Presidenza del Consiglio dei Ministri

L'IDENTIFICAZIONE DEL CORPO UMANO: PROFILI BIOETICI DELLA BIOMETRIA

26 novembre 2010

INDICE

Presentazione

Il documento affronta il tema della “biometria”, ossia delle nuove tecniche di identificazione o ‘misurazione’ dell’essere umano attraverso la rilevazione di determinate caratteristiche fisiche e comportamentali che vengono tradotte in sequenze matematiche e conservate in banche dati elettroniche. Il testo, a partire da una sintetica descrizione dello stato dell’arte sul piano scientifico e tecnologico, inquadra le problematiche sotto l’aspetto biogiuridico e bioetico, nell’ambito di una riflessione sul corpo e sulle esigenze di sicurezza e riservatezza.

Il CNB si sofferma sui vantaggi che l’impiego di queste nuove tecnologie offre per la tutela dell’ordine pubblico nell’ambito delle relazioni interpersonali e mette in luce i possibili rischi di un uso distorto e incontrollato, con particolare riferimento alla discriminazione, stigmatizzazione o all’emarginazione sociale. Il CNB esprime alcune raccomandazioni a tutela della persona (uso della biometria solo per ragioni di necessità e con proporzionalità, sempre con un consenso informato e riconoscendo il diritto di accesso ai dati e il c.d. ‘diritto di oblio’) e ai fini della regolazione delle applicazioni biometriche, a livello internazionale e nazionale.

Il documento è stato elaborato dai coordinatori del gruppo di lavoro, Proff. Salvatore Amato e Cinzia Caporale, con la collaborazione per gli aspetti tecnico - scientifici del Ing. Mario Savastano, primo ricercatore al CNR di Napoli ed esperto in questo settore. Al gruppo hanno partecipato i Proff. Luisella Battaglia, Riccardo Di Segni, Giancarlo Umani Ronchi, Monica Toraldo di Francia, Grazia Zuffa. Il documento è stato votato all’unanimità: hanno votato i Proff. Salvatore Amato, Luisella Battaglia, Adriano Bompiani, Stefano Canestrari, Cinzia Caporale, Antonio Da Re, Lorenzo d’Avack, Riccardo Di Segni, Emma Fattorini, Silvio Garattini, Marianna Gensabella, Claudia Mancina, Assunta Morresi, Demetrio Neri, Andrea Nicolussi, Laura Palazzani, Vittorio Possenti, Rodolfo Proietti, Lucetta Scaraffia, Monica Toraldo di Francia, Giancarlo Umani Ronchi. I Proff. Francesco D’Agostino e Romano Forleo assenti alla riunione plenaria hanno espresso successivamente la loro adesione.

Il Presidente
Prof. Francesco Paolo Casavola

1. Preambolo

L'identificazione degli esseri umani è un'esigenza cognitivamente e psicologicamente fondamentale che si è manifestata senza eccezioni in ogni società. Essa ha assunto una crescente importanza soprattutto alla luce delle esigenze di sicurezza nei rapporti interpersonali e nelle relazioni economiche, sollevate in maniera globale in tutti i Paesi e a tutti i livelli.

Al fine di automatizzare la procedure di identificazione o di verifica dell'identità, negli ultimi anni si è affermata una specifica disciplina tecnico-scientifica denominata "biometria" che si prefigge di raggiungere i suddetti scopi attraverso la valutazione di caratteristiche fisiche e/o comportamentali degli esseri umani[1], acquisite da sensori elettronici, elaborate da appositi algoritmi matematici e trasformate in modelli numerici. Le caratteristiche devono essere agevolmente misurabili, peculiari di una data persona, ovvero uniche e univoche a fronte di un'ampia variabilità nella popolazione, e devono rimanere quanto più possibile costanti nel tempo.

Lo sviluppo tecnologico ha reso i mezzi e gli strumenti di identificazione estremamente sofisticati, complessi ed efficienti, accrescendo le opportunità e i benefici, ma nello stesso tempo moltiplicando le occasioni di controllo sociale.

Il corpo ha assunto il ruolo di una vera e propria *password*[2], ovvero di un codice di riconoscimento vivente che si integra e interagisce col mondo delle macchine. L'unicità delle nostre caratteristiche individuali può infatti essere riconosciuta attraverso quel che *siamo* (volto, impronte digitali, DNA etc.), e quel che *facciamo* (voce, andatura, firma etc.). L'una e l'altra caratteristica possono inoltre essere associate a quel che *abbiamo* (passaporto, carte di credito, tessere etc.), o *conosciamo* (pin, codici di accesso etc.).

Nessuno di questi elementi di rilevazione costituisce isolatamente e di per sé un problema bioetico, ma in associazione tra loro e collegati sistematicamente e stabilmente attraverso reti informatiche, essi potrebbero condizionare profondamente i modi di apparire e di agire di ciascun individuo, se non addirittura divenire uno strumento di emarginazione e stigmatizzazione. Il riferimento è a possibili usi impropri o a veri e propri abusi in quanto la biometria interpreta il corpo umano come mera fonte di informazioni che possono essere trattate in maniera talora ignota ai diretti interessati, e questo per fini ulteriori rispetto a quelli dichiarati e da soggetti diversi e talora sconosciuti o non conoscibili dalla persona coinvolta. Il problema della tutela dell'identità individuale assume quindi profili che vanno ben al di là delle tradizionali soglie di rispetto della privacy, poiché concreto è il rischio di porre i processi di identificazione, e quindi di rilevanza sociale ed esistenziale, al di fuori del controllo degli individui.

In effetti, se in passato la biometria aveva un ruolo ben preciso e circoscritto all'ambito investigativo e giudiziario, nel contesto attuale i campi applicativi coinvolgono sfere sempre più ampie e rilevanti della vita di relazione: dall'accesso a determinati luoghi, al godimento di particolari servizi, alla

[1] Esistono applicazioni dedicate anche al riconoscimento biometrico degli animali.

[2] A. Davis, *The Body as Password*, On Newsstands Now, issue 5.07, July 1997 (Wired), reperibile (alla data del 21/11/10) all'indirizzo: http://www.wired.com/wired/archive/5.07/biometrics.html; A.K. Jain et al, *Biometrics: personal identification in networked society*, Kluwer Academic Publisher Group, 1998.

tracciabilità, con una progressione tecnologica esponenziale in molteplici campi (tutela della salute, prevenzione delle frodi sanitarie, protezione delle informazioni mediche riservate, monitoraggio dell'accesso ad aree riservate, efficienza nel commercio, sicurezza in campo finanziario e militare, controllo delle frontiere e dei flussi migratori etc.), e con un corrispondente ampliamento del mercato. Un ruolo aggiuntivo della biometria, attualmente marginale e comunque esterno alla definizione classica dell'ambito di applicazione di queste tecnologie, potrebbe configurarsi quale contributo alla diagnosi di malattie.

I vantaggi in tutti questi settori appaiono del tutto evidenti poiché i dati biometrici sono più difficili da falsificare, più semplici da usare ed è impossibile dimenticarli o perderli. L'utente ha quindi tutto l'interesse a un progressivo incremento dell'uso della biometria, pretendendo però allo stesso tempo, anche in termini di innovazione scientifica e tecnologica, modalità di registrazione dei dati biometrici affidabili (*accountability*), e sistemi di gestione dei dati trasparenti, garantiti ed efficienti (*reliability*).

L'istanza sociale di *accountability* e *reliability* è strettamente connessa ai problemi di *governance* relativamente alla gestione e al controllo dell'insieme dei dati raccolti a livello nazionale e internazionale. La naturale fluidità ed extraterritorialità delle informazioni modifica infatti radicalmente le garanzie offerte dalle tradizionali forme di tutela amministrativa e giudiziaria riguardo alla salvaguardia delle libertà personali e della riservatezza, ponendo interrogativi tanto più pressanti quanto più è rapida la circolazione delle informazioni e l'intensità degli scambi.

