fare pieno uso delle nuove tecnologie, che saranno adattate a ciascun tipo di informazione.

[428] A questo proposito, P. DE HERT, V. PAPAKONSTANTINOU, C. RIEHLE, *Data protection in the third pillar: cautious pessimism*, in *Crime, rights and the EU: the future of police and judicial cooperation*, London, Publisher: Justice, 2008, p. 137, reperibile in *http://www.vub.ac.be/LSTS/pub/Dehert/224.pdf*. Si vedano altresì P. DE HERT, *What are the risks and what guarantees need to be put in place in view of interoperability of police databases?*, in European Parliament. Directorate-General for Internal Policies of

trattamento dei dati personali, biometrici in particolare, e conseguentemente a favorirne lo scambio, basti pensare, per esempio, al sistema Eurodac, di cui si dirà.

Per quanto l'interoperabilità sia suscettibile di creare problematiche di vasta portata, soprattutto legate alla possibilità di utilizzare i dati per finalità diverse o comunque non autorizzate rispetto a quelle per cui sono stati originariamente raccolti (c.d. *function creep*)[429], nondimeno contrastarla potrebbe risultare, a livello europeo, un'operazione futile e controproducente, poiché l'alternativa consisterebbe nella creazione di un *database* centrale delle forze di polizia degli Stati membri, opzione che non può non destare altrettanta preoccupazione, data la facilità di controllo generalizzato delle persone che tale scelta ingenererebbe[430].

In particolare, si possono individuare quattro aree sensibili che presentano specifici rischi[431].

---

the Union, Area of Justice, Freedom & Security. Collection of Standard Briefing Notes by External Experts, Brussels, Parlement Européen (Ed.), Jan. 2006 - March 2006, p. 170, spec. nota n. 5 e P. DE HERT, S. GUTWIRTH, *Interoperability of Police Databases within the EU: An Accountable Political Choice?*, in 20 *International Review of Law Computers & Technology* (2006), 25, ove si afferma che "*European governmental power will increase with law enforcement authorities becoming more all-knowing through interoperable 'European' systems that work on the basis of the principle of availability*".

[429] A questo riguardo, si veda E. MORDINI, S. MASSARI, *Body, biometrics and identity*, cit., 490, ove l'a. dichiara che generalmente il *function creep* è legato a tre questioni: 1. Un vuoto politico, che appare il problema più rilevante, poiché accade sovente che mentre le organizzazioni ricorrono a nuove strumentazioni tecnologiche, contemporaneamente non vengono pensate e create politiche specifiche, cosicché queste tecnologie finiscono con l'essere guidate esclusivamente dagli interessi dei singoli; 2. Una domanda che non viene soddisfatta, di modo che le informazioni raccolte per uno scopo sono utilizzate per un altro se permane un bisogno a cui non viene data risposta soddisfacente; 3. Infine, il c.d. effetto "*slippery slope*". Circa l'utilizzo di informazioni per finalità diverse rispetto a quelle per cui sono raccolte, si veda anche il significativo esempio riportato da C. Sarzana: negli anni '80, al fine di localizzare il terrorista Rudolf Clemens Wagner, la polizia tedesca utilizzò i dati relativi al consumo di energia elettrica di un'intera città, cosicché un "innocente che rispondeva a determinati criteri, diventava improvvisamente sospettato di terrorismo…", C. SARZANA, *Evoluzione tecnologica e diritti dell'individuo*, in *Dir. Inf.*, 1992, 403, nota n. 11.

[430] Così P. DE HERT, *What are the risks and what guarantees need to be put in place in view of interoperability of police databases?*, cit., 170-171; P. DE HERT, S. GUTWIRTH, *Interoperability of Police Databases within the EU: An Accountable Political Choice?*, cit., 25.

[431] Si veda, ancora, P. DE HERT, *What are the risks and what guarantees need to be put in place in view of interoperability of police databases?*, cit., 172-180, e il corrispondente P. DE HERT, S. GUTWIRTH, *Interoperability of Police Databases within the EU: An Accountable Political Choice?*, cit., 25-31 . Si è sostenuto che "*key-interoperability is indeed not an uncontroversial topic, and politically as sensible ad interoperability of content*" e "*key-interoperability based on numbers is no less innocent than biometrical key-interoperability*" (p. 175). In particolare, si è affermato: "*The idea of interoperability should be implemented with care and respect for the plurality of the good. In our social democratic state, citizens*

Anzitutto, l'interoperabilità con i sistemi al di fuori della UE, ove, anche nei paesi in cui è stato raggiunto un certo grado di protezione dei dati personali, rimane tuttavia il problema del controllo e dell'applicazione dei rimedi previsti[432].

In secondo luogo, l'interoperabilità delle chiavi, ovvero la possibilità di condividere le chiavi alfanumeriche grazie a cui è possibile accedere alle informazioni, ivi incluse quelle biometriche.

In terzo luogo, l'uso dei dati da parte di autorità di polizia di altri paesi ovvero per mano di organismi che perseguono scopi diversi da quello di garantire la sicurezza: a ragione, si è richiamata la responsabilità dei governanti a considerare seriamente la pluralità dei "beni", talora non coincidenti, che un sistema democratico è chiamato a garantire, uno dei quali, ma non unico, è la sicurezza.

Infine, l'interoperabilità trova ampia applicazione nell'ambito di quelle indagini di *intelligence* ove si ricorre all'uso di *tutte* le informazioni che si possono rinvenire sul conto di una persona, e in particolare alle tecniche di analisi criminale.

La conservazione dei dati biometrici in un dispositivo portatile, come una *smart card*[433], offre, viceversa, maggiori garanzie per quanto riguarda la tutela della riservatezza e la protezione dei dati, poiché lo strumento rimane nelle mani

---

have to deal with government for a number of reasons. It would be disrespectful of the ideas behind data protection to see government as a whole that may use 'its' information, taken from whatever governmental database, at random" (p. 176).

[432] Riguardo al trasferimento transfrontaliero di dati tra paesi aventi diversa giurisdizione, si veda G. GUNASEKARA, *The 'final' privacy frontier? Regulating trans-border data flows*, cit., 370, ove si dichiara, viceversa, che non vi è ragione per impedire in assoluto i trasferimenti di dati verso paesi dotati di una legislazione che offre minori garanzie, come potrebbe essere nel caso dell'America Latina o dell'Africa, poiché questi sviluppi potrebbero "*provide a spur for developing countries to bring their information privacy laws into line with those of developed nations*".

[433] Per una definizione di "*smart card*", si veda il documento del COUNCIL OF EUROPE, EUROPEAN COMMITTEE ON LEGAL COOPERATION (CDCJ), *Guiding principles for the protection of personal data with regard to smart cards*, Strasbourg, 12 May 2004, in *http://www.coe.int*, 2, per cui "*a «smart card» is thought of as a mobile carrier of personal data with automatic processing functions, which is issued to the data subject and processes personal data in accordance with the purposes and specifications of the issuer in connection with an information system related to it*".

dell'interessato, il quale, tuttavia, non è sovente a conoscenza di quanto effettivamente conservato nel dispositivo mobile in proprio possesso.

Si dovrebbero, invero, rispettare tutti i principi stabiliti in via generale per la protezione dei dati personali nell'ambito della legislazione nazionale, benché si pongano anche questioni di carattere specifico[434].

Controverso appare, in particolare, il problema di chi detenga il controllo legale sulle informazioni contenute nel dispositivo, se l'interessato, che ha il materiale possesso dello strumento, ovvero il titolare del trattamento. La prima ipotesi sembra la più condivisibile, poiché, come è stato detto, "*if biometric information is something that makes the individual special and perhaps unique, it arguably ought to belong to the individual from whom it was ultimately derived*"[435].

[434] Si vedano i *guiding principles* del citato documento COUNCIL OF EUROPE, EUROPEAN COMMITTEE ON LEGAL COOPERATION (CDCJ), *Guiding principles for the protection of personal data with regard to smart cards*, cit., 4-6. Per quanto riguarda le questioni specifiche, si considerino spec. pp. 2 e 3, ove si dichiara: "*The following guiding principles are not intended to be an exhaustive solution to all the data protection issues arising with respect to the use of smart cards. A smart card is always used as part of a wider information system and the overall effective protection of personal data used in such a system depends on many different factors and circumstances. The security of a system also greatly depends on the behaviour of the people who come into contact with it. Smart card technology is undergoing very rapid development. These guiding principles are intended to set out basic principles that will not significantly change with innovations in the technology. Nevertheless, it may be appropriate to supplement these principles in the light of the continuing developments in this field*". Nel documento si rinviene anche uno specifico riferimento ai dati biometrici, per i quali è raccomandata particolare attenzione (p. 3).

[435] Così Y. LIU, *Identifying Legal Concerns in the Biometric Context*, cit., 49, che conclude "*Theoretically, under no circumstances should we claim that the individual source loses the right to have legal control over his/her biometric information, which is inherently linked to him*". Nello stesso senso, P. DE HERT, *Biometrics: legal issues and implications*, cit., 10.

4. I diritti dell'interessato come fulcro dell'*habeas data*. In particolare, il diritto di accesso.

Esaurita l'analisi sui principi fondamentali che governano la disciplina sul trattamento dei dati biometrici, si intende ora approfondire la complessa posizione giuridica spettante all'interessato, inteso come "la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali" (Codice in materia di protezione dei dati personali, art. 4, comma 1°, lett. i).

L'art. 7 apre il titolo dedicato ai diritti di quest'ultimo, individuando essenzialmente tre tipologie di poteri[436]: il diritto di sapere se esistono dati che lo riguardano, ottenendone la comunicazione in forma intelligibile (comma 1°)[437], e di avere indicazioni di varia natura sul loro conto (comma 2°)[438]; il diritto di esercitare un controllo sulla qualità dei dati, ovvero di chiederne l'aggiornamento, la rettificazione, l'integrazione, o ancora la cancellazione, la trasformazione in forma anonima, il blocco (comma 3°); infine, il diritto di opporsi al trattamento per motivi legittimi (comma 4°).

Molto si è parlato in dottrina, e in parte è stato accennato anche nel corso di questo lavoro, sulla logica che governa il riconoscimento del diritto alla protezione dei dati personali, logica che si riverbera, *in primis*, sulla natura dei diritti dell'interessato, ponendo il problema se si debbano ricondurre nel novero dei diritti della personalità,

[436] Tale articolo si completa con i successivi artt. 8, 9, 10, rispettivamente sull'esercizio dei diritti di cui all'art. 7, sulle modalità di esercizio e sul riscontro dell'interessato.
[437] In particolare, il comma 1° prevede il diritto dell'interessato di "ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile". L'espressione "conferma" va letta esattamente nel senso di un vero e proprio diritto a sapere, non condizionato da una precedente situazione di conoscenza, cui il termine utilizzato dalla legge sembrerebbe rinviare, M. MESSINA, *I diritti dell'interessato*, cit., 80.
[438] Ai sensi del comma 2°, l'interessato "ha diritto di ottenere l'indicazione: a) dell'origine dei dati personali; b) delle finalità e modalità di trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentate designato ai sensi dell'art. 5, comma 2; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati".

ovvero nell'ambito del diritto di proprietà, lettura quest'ultima che, come si è visto, non troverebbe accoglimento[439].

Appare chiaro, in ogni caso, che il principio dell'*habeas data*, il cui fondamento, giova ricordare, si rinviene nel combinato disposto degli artt. 1 e 2 del Codice[440], trova la propria concretizzazione e specificazione anzitutto nell'insieme di prerogative riconosciute dall'art. 7, che diviene pertanto norma chiave dell'intera disciplina[441], accanto a quella che sancisce il principio del consenso informato del soggetto, di cui rappresenta altresì il presupposto[442].

In altri termini, per poter prestare validamente il proprio consenso, e indipendentemente dal tipo di dato trattato, il soggetto interessato deve ottenere alcune fondamentali indicazioni in via preliminare, segnatamente quelle indicate nei commi 1° e 2°: sapere se esistono dati raccolti sul proprio conto; conoscerne l'origine, le finalità e le modalità di trattamento; la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; gli estremi identificativi del titolare, dei responsabili e del rappresentante; i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati.

Si è già trattato, nel corso di questo lavoro, del ruolo del consenso informato e, in particolare, della relazione che intercorre tra consenso e identità[443]. Il legame con il

---

[439] Si veda cap. II, paragrafo 3.
[440] Si veda cap. III, paragrafo 5.
[441] Così CIRILLO G. P. (A CURA DI), *Il Codice sulla protezione dei dati personali*, cit., 37, ove si dichiara, rispetto all'art. 1, che "si potrebbe prospettare una lettura in cui gli specifici diritti dell'interessato siano delle facoltà o, se si vuole, il contenuto del suddetto diritto". In questo senso, anche C. LO SURDO, *Gli strumenti di tutela del soggetto «interessato» nella legge e nella sua concreta applicazione*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, cit., 638-639, secondo cui la possibilità di sapere "è la primaria condizione per la realizzazione di quel diritto all'autodeterminazione informativa […]". Così, infine, anche M. MESSINA, *I diritti dell'interessato*, cit., 77, per la quale "i diritti dell'interessato, funzionalmente connessi a quello della persona sui propri dati, costituiscono lo strumento per realizzare l'autodeterminazione della persona in materia di trattamento dei dati personali, scandendone, al contempo, il contenuto e l'effettiva operatività".
[442] Così G. FINOCCHIARO, *Una prima lettura della legge 31 dicembre 1996, n. 675, «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»*, in *Contr. e impr.*, 1997, 307.
[443] Vedi cap. II, paragrafo 6.

valore dell'identità[444], invero, appare assai forte anche guardando ai diritti di cui al comma 3° dell'articolo in esame, nell'esercizio dei quali è possibile che "i dati trattati siano costantemente lo specchio, seppur parziale, dell'interessato e corrispondano, pur nei limiti della parzialità, alla sua identità *effettiva* (non rappresentando di lui un'immagine superata)"[445].

Il ruolo dei diritti dell'interessato, così come indicati nell'art. 7, a ben vedere, si rivela cruciale nel caso del trattamento di dati biometrici.

Infatti, alcune caratteristiche possono variare con il passare degli anni, a seguito di incidenti ovvero per interventi chirurgici, determinando un mutamento talora consistente del campione biometrico stesso.

Se ciò accadesse, l'interessato facilmente si vedrebbe "rifiutato" in maniera sistematica dal sistema, per cui avrebbe il diritto di sapere se esistono dati che lo riguardano, oppure, per esempio, di chiederne l'aggiornamento o la rettificazione, affinché la sua identità reale rimanesse sempre corrispondente alla sua identità, per così dire, rivelata. Si deve, tuttavia, tener conto che alcun sistema di riconoscimento biometrico offre certezza assoluta sull'identità del soggetto, bensì solamente una "certezza probabilistica", per cui dipende dal responsabile del trattamento stabilire il grado di errori di riconoscimento che possono considerarsi tollerabili per quel tipo di applicazione e per quello specifico scopo che si intende perseguire[446].

---

[444] Vedi cap. II, paragrafi 3 e 4.

[445] Così M. MESSINA, *I diritti dell'interessato*, cit., 92.

[446] Tra le possibili cause di errato riconoscimento, si segnalano: "*(a) The person is not the same as the one whose biometric data are enrolled. The result is correct. The data do not match and the system rejects the data subject. (b) The system's enrolled biometric data are wrong. The data should be rectified. (c) The enrolled data are right but the secondary collection does not function well so the matching of biometric data does not succeed. The machine should be adjusted. (d) The system works perfectly well and the data are accurate; nevertheless the probabilistic character of the matching operation leads to the result that the system does not find a match*", COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, cit., punto n. 95.

Proprio in questo senso si è espresso il *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, che si è soffermato altresì sul requisito della intelligibilità, precisando che potrebbe rendersi necessario un apposito macchinario in grado di leggere i dati biometrici ovvero un esperto capace di interpretarli: il Rapporto considera che il responsabile del trattamento non possa negare tale diritto adducendo semplicemente la non disponibilità di un'apparecchiatura appropriata ovvero la mancanza di un esperto. Infine, il documento mette in guardia dal pericolo di richieste illecite di accesso, che possano configurare l'ipotesi di furto d'identità, di modo che, se il responsabile sospettasse il verificarsi di simile eventualità, dovrebbe avviare un'indagine più approfondita[447].

Nonostante la centralità che l'art. 7 è chiamato ad assumere nell'ambito dell'intera disciplina, si può lasciare un interrogativo aperto sulla sua effettiva operatività e sul perché i singoli siano ricorsi ad esso limitatamente.

S. Rodotà individua una serie di ragioni meritevoli di considerazioni, per l'ambito della biometria in modo particolare: la scarsa informazione e, talvolta, alfabetizzazione; i costi, in termini temporali e non, dell'accesso, ragion per cui, nella stessa Convenzione 108 del 1981, si ribadisce che l'interessato deve ottenere indicazioni circa i suoi dati "*without excessive delay or expense*" (art. 8, lett. b); il dislivello tra il potere dei singoli e i grandi centri di potere pubblici o privati; l'eccesso di divieti;

[447] *Ibidem*, *Right of access*, punti 80-85 e *Right of rectification and erasure*, punti n. 86-93. Il Rapporto, come è noto, applica ai dati biometrici la Convenzione 108 del 1981, che stabilisce all'art. 8: "*Any persons shall be enabled: a) to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form; c) to obtain, as the case may be, rectification ore erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention; d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with*".

infine, quella che il noto giurista definisce "la scarsa significatività delle informazioni fornite in assenza di dati sul funzionamento generale del sistema in cui sono inserite"[448].

5. Informazione, libertà, consenso.

Si intende, ora, approfondire il significato del sintagma "consenso informato" nel caso concreto del trattamento dei dati biometrici, essendo già stati delineati i tratti generali dell'istituto[449].

Come sottolineato dallo stesso Documento di lavoro sulla biometria[450], esso rappresenta un principio di primaria rilevanza nell'ambito in questione, costituendo la base di legittimazione per il trattamento di tali dati, di modo che può dirsi violato ogniqualvolta essi siano raccolti all'insaputa dell'interessato (si pensi all'immagine del volto o dell'iride sottratta a distanza)[451], ovvero quando ciò non sia ritenuto necessario, così come avviene, per esempio, in Inghilterra, per il prelievo di campioni di capelli, di unghie, oppure di saliva[452].

Significativo, a questo proposito, il documento *Biometrics in Québec: Application Principles*, volto a fornire indicazioni sull'applicazione alle tecnologie biometriche dei fondamentali principi legislativi in tema di tutela dei dati personali all'interno della provincia canadese. Una volta ribadita la necessità del consenso

[448] S. RODOTÀ, *Protezione dei dati e circolazione delle informazioni*, cit., 747.
[449] Si veda il cap. II.
[450] GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria*, cit., punto n. 3.4.
[451] Si veda, in particolare, il documento OECD, WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometrics-based technologies*, cit., 12-13, ove si precisa, relativamente alla scansione dell'iride, che essa, con il progresso tecnologico, può essere effettuata a distanze sempre maggiori e senza alcun coinvolgimento da parte del soggetto interessato.
[452] Così COMITÉ CONSULTATIF NATIONAL D'ETHIQUE POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ, CCNE, Avis n° 98, *Biométrie, données identifiantes et droits de l'homme*, cit., II, B). Il Comitato dunque raccomanda che vi sia "*une stricte application des dispositions relatives au consentement préalable au recueil des données, ainsi qu'une limitation effective de tout recueil effectué à l'insu des intéressés*" (cfr. IV, *Reccomandations*).

espresso della persona interessata (*principle 1*, *principle 2*), ne vengono enucleati i requisiti fondamentali: "*it must be in writing, given freely in an informed manner, specific, and limited time*" (*principle 4*). In particolare, il documento sottolinea che tali informazioni debbono rimanere confidenziali, fintanto che il soggetto non abbia acconsentito alla loro diffusione (*principle 7*)[453].

Prendendo ora in considerazione la normativa italiana, il trattamento di dati biometrici da parte di privati ovvero di enti pubblici economici è soggetto alla disciplina dettata dagli artt. 23 ss. del Codice in materia di protezione dei dati personali, che non solo esclude la rilevanza di dichiarazioni tacite (art. 23, comma 1°), ma prevede altresì che vengano rispettati i requisiti generali della libertà, specificità ed informazione (art. 13; art. 23, comma 3°). Il consenso, inoltre, può riguardare l'intero trattamento ovvero una o più operazioni dello stesso (art. 23, comma 2°).

Quanto alla libertà, ci si potrebbe interrogare sulla effettiva possibilità per il soggetto di godere di determinati servizi, per accedere ai quali sia necessaria la rilevazione e il trattamento di tali informazioni, qualora questi si rifiuti di prestare il proprio consenso[454].

In più occasioni, l'Autorità italiana Garante per la protezione dei dati personali ha sottolineato che "in relazione all'eventualità che taluno non possa o non intenda aderire alla rilevazione biometrica effettuata […], deve essere predisposto un sistema alternativo di identificazione"[455]. L'impossibilità potrebbe riguardare, più

[453] COMMISSION D'ACCÈSS À L'INFORMATION, *Biometrics in Québec: Application Principles. Making an Informed Choice*, July 2002, in *www.cai.gouv.qc.ca/home_00_portail/01_pdf/biometrics.pdf*.
[454] A questo proposito, si è infatti sostenuto: "*But when is voluntary cooperation truly voluntary? This is not solely determined by market conditions, but also by the existence of a fully-fledged alternative facility without biometrics, so that true freedom of choice is possible*", J. GRIJPINK, *Biometrics and Privacy*, cit., 158. Nello stesso senso, P. DE HERT, *Biometrics: legal issues and implications*, cit., 11, che si chiede: "*Is there a truly free consent when banks and credit card companies impose biometrics on their cards?*". Ancora, si veda il *principle 1*, *Alternatives to Biometrics*, del documento COMMISSION D'ACCÈSS À L'INFORMATION, *Biometrics in Québec: Application Principles. Making an Informed Choice*, cit.
[455] Si vedano, in particolare, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati personali biometrici per l'accesso a un complesso polifunzionale - 1 febbraio 2007*, doc. web n. 1381983, cit., punto n. 3.3; GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati biometrici*

comunemente, una menomazione fisica, mentre il diniego sarebbe espressione di quella libertà negativa che è dimensione basilare del consenso.