Esiste poi un diffuso timore che un sistema di identificazione sempre più sistematico, automatico e pervasivo possa condizionare i comportamenti: l'individuo corre il rischio di assumere rilevanza sociale solo per le tracce che lascia. Soprattutto, per la quantità e manipolabilità di queste tracce, e per la loro "portabilità" in forma di stringa matematica. Inoltre, se è possibile sostituire una carta di credito o chiedere la correzione di un dato errato nella carta di identità con una relativa facilità, non è altrettanto facile disfarsi di un algoritmo che rappresenta il corpo ed è contenuto in molteplici archivi elettronici. Inoltre, non solo i dati fisici possono essere acquisiti stabilmente, ma essi possono essere anche collegati con i dati personali relativi ad esempio alle condizioni di salute, ai gusti, alle abitudini, e ciò per finalità pubbliche o private, sociali o individuali, spesso misconosciute e in assenza di un esplicito consenso. Emerge cioè la praticabilità tecnica di nuove e sottili forme di controllo e quindi, per certi aspetti, anche di condizionamento della personalità, almeno nella misura in cui si affermasse un dovere di "permanenza" in un sistema biometrico complessivo e una responsabilità personale di "manutenzione" dei dati biometrici (punto 4.2).

La riflessione bioetica si trova dunque di fronte una tecnologia di fondamentale importanza per la qualità della vita delle persone e per la stabilità e sicurezza delle relazioni economiche e sociopolitiche, ma non può evitare di interrogarsi sul modo in cui questa tecnologia incide sull'esplicazione delle sfere di autonomia e riduce le zone di non interferenza. Una società che è in grado di registrare e memorizzare gran parte dei comportamenti individuali e delle scelte che gli individui fanno ogni giorno potrebbe smarrire i corretti equilibri tra libertà e sicurezza. Se la certezza e la sicurezza, che le rilevazioni biometriche intensificano e perfezionano, sono gli elementi fondamentali per l'esercizio della libertà e di alcuni diritti fondamentali, il controllo sistematico e

costante di un numero sempre più ampio e indeterminato di comportamenti potrebbe infatti costituire una forma discreta, ma non per questo meno insidiosa, di biosorveglianza, fino a imporre, per essere accettati socialmente, l'assunzione "obbligata" di un'identità. Quanto è auspicabile la costruzione di un mondo senza oblio? Un mondo in cui ciascuno ha valore anche in base alla quantità di "tracce" che affida stabilmente e definitivamente agli algoritmi dei meccanismi biometrici?

L'identità come diritto individuale posto a garanzia dell'esercizio delle libertà fondamentali verrà progressivamente eroso dai crescenti doveri di identificazione? Esiste un diritto all'*anonimato biometrico*? Fino a che punto si può garantire il segreto relativamente all'identità personale?

2. Note introduttive e status del dato biometrico

2.1. Tassonomia generale

La caratteristica biometrica rappresenta la caratteristica biologica o comportamentale di un individuo dalla quale possono essere estratte le informazioni che saranno utilizzate per il riconoscimento biometrico.

Le proprietà essenziali che una caratteristica biometrica dovrebbe possedere ai fini di un'autenticazione biometrica sono:

- *universalità*: tutti gli individui devono possederla;
- *unicità*: l'elemento di riferimento biometrico deve consentire di distinguere, nella maggior misura possibile, ogni singolo individuo da tutti gli altri;
- *permanenza*: l'elemento utilizzato per l'analisi biometrica deve garantire nel tempo un determinato livello di riconoscibilità;
- *collezionabilità*: la caratteristica biometrica deve essere misurabile quantitativamente e inseribile in un sistema stabile di rilevazione.

Partendo dall'assunto che 1) ogni processo biometrico inizia con l'iscrizione del soggetto interessato nel sistema e che 2) dalle sue caratteristiche biometriche viene generato un modello matematico detto *template*, per le tecnologie biometriche si distinguono due modalità operative che hanno una valenza del tutto diversa sia dal punto di vista tecnologico sia legale:

A. in modalità "Identificazione" si tenta di attribuire un'identità a un dato soggetto attraverso un raffronto di tipo "uno-a-molti" tra il *template* della caratteristica biometrica di quel soggetto, generato al momento della transazione, e tutti i *template* presenti in un dato archivio e relativi a un insieme di soggetti. Generalmente, a ogni *template* contenuto nell'archivio corrisponde un'identità e quindi la scoperta del *template* che, all'interno di una fascia di tolleranza, presenta la più alta similarità, equivale all'identificazione del soggetto. Anche se i dati biometrici di quel soggetto non fossero contenuti nell'archivio, questo sarebbe comunque di una qualche utilità potendosi escludere con ragionevole margine di errore che quel soggetto appartenga a quello specifico insieme;

B. in modalità "Verifica di Identità" si tenta di accertare se un soggetto è effettivamente chi dichiara di essere. Il procedimento consiste in un raffronto di

tipo “uno-a-uno” tra il *template* della caratteristica biometrica di quel soggetto, generato al momento della transazione e uno specifico *template* presente in un dato archivio. Ad esempio, attraverso la digitazione di un pin, il soggetto indica al sistema il *template* già presente nell’archivio con il quale effettuare la comparazione che porterà a verificare o meno se il soggetto sia effettivamente chi dichiara di essere. La modalità “Verifica di Identità” può anche espletarsi direttamente attraverso la comparazione del *template* generato al momento della transazione con quello conservato in una carta elettronica in possesso del soggetto interessato, a tutto vantaggio di un incremento del livello di protezione dei dati personali non dovendo il soggetto depositare il *template* relativo alla sua caratteristica biometrica in un archivio.

Altre distinzioni che si operano comunemente nel contesto biometrico, con forti ricadute dal punto di vista etico e legale, classificano i contesti applicativi in[3]:

- *manifesti od occulti*: a seconda che l’utente sia o meno al corrente di essere sottoposto a un sistema di identificazione biometrica (la maggior parte delle applicazioni sono manifeste, mentre possono essere occulte alcune applicazioni legate alle investigazioni di polizia o al mantenimento dell’ordine pubblico);
- *caratterizzati da utenti abituati all’utilizzo di tecnologie biometriche o meno*: a seconda che la popolazione degli utenti abbia o non abbia esperienza nell’uso dei sistemi biometrici;
- *presidiati o meno*: a seconda che il sistema biometrico sia o non sia presidiato, supervisionato o assistito da un operatore;
- *in condizioni ambientali standard o meno:* a seconda che il sistema si trovi o non si trovi a operare in condizioni ambientali standard (ovvero con valori di temperatura, umidità e soprattutto illuminazione che ricadono in un determinato intervallo di tolleranza);
- *pubblici o privati*: a seconda che gli utenti del sistema si trovino in ambiti pubblici (ad es. un controllo automatico di frontiera) oppure privati (ad es. accesso alla propria abitazione);
- a*perti o chiusi*: a seconda che i dati biometrici acquisiti risiedano unicamente nel luogo logico o geografico dell’applicazione o che possano essere esportati per altre applicazioni.

Ulteriori classificazioni prevedono anche: (a) la distinzione tra applicazioni *cooperative* o *non cooperative*, a seconda che siano o non siano necessari il consenso e la collaborazione dello stesso soggetto per realizzare la procedura di autenticazione/identificazione; (b) la distinzione tra identificazione biometrica *positiva*, in cui il soggetto fornisce la prova biometrica di effettivamente appartenere a un dato insieme (ad es.: di appartenere al gruppo di coloro che deve riscuotere la pensione), e *negativa*, in cui il soggetto afferma in base alle proprie credenziali biometriche di *non* appartenere a un dato insieme (ad es.: di non essere tra coloro che hanno già riscosso la pensione).

Infine, alcuni esperti distinguono tra le tecnologie biometriche che permettono sia l’identificazione sia la verifica di identità, e altre che permettono la sola verifica dell’identità, come ad esempio quella basata sul riconoscimento

[3] J.Wayman at al, *Biometric Systems, Technology, Design and Performance Evaluation*, Springer, 2004.

della geometria della mano. La differenza sta soprattutto nella capacità intrinseca della caratteristica biometrica presa in esame di distinguere tra gli utenti. I parametri misurati relativamente alla geometria della mano non variano in modo significativo nella popolazione: ciò implica l'impossibilità di effettuare un'identificazione, ma non preclude processi di verifica (anzi, si tratta del metodo elettivo per effettuare le verifiche).