La non predisposizione di misure di identificazione sostitutive, dunque, impedirebbe l'esplicarsi di una libera scelta, poiché il soggetto si troverebbe nella condizione di esprimere un consenso forzato, pur di accedere al servizio di proprio interesse, violando così quella "inderogabile esigenza di rispettare il corpo umano nell'utilizzo delle nuove tecnologie e nella rilevazione dei dati biometrici"[456].

Di qui l'importanza di predisporre, accanto a quelli biometrici, anche sistemi meno gravosi e più comuni di identificazione, come, per esempio, un P.I.N.[457], oppure un tradizionale documento di identificazione[458].

Relativamente alla c.d. informativa, ossia la dichiarazione, orale o scritta, che il titolare o il responsabile del trattamento fornisce all'interessato circa l'utilizzo dei suoi dati personali[459], essa deve comprendere tutti gli elementi di cui all'art. 13, e non limitarsi ad indicare la sola finalità del trattamento[460]. In particolare, andranno fornite le informazioni che riguardano la natura obbligatoria o facoltativa del conferimento dei dati; le conseguenze di un eventuale rifiuto; i soggetti che possono venire a conoscenza di tali informazioni; il diritto di accesso e i correlati diritti; gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato e del responsabile.

---

presso Banca San Paolo Imi S.p.A. - 23 gennaio 2008, doc. web n. 1490533, cit., punto n. 3.1; GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento del 23 gennaio 2008*, doc. web n. 1487903, cit., punto n. 3, ove il Garante rileva, tra le varie motivazione della pronuncia contraria al trattamento dei dati biometrici, anche la mancata predisposizione di tecniche alternative di verifica dell'identità dei soggetti interessati.

[456] Così GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Il decalogo su corpo e libertà*, Comunicato stampa - 09 maggio 2006, in *www.garanteprivacy.it*.

[457] Così GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sicurezza merci e controllo delle presenze presso aeroporti - 26 luglio 2006*, doc. web n. 1318582, cit., punto n. 3.3.

[458] Si veda il Comunicato stampa del 17 novembre 2005 del Garante per la protezione dei dati personali, in *www.garanteprivacy.it/garante/doc.jsp?ID=1190518*.

[459] G. M. CUBEDDU, Commento art. 13, in C. M. BIANCA, F. D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, cit., 304.

[460] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento del 23 gennaio 2008*, doc. web n. 1487903, cit., punto n. 3.

La stessa deve altresì includere indicazioni circa la possibilità di accedere alle misure alternative summenzionate, essendo "necessario che le informazioni da rendere agli interessati enuncino chiaramente tutte le modalità impiegate nel trattamento e la tipologia di dati personali utilizzati per ciascuna di esse"[461].

Il Garante ha infine predisposto, in base all'art. 13, comma 3°, una modalità semplificata di informativa scritta per i dati biometrici, da affiggere in corrispondenza dei luoghi ove tali sistemi vengono utilizzati[462].

In alcune circostanze, tuttavia, il trattamento può essere effettuato senza il consenso della persona interessata (art. 24), e ciò al fine di realizzare un concreto bilanciamento degli interessi in gioco. Per i dati biometrici valgono, in modo particolare, le ipotesi relative alla "salvaguardia della vita o dell'incolumità fisica di un terzo" (lett. e); allo "svolgimento delle investigazioni difensive […], o, comunque, per far valere o difendere un diritto in sede giudiziaria" (lett. f); al perseguimento di "un legittimo interesse del titolare o di un terzo destinatario di dati, […] qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato " (lett. g)[463].

L'Autorità ha inoltre stabilito che "il consenso dell'interessato deve ritenersi non necessario anche con riguardo alle operazioni di decrittazione dei dati trattati ad opera del vigilatore dei dati[464], le cui ulteriori operazioni di trattamento devono esaurirsi nella

---

[461] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Compiti del Garante - Uso delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro - 21 luglio 2005*, doc. web n. 1150679, cit., punto n. 3.

[462] Il modello di informativa può essere reperito in *http://www.garanteprivacy.it/garante/doc.jsp?ID=1246675*.

[463] A questo proposito, si veda GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Istituti di credito - Rilevazione di impronte digitali ed immagini: limiti e garanzie - 27 ottobre 2005*, doc. web n. 1246675, cit., punto n. 5.

[464] Quanto al "vigilatore dei dati", si tratta di una nuova figura, che si aggiunge a quelle tradizionalmente previste dal Codice. Tra queste ultime, si ricordano anzitutto il titolare del trattamento, che è colui al quale competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi incluso il profilo della sicurezza (art. 4, comma 1°, lett. f); il responsabile, ossia il soggetto, designato facoltativamente dal titolare, specificando analiticamente per iscritto i compiti da affidare, che per capacità, esperienza, ed affidabilità, può fornire idonea garanzia del pieno rispetto delle

sola comunicazione dei dati «in chiaro» ai soggetti sopra individuati o all'interessato che abbia esercitato il diritto di accesso riconosciutogli dall'art. 7 del Codice"[465].

Non pare, tuttavia, chiaro come possano armonizzarsi le suddette deroghe con la previsione di misure alternative di accesso per i soggetti che non vogliano prestare il proprio consenso, atteso che l'installazione di sistemi biometrici avviene sulla base di determinati principi, rispondendo sempre a concrete esigenze di sicurezza[466]. In altri termini, risulta un'aporia il fatto che, da una parte, sia necessario il consenso del soggetto per l'accesso ad un istituto di credito ove sia installato un sistema di rilevazione biometrica, essendo in gioco, principalmente, la salvaguardia dell'incolumità fisica di terzi ma, ad un tempo, si preveda la predisposizione di misure alternative, qualora questi rifiuti la propria collaborazione.

Un cenno merita anche la questione delle regole ulteriori per i soggetti pubblici. In tal caso, il Codice prevede, salvo in materia di sanità, che il consenso non sia richiesto (art. 18, comma 4°), purché in ogni caso venga rispettato il vincolo dell'utilizzo dei dati per lo svolgimento di funzioni istituzionali (art. 18, comma 2°).

Una conferma in tale senso si può ricavare dal provvedimento sulla Carta multiservizi della giustizia (Cmg). Si tratta di un progetto elaborato dal Ministro della giustizia volto a realizzare un sistema sicuro di accesso del personale dipendente e dei magistrati ai dati sensibili e giudiziari, utilizzando una carta elettronica ove siano registrati dati biometrici, segnatamente due *template* delle impronte digitali del

---

disposizioni vigenti, compreso l'ambito della sicurezza (art. 29); e gli incaricati, ossia le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile (art. 4, comma 1°, lett. h). Il vigilatore dei dati, invece, è stato istituito nell'ambito dei provvedimenti relativi alla sicurezza negli istituti di credito, e si tratta di "un soggetto indipendente dalla banca a cui viene affidato un compito importante a difesa dei cittadini". Segnatamente, questi è chiamato ad assumere il "delicato ruolo di custodire le chiavi crittografiche e di garantire la riservatezza dei clienti", GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Banche: impronte digitali, telecamere e diritti dei clienti*, Comunicato stampa del 17 novembre 2005, in *http://www.garanteprivacy.it/garante/doc.jsp?ID=1190523*.

[465] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Istituti di credito - Rilevazione di impronte digitali ed immagini: limiti e garanzie - 27 ottobre 2005*, doc. web n. 1246675, cit., punto n. 5.

[466] Si veda il paragrafo 1 del presente capitolo.

dipendente, per autenticare gli utenti in vista dell'accesso a postazioni di lavoro o dell'ingresso a particolari locali. Da tale documento è possibile dedurre, a fronte dell'assoluta mancanza di riferimenti al principio in esame, che i trattamenti di dati biometrici in ambito pubblico possano essere di fatto imposti[467].

6. (*Segue*) Consenso informato e dati biometrici sensibili.

Si è ipotizzato, nel corso di questo lavoro, che i dati biometrici siano suscettibili, in determinate ipotesi, di essere considerati come dati di natura sensibile e, nell'ambito di tale categoria, che possano altresì essere riguardati come in grado di rivelare lo stato di salute del soggetto[468].

Ai sensi dell'art. 26, comma 1°, dunque, il trattamento dei dati biometrici sensibili potrà avvenire da parte di privati o di enti pubblici economici "solo con il consenso scritto dell'interessato e previa autorizzazione del Garante"[469].

La *ratio* dello speciale regime riservato a questa categoria di informazioni può essere individuata nel fondamentale principio della dignità (art. 2), che si configura come "chiave di lettura" dell'intera disciplina posta a tutela del trattamento dei dati personali, ovvero come "bussola", volta ad orientare ogni decisione relativa al trattamento di dati personali, a fronte dei particolari e gravi pregiudizi che potrebbero derivare da un uso non appropriato di informazioni di natura sensibile[470].

---

[467] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *In progetto la carta multiservizi della giustizia (Cmg) per un accesso più sicuro ai sistemi informatici giudiziari. Le valutazioni del Garante*, doc. web n. 1185160, in *www.garanteprivacy.it*.

[468] Si veda il cap. III, paragrafo 9.

[469] Cfr. anche art. 23, comma 4°. Per la necessità del consenso scritto nel caso di trattamento di dati biometrici di natura sensibile, si è pronunciata S. BISI, *Il corpo come password: alcune considerazioni in tema di sistemi di autenticazione biometrica*, cit., 18.

[470] Sul punto, si veda in particolare E. PELLECCHIA, Commento art. 26, cit., 619.

Pertanto, come dichiarato dal Presidente del Garante per la protezione dei dati personali Francesco Pizzetti, nel discorso di presentazione della Relazione per l'anno 2007, l'Autorità richiede "un fermo e chiaro invito alla moderazione nell'uso di questi strumenti, in quanto potenzialmente lesivi della dignità delle persone", per cui è necessario che "si eviti di fare ricorso a queste tecniche secondo criteri discriminatori, specialmente di natura etnica o religiosa, che contrastino con la nostra Costituzione e con le Carte dei diritti fondamentali dell'uomo e del cittadino che il nostro Paese ha siglato"[471].

Vi sono ipotesi, invero, in cui il trattamento di dati sensibili stesso può avvenire senza il consenso dell'interessato, previa tuttavia autorizzazione del Garante (art. 26, comma 4°). Si tratta di eccezioni già considerate per i dati biometrici ordinari (art. 24, comma 1°, lett. e, lett. f), cui si aggiunge anche il caso in cui il trattamento si riveli necessario per adempiere ad obblighi previsti dalla legge nell'ambito di un rapporto di lavoro (art. 26, comma 4°, lett. d).

Per quanto riguarda, invece, il consenso all'utilizzo di quei particolari dati sensibili che sono quelli idonei a rivelare lo stato di salute del soggetto, l'art. 81 prevede che esso possa essere manifestato "con un'unica dichiarazione, anche oralmente". La scelta della non obbligatorietà della forma scritta, non sembra di fatto coerente con la finalità di tutelare la particolare delicatezza delle informazioni in esame, tanto più alla luce della più rigorosa disciplina stabilita per i dati sensibili in genere, giustificandosi solo sulla base di un eventuale risparmio economico e temporale[472].

---

[471] F. PIZZETTI, *Discorso del Presidente*, Roma, 16 luglio 2008, Relazione 2007, in *www.garanteprivacy.it*, 17-18.

[472] Così S. CACACE, Commento art. 81, in BIANCA C. M., F. D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, II, Padova, Cedam, 2007.

Infine, si intende accennare anche al problema del trattamento di dati biometrici sensibili in ambito pubblico, per i quali la regola generale stabilita dall'art. 20, comma 1°, prevede che il trattamento sia consentito "solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite".

7. Altri aspetti significativi in tema di trattamento di dati biometrici: dati biometrici semi sensibili, controllo preliminare e notificazione dei sistemi.

Una volta delineati i principi fondamentali che sono alla base della disciplina sul trattamento dei dati biometrici, e approfonditi alcuni aspetti essenziali circa la posizione giuridica dell'interessato, è opportuno soffermarsi brevemente su ulteriori punti che riguardano il trattamento stesso.

Si ricorda, anzitutto, che nel precedente capitolo è stato approfondito il problema della qualificazione giuridica dei dati biometrici. Chiarita la natura di dati personali, ci si è interrogati sulla possibilità di collocarli nel *genus* dei dati sensibili ovvero genetici. Non si è presa, tuttavia, in considerazione una terza categoria residuale, quella dei dati semi sensibili. Si tratta di dati che, ai sensi dell'art. 17, comma 1°, del Codice, non sono né sensibili né giudiziari, e pur tuttavia presentano "rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare"[473].

[473] La disposizione riprende l'art. 20 della direttiva n. 95/46/CE, che dispone: "Gli Stati membri precisano i trattamenti che potenzialmente presentano rischi specifici per i diritti e le libertà delle persone e provvedono a che tali trattamenti siano esaminati prima della loro messa in opera". Va precisato che il ricorso alla verifica preliminare si realizza in numerose ipotesi, e precisamente quelle previste dagli artt. 14, 37, 55, 91 e 167 del Codice. Si vedano, in particolare, per il commento all'articolo in esame, S. BERNARDI, Commento art. 17, in C. M. BIANCA, F. D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, I, Padova, Cedam, 2007, 450 e G. P. CIRILLO (a cura di), *Il Codice sulla protezione dei dati personali*, cit., 80-81.

Si può ritenere che, in più ipotesi, i dati biometrici rientrino in questa categoria poiché, quand'anche non siano propriamente di natura sensibile, tuttavia, come più volte è stato ribadito, facilmente il loro utilizzo può nuocere ai diritti, alle libertà fondamentali e alla dignità di colui al quale si riferiscono. Una esplicita conferma proviene altresì dall'art. 55, che parla di "trattamento di dati personali che implica maggiori rischi di un danno all'interessato, con particolare riguardo a banche di dati genetici o biometrici", disponendo che, se esso è effettuato dalle forze di polizia, vanno rispettate le misure e gli accorgimenti a garanzia dell'interessato di cui all'art. 17, previa comunicazione al Garante (art. 39).

Il trattamento dei dati biometrici semi sensibili va anzitutto sottoposto al c.d. *Prior Cheking* o verifica preliminare (art. 17, comma 2°), al fine di rafforzare l'attività di vigilanza, evitando che i controlli siano effettuati esclusivamente a posteriori[474].

Lo stesso Gruppo per la tutela dei dati personali, nel Documento di lavoro sulla biometria, raccomanda di considerare la possibilità di sottoporre i dati biometrici ad un controllo preliminare, "poiché tale tipo di trattamento presenta potenzialmente rischi specifici per i diritti e le libertà delle persone interessate", lasciando tuttavia ampia discrezionalità agli Stati membri ("Se gli Stati membri intendono introdurre…")[475].

L'Autorità italiana ha accolto pienamente la raccomandazione proveniente dall'organo consultivo europeo, ritenendo troppo rischioso procedere all'utilizzo di tali dati senza passare per questa via preventiva, di modo che tutti i pronunciamenti in tema di biometria sono successivi a richieste di verifica preliminare *ex* art. 17.

Una conferma circa la necessità del ricorso al *Prior Checking* nel trattamento dei dati biometrici, si può rinvenire nel pronunciamento del Garante del 27 ottobre 2005

[474] Così G. P. CIRILLO (a cura di), *Il Codice sulla protezione dei dati personali*, cit., 80-81.
[475] GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria*, cit., par. 3.5, 9.

sulla rilevazione di impronte digitali ed immagini[476], ove viene richiamato il provvedimento generale sulla videosorveglianza, nel quale si dispone che "i trattamenti di dati personali nell'ambito di una attività di videosorveglianza devono essere effettuati rispettando le misure e gli accorgimenti prescritti da questa Autorità, anche con un provvedimento generale, come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello del titolare (art. 17 del Codice), quando vi sono rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati"[477].

L'intervento in via preliminare è possibile evidentemente solo se il Garante ha ricevuto notizia, da parte del titolare, dell'intenzione di procedere al trattamento, nonché delle finalità, dell'oggetto e delle principali caratteristiche dello stesso[478].

La notificazione è obbligatoria, salvo tuttavia alcune eccezioni[479], per specifiche categorie di informazioni di natura particolarmente delicata, tra le quali rientrano, secondo l'art. 37, comma 1°, lett. a, anche i dati biometrici[480].

Si ricorda, infine, che la presente disposizione, insieme all'art. 55, è la sola del Codice a fare espresso riferimento ai dati in esame.

---

[476] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Istituti di credito - Rilevazione di impronte digitali ed immagini: limiti e garanzie - 27 ottobre 2005*, cit., par. 2.

[477] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Videosorveglianza – Provvedimento generale – 29 aprile 2004*, doc. web n. 1003482, in *www.garanteprivacy.it*, par. 3.2.1.

[478] Si veda, per i caratteri generali della notificazione, R. ROSETTI, commento artt. 37-38, in C. M. BIANCA, F. D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, cit., 734-772.

[479] Tra i casi da sottrarre a notificazione, si ricordano in particolare "i trattamenti non sistematici di dati genetici o biometrici effettuati da esercenti le professioni sanitarie, anche unitamente ad altri esercenti titolari dei medesimi trattamenti, rispetto a dati non organizzati in una banca di dati accessibile a terzi per via telematica […]" (n. 1, lett. a) e "i trattamenti di dati genetici o biometrici effettuati nell'esercizio della professione di avvocato, in relazione alle operazioni e ai dati necessari per svolgere le investigazioni difensive di cui alla legge n. 397/2000, o comunque per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria […]" (n. 2, lett. b), GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento relativo ai casi da sottrarre all'obbligo di notificazione - 31 marzo 2004*, doc. web n. 852561, in *www.garanteprivacy.it*.

[480] Oltre ai dati biometrici, nell'elenco di dati soggetti a notificazione rientrano anche, per la loro rilevanza, i dati genetici; i dati idonei a rivelare lo stato di salute e la vita sessuale del soggetto, comprese le informazioni relative alla procreazione assistita, alla sieropositività e al trapianto; i dati che riguardano la sfera psichica; infine, i dati relativi alla solvibilità economica, alla situazione patrimoniale, al corretto adempimento delle obbligazioni (art. 37, comma 1°).

8. (*Segue*) Misure di sicurezza. Cenni.

Altra questione da considerare è quella che riguarda l'utilizzo di tecniche idonee a garantire la sicurezza dei dati biometrici, per proteggerli dalla distruzione, perdita, diffusione ovvero accessi non autorizzati.

Il Garante per la protezione dei dati personali si è preoccupato in più occasioni della questione della sicurezza, prevedendo anzitutto due minimali e preliminari forme di garanzia, alle quali si è fatto più volte riferimento, ossia la conservazione delle informazioni biometriche all'interno di un dispositivo portatile piuttosto che di una base di dati centralizzata, e la loro cancellazione dopo un breve arco di tempo, generalmente non superiore ai sette giorni[481].

In particolare, nel provvedimento generale in tema di rilevazione di impronte digitali ed immagini all'interno di istituti di credito del 27 ottobre 2005, l'Autorità individua alcune misure più specifiche, cui i sistemi in esame dovrebbero sottostare[482].

Si dispone, in primo luogo, che i dati biometrici, una volta raccolti, siano immediatamente cifrati dal sistema, di modo che non possano essere salvati in un *database* come dati "grezzi". In secondo luogo, al fine di evitare errori di identificazione, l'immagine del cliente e l'impronta digitale devono essere associate in modo univoco. In terzo luogo, viene raccomandato l'utilizzo di sistemi crittografici "robusti", sia per le immagini che per le impronte. In questo caso, assume rilevanza la figura del più volte menzionato vigilatore dei dati, depositario delle chiavi crittografiche atte a leggere le informazioni criptate, e in assenza del quale non è permesso accedervi. Si prevede altresì che vengano adottate le misure previste in via generale per la

[481] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati (deliberazione n. 53 del 23 novembre 2006),*cit., par. 4.3.
[482] Vedi GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Istituti di credito - Rilevazione di impronte digitali ed immagini: limiti e garanzie - 27 ottobre 2005*, cit., par. 4, lett. c.

sicurezza dei sistemi e dei dati, di cui al Titolo V del Codice (artt. 31 ss.), e le misure minime disposte dal "Disciplinare tecnico in materia di misure minime di sicurezza" (Allegato B)[483]. Infine, i sistemi in esame devono "offrire una garanzia rigorosa di affidabilità e di integrità, anche sulla base di eventuali certificazioni od omologazioni dei dispositivi". Tali attestati di conformità vanno rilasciati dall'installatore al titolare della struttura presso la quale i sistemi biometrici vengono collocati (Allegato B, n. 25).

Tale elenco, evidentemente, non può considerarsi esaustivo. Lo stesso Garante ha individuato altre forme di garanzia per determinate applicazioni, come la possibilità di utilizzare una *password* al fine di proteggere maggiormente i dati crittografati[484]; se si tratta invece di dati memorizzati all'interno di una *smart card*, l'Autorità ha prescritto la sostituzione dell'indicazione nominativa con un codice individuale[485] e, in caso di smarrimento o di furto, "la disattivazione automatica, immediata e certa di funzioni di smart card o altre analoghe"[486].

Il Documento di lavoro sulla biometria si sofferma lungamente sul problema, prevedendo, tra le misure adottabili, "la cifratura dei modelli e la protezione delle chiavi di cifratura oltre al controllo e alla protezione dell'accesso, rendendo così virtualmente impossibile la ricostruzione dei dati originali a partire dai modelli"[487]. L'attenzione dell'organo europeo alla corretta conservazione delle informazioni biometriche è ben comprensibile, se si considera che "qualsiasi perdita delle caratteristiche di integrità, riservatezza e disponibilità a livello di basi di dati danneggerebbe tutte le future

[483] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Disciplinare tecnico in materia di misure minime di sicurezza*, doc. web. n. 1557184, in *www.garanteprivacy.it*,
[484] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Accesso ad aree riservate di particolari aziende: uso proporzionato di impronte digitali - 23 novembre 2005*, cit.
[485] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sicurezza merci e controllo delle presenze presso aeroporti - 26 luglio 2006*, cit., par. 3.1.
[486] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Il decalogo su corpo e libertà*, cit., punto n. 10.
[487] GRUPPO PER LA TUTELA DEI DATI PERSONALI (articolo 29), *Documento di lavoro sulla biometria,* cit., par. 3.6.

applicazioni basate sulle informazioni contenute in tali basi di dati e comporterebbe altresì danni irreparabili per le persone interessate"[488].

Attenzione alla questione della sicurezza dei dati biometrici è stata posta anche dal noto *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, ove vengono indicate alcune misure di protezione[489]. Si sostiene, anzitutto, che andrebbero stabiliti degli *standards* di qualità per i *software* e per gli *hardware* in relazione alle applicazioni su vasta scala dei sistemi in questione; in secondo luogo, tali *standards* dovrebbero essere regolarmente revisionati da un organo indipendente che faccia una valutazione complessiva del sistema biometrico; in terzo luogo, si propone l'utilizzo di algoritmi affidabili con cui estrarre il *template* dal dato grezzo e per il confronto dei *templates* tra loro; infine, si raccomanda l'uso della crittografia durante il processo di acquisizione delle informazioni, nonché per la conservazione ovvero trasmissione dei dati.

Invero, sembra opportuno non porre eccessiva enfasi sull'utilizzo dei metodi crittografici. Essi, infatti, non rappresentano una garanzia assoluta di tutela delle informazioni, poiché qualcuno sarà in possesso della chiave idonea ad aprire questa "serratura" e dunque sarà in grado di accedere al patrimonio informativo che si intende mantenere segreto[490]. Il problema, pertanto, non viene eliminato, bensì solamente spostato. In altre parole, quanto più si ricorre a strumenti capaci di rafforzare la *privacy* e la sicurezza delle informazioni, tanto più si pone la questione della sicurezza e della

[488] *Ibidem*.
[489] Si vedano i punti 75, 76 e 77 del documento.
[490] Per comprendere la portata del problema, si può considerare la conclusione di una pubblicazione in tema di crittografia, che contiene la seguente (ed efficace…) affermazione: "La sicurezza assoluta è, quindi, soltanto un mito: non esiste!!!", C. SARZANA DI S. IPPOLITO, *Le iniziative internazionali in tema di sistemi crittografici con riferimento alla tutela dei dati personali*, in *Dir. inf.*, 1998, 13. Fiducia sulla moderna crittografia è espressa da A. LYSYANSKAYA, *Come mantenere un segreto*, in *Le Scienze*, novembre 2008, n. 483, 106, ove tuttavia si ammette: "I crittografi non possono provare con assoluta certezza che un sistema crittografico sia inviolabile". Si vedano inoltre, in tema di RFID (*Radio-Frequency IDentification*), le osservazioni svolte da A. JUELS, *RFID Privacy. A Technical Primer for the Non-Technical Reader*, in K. STRANDBURG, D. S. RAICU (edited by), *Privacy and Technologies of Identity. A cross disciplinary conversation*, New York, Springer, 2006, 68-70.

gestione delle chiavi crittografiche, cosicché a qualcuno è sorto spontaneo l'interrogativo: "*Quid custodiet ipsos custodes?*", "*Chi sorveglierà gli stessi sorveglianti*?" [491].

9. Cittadinanza e biometria: lo *European passport*.

Una volta approfondita la questione del trattamento dei dati biometrici nel panorama giuridico italiano, pare opportuno dare uno sguardo ad alcune applicazioni concrete, per cogliere fino a che punto i sistemi in questione stiano facendo il loro ingresso all'interno delle istituzioni sopranazionali, dei singoli Stati, di organizzazioni, di enti pubblici o privati.

Si rivela particolarmente interessante, a questo proposito, volgere l'attenzione alla dimensione europea, ove si assiste ad una sempre maggiore implementazione delle tecniche biometriche con particolare riferimento all'ambito della cittadinanza, in vista, per così dire, di una "cittadinanza sicura". In particolare, i paesi membri dell'Unione si sono mostrati favorevoli al rafforzamento dei requisiti di sicurezza dei documenti da viaggio rilasciati ai cittadini membri, con l'introduzione dello *European passport*. Emblematico anche il caso dell'istituzione di una banca dati europea per i richiedenti asilo, che costituisce il sistema *Eurodac*.

Tra quelle menzionate, l'applicazioni certamente più significativa e di vasta scala è costituita dall'inserimento di dati biometrici all'interno dei passaporti[492]. La biometria entra, in questo modo, prepotentemente, nella vita quotidiana della

[491] L'interrogativo è al centro della questione della sicurezza informatica, per cui si veda il resoconto del dibattito svoltosi in California tra professionisti del settore, AA. VV., *Migliorare la sicurezza informatica*, in *Le Scienze*, novembre 2008, n. 483, 108.

[492] Si veda, per una ricostruzione dettagliata dei programmi internazionali in ambito di aviazione, A. PIERA, *Facilitation of air transport*, in 26 *Air & Space Law* (2001), 315-332, e A. PIERA, *The simplifying passenger travel programme and its legal implications*, in 28 *Air & Space Law* (2003), 132- 138.

maggioranza delle persone, rendendo affatto superflua un'indagine approfondita sui problemi, particolarmente di natura giuridica ed etica, che solleva.

Quanto al dato legislativo, l'introduzione di elementi biometrici nei documenti di viaggio ha seguito un iter complesso ove, se da una parte si riscontra un generale favore circa il ricorso a tali tecniche, dall'altra si evince la preoccupazione che sia assicurata una garanzia quanto più ampia possibile per i soggetti coinvolti.

L'atto fondamentale di tale percorso è stato l'adozione del regolamento (CE) n. 2252/2004 del Consiglio del 13 dicembre 2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri[493], dopo che la Commissione europea, il 18 febbraio 2004, aveva presentato una proposta di regolamento. Scopo della proposta era rendere più sicuri i passaporti mediante uno strumento giuridicamente vincolante, sulla scorta di quanto disposto dal Consiglio europeo di Salonicco del 19 e 20 giugno 2003, che aveva sostenuto la necessità di adottare una strategia coerente a livello dell'Unione in relazione all'utilizzo dei sistemi in esame, nonché di stabilire un nesso certo tra il titolare legittimo e il documento, mediante appunto il ricorso agli identificatori biometrici[494].

Passando ad un esame più dettagliato delle principali disposizioni del regolamento, esso stabilisce, anzitutto, che i passaporti e i documenti di viaggio debbano contenere un sopporto ove memorizzare l'immagine del volto. Gli Stati aggiungono le impronte digitali in formato interoperativo, dovendo altresì proteggere i dati così registrati (art. 1, par. 2). In secondo luogo, si precisa che la disciplina in esame non si applica a passaporti e documenti di viaggio temporanei né alle carte di identità

[493] In *GUCE* n. L 385 del 29.12.2004, considerando n. (1) e n. (2).
[494] GRUPPO DI LAVORO ARTICOLO 29, PROTEZIONE DATI, *Parere 3/2005 riguardante l'attuazione del regolamento CE n. 2252/2004 del Consiglio, del 13 dicembre 2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli stati membri (Gazzetta ufficiale L 385 del 29.12.2004, pp. 1-6)*, cit., 13.

rilasciate dagli Stati membri ai loro cittadini, bensì esclusivamente a passaporti e documenti di viaggio rilasciati dagli Stati membri (art. 1, par. 3). Quanto all'interessato, questi ha diritto sia di verificare i dati personali riportati, sia di chiederne eventuale rettifica o cancellazione, fatte salve in ogni caso le norme relative alla protezione dei dati personali (art. 4, par. 1). Per ciò che concerne, infine, la finalità dell'introduzione degli elementi biometrici in tali documenti, essa consiste nel verificare l'autenticità del documento e in secondo luogo l'identità del titolare (art. 4, par. 3, lett. a e b).

Come si è detto, l'adozione della proposta di regolamento è avvenuta non senza critiche, opposizioni e richieste di emendamento.

Il 28 ottobre 2004, la Commissione per le libertà civili, la giustizia e gli affari interni, prende in esame la proposta, presentando, nella relazione del 28 ottobre 2004 tenuta dall'eurodeputato Carlos Cohelo, numerosi emendamenti[495]. Pur essendo il relatore in linea di massima concorde con l'introduzione dell'identificatore biometrico, ciò nonostante egli ritiene necessario che "un certo numero di requisiti per la tutela dei diritti dei cittadini siano operativi prima che vengano emessi passaporti biometrici"[496].

Anzitutto, vanno rispettati i principi generali in tema di trattamento di dati personali, con particolare riferimento al principio di finalità e proporzionalità, indicando chiaramente e specificatamente nel testo giuridico l'obbiettivo che si intende perseguire, al fine di evitare ogni forma di sorveglianza occulta (emendamento 12), nonché chi utilizzerà i dati raccolti (emendamento 8). Particolare preoccupazione viene espressa riguardo alla possibile creazione di una banca dati centralizzata, che "violerebbe la finalità e il principio di proporzionalità, aumentando peraltro il rischio di abusi e di

[495] PARLAMENTO EUROPEO, COMMISSIONE PER LE LIBERTÀ CIVILI, LA GIUSTIZIA E GLI AFFARI INTERNI, *Relazione sulla proposta della Commissione di regolamento del Consiglio relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti dei cittadini dell'Unione (COM(2004)0116-C5-0101/2004-2004/0039(CNS))*, 28.10.2004, in *http://www.europarl.europa.eu/sides/getDoc.do?language=IT&pubRef=//EP//NONSGML+REPORT+A6-2004-0028+0+DOC+PDF+V0//IT*.
[496] *Ibidem*, *Motivazione*, 16.

snaturamento della funzione originaria della raccolta dei dati («*function creep*»)" e, ad un tempo, "aumenterebbe anche il rischio che si usino gli identificatori biometrici come «chiavi d'accesso» a varie banche di dati, interconnettendo in tale modo serie di dati" (emendamento 5, motivazione). Anche sul piano dell'attuazione tecnica, vengono previste specifiche garanzie, per evitare, ad esempio, che il microprocessore contenente i dati biometrici possa essere letto ad una distanza relativamente grande, permettendo così accessi non autorizzati[497].

Interessante rilevare anche la posizione della minoranza, che respinge *in toto* l'idea generale di introdurre identificatori biometrici nei documenti d'identità[498]. Sono sostanzialmente tre le ragioni di tale contrarietà. In primo luogo, si ritiene sussistano pericoli quanto a furti e abusi d'identità, alla possibilità di creare identità multiple, alla intercettazione di trasmissioni di dati, alla sorveglianza proattiva, e alla mancanza di accuratezza. In secondo luogo, si rileva che non è stato effettuato alcun chiaro calcolo sui costi e benefici di tale scelta, non essendo stati argomentati "la necessità, l'efficacia e i probabili effetti secondari dell'inclusione di identificatori biometrici nei documenti di identità". Infine, si sostiene che "la biometria non aumenta la sicurezza perché non collega una persona a una identità reale ma solo a una identità stabilita da un documento d'identità". In questo senso, può accadere paradossalmente che gli spostamenti aerei diventino meno sicuri, poiché un criminale che si registri sotto falsa identità potrà essere

[497] *Ibidem*, *Motivazione*, 17.

[498] *Ibidem*, *Opinione della minoranza*, 19. In questo senso, si veda anche G. HORNUNG, *The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards*, in 4 *SCRIPT-ed* (2007), 259-260, ove l'a. pone altresì il problema della sicurezza del *chip* di memorizzazione del dato, nonché quello dei costi del nuovo passaporto. Tra le varie critiche sollevate al regolamento n. 2252/2004, si ricordano inoltre quelle avanzate da P. DE HERT, W. SCHREURS, E. BROUWER, *Machine-readable identity documents with biometric data in the EU – part III*, in 23 *Keesing Journal of Documents & Identity* (2007), 29-30. Si contesta in particolare: 1. L'unilateralismo da parte del Consiglio, per cui importanti decisioni sono state prese senza lasciare spazio al dibattito pubblico, privando altresì il Parlamento europeo dell'esercizio dei suoi poteri legislativi; 2. L'idea di *standards* comuni per le ID *cards* nell'UE è nuova, e l'UE non ha il potere attualmente di adottare misure in relazione alle ID *cards*. 3. Non è stato tenuto in debito conto che informazioni sensibili potrebbero essere trasferite ad altri paesi tutte le volte che la verifica è richiesta ai controlli di frontiera.

riconosciuto positivamente, sotto la falsa identità acquisita, ad ogni controllo cui si sottoporrà.

Segue, il 2 dicembre del 2004, una risoluzione legislativa del Parlamento europeo sulla proposta della Commissione di regolamento del Consiglio relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici nei passaporti dei cittadini dell'Unione[499], che prevede, tra le misure più rilevanti, il rifiuto dell'inserimento obbligatorio delle impronte digitali e dell'istituzione di una base di dati centrale per i passaporti e documenti di viaggio (emendamento 5)[500]. Si richiama, nel medesimo emendamento, la necessità che il supporto di memorizzazione venga "altamente protetto" e si prevede altresì, a garanzia della sicurezza, che l'applicazione del regolamento sia "subordinata alla presentazione da parte delle autorità nazionali di protezione dei dati di una certificazione attestante che esse dispongono di poteri d'indagine e risorse sufficienti per attuare la direttiva 95/46/CE per quanto riguarda i dati raccolti conformemente ad essa" (emendamento 19). Degno di nota, infine, l'emendamento 8, ove si dichiara che "il supporto di memorizzazione può essere utilizzato solo: a) dalle autorità degli Stati membri competenti a leggere, memorizzare, modificare e cancellare dati, e b) dagli organismi autorizzati cui la legge conferisce la facoltà di leggere i dati, per la lettura dei dati", e il successivo emendamento 9, secondo cui ogni Stato membro dovrà munirsi di un apposito registro delle autorità competenti e degli organismi autorizzati.

---

[499] *Risoluzione legislativa del Parlamento europeo sulla proposta della Commissione di regolamento del Consiglio relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici nei passaporti dei cittadini dell'Unione (COM(2004)0116 — C5-0101/2004 — 2004/0039(CNS))*, in *GUCE* n. C 208 E/50 del 25.8.2005.

[500] Sulla inopportunità di creare una base di dati, si veda, in dottrina, P. DE HERT, W. SCHREURS, E. BROUWER, *Machine-readable identity documents with biometric data in the EU – part IV*, in 24 *Keesing Journal of Documents & Identity* (2007), 32-33, ove si sostiene che l'utilizzo di un *database* non previene gli attacchi terroristici, poiché spesso i terroristi vivono nel paese dove gli attacchi vengono perpetrati e in ogni caso sono sufficientemente intelligenti da assicurarsi che il loro nome non sia registrato in una base di dati in qualità di sospettati; le identità, inoltre, possono essere rubate mediante l'accesso al *database*; infine, una banca di dati biometrici può avere un enorme valore economico, anche per i governi.

Anche il Gruppo per la tutela dei dati personali (articolo 29) si è pronunciato in merito a tale questione, prima di adottare un apposito parere[501].

Nell'agosto del 2004, infatti, il presidente del summenzionato organo consultivo aveva inviato una lettera ai rappresentanti di altri organi europei, esprimendo contrarietà rispetto ad un possibile utilizzo di una base di dati centralizzata di dati biometrici, richiamando il rispetto dei principi di finalità e proporzionalità e la necessità di utilizzare sistemi tecnicamente validi, infine, precisando la necessità che venissero indicati i soggetti che potevano accedere e che fosse creato un apposito registro delle autorità nazionali. Successivamente, in un'altra lettera, veniva contrastata l'introduzione della seconda caratteristica biometrica, che doveva aggiungersi all'immagine del volto. Dopo questi interventi, il Gruppo perviene, il 30 settembre 2005, al parere n. 3/2005, ove, oltre a condividere in linea di generale la posizione del Parlamento europeo, si invita allo svolgimento di un adeguato dibattito sociale prima dell'introduzione di caratteristiche biometriche nei passaporti o in altri documenti, e altresì ad una rigorosa distinzione tra dati biometrici raccolti in base ad obblighi di legge e, viceversa, quelli raccolti sulla base del consenso dell'interessato[502].

Dopo tale lungo iter di discussioni e proposte di emendamenti, viene adottato il regolamento (CE) n. 444/2009 del Parlamento Europeo e del Consiglio del 28 maggio 2009, che modifica il regolamento (CE) n. 2252/2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri[503].

---

[501] Tale ricostruzione delle prese di posizione del Gruppo, è presentata nello stesso parere n. 3/2005, si veda GRUPPO DI LAVORO ARTICOLO 29, PROTEZIONE DATI, *Parere 3/2005 riguardante l'attuazione del regolamento CE n. 2252/2004 del Consiglio, del 13 dicembre 2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli stati membri (Gazzetta ufficiale L 385 del 29.12.2004, pp. 1-6)*, cit., 5-6.

[502] *Ibidem, Conclusioni (n. 1 e n. 3)*, 12.

[503] *Regolamento (CE) N. 444/2009 del Parlamento europeo e del Consiglio del 28 maggio 2009 che modifica il regolamento (CE) n. 2252/2004 del Consiglio relativo alle norme sulle caratteristiche di*

Cambiamenti significativi sono previsti anzitutto quanto alla scelta della caratteristica biometrica da memorizzare, disponendo che "i passaporti e i documenti di viaggio hanno un supporto di memorizzazione altamente protetto che contiene un'immagine del volto. Gli Stati membri aggiungono inoltre due impronte digitali, prese a dita piatte, in formato interoperativo […]" (art. 1, par. 2).

Tuttavia, la novità più rilevante introdotta dal suddetto testo legislativo consiste nel divieto del rilevamento delle impronte digitali a minori di età inferiore ai dodici anni (art. 1, par. 2 *bis*)[504], stabilendo tuttavia che tale limite è provvisorio, e può essere modificato in base ad uno studio sull'affidabilità dell'utilizzazione a fini di identificazione e verifica delle impronte digitali dei bambini con meno di dodici anni[505].

---

sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri, in GUCE n. L 141 del 6.6.2009.

[504] La questione dei minori era già stata sollevata nella *Proposta di regolamento del Parlamento europeo e del Consiglio, che modifica il regolamento (CE) n. 2252/2004 del Consiglio relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri* presentata dalla COMMISSIONE DELLE COMUNITÀ EUROPEE il 18.10.2007, in *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0619:FIN:IT:PDF*.
In particolare, si prevedeva di esentare dall'obbligo i bambini al di sotto dei sei anni dal momento che, nei progetti pilota condotti negli Stati membri, era emerso che le impronte digitali di questi ultimi non sembravano qualitativamente sufficienti per i controlli d'identità "uno a uno". A questo si aggiungeva la considerazione che, subendo tali caratteristiche cambiamenti importanti nel tempo, era difficile controllarle per l'intero periodo di validità del passaporto.

[505] Art. 5 bis: "[…] la Commissione presenta al Parlamento europeo e al Consiglio una relazione basata su uno studio approfondito e su vasta scala, realizzato da un'autorità indipendente sotto la supervisione della Commissione, che esamina l'affidabilità e la fattibilità tecnica, anche attraverso una valutazione della precisione dei sistemi in funzione, dell'utilizzazione a fini di identificazione e verifica delle impronte digitali dei bambini di età inferiore a dodici anni, ivi compreso un confronto dei tassi di respingimento ingiustificato registrati in ciascuno Stato membro, nonché - sulla base dei risultati di tale studio - un'analisi della necessità di norme comuni per quanto riguarda il processo di comparazione. Se necessario, la relazione è corredata di proposte volte ad adeguare il presente regolamento".
Come ulteriore misura di sicurezza e per tutelare maggiormente i bambini, sarà introdotto il principio "una persona - un passaporto". I passaporti, infatti, dovranno essere rilasciati «come documenti individuali», di modo che il documento e i dati biometrici siano collegati esclusivamente al titolare. Al momento, infatti, i bambini possono figurare sul passaporto dei genitori senza che i loro dati figurino nel microchip e ciò può facilitare la tratta dei bambini, dato che è difficile effettuare controlli affidabili sull'identità del bambino. In Italia, fino a 15 anni, il minore può lasciare il paese con un certificato o estratto di nascita vidimato dal questore (cosiddetto lasciapassare). Fino a 16 anni può viaggiare con l'iscrizione sul passaporto di un genitore o di chi ne fa le veci o con il passaporto individuale. Al compimento del 16° anno, il minore dovrà avere un proprio passaporto. Per richiedere il passaporto per il figlio minore è necessario l'assenso di entrambi i genitori (coniugati, conviventi, separati o divorziati), si veda il *Comunicato stampa* del 14.01.2009, *Passaporti biometrici: niente impronte digitali per i minori di dodici anni*, in *http://www.europarl.europa.eu/news/expert/infopress_page/019-46172-012-01-03-902-20090114IPR46171-12-01-2009-2009-false/default_it.htm*.

Si permette, invero, agli Stati membri che, prima della data di entrata in vigore del regolamento, hanno adottato una legislazione che prevede un limite di età inferiore a dodici anni, di continuare ad applicare questa soglia per una fase transitoria di quattro anni, benché il limite non possa mai essere inferiore a sei anni.

Sono altresì esenti dall'obbligo le persone per le quali tale misurazione è fisicamente impossibile. In tal caso, gli Stati membri consentono il rilevamento delle impronte delle altre dita, oppure, se anche questa operazione si rivelasse non realizzabile, essi possono rilasciare un passaporto temporaneo avente una validità di 12 mesi o inferiore (art. 1, par. 2 *ter*).

In ogni caso, va tenuto ben presente il richiamo effettuato dall'art. 1 *bis*, secondo cui il rilevamento degli identificatori biometrici va effettuato "nel rispetto dei diritti stabiliti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e della Convenzione delle Nazioni Unite sui diritti del fanciullo", e assicurando che "siano predisposte procedure appropriate a garanzia della dignità della persona interessata, in caso di difficoltà nel rilevamento".

Il processo di introduzione di elementi biometrici nei passaporti non è dunque avvenuto in maniera pacifica, né sembra che la polemica sollevata possa ritenersi conclusa. In particolare, si è detto che tale iter ha rivelato la mancanza di *democratic legitimacy* nell'ambito dell'Unione, dove non si è lasciato spazio al dibattito pubblico, e soprattutto il Parlamento europeo ha potuto esercitare un limitato potere di intervento. Si teme, pertanto, che il passaporto biometrico miri a creare nuove misure di sorveglianza, rendendo visibile non solo la mancanza di legittimità democratic all'interno dell'Ue, ma altresì divenendo un esempio problematico per il prossimo futuro[506].

[506] Così G. HORNUNG, *The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards*, in 4 *SCRIPT-ed* (2007), cit., 262.