2.2. Fasi di un processo biometrico e potenziali errori

In linea generale, le fasi di un processo biometrico sono le seguenti[4]:

- *acquisizione della caratteristica biometrica*: in questa fase l'utente presenta al sistema le proprie credenziali biometriche (ovvero le proprie caratteristiche biometriche) attraverso un *sensore*;
- *trasmissione dei dati:* i dati acquisiti vengono trasmessi dal sensore ad altre parti del sistema biometrico per le successive elaborazioni; il sensore potrebbe trovarsi in prossimità oppure a una certa distanza dal resto del sistema ed è importante valutare questo parametro sia in funzione dei rischi di vulnerabilità del sistema (cattura indebita di dati lungo il percorso), sia per il possibile degrado della qualità dell'informazione;
- *elaborazione dei dati*: in questa fase i dati vengono preparati per le successive fasi del processo biometrico; un'operazione cruciale che viene espletata in questa fase è quella della generazione del *template*, ovvero del modello matematico corrispondente al dato biometrico acquisito;
- *memorizzazione del template*: in fase di iscrizione nel sistema (*enrollment*), i *template* vengono memorizzati all'interno del sistema per le successive attività di raffronto dei dati*;*
- *comparazione*: il *template* presentato al momento della transazione viene confrontato, in termini di misura di similarità, con uno (modalità Verifica) o più (modalità Identificazione) *template* memorizzati;
- *validazione / matchin*g: in funzione del superamento di una soglia prestabilita, il sistema può validare una "Verifica di Identità" oppure, in modalità Identificazione, generare una lista di possibili candidati caratterizzati da un punteggio di "accoppiamento" (*matching*); il sistema attribuisce alla persona oggetto della transazione l'identità del candidato con il migliore punteggio di "accoppiamento".

Le prestazioni di un sistema biometrico si valutano su base statistica e sono funzione di innumerevoli parametri. Come qualsiasi sistema statistico di comparazione, l'identificazione biometria presenta dei margini di errore la cui entità varia a seconda del tipo di caratteristica biometrica utilizzata[5]. Sostanzialmente, i cambiamenti delle condizioni ambientali e di registrazione e acquisizione dei dati, così come i cambiamenti fisici (temporanei o permanenti) o il tempo intercorrente tra l'*enrollment* e la transazione biometrica, giocano un ruolo fondamentale riducendo le possibilità di riconoscimento.

Alcuni importanti parametri che misurano l'accuratezza di un sistema

[4] Idem.

[5] Ad esempio, gli errori compiuti da un sistema per il riconoscimento del volto sono generalmente maggiori di quelli riscontrabili in sistemi basati sul riconoscimento delle impronte digitali o dell'iride.

biometrico sono[6]:

- FAR (*False Acceptance Rate*): tasso di falsa accettazione che denota il numero di volte che un sistema fornisce un'indicazione inappropriata di superamento della soglia di "similarità" tra il dato acquisito e i dati archiviati; in un sistema con un alto valore di FAR, aumenta la possibilità di consentire l'accesso a un luogo oppure a un servizio da parte di un impostore;
- FRR (*False Rejection Rate*): tasso di falso rigetto che denota il numero di volte che il sistema fornisce un'indicazione inappropriata di non superamento della soglia di "similarità" tra il dato acquisito e i dati archiviati; in un sistema con un alto valore di FRR, aumenta la possibilità di negare erroneamente l'accesso a un luogo oppure a un servizio a un utente che invece è regolarmente autorizzato[7];
- ERR (*EER, Equal Error Rate*): i valori di FAR e FRR descrivono due curve in funzione del valore di soglia del sistema biometrico. Il punto di intersezione tra le curve del FAR e FRR (in cui i due tassi di errore assumono lo stesso valore) fornisce il valore di EER che, essendo sostanzialmente una misura dell'accuratezza globale di un sistema biometrico, può essere di grande aiuto nel determinare quale sistema sia più appropriato in un determinato scenario.

Ai fini operativi, è evidente che per ottenere alti livelli di sicurezza nelle applicazioni è necessario perseguire un basso livello di FAR (in questo caso, infatti, la priorità è che il sistema non accetti impropriamente soggetti non autorizzati). Tuttavia, fissando una soglia severa di accettazione delle credenziali biometriche, si potrà verificare un tasso di rigetto significativo (molti soggetti potrebbero cioè essere esclusi dall'accesso a un luogo o a un servizio). Analogamente, nel caso in cui fosse imperativo un tasso di rigetto (FRR) minore possibile, ad esempio per favorire l'accesso rapido di un grande numero di utenti, il sistema dovrebbe essere predisposto in modo da ridurre sensibilmente la soglia di accettazione. Naturalmente, però, ciò comporterebbe un aumento del tasso di accettazione indebita (FAR) e un conseguente decremento del livello di sicurezza.

Come si evince chiaramente, la ricerca del valore di soglia ottimale che permetta un efficace equilibrio tra FAR e FRR, rappresenta una delle difficoltà maggiori che incontrano i gestori di sistemi di autenticazione basati sulle tecnologie biometriche.

Infine, nel descrivere sommariamente i parametri che caratterizzano i sistemi biometrici, occorre tenere conto che una frazione degli utenti potrebbero non riuscire a registrarsi in un dato sistema biometrico oppure, anche se registrati, potrebbero successivamente non riuscire a eseguire una transazione biometrica. Il *Failure To Enroll Rate - FTER* e il *Failure To Acquire Rate - FTAR* corrispondono rispettivamente a queste due eventualità e sono

[6] Cfr. ad esempio: *Encyclopedia of Biometrics*, S.Z.Li editor, A.K.Jain Editorial Advisor, Springer Science+Business Media LLC, 2009; R. Bolle et al., *Guide to Biometrics*, Springer-Verlag New York Inc., 2004; A. J. Mansfield, J. L. Wayman, *Best Practices in Testing and Reporting Performance of Biometric Devices*, Version 2.01, August 2002, reperibile (in data 21/11/2010) all'indirizzo: www.cesg.gov.uk/policy_technologies/biometrics/media/bestpractice.pdf.

[7] Nella pratica, questa tipologia di errore è la più frequente e purtroppo genera frustrazione e diffidenza verso le tecnologie biometriche da parte degli utenti.

strettamente connessi ai concetti di accessibilità e usabilità dei sistemi biometrici che, come sarà messo in evidenza nel prosieguo del Documento, rappresentano due elementi fondamentali nella valutazione complessiva di un sistema biometrico.

2.3. Le tecnologie biometriche più diffuse

Le più comuni tecnologie biometriche sono basate sul riconoscimento di:

- impronte digitali;
- caratteristiche del volto;
- geometrie della mano;
- struttura vascolare del palmo e del dorso della mano;
- caratteristiche della voce;
- caratteristiche dell'iride;
- struttura vascolare della retina;
- dinamica di apposizione della firma;
- dinamica della digitazione;
- DNA[8].

A livello di ricerca, sono in fase di studio diverse altre tecnologie biometriche. Ad esempio, sono in corso di verifica le potenzialità offerte dai sistemi basati sul riconoscimento morfologico dell'orecchio e, nel contesto della valutazione delle caratteristiche biometriche comportamentali, i sistemi per il riconoscimento dell'andatura (*gait*).

3. Il contesto disciplinare delle tecnologie biometriche

Lo studio delle tecnologie biometriche implica conoscenze interdisciplinari che possono essere raccolte, in termini assolutamente generali, nella lista che segue:

- Elettronica;
- Informatica;
- Statistica;
- Medicina;
- Psicologia;
- Etica;
- Diritto.

Come si evince dall'elenco, molte delle aree disciplinari enumerate non rientrano in una dimensione prettamente "tecnica". Il loro apporto diventa molto significativo quando le applicazioni biometriche passano da una fase

[8] L'analisi del DNA è stata recentemente ammessa tra le tecnologie biometriche che sono all'attenzione del sub-comitato di standardizzazione ISO (ISO/IEC JTC1 SC 37 "Biometrics") anche se, a differenza di quanto avviene per tutte le altre tecnologie biometriche, almeno per il momento l'analisi del DNA non permette un'autenticazione in tempo reale. Quest'ultimo criterio non è tuttavia contemplato nella canonica definizione di tecnologie biometriche e quindi non impedisce di annoverare l'analisi del DNA tra di esse.

sperimentale di laboratorio all'implementazione in reali condizioni di esercizio. Tutte le esperienze maturate a livello internazionale hanno peraltro messo chiaramente in evidenza i pericoli derivanti da una scarsa considerazione degli aspetti medici, psicologici, etico-sociali e giuridici della biometria.