10. (*Segue*) L'Eurodac.

Altro significativo esempio di applicazione delle tecnologie biometriche in ambito europeo è dato dal sistema Eurodac, istituito in base al regolamento n. 2725/2000 del Consiglio europeo dell'11 dicembre 2000[507].

Grazie all'Eurodac, gli Stati membri possono identificare, mediante la rilevazione delle impronte digitali, tre "categorie" di persone: i richiedenti asilo, gli stranieri fermati nell'atto di attraversare irregolarmente una frontiera esterna dell'Unione europea, e gli stranieri che risiedono irregolarmente nel territorio di uno Stato membro. L'obbiettivo principale è quello di "concorrere alla determinazione dello Stato membro competente, ai sensi della convenzione di Dublino, per l'esame di una domanda di asilo presentata in uno Stato membro" (art. 1)[508], di modo che sia possibile stabilire se i richiedenti siano entrati nell'Unione privi dei documenti necessari, oppure se abbiano già richiesto asilo in un altro Stato membro. L'Eurodac, dunque, costituisce uno strumento atto a favorire l'applicazione della convenzione suddetta, mediante la rilevazione e il confronto delle impronte digitali.

Quanto al funzionamento, il sistema è costituito da una unità centrale, istituita presso la Commissione, dotata di una banca dati centrale informatizzata, gestita dalla

---

[507] In *GUCE* n. L 316/1 del 15.12.2000.

[508] Si veda, a proposito del problema del trattamento dei dati personali nell'Unione europea, P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione Europea*, cit., ove viene approfondito anche il problema della politica di asilo e del trattamento dei dati degli stranieri coinvolti, considerando la Convenzione di Dublino (pp. 298 ss.) e il regolamento "Eurodac" (pp. 310 ss.). Quanto alla Convenzione sulla determinazione dello Stato competente per l'esame di una domanda di asilo presentata in uno degli Stati membri delle Comunità europee, firmata a Dublino il 15 giugno 1990, entrata in vigore l'1 settembre 1997, essa "stabilisce i criteri per i individuare lo Stato su cui incombe l'obbligo giuridico di dar seguito alle domande di stranieri che chiedano il riconoscimento della qualifica di «rifugiato» ai sensi della Convenzione di Ginevra del 1951, e di condurle a termine; l'obbiettivo è di costituire un'area dove a ciascuno sia garantita una valutazione seria e legale delle proprie istanze, e dove le vittime di effettive violazioni dei diritti umani possano trovare accoglienza e un luogo per proseguire con dignità la propria vita" (pp. 299-300). Nel 2003 è entrato in vigore il "Regolamento Dublino II", Regolamento (CE) n. 343/2003 del Consiglio, del 18 febbraio 2003, che sostituisce le disposizioni della convenzione di Dublino del 1990 con una normativa comunitaria, in *GUCE* n. L 50/1 del 25.2.2003.

Commissione stessa “per conto degli Stati membri”, dove sono raccolte le impronte relative ai soggetti interessati (art. 3).

A seconda che lo straniero appartenga all’una o all’altra delle tre categorie individuate, i dati che lo riguardano subiranno un trattamento differenziato.

Anzitutto, se la procedura interessa un richiedente asilo di età non inferiore a 14 anni, di cui al capo II del regolamento, lo Stato membro rileva, conformemente alla prassi nazionale e nel rispetto delle convenzioni sui diritti dell’uomo, le impronte digitali di *tutte* le dita, e trasmette i dati ricavati all’unità centrale, che provvede alla registrazione nella banca dati centrale insieme ad altre informazioni personali necessarie ai fini dell’identificazione. Esse sono confrontate con quelle precedentemente trasmesse dal medesimo Stato membro, e dagli altri Stati. Tali informazioni vengono conservate per un periodo di 10 anni, e possono essere cancellate anticipatamente solo nel caso in cui il richiedente abbia ottenuto la cittadinanza di uno Stato membro prima della scadenza del termine previsto.

Per quanto riguarda gli stranieri fermati nell’atto di attraversare irregolarmente, per terra, per mare, oppure per aria, una frontiera esterna dell’Unione europea (capo III), valgono, in parte, le disposizioni suddette. Si scorgono, tuttavia, anche rilevanti differenze poiché, diversamente da quanto previsto per il caso precedente, i dati biometrici che arrivano all’unità centrale “sono registrati all’unico scopo di confrontarli con i dati relativi ai richiedenti asilo trasmessi successivamente alla stessa unità centrale” (art. 9). Questa disposizione, pertanto, vieta il confronto dei dati di chi ha varcato illegalmente la frontiera con quelli dei richiedenti asilo registrati precedentemente nel *database* ovvero con quelli di quanti verranno trovati in futuro a compiere il medesimo attraversamento illegalmente. Anche i tempi di conservazione sono differenti, essendo previsto un periodo di due anni a decorrere dal rilevamento, con

possibilità che le informazioni archiviate siano cancellate immediatamente se allo straniero viene rilasciato un permesso di soggiorno, se ha lasciato il territorio degli Stati membri, oppure se ha acquisito la cittadinanza di uno di essi.

Infine, per stabilire se gli stranieri che risiedono irregolarmente nel territorio di uno Stato membro abbiano già presentato una domanda di asilo in un altro Stato membro (capo IV), gli Stati, a differenza delle altre ipotesi, hanno la facoltà, e non l'obbligo, di rilevare e trasmettere le impronte all'unità centrale. Tali dati, inoltre, non sono salvati nel *database*: essi possono essere trasmessi all'unità esclusivamente con l'intento di verificare, raffrontandoli con i dati dei richiedenti asilo già registrati, se lo straniero abbia precedentemente fatto domanda altrove nell'Unione, né possono essere confrontati con i dati relativi a stranieri fermati mentre attraversavano irregolarmente una frontiera esterna.

Va tenuto presente, in ogni caso, che in via generale e per quanto non previsto, i trattamenti nazionali di tali dati devono avvenire sulla base delle norme nazionali attuative della direttiva n. 95/46, mentre quelli ad opera della Commissione sono soggetti al regolamento n. 45/2001.

Come accennato inizialmente, l'Eurodac non ha mancato di sollevare polemiche.

Qualcuno ha ritenuto il sistema rispettoso dei principi posti a garanzia della raccolta e del trattamento dei dati personali, in particolare di finalità limitata e di legalità, offrendo altresì "cautele e mezzi per una difesa concreta e valida del diritto alla vita privata dei singoli"[509], con "l'unica smagliatura […] che le impronte digitali del richiedente asilo, dopo che la sua domanda abbia trovato accoglimento, non vengono cancellate"[510].

---

[509] Così P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione Europea*, cit., 322.

[510] *Ibidem*, 316. Come è stato dichiarato, "la cancellazione non è effettuata sistematicamente, soprattutto perché lo Stato membro che ha inserito i dati non è informato della nuova posizione dell'interessato", *Relazione sulla valutazione del sistema di Dublino* della Commissione al Parlamento europeo e al

Tuttavia, quest'ultima non pare la sola crepa che il sistema ha mostrato di possedere[511]. Tra i maggiori problemi, sono stati evidenziati la mancanza di tempestività da parte degli Stati membri nella trasmissione dei dati all'unità centrale; il basso numero di ingressi irregolari registrati, presumibilmente dovuto al non rispetto dell'obbligo di rilevare le impronte; la stessa bassa qualità dei dati inviati all'Eurodac; infine, la non sempre corretta applicazione delle norme per il rispetto dei dati personali.

In particolare, per quanto riguarda la questione del trattamento dei dati personali biometrici nel settore dell'immigrazione, si scorgono due gravosi problemi: da una parte, il potenziale utilizzo di informazioni per finalità diverse da quelle per cui sono state raccolte, ad esempio come mezzo generale di prevenzione della criminalità; dall'altra, la creazione di un *database* contenente una grande quantità di dati potrebbe consentire ai governi di monitorare segretamente le attività degli individui[512].

Si deve rilevare, invero, che la Commissione europea stessa mostra nell'insieme un approccio positivo nei confronti del sistema in questione e del procedimento di rilevazione delle impronte digitali mirando, come futuro sviluppo, ad estendere l'obbligo di conservare le impronte anche per il caso degli stranieri che risiedono irregolarmente nel territorio, ai fini di contrastare l'immigrazione clandestina[513].

Pare in ogni caso lecita la preoccupazione che qualche attento osservatore ha manifestato nei confronti dell'Eurodac, con riferimento alla dimensione etica. In particolare, si è avvertito il pericolo della stigmatizzazione e strumentalizzazione dei

---

Consiglio, Bruxelles, 6.6.2007, COM(2007) 299 definitivo, rinvenibile in *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0597:FIN:EN:PDF*, par. 2.3.2.

[511] Si veda, a proposito di una valutazione complessiva del sistema di Dublino e in particolare dell'Eurodac, la summenzionata *Relazione sulla valutazione del sistema di Dublino* del 6.6.2007, spec. par. 2.3.2. e par. 2.3.3.

[512] Così J. REDPATH, *Biometrics and international migration*, in 43 *Ann. ist. super. sanità* (2007), 31. Si considerino inoltre, per i problemi che riguardano l'utilizzo della biometria nel settore dell'immigrazione, J. LODGE, *Freedom, security and justice: the thin end of the wedge for biometrics?*, in 43 *Ann. Ist. Super. Sanità* (2007); A. I. SCHOENHOLTZ, *Transatlantic Dialogue on Terrorism and International Migration*, in 41 *International Migration* (2003); T. PETERMANN, A. SAUTER, C. SCHERZ, *Biometrics at the Borders – the Challenges of a Political Technology*, in 20 *International Review of Law Computers* (2006).

[513] Si veda la *Relazione sulla valutazione del sistema di Dublino* del 6.6.2007, cit., par. 2.3.4. e par. 4.

soggetti coinvolti, con il rischio effettivo che "l'impronta digitale diventi il segno dell'illegalità iscritto sul corpo" [514].

11. Uno sguardo comparato. Il Regno Unito: *Identity Cards Act* e *UK Borders Act.*

Oltre alle applicazioni su vasta scala delle tecnologie biometriche nell'ambito dell'Unione europea, è interessante considerare brevemente se e in che modo la "questione biometria" sia entrata, in maniera rilevante, nel tessuto legislativo di singoli Stati.

Anzitutto, si intende esaminare il caso del Regno Unito, che rappresenta una delle aree in cui il dibattito sui sistemi biometrici appare più vitale. Il primo significativo intervento legislativo che attiene all'uso delle tecnologie biometriche in questo Paese è costituito dal *Identity Cards Act*, del 30 marzo 2006[515].

Al momento dell'entrata in vigore, tale legge suscitò un acceso dibattito, vedendo contrapporsi due schieramenti, l'uno favorevole, intravedendo soprattutto la possibilità di migliorare i servizi, di combattere il furto d'identità, di contrastare l'immigrazione illegale, di monitorare le attività criminali, di opporsi al terrorismo; l'altro, invece, contrario, alla luce soprattutto dei costi economici e sociali, in particolare derivanti dal possibile e rischioso uso non corretto dei dati personali ricavati[516].

---

[514] Così I. VAN DER PLOEG, *The illegal body: 'Eurodac' and the politics of biometric identification*, cit., 301. Nello stesso senso, A. SPROKKEREEF, P. DE HERT, *Ethical practice in the use of biometric identifiers within the EU*, in 3 *Law, Science and a Policy* (2007), spec. pp. 181 e 182; A. ALTERMAN, "*A piece of yourself": ethical issues in biometric identification*, cit., 146, ove l'a. dichiara, in riferimento all'etica kantiana, che si tratta di "*a clear case of taking the person as a mere thing, using their body as a means to an end*".

[515] La legge è rinvenibile in *http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060015_en.pdf*.

[516] Così P. BEYNON-DAVIES, *Personal identity management and electronic government. The case of the national identity card in the UK*, in 20 *Journal of Enterprise Information Management* (2007), 261 ss. Sul problema dei costi, si veda anche EUROPEAN BIOMETRICS PORTAL, EBP, *Biometrics in Europe, Trend Report 2007*, in *www.europeanbiometrics.info*, 36 ss.

Invero, sul piano storico, tale legge non rappresentò una novità assoluta, dal momento che già nel 1915 era stato emanato il *National Registration Act*, che stabiliva la registrazione obbligatoria della popolazione di Inghilterra, Galles e Scozia, compresa tra i 15 e i 65 anni, al fine di favorire la coscrizione e la politica militare durante la prima guerra mondiale. Una legge analoga era stata promulgata nel corso del secondo conflitto mondiale, e dagli anni '50 si erano succedute diverse proposte che riguardavano la creazione di una *ID card*[517].

Quanto alla legge del 2006, essa prevede, per prima cosa, l'istituzione di un registro nazionale, denominato *NIR* (*National Identity Register*), cui hanno diritto di essere registrati tutti i residenti che abbiano compiuto l'età di 16 anni, nonché ogni individuo che abbia risieduto nel Regno Unito o che sia intenzionato a farlo. Alcuni soggetti potrebbero, invero, essere privi di tale diritto sulla base delle disposizioni della medesima legge[518].

Il *database* così realizzato rappresenta il cuore della normativa, mentre la *Identity Card*, che la legge in esame regolamenta e che pure rimane centrale, ha una rilevanza secondaria, dal momento che viene eventualmente emessa solo dopo che siano stati inseriti nel *NIR* i c.d. "fatti registrabili" in relazione ad un determinato individuo[519].

---

[517] Si veda, in particolare, il dettagliato schema delle iniziative legislative presentato da P. BEYNON-DAVIES, *Personal identity management and electronic government. The case of the national identity card in the UK*, cit., 251 e, al medesimo riguardo, si veda altresì W. M. GROSSMAN, *Identifying Risks: National Identity Cards*, in 2 *SCRIPT-ed* (2005), spec. pp. 6 ss.

[518] Secondo il par. 2 (2): *The individuals entitled to be entered in the Register are — (a) every individual who has attained the age of 16 and, without being excluded under subsection (3) from an entitlement to be registered, is residing at a place in the United Kingdom; and (b) every individual of a prescribed description who has resided in the United Kingdom or who is proposing to enter the United Kingdom.*
Quanto ai soggetti esclusi, si veda il par. 2 (3): *Regulations made by the Secretary of State may provide that an individual residing in the United Kingdom is excluded from an entitlement to be registered if — (a) he is residing in the United Kingdom in exercise of an entitlement to remain there that will end less than the prescribed period after it was acquired; (b) he is an individual of a prescribed description who has not yet been resident in the United Kingdom for the prescribed period; or (c) he is residing in the United Kingdom despite having no entitlement to remain there.*

[519] Si veda, per i problemi giuridici della legge in esame, l'interessante contributo di C. SULLIVAN, *The United Kingdom Identity Cards Act 2006-Civil or Criminal?*, in 15 *International Journal of Law and Information Technology* (2007), 321. L'a., in particolare, ha riguardo alla possibile violazione dell'art. 6 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950.

Un "fatto registrabile" comprende, anzitutto, l'identità del soggetto, che è data dal nome o da altri nomi con cui è stato precedentemente conosciuto, dal genere, dal luogo e dalla data di nascita e, se deceduto, dalla data della morte, infine, dalle *caratteristiche esterne che sono suscettibili di essere utilizzate per la sua identificazione*, ossia dalle sue caratteristiche biometriche[520]. In particolare, tra le informazioni identificative rientrano una foto (della testa e delle spalle, che mostri le caratteristiche del viso), la firma, le impronte digitali, e altre caratteristiche biometriche[521]. Oltre all'identità, la legge include altri "fatti", che sono legati in modo particolare alla residenza dell'individuo[522].

Circa la rilevante questione dell'obbligatorietà o meno della registrazione all'interno del sistema identificativo nazionale e del possesso della carta d'identità così definita, la registrazione all'interno del *NIR* fino al 1 gennaio 2010 sarà obbligatoria solo per chiunque faccia domanda di un passaporto[523]. Per quanto riguarda, invece, la *ID Card*, essa sarà, in via generale, facoltativa: solo i soggetti per i quali è prevista la registrazione obbligatoria devono richiedere suddetto documento e rinnovarlo regolarmente. La legge non indica chiaramente quali siano questi soggetti, limitandosi a stabilire che si tratta di coloro i quali devono essere iscritti nel registro in accordo con un obbligo imposto da una legge del Parlamento, che sia stata approvata dopo

[520] Si veda il par. 1 (7): *In this section references to an individual's identity are references to — (a) his full name; (b) other names by which he is or has previously been known; (c) his gender; (d) his date and place of birth and, if he has died, the date of his death; and (e) external characteristics of his that are capable of being used for identifying him.*
[521] Si veda l'allegato alla legge, *Schedule 1, Information that may be recordered in register, Identifying information*.
[522] Così il par. 1 (5): *In this Act "registrable fact", in relation to an individual, means — (a) his identity; (b) the address of his principal place of residence in the United Kingdom; (c) the address of every other place in the United Kingdom or elsewhere where he has a place of residence; (d) where in the United Kingdom and elsewhere he has previously been resident; (e) the times at which he was resident at different places in the United Kingdom or elsewhere; (f) his current residential status; (g) residential statuses previously held by him; (h) information about numbers allocated to him for identification purposes and about the documents to which they relate; (i) information about occasions on which information recorded about him in the Register has been provided to any person; and (j) information recorded in the Register at his request.*
[523] Così C. SULLIVAN, *The United Kingdom Identity Cards Act 2006-Civil or Criminal?*, cit., 321.

l'approvazione della legge in esame, dunque presumibilmente persone che siano già sospettate di essere coinvolte in attività criminose[524]. Non è chiaro altresì quale sarà l'orientamento dopo l'1 gennaio 2010, anche se si prevede diventerà con il tempo obbligatorio per tutti i residenti di età superiore ai 16 anni essere iscritti al *NIR* e possedere una *ID card*[525].

La legge prevede inoltre sanzioni civili per le contravvenzioni che si verifichino principalmente in tre ambiti[526]: l'ambito delle registrazioni obbligatorie, in caso di una omissione nel richiedere la carta d'identità, se il soggetto è tenuto a farlo[527]; l'ambito delle notificazioni dei cambiamenti, se non vengono segnalate modifiche ed errori che sono relativi alla accuratezza del *NIR*[528]; infine, l'ambito di validità e di rinuncia della carta d'identità, per il non rispetto dei requisiti stabiliti ai fini dell'impiego della stessa[529]. A questo proposito, nel Regno Unito si è dibattuto, arrivando tuttavia a conclusioni incerte[530], se l'*Identity Cards Act* sia rispettoso del principio di non discriminazione, e segnatamente dell'art. 6 della *Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali* del 1950, che concerne il

[524] Si veda il par. 42 (1).
[525] Ancora, C. SULLIVAN, *The United Kingdom Identity Cards Act 2006-Civil or Criminal?*, cit., 321, ove si precisa che il governo inglese intende fare di questo sistema di identificazione nazionale il "*gold standard of identity verification*". Nello stesso senso, si è espresso anche lo EUROPEAN BIOMETRICS PORTAL, EBP, *Biometrics in Europe, Trend Report 2007*, cit., 37.
[526] L'ammontare delle sanzioni, di natura pecuniaria, viene stabilito dal Segretario di Stato, si veda il par. 31 (2).
[527] Si veda il par. 7.
[528] Si veda il par. 10.
[529] Si veda il par. 11. Ci si riferisce, in particolare, alle omissioni nella notifica della perdita, del furto, del danno, della falsificazione o della distruzione della carta d'identità, ovvero ai casi in cui un soggetto sia consapevolmente in possesso di una *ID card* senza avere tuttavia i requisiti necessari, come, per esempio, l'autorizzazione del Segretario di Stato. In questo caso si prevede la consegna del documento all'autorità di riferimento (par. 11 (3), (4)).
[530] Così C. SULLIVAN, *The United Kingdom Identity Cards Act 2006-Civil or Criminal?*, cit., 356, ove si sostiene che la risposta all'interrogativo se un individuo, costretto a registrarsi, possa invocare il diritto di non discriminazione sancito dall'art. 6, dipende dalle circostanze.

diritto a un equo processo, con particolare riferimento al principio della presunzione di innocenza[531].

Il secondo importante intervento legislativo nel Regno Unito in tema di biometria è costituito dal *UK Borders Act* del 30 ottobre 2007, una legge che stabilisce provvedimenti in tema di immigrazione e asilo[532].

In particolare, un'intera parte della legge è dedicata alla *Biometric registration* prevedendo, anzitutto, che il Segretario di Stato possa disporre che una persona soggetta a un controllo di immigrazione faccia domanda per il rilascio di un documento contenente le informazioni biometriche ("*biometric immigration document*")[533]. A questo proposito, la legge precisa che per "persona soggetta a un controllo di immigrazione" si intende una persona che, secondo quanto stabilito dall'*Immigration Act* del 1971, richiede il permesso di entrare o rimanere nel Regno Unito, mentre per "informazione biometrica" si intende un'informazione sulle caratteristiche fisiche esterne di una persona, includendo in particolare le impronte digitali e le caratteristiche dell'iride oppure di un'altra parte dell'occhio[534]. In secondo luogo, che tale documento

[531] Art. 6 - Diritto a un equo processo - 1. Ogni persona ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un tribunale indipendente e imparziale, costituito per legge, il quale sia chiamato a pronunciarsi sulle controversie sui suoi diritti e doveri di carattere civile o sulla fondatezza di ogni accusa penale formulata nei suoi confronti. La sentenza deve essere resa pubblicamente, ma l'accesso alla sala d'udienza può essere vietato alla stampa e al pubblico durante tutto o parte del processo nell'interesse della morale, dell'ordine pubblico o della sicurezza nazionale in una società democratica, quando lo esigono gli interessi dei minori o la protezione della vita privata delle parti in causa, o, nella misura giudicata strettamente necessaria dal tribunale, quando in circostanze speciali la pubblicità possa portare pregiudizio agli interessi della giustizia. 2. Ogni persona accusata di un reato è presunta innocente fino a quando la sua colpevolezza non sia stata legalmente accertata. 3. In particolare, ogni accusato ha diritto di: a. essere informato, nel più breve tempo possibile, in una lingua a lui comprensibile e in modo dettagliato, della natura e dei motivi dell'accusa formulata a suo carico; b. disporre del tempo e delle facilitazioni necessarie a preparare la sua difesa; c. difendersi personalmente o avere l'assistenza di un difensore di sua scelta e, se non ha i mezzi per retribuire un difensore, poter essere assistito gratuitamente da un avvocato d'ufficio, quando lo esigono gli interessi della giustizia; d. esaminare o far esaminare i testimoni a carico ed ottenere la convocazione e l'esame dei testimoni a discarico nelle stesse condizioni dei testimoni a carico; e. farsi assistere gratuitamente da un interprete se non comprende o non parla la lingua usata in udienza.
[532] La legge è rinvenibile in *http://www.opsi.gov.uk/si/si2009/em/uksiem_20090819_en.pdf.*
[533] Così il par. 5 (1) (a).
[534] Par. 15 (1).

sia utilizzato per scopi specifici e in circostanze prestabilite[535]. Infine, che la persona che esibisce un *biometric immigration document* fornisca anche le informazioni utili al fine di effettuare un confronto con le informazioni date in relazione alla presentazione della domanda per il documento.

La legge stabilisce che le disposizioni suddette possano, tra le diverse ipotesi previste, essere applicate in via generale oppure solo ad una specifica classe di persone soggette a controlli di immigrazione; specificare il periodo in cui debba essere fatta la domanda di un documento; disporre riguardo all'emissione del documento, e al contenuto stesso, poiché potrebbe anche non includere dati biometrici; stabilire che un *biometric immigration document* possa essere utilizzato congiuntamente ad un altro documento[536]. In specifici casi, previsti dalla legge, il Segretario di Stato potrebbe altresì annullare il documento in esame[537].

Altra importante disposizione della legge è quella che concerne l'utilizzo e la conservazione delle informazioni biometriche. Potrebbero, infatti, essere previste ipotesi in cui sia possibile utilizzare tali dati, in modo particolare per garantire la sicurezza nazionale, in relazione all'attività di controllo delle frontiere, oppure nell'ambito di

[535] Così il par. 5 (1) (b): *[The Secretary of State may make regulations…] — requiring a biometric immigration document to be used— (i) for specified immigration purposes, (ii) in connection with specified immigration procedures, or (iii) in specified circumstances, where a question arises about a person's status in relation to nationality or immigration.*

[536] Si veda il par. 5 (2): *Regulations under subsection (1) (a) may, in particular — (a) apply generally or only to a specified class of persons subject to immigration control (for example, persons making or seeking to make a specified kind of application for immigration purposes); (b) specify the period within which an application for a biometric immigration document must be made; (c) make provision about the issue of biometric immigration documents; (d) make provision about the content of biometric immigration documents (which may include non-biometric information); (e) make provision permitting a biometric immigration document to be combined with another document; (f) make provision for biometric immigration documents to begin to have effect, and cease to have effect, in accordance with the regulations; (g) require a person who acquires a biometric immigration document, without the consent of the person to whom it relates or of the Secretary of State, to surrender it to the Secretary of State as soon as is reasonably practicable; (h) permit the Secretary of State to require the surrender of a biometric immigration document in other specified circumstances; (i) permit the Secretary of State on issuing a biometric immigration document to require the surrender of other documents connected with immigration or nationality.*

[537] Si veda il par. 5 (3), che elenca molte ipotesi tra cui si ricordano, per esempio, il caso in cui il Segretario di Stato ritiene che il documento sia falso, incompleto oppure sia stato perso o rubato, o ancora, sia stato alterato, danneggiato o distrutto, ecc.

attività processuali. È altresì possibile che il Segretario di Stato disponga la distruzione di tali dati[538].

Infine, la legge prevede sanzioni in caso di contravvenzioni[539].

12. (*Segue*) La Francia e l'attività del CNIL.

Risulta interessante indagare, seppur per linee generali, l'orientamento di un'altra nazione europea rispetto alla biometria, la Francia. Di primo acchito, si riscontrano numerose analogie tra l'approccio al trattamento ai dati biometrici adottato da questo Paese e l'Italia.

Anzitutto, è opportuno precisare che la base legislativa per il trattamento dei dati personali, e dunque anche biometrici, in Francia, è la legge n. 17 del 6 gennaio 1978 ("*Loi relative à l'informatique, aux fichiers et aux libertés*"), modificata dalla legge n. 801 del 6 agosto 2004, "*relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*". Invero, già la legge del '78 conteneva riferimenti ai dati biometrici, stabilendo la necessità dell'autorizzazione della CNIL (*Commission Nationale de l'Informatique et des Libertés*), corrispondente in sostanza all'Autorità italiana Garante per la protezione dei dati personali, per "*les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes*" (art. 25, I, 8°) e del Consiglio di Stato, per "*les traitements de données à caractère personnel mis en oeuvre pour le compte de l'Etat qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes*" (art. 27, I, 2°).

[538] Così il par. 8.
[539] Par. 9 ss.

L'attività della CNIL è stata negli anni copiosa, similmente a quanto si è verificato nel nostro Paese per opera della corrispondente Autorità Garante, così come dimostra il gran numero di delibere prese, risoltesi sovente con il riconoscimento del diritto al trattamento dei dati biometrici da parte di quanti si appellavano all'autorità suddetta, altre, invece, con un chiaro diniego.

Passando in rassegna solo alcune tra le molte decisioni prese, è possibile verificare più direttamente il percorso e gli orientamenti della CNIL, e prendere atto della varietà di situazioni in cui i sistemi biometrici sono stati impiegati in Francia.

Già a partire dalla fine degli anni '90, si rivengono pronunce a questo proposito. Il provvedimento "*Banque de France*" del 10 giugno 1997, relativo all'accesso ad aree particolarmente critiche di un istituto bancario per mezzo di dispositivo di verifica dell'impronta digitale, si conclude con il *placet* dell'Autorità francese all'utilizzo di questi sistemi[540].

La stessa propensione favorevole, talora accompagnata da qualche riserva, si rinviene in altre decisioni.

Il 16 novembre del 2000 la Commissione si pronuncia sulla domanda, perpetrata dal Ministro dell'Istruzione francese, di istallare un sistema di rilevazione delle impronte digitali rivolto a parte del personale universitario per l'accesso ad alcuni locali dell'Università di Lille, al fine di controllare che coloro che accedono siano realmente abilitati, garantendo così la confidenzialità dei dati conservati, soprattutto quelli relativi ad esami e concorsi[541]. La rilevazione viene ritenuta pertanto dall'ente francese

[540] Si veda CNIL, *Délibération n°97-044 du 10 juin 1997, Délibération portant avis sur un projet d'arrêté présenté par la Banque de France concernant un traitement automatisé d'informations nominatives ayant pour finalité la gestion des contrôles d'accès des agents par empreintes digitales,* in *http://www.legifrance.gouv.fr*.

[541] CNIL, *Délibération n°00-056 du 16 novembre 2000, Délibération portant avis sur un projet d'arrêté présenté par le ministre de l'éducation nationale concernant un traitement automatisé d'informations nominatives ayant pour finalité le contrôle d'accès par la reconnaissance des empreintes digitales de certains personnels de l'éducation nationale, pour certains locaux de la cité académique de Lille,* in *http://www.legifrance.gouv.fr.*

proporzionata rispetto alle finalità perseguite, dal momento che "*certains impératifs spécifiques de sécurité, tels que la confidentialité des examens et concours, sont de nature à justifier le recours à un tel système dès lors qu'il serait limité à certains locaux déterminés et adapté à la nécessité d'authentifier ceux des membres du personnel habilités à y accéder "*.

Un altro caso di poco successivo ha come protagonista il celebre museo parigino del Louvre[542], che si rivolge alla Commissione per installare un sistema biometrico di rilevazione della geometria della mano, al fine di controllare l'orario di lavoro dei dipendenti e garantire la sicurezza delle opere d'arte. L'Autorità francese accoglie la richiesta, ritenendo i dati e i loro tempi di conservazione pertinenti e non eccedenti rispetto alle finalità del trattamento. La Commissione reputa altresì che il trattamento in questione sia proporzionato rispetto allo scopo perseguito, dal momento che il dato biometrico in questione si rivela "*difficilement susceptible d'être utilisé à des fins étrangères à la finalité recherchée par le responsable du traitement*", permettendo così "*de s'assurer que les données nécessaires au contrôle de l'accès ne sont ni perdues, ni falsifiées, ni échangées, que seules les personnes habilités peuvent pénétrer dans les locaux protégés et présente ainsi un degré de fiabilité*".

Ricorrendo ad analoga motivazione, trattandosi sempre del rilevamento della geometria della mano, l'Autorità francese ammette in più occasioni l'uso di tali sistemi,

[542] CNIL, *Délibération n°01-006 du 25 janvier 2001, Délibération portant avis sur un projet de décision présenté par l'établissement public du Musée du Louvre concernant un traitement de contrôle des accès et des horaires de certains personnels par la reconnaissance du contour de la main,* in *http://www.legifrance.gouv.fr.*

come è avvenuto, per esempio, in una mensa scolastica[543] oppure in un centro ospedaliero, per il controllo dell'orario d'entrata e di uscita del personale[544].

Si osserva che, oltre all'impronta digitale e alla geometria della mano, altro tipo di dato biometrico utilizzato sovente in Francia per il riconoscimento delle persone è l'immagine del reticolato delle vene delle dita della mano[545].

In altre occasioni, la CNIL si è invece pronunciata contro l'istallazione di sistemi biometrici, appellandosi sempre al fondamentale principio di proporzionalità.

Un primo esempio di diniego riguarda una Prefettura francese intenzionata a verificare gli orari di lavoro degli agenti territoriali mediante un sistema di verifica dell'impronta digitale, con il ricorso ad un *badge* d'accesso[546]. Per la Commissione, tale obbiettivo "*ne paraît pas de nature à justifier la constitution d'une base de données d'empreintes digitales des personnels d'une préfecture. Aussi, le traitement pris dans*

---

[543] CNIL, *Délibération n°02-070 du 15 octobre 2002, Délibération portant avis sur le traitement automatisé d'informations nominatives, mis en oeuvre par le collège Joliot Curie de Carqueiranne, destiné à contrôler l'accès au restaurant scolaire par la reconnaissance de la géométrie de la main,* in *http://www.legifrance.gouv.fr*.

[544] CNIL, *Délibération n°2005-135 du 14 juin 2005, Délibération autorisant la mise en oeuvre par le Centre hospitalier de Hyères d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires de ses employés*, in *http://www.legifrance.gouv.fr*. Si vedano, a questo proposito, anche la *Délibération n°2005-135 du 14 juin 2005, Délibération autorisant la mise en oeuvre par le Centre hospitalier de Hyères d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires de ses employés* e la *Délibération n°2006-098 du 06 avril 2006, Délibération portant autorisation de la mise en oeuvre par la société Carrefour d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle de l'accès à certains locaux.*

[545] Così CNIL, *Délibération n°2009-229 du 7 mai 2009 autorisant la mise en œuvre par la société NORD ORTHOPEDIE d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux (autorisation n°1336959*); *Délibération n°2009-193 du 26 mars 2009 autorisant la mise en œuvre par l'Institut des Neurosciences de Grenoble d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux (autorisation n°1338959)* ; *Délibération n°2009-230 du 7 mai 2009 autorisant la mise en œuvre par le CENTRE HOSPITALIER JULES LESCARDE d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux (autorisation n°1338580)* in *http://www.legifrance.gouv.fr*.

[546] CNIL, *Délibération n°00-057 du 16 novembre 2000, Délibération portant avis sur un projet d'arrêté présenté par le préfet de l'Hérault concernant un traitement automatisé d'informations nominatives ayant pour finalité la gestion du temps de travail des agents de la préfecture*, in *http://www.legifrance.gouv.fr*.

son ensemble n'apparaît-il ni adapté ni proportionné à l'objectif poursuivi". L'Autorità rileva, infatti, che le impronte digitali "*font de surcroît partie des données biométriques qui laissent des traces pouvant être exploitées à des fins d'identification des personnes à partir des objets les plus divers que l'on a pu toucher ou avoir en main et dès lors, la constitution d'une base de données d'empreintes digitales est susceptible d'être utilisée à des fins étrangères à la finalité recherchée par sa création*".

Un'altra richiesta di installazione di un sistema di rilevazione delle impronte digitali proviene dalla società *Rothschild Gestion*[547], ente specializzato nella gestione di portafogli, che intende ricorrere a tale dispositivo per rendere sicuro l'accesso alle sale in cui si trovano le apparecchiature informatiche e telefoniche. La Commissione rigetta la domanda, sottolineando in particolare che la creazione di una banca dati delle impronte digitali può comportare rischi per le libertà individuali, pertanto essa è lecita solo laddove particolari esigenze di sicurezza lo richiedano. La CNIL conclude, pertanto, che il trattamento in esame si rivela ancora una volta "*ni adapté ni proportionné à l'objectif poursuivi*".

Si riporta, infine, il caso di un rifiuto di una autorizzazione nei riguardi di una clinica intenzionata a controllare l'orario di lavoro degli impiegati ove, ancora una volta, si conclude : "*La Commission estime en conséquence que la constitution de bases de données d'empreintes digitales, compte tenu des caractéristiques de l'élément d'identification physique retenu et des usages possibles de ces bases de données, ne peut être admise que dans certaines circonstances particulières où l'exigence de sécurité et*

[547] CNIL, *Délibération n°2006-156 du 30 mai 2006, Délibération portant refus d'autorisation de la mise en oeuvre par la société Rothschild Gestion d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux locaux*, in *http://www.legifrance.gouv.fr*. Conclusioni analoghe a quelle dei casi precedenti si trovano nella decisione del CNIL, *Délibération n°2006-157 du 30 mai 2006, Délibération portant refus d'autorisation de la mise en oeuvre par la société Murano Urban Resort d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux chambres de l'hôtel.*

d'identification des personnes est impérieuse. Or, en l'espèce, l'objectif invoqué d'une meilleure gestion des temps de travail, s'il est légitime, ne paraît pas, en lui-même, de nature à justifier l'enregistrement dans un lecteur biométrique des gabarits des empreintes digitales des employés. En conséquence, le traitement pris dans son ensemble n'apparaît ni adapté ni proportionné à l'objectif poursuivi"[548].

La biometria in Francia, dunque, trova applicazione in un'ampia varietà di contesti. In via generale, la *Commission Nationale de l'Informatique et des Libertés* ha emanato alcune autorizzazioni uniche, relative all'una o all'altra tipologia di rilevazione biometrica. Tali documenti toccano i punti salienti sul trattamento dei dati personali: dal problema della finalità, a quello della identificazione della categoria dei dati personali trattati, dalla questione dei destinatari delle informazioni, a quella della conservazione dei dati, dalla libertà di circolazione delle persone coinvolte, alle misure di sicurezza, dal problema dell'informazione, ai diritti di accesso e rettificazione.

Si ricordano, a questo riguardo, le due autorizzazioni generali che riguardano il trattamento della geometria della mano[549] e una autorizzazione relativa invece alla rilevazione delle impronte digitali[550]. L'ultima, in ordine temporale, è la *Délibération n°2009-316 du 7 mai 2009 portant autorisation unique de mise en œuvre de dispositifs*

---

[548] CNIL, *Délibération n°2006-005 du 12 janvier 2006, Délibération portant refus d'autorisation de la mise en oeuvre par la clinique de Goussonville d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle des horaires des employés,* in *http://www.legifrance.gouv.fr*.

[549] Si vedano *Autorisation unique n°AU-009 - Délibération n°2006-103 du 27 avril 2006 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main etayant pour finalité l'accès au restaurant scolaire,* in *http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/103/#* e *Autorisation unique n°AU-007 - Délibération n°2006-101 du 27 avril 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail,* in *http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/105/#*.

[550] CNIL, *Autorisation unique n°AU-008 - Délibération n°2006-102 du 27 avril 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail,* in *http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/104/#*.

biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail, che riguarda il riconoscimento del personale, mediante la rilevazione del tracciato delle vene delle dita della mano, al fine di controllare l'accesso nei luoghi di lavoro[551]. Passando in rassegna alcune tra le principali disposizioni, anzitutto, si stabilisce che verrà registrato, all'interno di un supporto individuale in possesso dell'interessato, non il dato biometrico grezzo, ossia l'immagine, bensì la sua traduzione in un modello (art. 1). Quanto ai tempi di conservazione delle informazioni, si prevede che vengano salvate per l'arco di tempo in cui sarà prevista la limitazione della circolazione, stabilendo altresì che il periodo massimo sia di cinque anni (art. 4). Si dispone, inoltre, che il responsabile del trattamento adotti tutte le misure necessarie per garantire la sicurezza dei dati, in particolare mediante l'uso di algoritmi crittografici (art. 6), che fornisca agli interessati le informazioni necessarie (art. 7), e altresì garantisca il diritto di accesso e di rettifica (art. 8).

[551] L'autorizzazione è reperibile al sito *http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/205/#.*

CONCLUSIONI

A conclusione di questa ricerca, si avverte come il mondo della biometria non sia un mondo immaginario, dipinto in qualche romanzo di fantascienza, oppure in qualche rappresentazione cinematografica avveniristica, che fa ampio uso di effetti speciali. Si deve ammettere, diversamente, che la biometria è entrata a far parte della vita quotidiana di milioni di persone, le quali sempre più paiono destinate a confrontarsi con questa tecnologia, con le promesse di cui si fa portatrice, ma anche con i limiti e le contraddizioni che reca inevitabilmente con sé.

Si è visto, infatti, che nel nostro Paese i dispositivi di riconoscimento biometrico sono sovente utilizzati all'ingresso di istituti di credito, presso aree particolari di aziende, in siti archeologici e in ospedali. In Europa, le tecniche biometriche sono ampiamente impiegata nelle politiche di immigrazione e asilo e, ancora, sono utilizzate come metodo di riconoscimento nell'ambito del trasporto aereo. Nel Regno Unito si è potuto osservare che alcune leggi hanno espressamente previsto l'utilizzo dei sistemi di riconoscimento in questione, mentre in Francia vi è un ricorso alla biometria su vasta scala, come, per esempio, all'interno di istituti di credito, istituti scolastici, luoghi di lavoro e musei.

Invero, nonostante questa vasta e capillare diffusione, si è costretti ad ammettere che la biometria rimane un fenomeno per lo più sottaciuto, tanto a livello del vasto pubblico di utenti che ne fa, più o meno consapevolmente, utilizzo, e degli addetti ai lavori, quanto tra gli esperti delle diverse discipline di cui essa può costituire oggetto di studio e di interesse. Le conclusioni a cui si è pervenuti, pertanto, sono il punto di arrivo

di un complesso percorso di studio, ma pure una base di partenza per le questioni che permangono, allo stato attuale, dubbie, attendendo nuove indagini e nuovi sviluppi.

Si può osservare, in prima battuta, che le tecnologie considerate esercitano un impatto rilevante sul corpo umano, dal momento che il soggetto consente all'utilizzo di parti del proprio corpo a fini identificativi. Questo impatto coinvolge, anzitutto, il corpo quale entità biologica, ossia l'uomo come *bios*, benché in genere tali tecnologie non possano considerarsi invasive della sfera corporea nel senso tradizionale del termine. In misura maggiore esso riguarda, invero, il c.d. corpo elettronico. Infatti, a partire dalla ricostruzione di alcuni diritti fondamentali della persona nel contesto dell'attuale progresso tecnologico, quali in particolare il diritto all'identità personale e il diritto all'integrità, è emerso come si vada delineando, accanto alla nozione tradizionale di corpo umano, anche questa nuova dimensione della corporeità, elettronica appunto. La persona umana, in altri termini, si colloca sempre più nel mondo anche come flusso di dati e di informazioni. Non solo il corpo fisico, dunque, ma altresì il corpo elettronico, e segnatamente il corpo come *password* disegnato dalle tecnologie biometriche, invoca un'attenta tutela, che abbia riguardo anche all'identità e all'integrità di tale "nuovo corpo".

La soluzione giuridica offerta ai problemi posti da tali nuove tecnologie può rivelarsi dunque insufficiente, se la questione del trattamento dei dati biometrici non viene affrontata alla radice, ossia a partire dal corpo biologico stesso, e dalla relazione che intercorre tra il dato biometrico e la fonte da cui è ricavato. La leggerezza con cui si è talora deciso di ricorrere a questo tipo di strumentazione, testimonia che non si è ancora diffusa la percezione che le tecnologie biometriche possano condurre ad una sempre maggiore strumentalizzazione del corpo umano, e della persona[552]. Esemplare

[552] Si veda, per esempio, il significativo caso della rilevazione delle impronte digitali effettuata da parte del Consiglio dell'Ordine degli Avvocati di Santa Maria Capua Vetere per verificare le presenze dei

l'approccio adottato in Francia dal noto *Comité Consultatif National d'Ethique pour les Sciences de la Vie et de la Santé* (CCNE), che, nel più volte citato documento *Biométrie, données identifiantes et droits de l'homme*, ha colto il nocciolo del problema, chiedendosi se i dati biometrici possano portare a una «*instrumentalisation du corps et en quelque sorte à une déshumanisation, en réduisant une personne à quelques mesures biométriques*»[553].

La stessa attenzione, invero, si desume in Italia dai pronunciamenti e dagli interventi del Garante per la protezione dei dati personali, che ha invitato a un uso limitato degli strumenti di rilevazione biometrica, proponendo di far ricorso, se non strettamente necessario, a mezzi alternativi di identificazione e riconoscimento, "meno invasivi della sfera personale, della libertà individuale e che non coinvolgono il corpo […]"[554], sussistendo una "inderogabile esigenza di rispettare il corpo umano"[555], in nome soprattutto del principio della dignità. L'Autorità italiana, dunque, ha inteso mettere in luce la relazione che intercorre tra corpo biologico e biometria, mostrando come essa vada assunta fin dall'inizio, a fronte dell'istallazione di qualunque sistema di rilevazione di dati biometrici.

Il percorso seguito nel presente lavoro, che parte dal *corpus* per giungere al *datum*, ha rivelato, inoltre, come il problema del trattamento dei dati biometrici si ponga solo in seconda battuta, e come tali dati vadano riguardati sotto una luce di specialità. A questo proposito, ci si è imbattuti in una grande varietà di dati e di

---

praticanti ai corsi di formazione forense. In questa circostanza, il Garante vietò il trattamento dei dati biometrici, essendo possibile l'adozione di sistemi alternativi di controllo, maggiormente proporzionati rispetto allo scopo perseguito, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento del 23 gennaio 2008*, doc. web n. 1487903, cit.