3.1. Profili biogiuridici delle tecnologie biometriche

Partendo dal presupposto che 1) il contesto delle applicazioni biometriche è ragionevolmente vasto, 2) esistono opinioni sostanzialmente differenti sull'applicabilità di sistemi biometrici a seconda del contesto sociale e geopolitico e 3) la normativa soprattutto in tema di protezione dei dati personali è continuamente in evoluzione, si può affermare che alcuni parametri di massima, legati strettamente al contesto giuridico della tutela delle libertà fondamentali, regolano l'applicabilità dei sistemi biometrici. Innanzitutto va ricordato che l'art. 10 della Convenzione sui diritti dell'uomo e sulla biomedicina include il rispetto della dimensione privata in relazione alle informazioni sanitarie (art. 10). Inoltre, la Carta dei diritti fondamentali dell'Unione europea, all'art. 8 (*Protezione di dati di carattere personale*) indica chiaramente alcune fondamentali linee di condotta in base alle quali "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati 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. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

Dinanzi a questo orizzonte ancora in via di definizione, la giurisprudenza ha elaborato un contesto complessivo di liceità attorno all'esigenza di garantire il diritto alla riservatezza attraverso il rispetto di alcuni valori fondamentali alla luce degli artt. 3 e 11 del Codice in materia di protezione dei dati personali (D.Lgs. 30 giugno 2003, n. 196), oltre che dell' art. 6 della direttiva n. 95/46/CE:

- *proporzionalità*: il contesto dell'applicazione biometrica dovrebbe essere caratterizzato da un'adeguata ponderazione del rapporto tra sacrifici imposti alla libertà personale e sussistenza di specifiche esigenze di sicurezza. In generale, la prevenzione di condizioni di potenziale pericolo, sia per i singoli sia per la collettività, è stata considerata come fattore sufficiente per l'implementazione di un sistema biometrico qualora non fosse possibile conseguire in altro modo e con la stessa efficienza i medesimi risultati. In altri termini, il principio di proporzionalità è un principio basilare nella legislazione comunitaria ed è sottolineato da numerosi documenti normativi. Viene quindi considerato un fattore decisivo nelle scelte inerenti l'applicabilità dei sistemi biometrici, operate dalle varie autorità nazionali delegate alla protezione di dati;
- *necessità*: il contesto in cui si implementa l'applicazione biometrica non permette il ricorso ad altri tipi di tecnologia meno invasive e altrettanto sensibili, che siano in grado di ottenere gli stessi risultati offerti dalle tecnologie biometriche.

Proporzionalità e *necessità* vanno valutate in relazione alle *finalità* perseguite, con particolare riferimento al contesto in cui i dati sono assunti e trattati, e al rapporto di *pertinenza* tra fini e mezzi.

Va tenuto presente che il rispetto dell'identità costituisce uno dei diritti fondamentali dell'uomo. All'identità si collegano la dignità e l'integrità personale. L'una e l'altra presuppongono che a ciascun individuo corrisponda una

particolare singolarità di cui il diritto deve non solo tener conto, ma consentire l'espressione più ampia nella varietà dei contesti esistenziali. Citando Paul Ricouer, il parere n. 98 del 26 aprile 2007 del *Comité Consultatif National d'Ethique pour les Sciences de la Vie et de la Santé* in tema di "*Biométrie, données identifiantes et droits de l'homme*" ricorda che l'identità è costituita da due elementi inseparabili: l'esteriorità del corpo, «mêmeté », con cui entriamo fisicamente a contatto con gli altri e con il mondo che ci circonda, e la dimensione interiore e biografica, «ipséité», che esprime i nostri valori più profondi, quelli che danno un senso alla vita e attorno ai quali si costruisce la libertà. Il CNB concorda con questa prospettiva. Se l'esperienza giuridica si fonda sulla rilevazione e sulla tutela dell'immediatezza del dato fisico, è per consentire all'elemento impalpabile dell'interiorità di esprimersi e realizzarsi. Quindi, oltre agli evidenti vantaggi per la sicurezza sociale, ogni perfezionamento degli strumenti di identificazione costituisce in astratto anche un aumento delle possibilità di godere dei diritti fondamentali e di ottenere la tutela delle proprie posizioni soggettive: dalla necessità di accedere e utilizzare il proprio conto corrente, la propria auto, il proprio biglietto aereo, alla possibilità di dimostrare la propria estraneità o la propria partecipazione a un determinato evento. Non va neppure trascurato che, sotto alcuni punti di vista, i dati biometrici potrebbero evitare la necessità di comunicare quelle informazioni estremamente personali previste dagli attuali documenti identificativi (ad es.: luogo e data di nascita, sesso, stato civile etc.), oppure, in altro ambito, i propri dati sanitari (ad es.: patologie infettive), migliorando quindi il grado di riservatezza dei soggetti coinvolti.

Esiste tuttavia il non trascurabile rischio che, sotto altri aspetti, il dato biometrico riveli un'informazione in eccesso e venga impiegato per scopi che vanno oltre le finalità previste di autenticazione, dando luogo a uno specifico fenomeno che in gergo viene definito *function-creep*, ovvero "incrocio indebito dei dati"[9] o espansione indebita dell'utilizzo dei dati. Ad esempio: il DNA, oltre all'identità genetica, consente di acquisire informazioni sulla predisposizione a contrarre malattie e in generale sul fenotipo individuale; il metodo del riconoscimento della retina, parte dell'occhio caratterizzata da una forte vascolarizzazione, può segnalare la presenza di ipertensione o diabete; l'analisi dell'iride può evidenziare l'uso di alcool o di sostanze stupefacenti; la temperatura o alcune caratteristiche di zone del volto possono rilevare particolari condizioni psico-fisiche anche patologiche. È possibile che, all'insaputa o finanche contro la volontà del soggetto, questi dati vengano acquisiti e poi divulgati. Ciò può determinare una circolazione distorta delle informazioni che, in casi estremi, potrebbe dar luogo a inquietanti scenari potenzialmente incontrollati.

Un'ulteriore fonte di preoccupazione è rappresentata dalla possibile aggregazione dei dati. Attraverso la sovrapposizione dei dati biometrici con altre informazioni (ad esempio mediche, finanziarie o comportamentali) è possibile immaginare un uso centralizzato e combinato di essi ai fini della cosiddetta profilazione o *profiling*. La profilazione si può definire come l'azione o il processo con cui un individuo diviene oggetto di particolari attenzioni sulla

[9] CE – Gruppo di Lavoro per la Tutela delle Persone riguardo al Trattamento dei Dati Personali, Parere 3/2005 riguardante l'attuazione del regolamento CE n. 2252/2004 del Consiglio (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 - WP112 (Gazzetta ufficiale L 385 del 29.12.2004, pp. 1-6), adottato il 30 settembre 2005.

base dell'osservazione di specifiche caratteristiche o comportamenti in base ai quali, estrapolando le informazioni che lo riguardano (*knowledge discovery in data base, data mining*), si creano diversi profili di attenzione o sospetto.

La profilazione è una delle tecniche più usate ad esempio per combattere il terrorismo e implica, senza controllo giudiziale, il collocamento di determinati soggetti, in base a dati raccolti a loro insaputa, in specifiche categorie di rischio, precludendo loro la possibilità di entrare in determinati paesi o di godere di determinati servizi. Queste schedature preventive e informali hanno sempre e utilmente fatto parte della prassi operativa degli apparati di polizia[10]. Ora però la tecnologia aumenta le possibilità di biosorveglianza fino a poter costituire, se applicata in maniera capillare e indiscriminata, un'inversione dell'onere della prova per cui la presunzione di innocenza, fondamento della tutela della libertà individuale e dello Stato di diritto, si potrebbe trasformare in una forma di presunzione di colpevolezza. In casi estremi, un soggetto potrebbe trovarsi costretto, senza aver commesso alcuno specifico reato, a dover giustificare l'insieme delle sue condotte per dimostrare che non rappresenta un pericolo. Ma è possibile anche ipotizzare eventuali discriminazioni nell'accesso ai posti di lavoro e in molte altre sfere della vita economica e sociale.

Andrebbero quindi messi in giusta evidenza i rischi della profilatura, vietando l'incrocio dei dati suscettibili di stigmatizzazione o emarginazione e consentendone l'utilizzazione solo in casi rilevanti, legalmente predeterminati, con adeguate forme di tutela e controllo da parte di organi di cui sia garantita la terzietà. Sotto questo punto di vista, sarebbe anche importante prevedere un diritto di accesso, tendenzialmente incondizionato, che consenta a ciascun soggetto interessato di conoscere quali dati siano raccolti sul suo conto, da chi, per quali finalità, da quanto tempo e per quanto tempo.

Va, infatti, tenuto presente che l'istituzione di archivi per conservare stabilmente alcuni dati personali di particolare importanza (ad es. i registri dello stato civile o i casellari giudiziali) è stato un compito esclusivo dello Stato, rigidamente regolamentato e finalizzato a garantire la certezza dei rapporti e la pubblica sicurezza. Oggi, la facilità nei processi di archiviazione informatica moltiplica le possibilità tecniche, assolutamente eterogenee e non codificate, di costruire banche dati private. Rimane il primato pubblico nell'accertamento dell'identità legato al dovere di garantire la sicurezza, ma a questo primato non corrisponde più un monopolio sulle informazioni personali, anzi le banche dati private (nell'accezione più vasta del termine), eccedono ormai di gran lunga, per quantità e qualità, le banche pubbliche. Si verifica inoltre una costante commistione di pubblico e privato: lo Stato assume informazioni tendenzialmente private (ad es.: salute, condizioni finanziarie etc.), e il privato assume informazioni a rilevanza pubblica (ad es.: l'identità necessaria per viaggiare, per effettuare transazioni commerciali etc.).

Tutto ciò, per certi versi, rende sempre più complessa la possibilità da parte del cittadino di verificare e controllare il rispetto delle norme di tutela (a volte questo controllo ha carattere amministrativo, a volte contrattuale, a volte

[10] In senso stretto, le origini della tecnica investigativa del *profiling* vengono fatte risalire agli anni Cinquanta, quando la polizia di New York fece ricorso alla psichiatria per mettere assieme indizi eterogenei finalizzati a ricostruire il profilo del possibile responsabile di una serie di attentati. Ma già nel 1879 Alphonse Bertillon, un celeberrimo ispettore della polizia francese, aveva proposto un sistema di misurazioni anatomiche (tra cui la lunghezza di braccia e piedi) per identificare e schedare i criminali recidivi.

non è né l'uno né l'altro). Per altri versi, l'uso generalizzato, pubblico e privato, delle tecnologie biometriche e delle associate possibili profilazioni, nonché la diffusione estrema di archivi, potrebbero rendere la popolazione insensibile ai rischi connessi alla tutela della propria riservatezza, creando un senso di impotenza e di indifferenza in cui è più facile il progressivo radicarsi di una società della biosorveglianza caratterizzata da una pericolosa rassegnazione alla confusione tra persona fisica e persona virtuale.

3.2. Profili bioetici essenziali

3.2.1. Il corpo umano come password

Nelle tecnologie biometriche il corpo diventa un vero e proprio strumento di riconoscimento e pertanto, per garantire l'autenticazione occorrono nuovi e specifici accorgimenti. In termini generali, la caratteristica fisica o comportamentale adoperata per il riconoscimento e utilizzata al momento della prima registrazione nel sistema dovrebbe risultare per quanto possibile simile a quella acquisita al momento della transazione biometrica effettiva.

L'obbligazione tecnica si traduce, nella pratica, in azioni solo apparentemente semplici. Ad esempio, è necessario che nei documenti biometrici l'espressione del viso assunta nelle fotografie di riferimento e riproposta al momento della transazione sia per quanto possibile neutra e pertanto più facilmente riproducibile. In tal senso, esistono già apposite linee guida e tabelle esplicative, preparate dalle organizzazioni preposte alla standardizzazione dei dati, per fornire precise indicazioni sull'espressione del viso da assumere sia nella fase di registrazione nel sistema biometrico sia in quello dell'autenticazione. Alla luce delle tendenze emerse nei Paesi più avanzati tecnologicamente, tali istruzioni dovrebbero essere estese anche ai minori che in tal modo verrebbero assimilati completamente al mondo degli adulti. Ancora, i polpastrelli delle dita, attraverso il cui essudato vengono raccolte le impronte digitali, non si dovrebbero danneggiare nel corso della vita, ad esempio a causa del contatto delle mani con acidi corrosivi. Allo stesso modo, se la caratteristica biometrica fosse l'iride, nel caso di operazioni di cataratta che ne dovessero alterare la morfologia, l'utente che volesse conservare con sicurezza la propria 'biometricità' dovrebbe registrarsi di nuovo nel sistema a causa della possibile alterazione delle caratteristiche morfologiche dell'iride.

È evidente che le esigenze del riconoscimento possono avere profonde implicazioni nel contesto della vita sociale, imponendo nuove regole di condotta suscettibili di assumere profonde implicazioni bioetiche. Si sta affermando l'idea che, per motivi di sicurezza e di certezza dei rapporti, sia necessario introdurre una sorta di dovere di *permanenza* e di *manutenzione* biometriche del proprio corpo che non ha precedenti nella storia della cultura e dell'esperienza giuridica (vedi par. 4.4.). Le regole attualmente in vigore nel contesto delle libertà fondamentali consentono al singolo individuo adulto e in parte anche ai minori di disporre a piacimento del proprio aspetto esteriore e di non doversi preoccupare particolarmente se i propri polpastrelli si alterano o se il proprio viso viene riplasmato dalla chirurgia estetica. L'alterazione del corpo costituisce una manifestazione atavica della libertà personale sulla base di tendenze di tipo sociale, etnico, religioso oppure anche soltanto estetico o ludico. Ciò riguarda sia le modifiche esteriori non permanenti (alterazioni di tipo

cosmetico, ornamenti etc.) sia quelle permanenti (tatuaggi, piercing, chirurgia etc.).

In futuro queste abitudini potrebbero subire un drastico ridimensionamento, anche semplicemente volontario, per evitare di dover ricostruire la propria identità sociale ogni volta che le proprie credenziali biometriche risultassero inattendibili, proprio come accade se si presenta un documento cartaceo usurato o alterato. Il modo di apparire potrebbe quindi diventare prevalente sul modo di essere, sul modo in cui ciascun individuo plasma la propria immagine unica in relazione alle esigenze più profonde della propria personalità. L'immagine, da simbolo dell'identità personale, da strumento con cui ciascuno decide di offrirsi allo sguardo altrui e di comunicare qualcosa di sé agli altri, si potrebbe trasformare in un puro vincolo, nello strumento con cui vengono imposti i processi di identificazione.

Risultano a questo punto evidenti, al di là degli aspetti normativi o in generale coercitivi, le profonde influenze psicosociali che comunque la biometria avrà nel prossimo futuro, compresa la possibile sensazione di incertezza rispetto all'immagine di sé e alla propria capacità di venire riconosciuti dai sistemi biometrici.

3.2.2. Modificazioni volontarie di carattere non permanente

Le modificazioni volontarie di carattere non permanente del proprio aspetto sono genericamente di competenza delle tecnologie biometriche basate sul riconoscimento del volto. In questa categoria possono essere collocate tutte le modificazioni di carattere reversibile che vanno dalla cosmetica all'uso di ornamenti, fino ad arrivare alla modifica naturale di tipo tricologico del proprio viso.