[553] COMITÉ CONSULTATIF NATIONAL D'ETHIQUE POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ, CCNE, Avis n° 98, *Biométrie, données identifiantes et droits de l'homme*, I – *Une approche transformée de l'identité de l'homme*, 26 avril 2007, cit., p. 6.

[554] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Compiti del Garante - Uso delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro - 21 luglio 2005*, doc. web n. 1150679, cit.

[555] Si veda GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Il decalogo su corpo e privacy*, Comunicato stampa - 09 maggio 2006, cit.

applicazioni. Ciò impone notevole attenzione, sia da parte del legislatore, sia da parte di quanti sono chiamati a decidere della liceità o meno nell'utilizzo dei sistemi in esame. Non si può, in altri termini, generalizzare, creando un'unica categoria indistinta di dati biometrici. Il riduzionismo, in questo ambito così come, sovente, in altri, impedirebbe una onesta valutazione, e ad un tempo ostacolerebbe l'opportunità che questa tecnologia offre, se ben utilizzata e nei tempi e luoghi opportuni, di svolgere un servizio per l'uomo. È da perseguire, dunque, una strada che distingua un dato biometrico da un altro, un'applicazione da un'applicazione differente, evitando scorciatoie, poiché la specificità di ogni dato e degli ambiti di impiego impone soluzioni giuridiche differenziate. Tale è stato l'orientamento seguito dall'Autorità italiana Garante per la protezione dei dati personali, le cui decisioni si sono rivelate frutto di valutazioni accurate, sempre condotte sulla base dei principi generali sul trattamento dei dati personali, e che hanno permesso di stabilire, di volta in volta, se un determinato trattamento era ammissibile o meno.

In sintesi, dunque, sono due le fondamentali acquisizioni a cui si è pervenuti. La prima, è ben espressa dalle parole di Stefano Rodotà: "L'unità della persona può essere ricostruita solo estendendo al corpo elettronico il sistema di garanzie costruito per il corpo fisico"[556]. La seconda, alla luce della giurisprudenza del Garante, è la centralità dei principi generali sul trattamento dei dati personali, che hanno consentito di dirimere molte questioni, soppesando e bilanciando interessi e situazioni contrapposte.

[556] S. RODOTÀ, *Trasformazioni del corpo,* cit., 22.

BIBLIOGRAFIA

AA. VV., *Migliorare la sicurezza informatica,* in *Le Scienze*, novembre 2008, n. 483, 108-111.

AA.VV., *Diritti, nuove tecnologie, trasformazioni sociali. Scritti in memoria di Paolo Barile,* Padova, Cedam, 2003.

ACUÑA ROZO E., *Habeas Data costituzionale: nuova garanzia giurisdizionale del diritto pubblico latinoamericano,* in *Dir. pub. comp. ed eur.*, 2002, IV, 1921-1945.

ACUÑA ROZO E., voce «Habeas corpus (America Latina)», nel *Digesto IV ed., Disc. pen.,* Aggiornamento I, Utet, 2005, 669-706.

AGOSTINI A., *Biometria e privacy: i presunti nemici a confronto,* Bologna, edis, 2006.

ALPA G., ANSALDO A., *Le persone fisiche,* in *Commentario Schlesinger*, Giuffrè, *sub* artt. 1-10, 1996, 247-271.

ALPA G., *Identità e discriminazioni*, in *Nuova giur. civ. comm*., suppl. fasc. 4/2007, 33-35.

ALTERMAN A., *"A piece of yourself": ethical issues in biometric identification*, in 5 *Ethics and Information Technology* (2003), 139-150.

AMATO S., *Diritto e corpo: il soggetto «incarnato»*, in *Dem. e dir.*, 1988, 63-89.

ASSOSECURITY, *La gestione dell'identità digitale*, 2006.

ATELLI M., MAZZEO M., *Le definizioni del Codice dei dati personali*, in CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *Il Codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 29-49.

AZZONI G., *L'arbitrarietà del corpo umano,* in D'AGOSTINO F. (a cura di), *Corpo esibito, corpo violato, corpo venduto, corpo donato. Nuove forme di rilevanza giuridica del corpo umano,* Milano, Giuffrè, 2003, 57-99.

BACK IMPALLOMENI E., *I riflessi del Nuovo Ordine Economico Internazionale sul processo evolutivo del diritto spaziale,* in *Aspetti e problemi del Nuovo Ordine Economico Internazionale,* Padova, Cedam, 1987, 25-38.

BACK IMPALLOMENI E., *Il concetto di patrimonio comune dell'umanità applicato ai corpi celesti,* in *Spazio cosmico e corpi celesti nell'ordinamento internazionale*, Padova, Cedam, 1983, 57-82.

BACK IMPALLOMENI E., *Sfruttamento delle risorse della luna e patrimonio comune dell'umanità,* in CATALANO SGROSSO G. (a cura di), *Diritto dello spazio - Recenti sviluppi e prospettive,* Padova, Cedam, 1994, 225-235.

BACK IMPALLOMENI E., *Il concetto di res communis omnium applicato allo spazio e ai corpi celesti,* in *Spazio cosmico e corpi celesti nell'ordinamento internazionale,* Padova, Cedam, 1983.

BARGELLI E., Commento art. 7, in BIANCA C. M., BUSNELLI F. D. (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»),* I, Padova, Cedam, 2007, 130-141.

BARTOLOMMEI S., *Corpo e cura di sé alla fine della vita: sulle "dichiarazioni anticipate di trattamento",* in *L'Arco di Giano,* 2005, n. 44, 111-127.

BASSOLI E., *Regole ulteriori per privato ed enti pubblici economici,* in CASSANO G., FADDA S. (a cura di), *Codice in materia di protezione dei dati personali,* Milano, Ipsoa, 2004, 162 ss.

BAUD J. P., *Il caso della mano rubata. Una storia giuridica del corpo,* Milano, Giuffrè, 2003.

BAVETTA V., voce «Identità (diritto alla)», in *Enc. del dir.*, XIX, Giuffrè, 1970, 953-957.

BAYNE T., LEVY N., *Amputees by Choice: Body Integrity Identity Disorder and the Ethics of Amputation,* in 22 *J. Appl. Philos.* (2005), 75-86.

BELLAVISTA A., *Quale legge per le banche dati?,* in *Riv. crit. dir. priv.*, 1991, 677-738.

BELLELLI A., *Aspetti civilistici della sperimentazione umana,* Padova, Cedam, 1983.

BERLINGUER G., *Il corpo come merce o come valore,* in RODOTÀ S. (a cura di), *Questioni di bioetica,* Roma, Laterza, 1993, 74-99.

BERNARDI S., Commento art. 17, in BIANCA C. M.,. BUSNELLI F. D. (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»),* I, Padova, Cedam, 2007, 450-455.

BEWLEY-TAYLOR D. R., *US concept wars, civil liberties and the technologies of fortification,* in 43 *Crime, Law & Social Change* (2005), 81-111.

BEYNON-DAVIES P., *Personal identity management and electronic government. The case of the national identity card in the UK*, in 20 *Journal of Enterprise Information Management* (2007), 244-270.

BIANCA C. M., BUSNELLI F. D. (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, I, Padova, Cedam, 2007.

BIANCA C. M., F. D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, II, Padova, Cedam, 2007.

BIANCHI E., *Corpo da rispettare anche nell'indegnità*, in *Avvenire*, sezione "Agorà", 23 settembre 2007, 4-5.

BIASIOTTI A., *Le tecnologie biometriche. Sicurezza, contrattualistica, privacy*, Roma, EPC LIBRI, 2002.

BIFULCO R., *Dignità umana e integrità genetica nella Carta dei diritti fondamentali dell'Unione Europea*, in *Bioetica*, 2003, 443-478.

BISI S., *Il corpo come password: alcune considerazioni in tema di sistemi di autenticazione biometrica*, in *Ciberspazio e diritto*, 2005, 3-35.

BISI S., *Il furto d'identità: panoramica attuale e prospettive giuridiche*, in *Ciberspazio e diritto*, 2004, 303-336.

BOCCHI L., *Libertà personale e visita di leva: il rilevamento dattiloscopico*, in *Riv. trim. dir. pubbl.*, 1992, 134-157.

BOMPIANI A., *La clonazione: considerazioni sulle normative internazionali*, in *Medicina e Morale*, 1998, 581-599.

BONACCHI G., *Corpi di donna e scritture dell'uomo: spunti storici*, in *Democrazia e diritto*, n. 1, 1996, 3-20.

BOZZI L., *Le regole generali per il trattamento dei dati*, in CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *Il Codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 83-106.

BUTTARELLI G., Commento art. 3, in BIANCA C. M., BUSNELLI F. D. (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, I, Padova, Cedam, 2007, 32-40.

BUTTARELLI G., *Profili generali del trattamento dei dati personali*, in G. SANTANIELLO (a cura di), *La protezione dei dati personali*, nel *Trattato di diritto amministrativo*, diretto da G. SANTANIELLO, XXXVI, Cedam, 2005, 61-92.

CACACE S., Commento art. 81, in BIANCA C. M., F. D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, II, Padova, Cedam, 2007, 1262-1267.

CACACE S., *Il consenso informato del paziente al trattamento sanitario*, in *Danno e resp.*, 2007, 283-290.

CALÒ E., *Sulla libertà del consenso informato*, in *Riv. trim. dir. e proc. civ.*, 1999, 227-232.

CARDARELLI F., *Le banche dati pubbliche*, in *Dir. inf.*, 2002, 321-341.

CARDARELLI F., SICA S., ZENO-ZENCOVICH V., *Il codice dei dati personali. Temi e problemi*, Milano, Giuffrè, 2004.

CARNELUTTI F., *Problema giuridico della trasfusione di sangue*, in *Foro it.*, IV, 1938, 90-103.

CASONATO C., *Introduzione al biodiritto. La bioetica nel diritto costituzionale comparato*, Quaderni del Dipartimento di Scienze Giuridiche dell'Università di Trento, n. 57, 2006.

CASSANO G., FADDA S. (a cura di), *Codice in materia di protezione dei dati personali*, Milano, Ipsoa, 2004.

CASSANO G., FADDA S. (a cura di), *Codice in materia di protezione dei dati personali*, IPSOA, 2004.

CASSANO G., *Il diritto all'identità personale*, in *Nuova giur. civ. comm.*, 1997, II, 351-370.

CERRI A., voce «Identità personale», in *Enc. giur. Treccani*, 1995, 1-8.

CIRILLO G. P. (a cura di), *Il Codice sulla protezione dei dati personali*, Milano, Giuffrè, 2004.

CLARKE R., *Human identification in information systems: management challenges and public policy issues*, in 7 *Information Technology & People* (1994), 6-37.

CNIL, *Autorisation unique n°AU-007 - Délibération n°2006-101 du 27 avril 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail*, in *http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/105/#*.

CNIL, *Autorisation unique n°AU-008 - Délibération n°2006-102 du 27 avril 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail*, in *http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/104/#*.

CNIL, *Autorisation unique n°AU-009 - Délibération n°2006-103 du 27 avril 2006 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main étayant pour finalité l'accès au restaurant scolaire,* in *http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/103/#.*

CNIL, *Délibération n°00-056 du 16 novembre 2000, Délibération portant avis sur un projet d'arrêté présenté par le ministre de l'éducation nationale concernant un traitement automatisé d'informations nominatives ayant pour finalité le contrôle d'accès par la reconnaissance des empreintes digitales de certains personnels de l'éducation nationale, pour certains locaux de la cité académique de Lille,* in *http://www.legifrance.gouv.fr.*

CNIL, *Délibération n°00-057 du 16 novembre 2000, Délibération portant avis sur un projet d'arrêté présenté par le préfet de l'Hérault concernant un traitement automatisé d'informations nominatives ayant pour finalité la gestion du temps de travail des agents de la préfecture,* in *http://www.legifrance.gouv.fr*.

CNIL, *Délibération n°01-006 du 25 janvier 2001, Délibération portant avis sur un projet de décision présenté par l'établissement public du Musée du Louvre concernant un traitement de contrôle des accès et des horaires de certains personnels par la reconnaissance du contour de la main,* in *http://www.legifrance.gouv.fr*.

CNIL, *Délibération n°02-070 du 15 octobre 2002, Délibération portant avis sur le traitement automatisé d'informations nominatives, mis en oeuvre par le collège Joliot Curie de Carqueiranne, destiné à contrôler l'accès au restaurant scolaire par la reconnaissance de la géométrie de la main,* in *http://www.legifrance.gouv.fr.*

CNIL, *Délibération n°2005-135 du 14 juin 2005, Délibération autorisant la mise en oeuvre par le Centre hospitalier de Hyères d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires de ses employés,* in *http://www.legifrance.gouv.fr*.

CNIL, *Délibération n°2005-135 du 14 juin 2005, Délibération autorisant la mise en oeuvre par le Centre hospitalier de Hyères d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires de ses employés*, in *http://www.legifrance.gouv.fr*.

CNIL, *Délibération n°2006-005 du 12 janvier 2006, Délibération portant refus d'autorisation de la mise en oeuvre par la clinique de Goussonville d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle des horaires des employés,* in *http://www.legifrance.gouv.fr.*

CNIL, *Délibération n°2006-098 du 06 avril 2006**,** Délibération portant autorisation de la mise en oeuvre par la société Carrefour d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle de l'accès à certains locaux*, in *http://www.legifrance.gouv.fr*.

CNIL, *Délibération n°2006-156 du 30 mai 2006, Délibération portant refus d'autorisation de la mise en oeuvre par la société Rothschild Gestion d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux locaux*, in *http://www.legifrance.gouv.fr.*

CNIL, *Délibération n°2006-157 du 30 mai 2006**,** Délibération portant refus d'autorisation de la mise en oeuvre par la société Murano Urban Resort d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux chambres de l'hôtel,* in *http://www.legifrance.gouv.fr.*

CNIL, *Délibération n°2009-193 du 26 mars 2009 autorisant la mise en œuvre par l'Institut des Neurosciences de Grenoble d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux (autorisation n°1338959),* in *http://www.legifrance.gouv.fr*.

CNIL, *Délibération n°2009-229 du 7 mai 2009 autorisant la mise en œuvre par la société NORD ORTHOPEDIE d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux (autorisation n°1336959*), in *http://www.legifrance.gouv.fr*.

CNIL, *Délibération n°2009-230 du 7 mai 2009 autorisant la mise en œuvre par le CENTRE HOSPITALIER JULES LESCARDE d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux (autorisation n°1338580)* in *http://www.legifrance.gouv.fr*.

CNIL, *Délibération n°2009-316 du 7 mai 2009 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail*, in *http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/205/#.*

CNIL, *Délibération n°97-044 du 10 juin 1997**,** Délibération portant avis sur un projet d'arrêté présenté par la Banque de France concernant un traitement automatisé d'informations nominatives ayant pour finalité la gestion des contrôles d'accès des agents par empreintes digitales,* in *http://www.legifrance.gouv.fr*.

CNIPA, *Linee guida per l'impiego delle tecnologie biometriche nelle pubbliche amministrazioni. Indicazioni operative,* in *www.cnipa.gov.it/site/_files/I%20Quaderni%2017.pdf*, 2005.

CNIPA, *Linee guida per le tecnologie biometriche*, in *www.cnipa.gov.it/site/_files/Linee%20guida%20tecnologie%20biometriche.pdf*, 8-10-2004.

COLONNA V., *Il danno da lesione della privacy*, in *Danno e resp.*, 1999, 18-35.

COMITATO NAZIONALE PER LA BIOETICA, *Nanoscienza e Nanotecnologie*, 9 giugno 2006, in *http://www.governo.it/bioetica/testi/Nanoscienze_Nanotecnologie.pdf.*

COMITATO NAZIONALE PER LA BIOETICA, *Problemi bioetici in una società multietnica. La circoncisione: profili bioetici*, 1998.

COMITÉ CONSULTATIF NATIONAL D'ETHIQUE POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ, CCNE, Avis n° 96, *Questions éthiques posées par les nanosciences, les nanotechnologies et la santé* (Paris, le 1er février 2007), in *http://www.ccne-ethique.fr/docs/fr/avis096.pdf.*

COMMISSION D'ACCÈSS À L'INFORMATION, *Biometrics in Québec: Application Principles. Making an Informed Choice*, July 2002, in *www.cai.gouv.qc.ca/home_00_portail/01_pdf/biometrics.pdf.*

COMMISSION OF THE EUROPEAN COMMUNITIES, *Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs*, Brussels, 24.11.2005, in *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0597:FIN:EN:PDF*.

COMMISSIONE DELLE COMUNITÀ EUROPEE, *Proposta di regolamento del Parlamento europeo e del Consiglio, che modifica il regolamento (CE) n. 2252/2004 del Consiglio relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati* membri, 18.10.2007, in *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0619:FIN:IT:PDF*.

COMMISSIONE DELLE COMUNITÀ EUROPEE, *Relazione sulla valutazione del sistema di Dublino*, Bruxelles, 6.6.2007, COM(2007) 299 definitivo, in *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0597:FIN:EN:PDF*.

COMPORTI M., *Le cose, i beni, ed i diritti reali*, in *Istituzioni di diritto privato*, (a cura di) BESSONE M., Torino, Giappichelli, 2005, 319 ss.

CONSIGLIO DELL'UNIONE EUROPEA, *Regolamento (CE) n. 2252/2004 del Consiglio del 13 dicembre 2004 relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri*, in *GUCE* n. L 385 del 29.12.2004.

COSSU C., *Il diritto alla riservatezza nel nuovo diritto delle banche dati*, in *Giur. it.*, 1997, IV, 362-376.

COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, in *http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/2Biometrics_2005_en.pdf*, February 2005.

COUNCIL OF EUROPE, EUROPEAN COMMISSION AGAINST RACISM AND INTOLERANCE (ECRI), *Recommendation n. 11 on combating racism and racial discrimination in policing*, in *http://www.coe.int/t/dghl/monitoring/ecri/activities/gpr/en/recommendation_n11/e-RPG%2011%20-%20A4.pdf*.

COUNCIL OF EUROPE, EUROPEAN COMMITTEE ON LEGAL COOPERATION (CDCJ), *Guiding principles for the protection of personal data with regard to smart cards*, Strasbourg, 12 May 2004, in *http://www.coe.int*.

COUNCIL OF EUROPE, PARLIAMENTARY ASSEMBLY, EXPLANATORY MEMORANDUM BY THE RAPPORTEUR, *Europe's fight against economic and transnational organized crime: progress or retreat?*, 6 April 2001, in *http://assembly.coe.int/documents/workingdocs/doc01/edoc9018.htm*.

COUNCIL OF EUROPE, *Rec(2007)1 of the Committee of Ministers to member States on Co-operation against terrorism between the Council of Europe and its member states, and the International Criminal Police Organization (ICPO-Interpol)*, in *http://www.coe.int/t/e/legal_affairs/legal_cooperation/fight_against_terrorism/2_Adopted_Texts/Rec_2007_1E%20Interpol.pdf*.

COUNCIL OF EUROPE, *The Hague Programme: Strengthening Freedom, Security and Justice in the European Union*, Brussels, 13 December 2004, in *http://ec.europa.eu/justice_home/doc_centre/doc/hague_programme_en.pdf*.

CRISCUOLI G., *L'acquisto delle parti staccate del proprio corpo e gli artt. 820 e 821 del c.c.*, in *Dir. fam. e pers.*, 1985, 268 ss.

CRISCUOLI R., *La biomedicina ed il principio di identità genetica nel diritto europeo*, in *Nuove Autonomie*, 2002, 661-682.

CUBEDDU G. M., Commento art. 13, in BIANCA C. M., BUSNELLI F. D. (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, I, Padova, Cedam, 2007, 293-319.

CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *Il Codice del trattamento dei dati personali*, Torino, Giappichelli, 2007.

D'AGOSTINO F. (a cura di), *Corpo esibito, corpo violato, corpo venduto, corpo donato. Nuove forme di rilevanza giuridica del corpo umano*, Milano, Giuffrè, 2003.

D'AGOSTINO F. (a cura di), *Il corpo deformato. Nuovi percorsi dell'identità personale*, Milano, Giuffrè, 2002.

D'AGOSTINO F., *Bioetica*, Torino, Giappichelli, 1998.

D'AGOSTINO F., *Individualità e biometria*, in *L'Arco di Giano*, n. 45, 2005, 3-7.

D'AGOSTINO F., *Introduzione*, in COTTA S., AMATO MANGIAMELI A. C., AMATO S., LISITANO A., VITALE V., *Diritto e corporeità. Prospettive filosofiche e profili giuridici della disponibilità del corpo umano*, Milano, Jaca Book, 1987, 7-14.

D'AGOSTINO F., *Le prospettive della biopolitica*, Relazione tenuta il 20 ottobre 2007, presso il Centro Congressi dell'Università di Pisa, in *http://www.siti.chiesacattolica.it/siti/allegati/344/Relazione%20DAgostino.doc*.

D'AGOSTINO F., *Riflessioni sui diritti della corporeità*, in *Rivista di teologia morale*, 1981, n. 50, 201-212.

D'ANTONIO V., *I dati genetici*, in CARDARELLI F., SICA S., ZENO-ZENCOVICH V., *Il codice dei dati personali. Temi e problemi*, Milano, Giuffrè, 2004.

D'ARRIGO C. M., *Autonomia privata e integrità fisica*, Milano, Giuffrè, 1999.

D'ARRIGO C. M., voce «Integrità fisica», in *Enc. del dir.*, Aggiornamento-IV, Giuffrè, 2000, 712-737.

D'ORAZIO R., *Il principio di necessità nel trattamento dei dati personali*, in CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *Il Codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 19-27.

DE CESARIS A. M., voce «Habeas corpus», in *Enc. giur. Treccani*, XV, Ed. Enc. it, 1989, 1- 6.

DE CUPIS A., *Il diritto sulle parti staccate del corpo umano e il diritto sul cadavere umano*, nel *Trattato Cicu-Messineo*, IV, Giuffrè, 1982, 159 ss.

DE CUPIS A., *Sull'equiparazione delle parti staccate del corpo umano ai frutti naturali*, in *Riv. trim. dir. e proc. civ.*, 1986, 137-138.

DE CUPIS A., voce «Corpo (Atti di disposizione del proprio)», nel *Noviss. Digesto it.*, IV, Utet, 1959, 854-855.