Purtroppo non sono completamente noti gli effetti di questo cambiamento per ciò che attiene all'accuratezza del riconoscimento del volto. Ciò che è stato maggiormente studiato è il problema posto dall'uso di occhiali: mentre per quelli da vista non sembrano sussistere particolari difficoltà a patto che la lente non provochi una magnificazione considerevole della zona periorbitale, l'uso di alcuni tipi degli occhiali da sole può ancora porre serie pregiudiziali al successo della transazione biometrica anche se sono in fase sperimentale avanzata alcune tecnologie che riducono, fino ad annullarla, l'influenza che essi esercitano sull'accuratezza del riconoscimento biometrico.

3.2.3. Modificazioni volontarie di carattere permanente

L'uso sempre più intenso delle tecnologie biometriche a fini investigativi o giudiziari sta provocando il crescente problema delle alterazioni volontarie permanenti delle proprie caratteristiche biometriche, sia a fini estetici sia per evitare in modo deliberato una possibile identificazione. Ad oggi, tale fenomeno interessa in particolar modo il comparto biometrico del riconoscimento delle impronte digitali che possono essere danneggiate intenzionalmente fino al punto di rendere un soggetto totalmente non identificabile. In generale, questo problema va analizzato anche allo scopo di prevenire abusi e reati che potrebbero essere perpetrati anche su terze persone (talvolta persino sui minori).

3.2.4. Il dovere della conservazione delle caratteristiche biometriche

Come attualmente succede di prassi per i tradizionali documenti cartacei

che in caso di deterioramento possono essere rifiutati come documento di identificazione, così, in un futuro regolato in maniera sempre più estesa da transazioni di tipo biometrico, un danneggiamento delle proprie caratteristiche biometriche, ad esempio un'usura atipica dei polpastrelli con conseguente difficoltà nel rilascio delle impronte digitali, potrebbe avere effetti importanti dal punto di vista del riconoscimento. In taluni casi, analogamente a quanto accade nel caso dei documenti deteriorati, una caratteristica biometrica deteriorata potrebbe portare a un diniego alla transazione da parte dei soggetti addetti al controllo o da parte del sistema stesso.

Andrebbe a questo punto messo nella giusta evidenza il limite delle tecnologie biometriche nei confronti delle tradizionali modalità di riconoscimento. Mentre è infatti possibile la riemissione di un documento di identità analogo a quello deteriorato e formalmente corretto, nel caso delle caratteristiche biometriche, l'elemento fisico, una volta alterato, potrebbe non essere mai più adatto a un riconoscimento. Si creerebbe così una sorta di *incapace biometrico* per quella data caratteristica fisica.

3.2.5. Diritto all'anonimato

Dal momento che la biometria opera, per definizione, mediante l'attribuzione di un'identità o una verifica della stessa, si prospettano certamente interferenze con i sistemi sociali di sicurezza. La preservazione della sfera personale come elemento intimo fondamentale implica l'esistenza di un diritto all'anonimato o quanto meno di ampie sfere sottratte al controllo altrui. La riservatezza non può, tuttavia, giustificare un diritto assoluto di non interferenza tutte le volte in cui qualcuno è esposto al pubblico o assume un comportamento che coinvolge la relazione tra più soggetti. In altre parole, non esiste un diritto assoluto all'anonimato che tuttavia in molte diverse circostanze è garantito. In quali casi ciò sia desiderabile è oggetto di discussione e tuttavia le tecnologie biometriche potrebbero attenuare tale libertà.

Un chiaro esempio della sensibilità dell'argomento può essere fornito dagli accesi scambi di vedute in Paesi che stanno programmando la realizzazione di documenti di identità basati su identificatori di tipo biometrico. Il processo implica infatti necessariamente la realizzazione di registri nazionali delle identità e alcuni osservatori, nonché parti dell'opinione pubblica, vedono in ciò un grave attentato per le libertà personali e per l'anonimato. Il rischio aumenta ulteriormente per effetto della potenziale applicazione delle tecniche di *profiling* che si diffonde in maniera crescente.

3.2.6. Discriminazione di alcune fasce della popolazione

Un importante aspetto della biometria con chiare implicazioni di carattere etico è dato dalla possibile discriminazione di alcune fasce della popolazione di utenti. Oltre ovviamente ai portatori di handicap per i quali l'uso delle tecnologie biometriche è comunque, in termini generali, più complesso e necessita di particolari accorgimenti, si parla sempre più apertamente di *disabilità biometrica* e cioè della difficoltà se non impossibilità a usare tecnologie biometriche che si riscontra per determinate categorie di utenti.

È noto infatti che, come per altri fenomeni legati alla natura umana, anche per ciò che attiene alle tecnologie biometriche, esiste una finestra temporale rispetto alla quale le prestazioni dei sistemi sono ottimali. Tuttavia, se le applicazioni biometriche, come nelle previsioni degli esperti, diventeranno di

uso comune, esse interesseranno utenti di tutte le età e già è noto, ad esempio, che le persone appartenenti alle fasce di età più alta o più bassa di quella "ottimale" possono andare incontro a una serie di difficoltà nell'uso di queste tecnologie.

Ad esempio, se ci riferiamo al riconoscimento delle impronte digitali, tecnologia biometrica per eccellenza, la progressiva secchezza dell'epidermide unita a un assottigliamento delle creste papillari, fenomeni legati all'età anagrafica, è causa di un'importante perdita di definizione nell'acquisizione delle impronte, al punto che alcuni programmi biometrici per l'immigrazione fissano un limite superiore di età per il rilascio delle impronte digitali[11]. Analogamente, non ci sono indicazioni precise sulla stabilità temporale delle caratteristiche vascolari su cui poggiano molte nuove tecnologie biometriche.

L'eventuale equiparazione automatica del corpo umano a una *password* non considera cioè con la dovuta attenzione la caducità temporale degli elementi fisici individuali usati per il riconoscimento. Allo stato attuale, non esistono tecnologie biometriche in grado di compensare ai fini dell'autenticazione biometrica le ineluttabili modificazioni causate dal progredire dell'età, cambiamenti che rendono talora persino inutilizzabili alcune di queste tecnologie (per le quali sarà appropriato introdurre precisi limiti di età per l'utilizzo). La stessa analisi della vascolarizzazione di alcune parti del corpo, considerata adatta a un'applicazione senza eccessivi vincoli di età, è probabilmente ancora troppo recente per comprenderne le effettive potenzialità.

Un'alternativa futuribile a tali limiti rigidi potrebbe consistere nell'utilizzo di soglie variabili dei sistemi biometrici in funzione dell'età anagrafica degli utenti (in possesso di una carta elettronica contenente i dati anagrafici). Questo approccio, seppure causa di inevitabili incrementi nei costi di progettazione e gestione di un sistema biometrico, potrebbe consentire il superamento della rigida discriminazione in base all'età, facendo sentire gli anziani ancora inseriti in processi tecnologici. L'essere esclusi t*out-court*, potrebbe infatti aumentare in loro la sensazione che il progredire dell'età corrisponda a una perdita tragica delle proprie potenzialità, anche nei termini dell'uso di tecnologie innovative.

Altrettanto vale per i minori[12]. Anche per loro l'uso della biometria solleva una serie di problemi di carattere tecnico oltre che ovviamente etico, in particolare per il fatto che in questa categoria di utenti le parti del corpo utilizzabili per l'acquisizione dei dati biometrici non sono ancora perfettamente formate o sono ancora in una fase di rapida evoluzione. Uno degli aspetti più delicati è rappresentato inoltre dalla pressoché totale mancanza di studi specifici.

Mentre non si può negare il fortissimo valore etico sotteso dalle tecnologie biometriche per ciò che attiene al contrasto del traffico di esseri umani, in particolare dei bambini, fortemente condizionato e limitato dall'impiego di tali tecnologie, è altrettanto vero che l'uso della biometria per i minori andrebbe definito in un contesto di forte cautela per gli eventuali effetti psicologici potenzialmente riferibili all'uso di tecnologie che, perlomeno allo stato attuale,

[11] Una situazione simile, di limite intrinseco della raccolta di impronte digitali, riguarda anche i bambini, le cui impronte digitali sono ancora in veloce e profonda evoluzione. Ciò potrebbe comportare una sostanziale inaffidabilità delle tecniche e soprattutto la necessità di aggiornare continuamente i *template*, con una freequenza molto alta.

[12] In questo caso si intende una fascia di popolazione che, in termini generali, va dai 2 ai 14-15 anni.

vengono percepite dall'opinione pubblica come correlate ad aspetti investigativi e giudiziari.

In realtà, tale caratterizzazione fa riferimento soprattutto all'uso delle impronte digitali che, negli anni, si sono effettivamente rivelate un valido supporto nelle operazioni di ordine pubblico. È anche vero comunque che esistono altre tecnologie biometriche le quali, essendo state sviluppate negli ultimi anni, sono caratterizzate da collegamenti psicologici meno immediati e andrebbero forse privilegiate nelle applicazioni rivolte ai minori, ad esempio nell'accesso agli edifici scolastici, in modo da non far loro associare il processo biometrico ad altre procedure adoperate con una certa severità in contesti differenti.

Il riconoscimento biometrico del volto sembra, in prima battuta, la tecnologia più adatta a un impiego nel mondo dei minori anche se, a causa dei forti mutamenti di tipo somatico anche del volto, la cosiddetta *currency* che rappresenta il parametro temporale entro il quale il riconoscimento del volto presenta buone probabilità di successo, è esigua e quindi sono richiesti accorgimenti, quali iscrizioni ripetute nel sistema biometrico.

Infine, al di là delle forme di emarginazione legate a queste nuove manifestazioni di *disabilità biometrica* o di inopportunità di utilizzo di determinate tecnologie per alcune fasce di popolazione, va condannato l'uso di strumenti di rilevazione, comprese le tecnologie biometriche, ove applicato a una sola parte della popolazione qualora ne venisse compromesso il principio costituzionale di eguaglianza.

4. Scenari a lungo termine

Formulando previsioni a più ampio raggio e più a lungo termine, alcuni esperti sostengono che le tecnologie biometriche rappresenteranno solo la punta di un iceberg relativamente all'analisi molto accurata cui verranno sottoposti gli utenti. Le informazioni desumibili da un'osservazione biometrica sono infatti di numero e qualità sicuramente superiore a quelli necessari per la singola transazione con queste tecnologie.

Ad esempio, come messo in luce nel paragrafo 3.2., attraverso il singolo riconoscimento biometrico di alcune caratteristiche fisiche (ad esempio, volto, retina o iride), possono essere desunte una serie di informazioni relative al quadro clinico dell'utente e soprattutto al suo stato psico-emotivo, con tutti gli eventuali rischi di una loro eventuale diffusione o utilizzazione impropria. Analogamente, la sempre più diffusa videosorveglianza nei luoghi pubblici e il contestuale riconoscimento biometrico (occulto) potrebbero tracciare tutti gli spostamenti di una persona, arrivando a individuare la sue preferenze in termini di acquisti o le persone con cui si accompagna.

Certamente, il livello tecnologico di oggi, che è ancora limitato, e l'irrilevanza di acquisire e conservare un numero così alto di informazioni (si produce un eccesso di dati di fatto non gestibili per alcuno scopo) inducono a ritenere che non esista un vero pericolo di scenari foschi. Tuttavia, appare opportuno non limitarsi a prendere atto degli indiscutibili vantaggi relativi alla sicurezza individuale e collettiva e di carattere più generale sulla qualità di vita degli individui. Occorre, viceversa, esaminare le eventuali ricadute negative di questo pervasivo e testardo accumulo di dati, che potrebbero incidere sulle libertà fondamentali e sul rapporto di ciascun individuo con gli altri e con il

proprio corpo, fissando alcuni limiti nell'uso delle tecnologie biometriche che rendano il loro impiego più consono sul piano etico e sociale.

4.1. Preferenza per l'uso di tecnologie basate su caratteristiche biometriche che non lasciano tracce e per l'esclusione di archivi centralizzati

Man mano che le tecnologie biometriche si diffondono, appare più agevole effettuare una classificazione sia, come abbiamo visto, in merito al contesto applicativo più consono sul piano tecnico, sia dal punto di vista di possibili rischi sociali per gli utenti.

Un'interessante classificazione è stata proposta dalla *Commission Nationale de l'Informatique et des Libertés* (CNIL) francese, riguardo le tecnologie biometriche che lasciano o non lasciano tracce. La CNIL si riferisce a tracce 'materiali', ovvero al fatto che le impronte digitali, ad esempio, vengono lasciate ovunque sugli oggetti che tocchiamo e quindi potrebbero essere catturate in un secondo momento da chiunque ed eventualmente usate in maniera fraudolenta. Il diffondersi della biometria rende questa possibilità realistica su più ampia scala.

In linea di massima, si può dire che il rischio che dati biometrici ottenuti da tracce fisiche lasciate da un individuo a sua insaputa (ad es.: impronte digitali) siano utilizzati per finalità improprie è potenzialmente inferiore se i dati, invece di essere memorizzati in archivi centralizzati, restano con la persona stessa attraverso l'uso di carte elettroniche (Verifica di Identità) senza essere accessibili a terzi[13].

Un'archiviazione centralizzata dei dati biometrici aumenta altresì il rischio che tali dati vengano utilizzati per collegare altri aggregati di dati personali creando nel complesso una profilazione dei soggetti interessati. La biometria, potrebbe cioè agire da elemento di raccordo tra informazioni eterogenee producendo informazioni coerenti sulla vita privata delle persone e sulle loro abitudini nei settori più svariati. In questo senso, rendere interoperabili banche dati diverse, se da un lato genera sistemi efficienti e può costituire un valore aggiunto della biometria quale tecnologia abilitante, dall'altro lato rende possibile la massima interconnessione di dati con tutti i possibili pericoli associati[14].

È quindi chiaro che l'uso di tecnologie basate su caratteristiche biometriche che non lasciano tracce, e basate sulla preferenza di sistemi a basso impatto di archiviazione e comunque di archivi non interoperabili, risolverebbe alcuni dei problemi etico-giuridici legati alla biometria, attenuando le potenziali diffidenze degli utenti.

4.2. Il diritto all'oblio

La memoria è un elemento fondamentale dell'identità individuale e delle relazioni sociali. È difficile immaginare qualsiasi sviluppo interiore e qualsiasi progresso culturale senza la conservazione e l'organizzazione delle tracce del

[13] CE – Gruppo di Lavoro per la Tutela delle Persone riguardo al Trattamento dei Dati Personali, Documento di lavoro sulla biometria, 12168/02/IT - WP 80, adottato il 1° agosto 2003.
[14] Idem.

passato nelle molteplici forme che possono assumere (ricordo, storia, opinione, pregiudizio etc.). L'oblio è altrettanto importante per operare una selezione all'interno di questo insieme di elementi, evitando gli accumuli inutili o dannosi. Per garantire la stabilità sociale e tutelare i diritti e le libertà fondamentali degli individui l'esperienza giuridica ha dovuto elaborare forme artificiali di oblio (pur nella loro diversità: cancellazione dal casellario giudiziario, prescrizione, amnistia, indulto etc.), laddove la morale affida al perdono l'estremo sforzo interiore per superare il passato. Sotto questo punto di vista la biometria non pone nulla di nuovo: si limita a offrire una raccolta maggiormente intensa, assidua e capillare della massa di informazioni. Tuttavia, proprio per essere, nello stesso tempo, più sistematica e più frammentaria, più assidua e più sporadica, la rilevazione biometrica accentua le possibilità di interferenza sulla vita individuale. Se gli sviluppi economici e le giuste esigenze di sicurezza vanificano ogni pretesa di garantire un diritto assoluto all'anonimato, diventa fondamentale elaborare nuove e più complesse forme del diritto all'oblio. È quanto già avviene con il materiale biologico che viene anonimizzato (collegato cioè con simboli o codici numerici per impedire di risalire, senza apposite autorizzazioni, all'identità della persona a cui appartengono). In questo modo viene garantita la riservatezza di tutte le informazioni del referente originario, senza impedire che, in casi eccezionali e a determinate condizioni, se ne possa rintracciare l'identità (sempre che la persona non abbia richiesto un'anonimizzazione irreversibile). Lo stesso modello dovrebbe essere seguito per le rilevazioni biometriche, prevedendo processi certi e trasparenti di cancellazione o anonimizzazione, e ribadendo con forza sia il principio dell'eccezionalità dell'accumulo e dell'incrocio delle informazioni, in particolare quando esse vengono acquisite attraverso strumenti non cooperativi e occulti, bandendo energicamente ogni tentativo di *function creep*.