DE CUPIS A., voce «Integrità fisica (diritto alla)», in *Enc. giur. Treccani*, XVII, Ed. Enc. it., 1989, 1-6.

DE HERT P., *Biometrics: legal issues and implications*, in *http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20Biometrics%20March%2005/Legal Implications_Paul_de_Hert.pdf*, 2005.

DE HERT P., GUTWIRTH S., *Interoperability of Police Databases within the EU: An Accountable Political Choice?*, in 20 *International Review of Law Computers* (2006), 21-35.

DE HERT P., GUTWIRTH S., *Making sense of privacy and data protection: a prospective overview in the light of the future of identity, location-based services and virtual residence*, in EUROPEAN COMMISSION, JRC, IPTS, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A prospective Overview*, in *http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20STUDY/20823-ExeSummEN.pdf*, 2003, 111-148.

DE HERT P., SCHREURS W., BROUWER E., *Machine-readable identity documents with biometric data in the EU – part II*, in 22 *Keesing Journal of Documents & Identity* (2007), 23-26.

DE HERT P., SCHREURS W., BROUWER E., *Machine-readable identity documents with biometric data in the EU – part III*, in 23 *Keesing Journal of Documents & Identity* (2007), 27-32.

DE HERT P., SCHREURS W., BROUWER E., *Machine-readable identity documents with biometric data in the EU – part IV*, in 24 *Keesing Journal of Documents & Identity* (2007), 29-35.

DE HERT P., *What are the risks and what guarantees need to be put in place in view of interoperability of police databases?*, in *European Parliament. Directorate-General for Internal Policies of the Union, Area of Justice, Freedom & Security. Collection of Standard Briefing Notes by External Experts*, Brussels, Parlement Européen (Ed.), Jan. 2006 - March 2006, 169-182.

DE SCHUTTER O., RINGELHEIM J., *Ethnic Profiling: A Rising Challenge for European Human Rights Law*, in 71 *The Modern Law Review* (2008), 358-384.

DE SIERVO U., *Tutela dei dati personali e riservatezza*, in AA.VV., *Diritti, nuove tecnologie, trasformazioni sociali. Scritti in memoria di Paolo Barile*, Padova, Cedam, 2003, 297-314.

DEGNI F., *Sulla trasfusione obbligatoria di sangue*, in *Foro it.*, IV, 1938, 129-133.

DELL'OSSO G., DE PALMA T., *Il distacco di parti da soggetto vivente nei suoi riflessi medico-legali*, in *Riv. it. med. leg.*, 1983, 76-82.

DI GIANDOMENICO A., *Identità e bioetica*, in SERRA T. (a cura di), *L'identità e le identità*, Torino, Giappichelli, 2003, 37-49.

DICKENSON D., WIDDERSHOVEN G., *Ethical Issues in Limb Transplants*, in 15 *Bioethics* (2001), 110-124.

DIFFIE W., LANDAU S., *Il selvaggio mondo delle intercettazioni*, in *Le Scienze*, novembre 2008, n. 483, 67-75.

DOGLIOTTI M., *L'identità personale*, nel *Trattato Rescigno*, II, 1, Utet, 1999, 145-184.

DOGLIOTTI M., *Le persone fisiche*, nel *Trattato Rescigno*, 2, Utet, 1999, 111 ss.

DONATI A., *Consenso informato e responsabilità da prestazione medica*, in *Rass. dir. civ.*, 2000, 1-47.

DUBBELD L., *Observing Bodies. Camera Surveillance and the Significance of the Body*, in 5 *Ethics and Information Technology* (2003), 151-162.

DUNI G., *Conclusioni: cosa chiedono i giuristi ai tecnici?*, in *Riv. giur. sarda*, 2001, fasc. 1, 315-320.

DUNI G., *L'autenticità degli atti in forma elettronica*, in *Riv. giur. sarda*, 2001, fasc. 1, 295-298.

EGE, *Citizen rights and new technologies: a European challenge. Report of the European Group on Ethics in Science and New Technologies on the Charter on Fundamental Rights related to technological innovation as requested by President Prodi on February 3, 2000*, Brussels, May 23, 2000, in *http://ec.europa.eu/european_group_ethics/docs/prodi_en.pdf*.

EPSTEIN C., *Guilty Bodies, Productive Bodies, Destructive Bodies: Crossing the Biometric Borders*, in 1 *International Political Sociology* (2007), 149-164.

ESPOSITO R., *Bios. Biopolitica e filosofia*, Torino, Einaudi, 2004.

EUROPEAN BIOMETRICS PORTAL, EBP, *Biometrics in Europe, Trend Report 2007*, in *www.europeanbiometrics.info*.

EUROPEAN COMMISSION, *Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizen's Freedoms and Rights, Justice and Home Affaire (LIBE)*, in *http://ec.europa.eu/justice_home/doc_centre/freetravel/doc/biometrics_eur21585_en.pdf*, 2005.

EUROPEAN COMMISSION, JRC, IPTS, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A prospective Overview*, in

http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20STUDY/20823-ExeSummEN.pdf, 2003.

EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES (EGE), *Opinion on the ethical aspects of nanomedicine*, N° 21, 17 January 2007, in *http://ec.europa.eu/european_group_ethics/activities/docs/opinion_21_nano_en.pdf*.

FACCI G., *Il dovere di informazione del sanitario* (parte prima), in *Nuova giur. civ. comm*., 2006, II, 558-570.

FERRANDO G., *Diritto e scienze della vita. Cellule e tessuti nelle recenti direttive europee*, in *Familia*, 2005, 1157-1179.

FERRANDO G., *Consenso informato del paziente e responsabilità del medico, principi, problemi e linee di tendenza*, in *Riv. crit. dir. priv*., 1998, 37-87.

FERRI G. B., *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ.*, 1990, I, 801-823.

FIDIS, *ID-related Crime: Towards a Common Ground for Interdisciplinary Research*, in *http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp5-del5.2b.ID-related_crime.pdf*, 05 May 2006.

FILIPPI S., *La clonazione umana e il diritto alla propria identità genetica*, in *Arch. giur.*, fasc. IV, 2001, 509-526.

FILIPPONIO A., *Il corpo: principio d'identità. Un'introduzione* in D'AGOSTINO F. (a cura di), *Il corpo de-formato, nuovi percorsi dell'identità personale*, Milano, Giuffrè, 2002, 95-100.

FINOCCHIARO G., *Alcune riflessioni sul trattamento dei dati personali*, in *Contr. e impr.*, 2006, 1426-1437.

FINOCCHIARO G., *Una prima lettura della legge 31 dicembre 1996, n. 675, «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»*, in *Contr. e impr.*, 1997, 299-317.

FJELLSTROM R., *Respect for Persons, Respect for Integrity*, in 8 *Medicine, Health Care and Philosophy* (2005), 231-242.

FLORA M. G. P., *Biometria e clonazione delle impronte digitali*, in *Dir. Internet*, 2006, 627-629.

FOUCAULT M., *Sorvegliare e punire. Nascita della prigionia*, Torino, Einaudi, 2005.

FROSINI T. M., *Tecnologie e libertà costituzionali*, in *Dir. Inf.*, 2003, 487-504.

FROSIO G., *Cosa resta della privacy? – diritto alla riservatezza dell'"uomo medio" dopo l'11 settembre*, in *Ciberspazio e diritto*, 2005, 173-227.

FUČEK I., S.I., *Prospettive teologiche ed etiche in tema di corporeità umana*, in *Medicina e Morale*, 1990, 933-948.

FUNGHI P., GIUNTA F. (a cura di), *Medicina, bioetica e diritto. I problemi e la loro dimensione normativa*, Pisa, Edizioni ETS, 2005, 132 ss.

GADDINI R., *Alterazioni, corpo e identità* in D'AGOSTINO F. (a cura di), *Il corpo de-formato, nuovi percorsi dell'identità personale*, Milano, Giuffrè, 2002, 101-111.

GAINOTTI A. S., SPAGNOLO G., *Test genetici: a che punto siamo in Europa? A margine del Rapporto e delle Raccomandazioni della Commissione Europea sugli aspetti etici, giuridici e sociali dei test genetici*, in *Medicina e Morale*, 2004, n. 4, 737-766.

GALDI M., *Profili costituzionali della clonazione umana*, in *Dir. e giur.*, 2001, 69-87.

GALLO P., *Il dopo 11 settembre: un nuovo concetto giuridico di «pericolo». Tra libertà individuale ed esigenze di tutela della sicurezza collettiva*, in *Jus*, 2007, 427-438.

GAMBARO A., *La proprietà*, nel *Trattato Iudica-Zatti*, Giuffrè, 1990.

GAMBINO G., *Il corpo de-formato tra cultura diagnostica e "geneticizzazione" della medicina*, in D'AGOSTINO F. (a cura di), *Il corpo deformato, nuovi percorsi dell'identità personale*, Milano, Giuffrè, 2002, 39-51.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Accesso ad aree riservate di particolari aziende: uso proporzionato di impronte digitali - 23 novembre 2005*, doc. web n. 1202254, in *www.garanteprivacy.it.*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Autorizzazione al trattamento dei dati genetici – 22 febbraio 2007*, G. U. n. 65 del 19 marzo 2007, doc. web n. 1389918, in *www.garanteprivacy.it*.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Banche: impronte digitali, telecamere e diritti dei clienti*, Comunicato stampa del 17 novembre 2005, in *http://www.garanteprivacy.it/garante/doc.jsp?ID=1190523*.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Compiti del Garante - Uso delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro - 21 luglio 2005*, doc. web n. 1150679, in *www.garanteprivacy.it.*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Dati biometrici e Rfid nelle banche - 23 febbraio 2006*, doc. web n. 1251535, in *www.garanteprivacy.it.*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Il decalogo su corpo e libertà*, Comunicato stampa - 09 maggio 2006, doc. web n. 1277433, in *www.garanteprivacy.it*.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *In progetto la carta multiservizi della giustizia (Cmg) per un accesso più sicuro ai sistemi informatici giudiziari. Le valutazioni del Garante*, doc. web n. 1185160, in *www.garanteprivacy.it*.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Istituti di credito - Rilevazione di impronte digitali ed immagini: limiti e garanzie - 27 ottobre 2005*, doc. web n. 1246675, in *www.garanteprivacy.it.*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati (deliberazione n. 53 del 23 novembre 2006)*, in *www.garanteprivacy.it*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento del 23 gennaio 2008*, doc. web n. 1487903, in *www.garanteprivacy.it.*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento relativo ai casi da sottrarre all'obbligo di notificazione - 31 marzo 2004*, doc. web n. 852561, in *www.garanteprivacy.it*.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Riconoscimento vocale e gestione di sistemi informatici - 28 febbraio 2008*, doc. web n. 1501094, in *www.garanteprivacy.it.*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sicurezza di siti archeologici e uso di dei dati biometrici – 8 novembre* 2007, doc. web n. 1461908, in *www.garanteprivacy.it*.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sicurezza merci e controllo delle presenze presso aeroporti - 26 luglio 2006*, doc. web n. 1318582, in *www.garanteprivacy.it.*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento dei dati biometrici di dipendenti per garantire la salute pubblica - 15 febbraio 2008*, doc. web n. 1497675, in *www.garanteprivacy.it.*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati biometrici con finalità di verifica della presenza dei dipendenti e di accesso a particolari aree produttive - 15 giugno 2006*, doc. web n. 1306551, in *www.garanteprivacy.it.*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati personali biometrici per l'accesso a un complesso polifunzionale - 1 febbraio 2007*, doc. web n. 1381983, in *www.garanteprivacy.it.*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati biometrici presso Cariprato S.p.A. - 23 gennaio 2008*, doc. web n. 1490382, in *www.garanteprivacy.it.*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati biometrici presso Banca San Paolo Imi S.p.A. - 23 gennaio 2008*, doc. web n. 1490533, in *www.garanteprivacy.it.*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati biometrici nelle operazioni di trasfusione – 19 giugno 2008*, doc. web n. 1532480, in *www.garanteprivacy.it*.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati biometrici presso Banca San Paolo Imi S.p.A. – 23 gennaio 2008*, doc. web n. 1490533, in *www.garanteprivacy.it*.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Uso della biometria per identificazione del personale nelle banche - 15 giugno 2006*, doc. web n. 1306098, in *www.garanteprivacy.it.*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Videosorveglianza - Impronte digitali per l'accesso in banca - 11 dicembre 2000*, doc. web n. 30903, in *www.garanteprivacy.it.*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Videosorveglianza - Raccolta di impronte digitali associate ad immagini per l'accesso a banche – 7 marzo 2001*, doc. web n. 30947, in *www.garanteprivacy.it.*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Videosorveglianza – Provvedimento generale – 29 aprile 2004*, doc. web n. 1003482, in *www.garanteprivacy.it*.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Videosorveglianza e biometria – Trattamento dati personali mediante utilizzo di impronte digitali*, 19 novembre 1999, doc. web n. 42058, in *www.garanteprivacy.it*.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Videosorveglianza e dati biometrici - Rilevazioni biometriche presso istituti di credito - 28 settembre 2001*, doc. web n. 39704, in *www.garanteprivacy.it*

GARFINKEL S. L., *Informazioni del mondo, unitevi!*, in *Le Scienze*, novembre 2008, n. 483, 98.

GEMMA G., voce «Integrità fisica», nel *Digesto pubbl.*, VIII, Utet, 1993, 450-465.

GERRA G., *Alcune tecniche di identificazione biometrica di pratica attuabilità*, in *Riv. giur. sarda*, 2001, fasc. 1, 303-306.

GIACALONE P., *Il riconoscimento biometrico e l'utilizzo della firma digitale*, in *Riv. giur. sarda*, 2001, fasc. 1, 307-309

GIANNANTONIO E., *Il nuovo disegno di legge sulle banche di dati* personali, in *Dir. inf.*, 1991, 67-99.

GIANNANTONIO E., voce «Dati personali (tutela dei)», in *Enc. del dir.*, Aggiornamento III, Giuffrè, 1999, 483-492.

GIANNICHEDDA M. G., voce «Corpo», in *Diritti umani, cultura dei diritti e dignità della persona nell'epoca della globalizzazione. Dizionario*, I, Utet, 2007, 203-209.

GIARDINA S., MELE V., *Biotecnologie e "somatopoiesi": inquietudini del corpo e dilemmi bioetici nella letteratura,* in *Medicina e Morale,* 2006, 303-325.

GIULIANO A., *Dieci e tutte diverse. Studio sui dermatoglifi umani,* Torino, Tirrenia Stampatori, 2004.

GORGONI MARILENA, *La «stagione» del consenso e dell'informazione: strumenti di realizzazione del diritto alla salute e di quello all'autodeterminazione,* in *Resp. civ. e prev.*, 1999, 488-502.

GRANELLI CASTIGLIONE A., PAGANELLI M., BRAIDOTTI A., VENTURA F., *Riflessioni bioetiche circa il trapianto di mano*, in *Medicina e Morale*, 2005, 787-797.

GRIJPINK J., *Biometrics and identity fraud protection. Two barriers to realizing the benefits of biometrics – A chain perspective on biometrics, and identity fraud – Part II*, in 21 *Computer Law & Security Report* (2005), 249-256.

GRIJPINK J., *Biometrics and Privacy*, in 17 *Computer Law & Security Report* (2001), 154-160.

GRIJPINK J., *Identity fraud as a challenge to the constitutional state*, in 20 *Computer Law & Security Report* (2004), 29-36.

GROSSMAN W. M., *Identifying Risks: National Identity Cards*, in 2 *SCRIPT-ed* (2005), 5-19.

GRUPPO DI LAVORO ARTICOLO 29, PROTEZIONE DATI, *Parere 3/2005 riguardante l'attuazione del regolamento CE n. 2252/2004 del Consiglio, del 13 dicembre 2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli stati membri (Gazzetta ufficiale L 385 del 29.12.2004, pp. 1-6)*, in *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp112_it.pdf*.

GRUPPO PER LA TUTELA DEI DATI PERSONALI (ARTICOLO 29), *Documento di lavoro sulla biometria*, 1°agosto 2003, in *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp67_it.pdf*.

GUARDINI R., *La fine dell'epoca moderna. Il potere*, Brescia, Morcelliana, 2004.

GUNASEKARA G., *The 'final' privacy frontier? Regulating trans-border data flows*, in 15 *International Journal of Law and Information Technology* (2007), 362-393.

GUTWIRTH S., *Biometrics between opacity and transparency*, in 43 *Ann. ist. super. sanità* (2007), 61-65.

HAREL A., *Biometrics, identification and practical ethics*, in *http://www.europeanbiometrics.info/resources/index.php?Id_folder_tx=10#10*, 2001, 1-16.

HOOFNAGLE C. J., *Identity Theft: Making the Known Unknowns Known*, in 21 *Harvard Journal of Law & Technology* (2007), 98-122.

HOQUE S. M., *Government responses to terrorism: critical views of their impacts on people and public administration*, in 62 *Public Administration Review* (2002), 170-180.

HORNUNG G., *The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards*, in 4 *SCRIPT-ed* (2007), 246-262.

IAMICELI P., *Liceità, correttezza, finalità nel trattamento dei dati personali*, in PARDOLESI R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003, 395-467.

ICAO, *Biometric deployment of Machine Readable Travel Documents, ICAO TAG MRDT/NTWG, Technical Report*, in *http://www.policylaundering.org/archives/ICAO/Biometrics_Deployment_Version_2.0.pdf*, 21 May 2004.

ICAO, TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS (TAG-MRDT), Montréal, 23 March 2007, *Machine Readable Travel Documents (MRDTs): history, interoperability, and implementation*, in *http://www2.icao.int/en/MRTD/Downloads/Technical%20Report/ICAO_MRTD_History_of_Interoperability.pdf*.

INTERNATIONAL BIOMETRICH GROUP (IBG), *How is "Biometrich" defined?*, in *www.biometricgorup.com/reports/public/reports/biometric_definition.html*.

INTRONA F., MAZZAROLO C., *Manipolazione genetica, procreazione assistita, clonazione umana (ed altro ancora): il silenzio del legislatore italiano ed il codice penale spagnolo del 1995*, in *Riv. it. med. leg.*, 2001, 953-981.

ISRAEL G., *La macchina vivente. Contro le visioni meccanicistiche dell'uomo*, Torino, Bollati Boringhieri, 2004.

JAIN A. K., BOLLE R., PANKANTI S. (edited by), *Biometrics: personal identification in networked society*, Kluwer Academic Publishers, 1999.

JAIN A. K. e PANKANTI S., *Oltre le impronte digitali*, in *Le Scienze*, novembre 2008, n. 483, 76-79.

JOHNSON P., WILLIAMS R., *European securitization and biometric identification: the uses of genetic profiling*, in 43 *Ann. Ist. Super. Sanità* (2007), 36-43.

JONES P., WILLIAMS P., HILLIER D., COMFORT D., *Biometrics in retailing*, in 35 *International Journal of Retail & Distribution Management* (2007), 217-222.

JUELS A., *RFID Privacy. A Technical Primer for the Non-Technical Reader*, in STRANDBURG K., RAICU D. S. (edited by), *Privacy and Technologies of Identity. A cross disciplinary conversation*, New York, Springer, 2006, 57-73.

KIRSCHEN S., *Il codice della privacy, fra tradizione ed innovazione*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, I, Milano, Giuffrè, 2006, 5-105.

KUHSE H., *Il corpo come proprietà. Ragioni di scambio e valori etici*, in RODOTÀ S. (a cura di), *Questioni di bioetica*, Roma, Laterza, 1993, 65-73.

LAURIE G., *Genetic privacy. A challenge to medico-legal norm*, Cambridge University press, 2002.

LEE V., *Biometrics and identity fraud*, in *Biometric Technology Today* (February 2008), 7-11.

LIU Y., *Identifying Legal Concerns in the Biometric Context*, in 3 *Journal of International Commercial Law and Technology* (2008), 45-54.

LO SURDO C., *Gli strumenti di tutela del soggetto «interessato» nella legge e nella sua concreta applicazione*, in PARDOLESI R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003, 617-750.

LOCKWOOD M., *La donazione non altruistica di organi in vita*, in RODOTÀ S. (a cura di), *Questioni di bioetica*, Roma, Laterza, 1993.

LODGE J., *Freedom, security and justice: the thin end of the wedge for biometrics?*, in 43 *Ann. Ist. Super. Sanità* (2007), 20-26.

LOMBARDI VALLAURI L., *Identità, Identificazioni*, in *Nuova giur. civ. comm.*, supplemento fasc. 4/2007, 11-19.

LOSANO M. G., *Un progetto di legge sulla protezione dei dati personali*, in *Dir. inf.*, 1987, 465-474.

LOWRANCE W. W., *Learning from Experience. Privacy and the Secondary Use of Data in Health Research*, in *http://www.nuffieldtrust.org.uk/ecomm/files/161202learning.pdf*.

LYON D., *Biometrics, identification and surveillance*, in 22 *Bioethics* (2008), 499-508.

LYON D., *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano, Feltrinelli, 2001, 96.

LYON D., *Technology vs. "Terrorism": circuits of city surveillance since September 11th*, in 27 *International Journal of Urban and Regional Research* (2003), 666-678.

LYSYANSKAYA A., *Come mantenere un segreto*, in *Le Scienze*, novembre 2008, n. 483, 101-107.

MACIOCE F., *Il corpo digitale. Profili etici dei rilievi biometrici: il caso della carta di identità elettronica*, in *L'Arco di Giano*, 2005, n. 45, 33-41.

MACIOCE F., *Il corpo. Prospettive di filosofia del diritto*, Roma, Aracne, 2002.

MARCUM A., *Biomechanical and Phenomenological Models of the Body. The Meaning of Illness and Quality of Care*, in 7 *Medicine, Health Care and Philosophy* (2004), 311-320.

MARINI G., *La giuridificazione della persona. Ideologie e tecniche nei diritti della personalità*, in *Riv. dir. civ.*, 2006, 359- 394.

MARZANO PARISOLI M. M., *Il corpo tra diritto e diritti*, in *Materiali per una nuova storia della cultura giuridica*, 1999, 527-552.

MARZANO PARISOLI M. M., *Norme e natura: una genealogia del corpo umano*, Napoli, Vivarium, 2001.