Particolare cura dovrebbe essere posta, da parte dei singoli legislatori e degli organismi internazionali, nel rendere effettivo il diritto all'oblio, non solo prevedendo forme semplici e rapide del suo esercizio, ma ponendo chiaramente a carico di chi ha registrato i dati l'obbligo di provare la necessità, la proporzionalità e la pertinenza della raccolta di essi. Il ricordo, quando è affidato agli schematismi di un *ubiquitous and autonomic computing*, può diventare una forma sottile e irreversibile di discriminazione, la condanna a non poter sfuggire alle tracce del proprio passato. Per questo motivo l'oblio non può più continuare a essere considerato un'eccezione, una concessione individuale o sociale legata a sofferte scelte morali o a particolari situazioni. Deve diventare un aspetto del diritto fondamentale all'identità personale, il diritto a non essere schedati, classificati, eventualmente emarginati in maniera irreversibile sulla base di informazioni assunte a propria insaputa, attraverso criteri non trasparenti e per finalità in gran parte ignote. La crescita, in termini di efficienza e sicurezza, delle acquisizioni biometriche, dovrebbe quindi accompagnarsi all'aumento proporzionale delle possibilità di tutela e auspicabilmente della consapevolezza pubblica. Se non è possibile pretendere l'anonimato, è fondamentale che almeno siano garantite le condizioni per ottenere l'oblio.

5. Sintesi e raccomandazioni

L'introduzione diffusa nella vita civile di sistemi biometrici potrebbe interferire in linea di massima con quel grado di riservatezza che viene

attualmente riconosciuto alla persona dalla tradizione etico-giuridica. Occorre, pertanto, che ogni iniziativa in merito sia adeguatamente giustificata sul piano della necessità e proporzionalità, accolta dall'opinione pubblica e disciplinata dallo Stato, valutando opportunamente il rapporto tra vantaggi e rischi nei diversi settori della vita privata e pubblica delle persone.

Il CNB ritiene che l'utilizzazione di sistemi biometrici di identificazione sia estremamente importante per facilitare gli accessi e il godimento di servizi, nelle relazioni umane, nella gestione della salute, nelle transazioni commerciali e finanziarie, e in generale per scopi facilitativi. In particolare, la biometria è cruciale per incrementare la sicurezza che a sua volta è condizione fondamentale per l'esercizio della libertà e per la realizzazione della personalità individuale. Oltre a essere più sicuri e facili da usare, i sistemi biometrici potrebbero essere essi stessi catalogati come tecnologie in grado di aumentare le sfere di riservatezza[15], evitando ad esempio di dover fornire alcuni dati sensibili che attualmente sono indispensabili nei processi di identificazione (ad es: data di nascita, sesso, nazionalità, stato civile, indirizzo personale etc.).

Questi innegabili vantaggi non escludono che l'uso indiscriminato della biometria, per il fatto di creare materialmente le condizioni che possono consentire a soggetti diversi di acquisire, collegare stabilmente e utilizzare, spesso in maniera occulta e per i fini più svariati, una pluralità di dati fisici e comportamentali, possa comunque determinare rischi consistenti di discriminazione, stigmatizzazione ed emarginazione.

Una forma di discriminazione si verificherebbe ad esempio tutte le volte in cui questi mezzi fossero usati solo nei confronti di una parte della popolazione per accentuare il controllo sociale, ma anche per disincentivare l'inserimento nella vita di relazione o per sottolineare una "differenza". Esiste poi la possibilità di discriminazioni particolarmente frustranti su singoli individui in base a errori del sistema che non si riescono facilmente a emendare, data la complessità e il numero delle banche dati nonché degli incroci tra le stesse. La stigmatizzazione si potrebbe generare attraverso le procedure di profilazione (*profiling*) creando, *a priori*, dei profili di "sospetto" in base a delle caratteristiche fisiche o comportamentali sulla cui base potrebbe essere impedito a determinati soggetti di accedere a certi luoghi o godere di determinati servizi. Il fenomeno può avere sia carattere pubblico (ad es.: lotta la terrorismo e alla delinquenza organizzata), sia privato (ad es.: il rifiuto di determinate prestazioni sanitarie a un certa categoria di soggetti), e presenta caratteri particolarmente inquietanti se avviene in maniera occulta, magari legata all'utilizzazione distorta di informazioni acquisite in eccesso che vanno ben oltre le finalità di immediata identificazione (*function-creep*, cfr. par. 3.1). Casi di emarginazione potrebbero riguardare alcune categorie di utenti (anziani, bambini, persone con disabilità) che si trasformerebbero in veri e propri *disabili biometrici*, esclusi dall'uso di determinati servizi o dall'accesso a particolari luoghi, o comunque costretti ad affrontare difficoltà e ostacoli anche molto onerosi.

Inoltre, discriminazione, stigmatizzazione ed emarginazione accentuerebbero il rischio che sotto il profilo psicologico il soggetto avverta sempre più il corpo come qualcosa di estraneo, ostile, nemico che appartiene più alla società, attraverso la molteplicità dei processi di identificazione e l'infinità delle tracce registrate e utilizzate, che a se stesso e alla libera esplicazione della personalità. Tutto ciò sarebbe ancora più evidente e

[15] PET (*Privacy Enhancing Technologies*).

profondo se si manifestasse un dovere di *permanenza* nei propri dati biometrici e di *manutenzione* di ciascuno di essi.

Alla luce di possibili usi non appropriati e dei rischi potenziali delle tecnologie biometriche il CNB raccomanda:

1. ai fini della tutela della persona:

a) che l'introduzione di sistemi biometrici avvenga costantemente sulla base dei principi di necessità e proporzionalità;

b) che sia garantita il più possibile l'applicazione del consenso informato preventivo sia alla raccolta dei dati sia al loro utilizzo, dando un'informativa esauriente sulle finalità;

c) che sia favorita l'utilizzazione di tecnologie che implichino un uso limitato di archivi centralizzati e interoperabili;

d) che sia riconosciuto il diritto di accesso da parte di ciascun soggetto interessato alle banche dati biometriche che lo riguardano, per conoscere quali dati siano stati raccolti, da chi e per quali finalità, da quanto tempo e per quanto tempo, e a quali altri dati siano stati associati;

e) che sia riconosciuto il diritto all'oblio come un aspetto dei diritti fondamentali della persona, prevedendo per quanto possibile processi certi e trasparenti di cancellazione o anonimizzazione dei dati biometrici, e muovendo in ogni caso dall'idea dell'eccezionalità dell'accumulo dei dati e dell'incrocio delle informazioni, in particolare quando essi vengono acquisiti attraverso strumenti non cooperativi e occulti.

2. ai fini dell'organizzazione e regolazione delle applicazioni biometriche:

f) che siano identificabili chiaramente i soggetti giuridici pubblici e privati o le autorità preposte alla raccolta dei dati biometrici, e le loro finalità;

g) che sia istituito, oltre all'Autorità garante della privacy e in stretta collaborazione con essa, un organo terzo che controlli chi acquisisce dati biometrici, come e a che scopo, e come essi vengano gestiti; oppure, in alternativa, il CNB raccomanda che vengano rafforzate le funzioni e le competenze dell'Autorità garante della privacy, in modo da affrontare il complesso dei profili etico-giuridici posti dalla biometria;

h) che venga elaborato e adottato, analogamente a quanto accaduto per la videosorveglianza, un provvedimento quadro che regoli l'utilizzo delle tecnologie biometriche e la loro gestione.

Il CNB auspica, infine, che si mettano in opera interventi europei e internazionali tra tutti i Paesi al fine di adottare legislazioni interne che vietino ogni forma di applicazione discriminatoria, che impediscano ogni utilizzazione della biometria che sia indebita o per finalità aliene rispetto a quelle previste (*function creep*), e che inglobino i principi di *disabilità biometrica* e cioè dell'impossibilità o difficoltà nell'uso di tecnologie biometriche che sono talora riscontrabili in determinate categorie di utenti.