MAZZEO M., *La notificazione e le comunicazioni al garante*, in PANETTA R. (a cura di), *Libera circolazione e protezione dei dati personali*, I, Milano, Giuffrè, 2006, 624-652.

MAZZONI C. M., *Avvertenza*, in BAUD J. P., *Il caso della mano rubata. Una storia giuridica del corpo*, Milano, Giuffrè, 2003, IX-X.

MAZZONI C. M., *Il corpo e le sue immagini*, in *Riv. crit. dir. priv.*, 2005, 449-454.

MAZZONI C. M., *Il corpo nascosto dei giuristi*, in *Riv. crit. dir. priv*, 2008, 339-346.

MELONI S. M., *Il trattamento dei dati da parte di soggetti privati: la disciplina del consenso*, 197- 220, in CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *Il Codice del trattamento dei dati personali*, Torino, Giappichelli, 2007.

MESSINA M., *I diritti dell'interessato*, in CARDARELLI F., SICA S., ZENO-ZENCOVICH V. (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, Giuffrè, 2004, 65-109.

MESSINETTI D., *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, 339-407.

MESSINETTI D., *Identità personale e processi regolativi della disposizione del corpo*, in *Riv. crit. dir. priv.*, 1995, 197-229.

MESSINETTI R., *Pluralità dei circuiti comunicativi e autodeterminazione informativa della persona*, nota a TRIB. PERUGIA, 31.5.2006, n. 709, in *Danno e resp.*, 2007, 689-700.

MIRABELLI G., *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Dir. inf.*, 1993, 313-330.

MITCHISON N., WILIKENS M., BREITENBACH L., URRY R., PORTESI S., *Identity Theft. A Discussion Paper*, European Commission, Joint Research Centre, 2004

MORDINI E., MASSARI S., *Body, biometrics and identity*, in 22 *Bioethics* (2008), 488-498.

MORDINI E., OTTOLINI C., *Body identification, biometrics and medicine: ethical and social considerations*, in 43 *Ann. ist. super. sanità* (2007), 51-60.

MORDINI E., OTTOLINI C., *Implicazioni etiche e sociali della biometria*, in *L'Arco di Giano*, 2005, n. 45, 53-72.

MULLER B. J., *(Dis)Qualified bodies: securitization, citizenship and 'identity management'*, in 8 *Citizenship Studies* (2004), 279-294.

MUSSO G. R., voce «Habeas corpus», nel *Digesto pen.*, VI, 1992, 58-64.

NAFFINE N., *The Legal Structure of Self-Ownership: Or the Self-Possessed Man and the Woman Possessed*, in 25 *Journal of Law and Society* (1998), 193-212.

NANAVATI S., THIEME M., NANAVATI R., *Biometrics. Identity verification in a networked world*, Wiley Computer Publishing, 2002.

NAVARRETTA E., Commento art. 11, in BIANCA C. M., BUSNELLI F. D. (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, I, Padova, Cedam, 2007, 241-270.

NIGER S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, Cedam, 2006.

O'NEIL P. H., *Complexity and Counterterrorism: Thinking about Biometrics*, in 28 *Studies in Conflict & Terrorism* (2005), 547-566.

OECD, WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Biometric-based technologies*, in *http://www.olis.oecd.org/olis/2003doc.nsf/LinkTo/NT000070D6/$FILE/JT00166988.PDF*, 30-Jun-2004.

OLIVO F., *Dati personali e situazioni giuridiche soggettive*, in *Giust. civ.*, 2002, II, 157-166.

PAESANO G., *Clonazione umana e diritto all'identità*, in *Dir. fam. e pers.*, 2004, 546-591.

PALAZZANI L., *Corpo e persona: i percorsi filosofici della bioetica e della biogiuridica*, in D'AGOSTINO F. (a cura di), *Il corpo de-formato, nuovi percorsi dell'identità personale*, Milano, Giuffrè, 2002, 113-147.

PALLARO P., *Libertà della persona e trattamento dei dati personali nell'Unione Europea*, Milano, Giuffrè, 2002.

PALMERINI E., *Le scelte sul corpo: i confini della libertà di decidere*, Consiglio Superiore della Magistratura – Roma, 9-10 giugno 2005, in *http://appinter.csm.it/incontri/relaz/11876.pdf*, 1-12.

PANETTA R. (a cura di), *Libera circolazione e protezione dei dati personali*, I, Milano, Giuffrè, 2006.

PANETTA R. (a cura di), *Libera circolazione e protezione dei dati personali*, II, Milano, Giuffrè, 2006.

PARDOLESI R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003.

PARDOLESI R., nota a CASS., sez. I civ., 22.6.1985, n. 3769, in *Foro it.*, 1985, I, 2211.

PARDOLESI R., *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in PARDOLESI R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003, 1-57.

PARLAMENTO EUROPEO, COMMISSIONE PER LE LIBERTÀ CIVILI, LA GIUSTIZIA E GLI AFFARI INTERNI, *Relazione sulla proposta della Commissione di regolamento del Consiglio relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti dei cittadini dell'Unione (COM(2004)0116-C5-0101/2004-2004/0039(CNS))*, 28.10.2004, in *http://www.europarl.europa.eu/sides/getDoc.do?language=IT&pubRef=//EP//NONSGML+REPORT+A6-2004-0028+0+DOC+PDF+V0//IT*.

PARLAMENTO EUROPEO, *Comunicato stampa* del 14.01.2009, *Passaporti biometrici: niente impronte digitali per i minori di dodici anni*, in *http://www.europarl.europa.eu/news/expert/infopress_page/019-46172-012-01-03-902-20090114IPR46171-12-01-2009-2009-false/default_it.htm*.

PARLAMENTO EUROPEO, *Risoluzione legislativa del Parlamento europeo sulla proposta della Commissione di regolamento del Consiglio relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici nei passaporti dei cittadini*

dell'Unione (COM(2004)0116 — C5-0101/2004 — 2004/0039(CNS)), in *GUCE* n. C 208 E/50 del 25.8.2005.

PARLAMENTO EUROPEO E CONSIGLIO, *Regolamento (CE) N. 444/2009 del Parlamento europeo e del Consiglio del 28 maggio 2009 che modifica il regolamento (CE) n. 2252/2004 del Consiglio relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri*, in GUCE n. L 141 del 6.6.2009.

PATTI S., Commento art. 23, in BIANCA C. M., BUSNELLI F. D. (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, Padova, Cedam, 2007, 541-556.

PAVONI R., voce «Biotecnologie», in *Diritti umani, cultura dei diritti e dignità della persona nell'epoca della globalizzazione. Dizionario*, I, Utet, 2007, 90-95.

PAYE J. C., *Gran Bretagna: fine dell'habeas corpus,* in *Democrazia e diritto*, 2005, 211-216.

PEJAŚ J., PIEGAT A. (edited by), *Enhanced methods in computer security, biometric and artificial intelligence systems*, Kluwer Academic Publishers, 2005.

PELLECCHIA E., Commento art. 26, in BIANCA C. M., BUSNELLI F. D. (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, I, Padova, Cedam, 2007, 616-645.

PENASA S., *Alla ricerca dell'anello mancante: il deposito dello strumento di ratifica della Convenzione di Oviedo*, in *http://www.forumcostituzionale.it*.

PERLINGIERI P., *La tutela giuridica della «integrità psichica» (a proposito delle psicoterapie)*, in *Riv. trim. dir. e proc. civ.*, 1972, 2, 763-777.

PESANTE M., *Corpo umano (Atti di disposizione)*, in *Enc. del dir.*, X, Giuffrè, 1962, 653 ss.

PETERMANN T., SAUTER A., SCHERZ C., *Biometrics at the Borders – the Challenges of a Political Technology*, in 20 *International Review of Law Computers* (2006), 149-166.

PETRONE M., *Banche di dati e tutela della "privacy". Riflessi penalistici*, in *Dir. Inf.*, 1988, 81-87.

PICCINNI M., *Il consenso al trattamento medico del minore*, Padova, CEDAM, 2007.

PICOTTI L., *Trattamento dei dati genetici, violazione della privacy e tutela dei diritti fondamentali nel processo penale*, in *Dir. inf.*, 2003, 689-725.

PIERA A., *Facilitation of air transport*, in 26 *Air & Space Law* (2001), 315-332.

PIERA A., *The simplifying passenger travel programme and its legal implications*, in 28 *Air & Space Law* (2003), 132- 138.

PIERUCCI A., *Videosorveglianza e biometria*, in PANETTA R. (a cura di), *Libera circolazione e protezione dei dati personali*, II, Milano, Giuffrè, 2006, 1627-1682.

PINO G., *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, Il Mulino, 2003.

PIRAINO LETO A., *Il diritto ad essere se stessi*, in *Dir. fam. e pers.*, 1990, 601-606.

PIZZETTI F., *Discorso del Presidente*, Roma, 16 luglio 2008, Relazione 2007, in *www.garanteprivacy.it*.

POGGI F., *Tra anima e corpo. Il problema degli stati soggettivi nella filosofia della mente contemporanea*, in *Materiali per una nuova storia della cultura giuridica*, 2007, 161-181.

PRINS C., *Body ID*, in 3 *The EDI Law Review* (1997), 159-160.

PRINS C., *Making Our Body Identify for Us: Legal Implications of Biometric Technologies*, in 14 *Computer Law & Security Report* (1998), 159-165.

PRINS C., *When personal data, behaviour and virtual identities become a commodity: would a property rights approach matter?*, in 3 *SCRIPT-ed* (2006), 270-303.

PUNZI A., *La persona nei dati. Ragioni e modelli di una regolamentazione*, in CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *Il Codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 761-775.

REDPATH J., *Biometrics and international migration*, in 43 *Ann. ist. super. sanità* (2007), 27-35.

REID P., *Biometrics for network security,* Upper Saddle River, 2004.

RENDTORFF J. D., *Basic Ethical Principles in European Bioethics and Biolaw: Autonomy, Dignity, Integrity and Vulnerability – Towards a Foundation of Bioethics and Biolaw*, in 5 *Medicine, Health Care and Philosophy* (2002), 235-244.

RESCIGNO P. (a cura di), *Codice Civile*, 5 ed., Milano, Giuffrè, 2003, *sub* art. 5.

RESTA G., *Identità personale, identità digitale,* in *Dir. inf.*, 2007, 511- 531.

RESTA G., *Il diritto alla protezione dei dati personali*, in CARDARELLI F., SICA S., ZENO-ZENCOVICH V. (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, Giuffrè, 2004, 11-63.

RESTA G., *Privacy e processo civile: il problema della litigation «anonima»,* in *Dir. inf.*, 2005, 681-725.

RESTA G., *Proprietà, corpo e commodification nel dibattito nordamericano,* in *Riv. crit. dir. priv.*, 1995, 798 ss.

RODOTÀ S., , *La privacy secondo l'Europa,* in *Le Scienze,* novembre 2008, n. 483, 60-65.

RODOTÀ S., *Avventure del corpo,* in *Notizie di Politeia,* 2006, n. 84, 45-56.

RODOTÀ S., *Dal soggetto alla persona,* Napoli, Editoriale Scientifica, 2007.

RODOTÀ S., *Ipotesi sul corpo "giuridificato",* in *Riv. crit. dir. priv.*, 1994, 467-490.

RODOTÀ S., *La vita e le regole*, Milano, Feltrinelli, 2006.

RODOTÀ S., *Persona, riservatezza, identità. Prime note sistematiche sulla tutela dei dati personali,* in *Riv. crit. dir. priv*., 1997, 583-609.

RODOTÀ S., *Prefazione,* in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, I, Milano, Giuffrè, 2006.

RODOTÀ S., *Protezione dei dati e circolazione delle informazioni,* in *Riv. crit. dir. priv.*, 1984, 721-772.

RODOTÀ S., *Quattro paradigmi per l'identità,* in *Nuova giur. civ. comm.*, supplemento fasc. 4/2007, 21-32.

RODOTÀ S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma, Laterza, 1997.

RODOTÀ S., *Tra diritti fondamentali ed elasticità normativa: il nuovo Codice sulla privacy,* in *Eur. e dir. priv.*, 2004, 1-11.

RODOTÀ S., *Tra diritto e società. Informazione genetica e tecniche di tutela,* in *Riv. crit. dir. priv.*, 2000, 571-604.

RODOTÀ S., *Trasformazioni del corpo,* in *Pol. dir.*, 2006, 3-24.

RODOTÀ S., *Una scommessa impegnativa sul terreno dei muovi diritti*, Discorso del Garante per la protezione dei dati personali tenuto l'8 maggio 2001 alla presentazione della relazione del 2001, in *www.interlex.it/675/rodota6.htm*.

ROMBOLI R., *Delle persone fisiche,* nel *Commentario Scialoja-Branca,* Zanichelli-Foro it.,1988, *sub* art. 5, 225 ss.

ROMBOLI R., *I limiti alla libertà di disporre del proprio corpo nel suo aspetto«attivo» e in quello «passivo»*, nota a CORTE COST., 22.10.1990, n. 471, in *Foro it.*, 1991, I, 15 ss.

ROSETTI R., Commento artt. 37-38, in BIANCA C. M., BUSNELLI F. D. (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, I, Padova, Cedam, 2007, 734-772.

RUOTOLO M., nel *Commentario alla Costituzione*, I, Utet, 2006, *sub*. art 13, 321-341.

RUOTOLO M., voce «Habeas corpus», in *Diritti umani, cultura dei diritti e dignità della persona nell'epoca della globalizzazione. Dizionario*, II, Utet, 2007, 695-699.

RUSSO M. T., *Dal corpo proprio al corpo estraneo: cultura post moderna e immagini del corpo*, in D'AGOSTINO F. (a cura di), *Corpo esibito, corpo violato, corpo venduto, corpo donato. Nuove forme di rilevanza giuridica del corpo umano*, Milano, Giuffrè, 2003, 101-120.

SADUN BORDONI G., *Corpo e potere: biopolitica del totalitarismo*, in D'AGOSTINO F. (a cura di), *Corpo esibito, corpo violato, corpo venduto, corpo donato. Nuove forme di rilevanza giuridica del corpo umano*, Milano, Giuffrè, 2003, 121-141.

SANNA E., *Le garanzie di sicurezza e autenticità delle informazioni in rete; in particolare del mandato informatico di pagamento*, in *Riv. giur. sarda*, 2001, fasc. 1, 310-315.

SANTANIELLO G. (a cura di), *La protezione dei dati personali*, nel *Trattato di diritto amministrativo*, diretto da SANTANIELLO G., XXXVI, Cedam, 2005.

SANTORO PASSARELLI F., *Dottrine generali del diritto civile*, Napoli, 1962, VII ed., 51 ss.

SANTOSUOSSO A., *Persone fisiche e confini biologici: chi determina chi*, in *Pol. dir.*, 2002, 525-547.

SARZANA C., *Evoluzione tecnologica e diritti dell'individuo*, in *Dir. Inf.*, 1992, 393-411.

SARZANA DI S. IPPOLITO C., *Le iniziative internazionali in tema di sistemi crittografici con riferimento alla tutela dei dati personali*, in *Dir. inf.*, 1998, 1-13.

SCHLESINGER P., *La persona*, in *Riv. dir. civ.*, 2008, 379-393.

SCHOENHOLTZ A. I., *Transatlantic Dialogue on Terrorism and International Migration*, in 41 International Migration (2003), 173-192.

Serdyukov Yu. M., *Human information integrity*, in 77 *Herald of the Russian Academy of Sciences* (2007), 474-478.

SGRECCIA E., *Corpo e persona*, in RODOTÀ S. (a cura di), *Questioni di bioetica*, Roma, Laterza, 1993, 113-122.

SGRECCIA E., *La persona umana e il suo corpo*, in *Manuale di bioetica*, I, Milano, Vita e pensiero, 2003, 105-137.

SIDDI M. C., *Chiavi biometriche e impatto sulla pubblica amministrazione*, in *Riv. giur. sarda*, 2001, fasc. 1, 298-303.

SIMONCINI A., LONGO E., nel *Commentario alla Costituzione*, I, Utet, 2006, *sub*. art. 32, 655-674.

SOBEL R., *The Demeaning of Identity and personhood in National Identification Systems*, in 15 *Harvard Journal of Law & Technology* (2002), 319-387.

SPAGNOLO A. G., DALOISO V., *Outlining ethical issues in nanotechnologies*, in *Bioethics*, 2008, 1 ss.

SPROKKEREEF A., DE HERT P., *Ethical practice in the use of biometric identifiers within the EU*, in 3 *Law, Science and a Policy* (2007), 177-201.

STAMMATI S., *Costituzione, clonazione umana, identità genetica*, in *Giur. cost.*, 1999, 4067-4109.

STILO L., *Il diritto all'autodeterminazione informativa: genesi storica di un diritto fondamentale dell' "HOMO TECNOLOGICUS"*, in *Nuovo dir.*, 2002, 7-8, 23.

STRANDBURG K., RAICU D. S. (edited by), *Privacy and Technologies of Identity. A cross disciplinary conversation*, New York, Springer, 2006.

SULLIVAN C., *The United Kingdom Identity Cards Act 2006-Civil or Criminal?*, in 15 *International Journal of Law and Information Technology* (2007), 320-361.

TALLACCHINI M., *Biotecnologie e consenso informato. Un inizio…*, in *Notizie di Politeia*, 1999, n. 54, 3-12.

TALLACCHINI M., *Bodyright. Corpo biotecnolgico e diritto*, in *Biblioteca della libertà*, 1998, 21-50.

TALLACCHINI M., *Habeas Corpus? Il corpo umano tra non-commerciabilità e brevettabilità*, in *Bioetica*, 1998, 531-552.

TALLACCHINI M., *Il corpo e le sue parti. L'allocazione giuridica dei materiali biologici umani*, in *Medicina e Morale*, 1998, 499-544.

TALLACCHINI M., *Retorica dell'anonimia e proprietà dei materiali biologici umani*, in D'AGOSTINO F. (a cura di), *Corpo esibito, corpo violato, corpo venduto, corpo donato. Nuove forme di rilevanza giuridica del corpo umano*, Milano, Giuffrè, 2003, 171-192.

TOMMASI S., *Consenso informato e disciplina dell'attività medica*, in *Riv. crit. dir. priv.*, 2003, 555-577.

TOSCANO G., *Informazione, consenso e responsabilità sanitaria*, Milano, Giuffrè, 2006.

TRONCARELLI B., *Il corpo nella prospettiva antiriduzionistica della complessità*, in D'AGOSTINO F. (a cura di), *Corpo esibito, corpo violato, corpo venduto, corpo donato. Nuove forme di rilevanza giuridica del corpo umano*, Milano, Giuffrè, 2003, 193-221.

TRUCCO L., I*ntroduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Torino, Giappichelli, 2004.

VACCARO D., *Il corpo controllato tra nuove tecnologie e tutela della dignità*, in *http://www.computerlaw.it/public/Vaccaro%20il%20corpo%20controllato%201.pdf*, I parte.

VAN DER PLOEG I., *Biometric identification technologies: ethical implications of the informatization of the body*, in *http://www.biteproject.org/documents/policy_paper_1_july_version.pdf*.

VAN DER PLOEG I., *Biometrics, and the body as information: normative issues of the socio-technical coding of the body*, in *http://www.bmg.eur.nl/smw/publications/vdp_02.pdf* .

VAN DER PLOEG I., *Genetics, biometrics, and the informatization of the body*, in 43 *Ann. Ist. Super. Sanità* (2007), 44-50.

VAN DER PLOEG I., *The illegal body: 'Eurodac' and the politics of biometric identification*, in 1 *Ethics and Information Technology* (1999), 295-302.

VAN DER PLOEG I., *The Politics of Biometric Identification. Normative aspects of automated social categorization*, in *www.biteproject.org/documents/politics_of_biometric_identity%20.pdf*.

VECCHI P. M., *Commento art. 4, 1°comma, lett. b*, in BIANCA C. M., BUSNELLI F. D. (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, I, Padova, Cedam, 2007, 54-55.

VENUTI M. C., *Gli atti di disposizione del corpo*, Milano, Giuffrè, 2002.

VENUTI M. C., *Integrità della persona e multietnicità*, in *Familia*, 2003, 601-616.

VICIANI S., *Brevi osservazioni sul trattamento dei dati inerenti la salute e la vita sessuale in ambito sanitario*, in *Riv. crit. dir. priv.*, 2007, 315-323.

VICIANI S., *L'autodeterminazione "informata" del soggetto e gli interessi rilevanti (a proposito dell'informazione sul trattamento sanitario)*, in *Rass. dir. civ.*, 1996, 272-308.

VITALONE A., *Mutilazione genitale femminile e diritti umani*, in *Giur. merito*, 2001, 854-870.

WOODWARD J. D., ORLANS N. M., HIGGINGS P. T., *Identity Biometrics*, McGraw-Hill, 2003.

ZATTI P., *Dimensioni ed aspetti dell'identità nel diritto privato attuale*, in *Nuova giur. civ. comm.*, supplemento fasc. 4/2007, 1-9.

ZATTI P., *Il corpo e la nebulosa dell'appartenenza*, in *Nuova giur. civ. comm.*, 2007, II, 1-18.

ZATTI P., *Il diritto a scegliere la propria salute (in margine al caso S. Raffaele)*, in *Nuova giur. civ. comm.*, II, 2000, 1-12.

ZATTI P., *Verso un diritto per la bioetica: risorse e limiti del discorso giuridico*, in *Riv. dir. civ.*, 1995, I, 43-57.

ZEKOS G. I., *State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction*, in 15 *International Journal of Law and Information Technology* (2007), 1-37.

ZENO-ZENCOVICH V., voce «Identità personale», nel *Digesto IV ed., Disc. priv., sez. civ.*, IX, Utet, 1993, 294-303.

ZHANG D. D., *Automated biometrics. Technologies and systems*, Kluwer Academic Publishers, 2000.

ZOPPINI A., *Le "nuove proprietà" nella trasmissione ereditaria della ricchezza (note a margine della teoria dei beni)*, in *Riv. dir. civ.*, 2000, I, 185 ss.

ZORKADIS V., DONOS P., *On biometrics-based authentication and identification from a privacy-protection perspective. Deriving privacy-enhancing requirements*, in 12 *Information Management & Computer Security* (2004), 125-137.

ZWART H., *Medicine, Symbolization and the "Real" Body – Lacan's Understanding of Medical Science*, in 1 *Medicine, Health Care and Philosophy* (1998), 107-117.