

Il Volto e il Nome. Implicazioni Etiche, Sociali e Antropologiche delle Tecniche di Identificazione Biometriche

The Face and the Name. Ethical, Social and Anthropological Implications of Biometrical Identification

E MORDINI

Coordinatore del progetto europeo BITE

La Commissione Europea ha promosso un progetto di ricerca biennale sulle implicazioni bioetiche della biometria, il progetto BITE (Biometric Identification Technology Ethics, www.biteproject.org). Il progetto, coordinato dal Centro per la Scienza, la Società e la Cittadinanza di Roma, raccoglie tre università (La Sapienza di Roma, l'Università di Lancaster, l'Università Erasmus di Rotterdam), due aziende leader europee (la Humanscan tedesca e la Optel polacca), un'organizzazione internazionale che è direttamente coinvolta nel dibattito politico sull'uso dei passaporti biometrici (l'Organizzazione Internazionale delle Migrazioni), un centro di bioetica (European Institute of Bioethics), e il più importante gruppo mondiale di certificazione delle tecnologie biometriche (l'International Biometric Group). Il progetto si sta sviluppando attraverso una serie di meeting in Gran Bretagna, Italia, Germania, Svizzera, Polonia e terminerà con una conferenza a Bruxelles nel febbraio 2007.

I lettori dell'Odissea hanno certamente presente la scena dell'agnizione di Ulisse da parte della nutrice Euriclea. Siamo nel canto XIX del poema. dopo un peregrinare durato dieci anni Ulisse è infine giunto a Itaca, sua patria, di cui egli è re. La regina Penelope, sua moglie, lo ha accolto, straniero, senza riconoscerlo e comanda alla vecchia massaia di lavargli i piedi, un gesto che in tutta la cultura antica contrassegna la pietà dell'ospite per il viandante stanco. Ulisse, che vuole mantenere l'incognito, è preoccupato perché sa che sarà riconosciuto se si scoprirà una cicatrice che egli ha sulla coscia. Così si rintana nell'angolo più buio della stanza per celare almeno alla regina la propria identità. Intanto Euriclea parla del re scomparso, di come egli avrebbe oggi la stessa età del viandante, e di come i due uomini si assomiglino. Poi la vecchia sfiora la coscia di Ulisse e allora, con un balzo di sorpresa, lascia cadere il piede dell'eroe nel bacile, vorrebbe gridare dalla gioia perché ha riconosciuto chi si cela dietro le sembianze dello straniero, ma Ulisse la prende per la gola e la obbliga a tacere. Non è ancora giunto il suo momento.

Indirizzo per la corrispondenza
Address for correspondence

Prof. Emilio Mordini
Centro per la Scienza, la Società e la Cittadinanza
Via Sistina, 37
00187 Roma ITALY
E-mail: e.mordini@bioethics.it

L'ambiguità di tutta la vicenda è difficile da cogliere per noi moderni, ma certo appariva fortissima all'ascoltatore greco. Come è possibile che un re, un eroe, sia segnato da un marchio sulla pelle, una cicatrice? Il riconoscimento attraverso un segno corporeo, che a noi può apparire banale, è carico di senso. La cultura greca era una cultura che aveva orrore dei segni sulla pelle, erano i barbari e gli schiavi che avevano pelli segnate da cicatrici, scarificate, marchiate. La pelle dell'uomo greco è bianca e glabra, levigata con cura maniacale da sabbia, oli e pietra pomice. Quanto poco fosse valutato il riconoscimento attraverso un segno del corpo è testimoniato molti secoli dopo - in una atmosfera culturale ormai lontana dalla cultura omerica - da Aristotele. Discutendo dell'agnizione nei capitoli 11, 14 e 16 della *Poetica*, il filosofo ne elenca le forme drammatiche, per concludere che quella attraverso marchi sulla pelle, cicatrici e altri segni (*seméia*) è la meno nobile e la più triviale da scegliere come espediente teatrale. Perché i greci avevano una tale disistima verso i corpi "segnati"? Certamente per ragioni contingenti, ma anche per ragioni antropologiche più profonde. La civiltà greca è infatti fiera del suo umanesimo, che si fonda principalmente su un'emancipazione dal puro ordine biologico e naturale. Si può confrontare, ad esempio, un'altra famosa agnizione, nel canto VI dell'Iliade. Qui è il giovane Glauco ad essere interrogato dall'eroe Diomede, che, prima di ucciderlo in duello, vuole saperne il nome, e Glauco risponde: "Titide magnanimo perché mi domandi la stirpe? Come stirpi di

foglie, così le stirpi degli uomini; Le foglie, alcune le getta il vento a terra, altre la selva fiorente le nutre al tempo di primavera; così le stirpi degli uomini: nasce una, l'altra dilegua. Se anche questo però vuoi sapere, per conoscerla bene la stirpe mia, molti la sanno fra gli uomini [...]” (Iliade, VI, 145-150, trad. R. Calzecchi Onesti). Se mai vi è una differenza tra le generazioni degli uomini e quelle delle foglie, essa sta proprio in ciò: che non sono le apparenze fisiche che permettono di riconoscere gli uomini, ma la stirpe, il *genos*. Certo, il poeta sembra dirci che si tratta di una distinzione fragile, forse persino illusoria, ma è tutto ciò che noi possediamo. E, in effetti, dopo che il giovane Glauco avrà declinato le sue origini, il potente Diomede lo riconoscerà e lo risparmierà: “Ma dunque tu sei ospite ereditario e antico per me! [...] Scambiamoci le armi l'un l'altro; anche costoro sappiano che ci vantiamo di essere ospiti antichi” (Iliade, VI, 210, 230, trad. R. Calzecchi Onesti). Il rifiuto della pelle marchiata, è quindi per i Greci innanzitutto espressione della dignità dell'uomo greco, del suo essere individuo segnato dall'appartenenza ad una comunità umana (*genos* o *pólis* che sia). L'identità del uomo greco, potremmo dire in termini moderni, non è mai un'identità razziale o biologica ma è sempre un'identità culturale.

Abbiamo quindi visto una delle ragioni dello scandalo contenuto nella cicatrice di Ulisse ma la repulsione della cultura greca verso la “pelle scritta” affondava le sue radici in regioni ancora più profonde. Nella tradizione greca erano infatti gli dei dell'oltretomba a governare il mondo dei segni e della scrittura (Piccaluga G, 1988). Ad esempio Radamantos, il giudice infernale, prima legge i peccati sui corpi dei morti, poi, sempre sui quei corpi, scrive la sentenza di condanna. La vita scrive sul e nel nostro corpo ed uno dei processi che debbono accadere perché sia possibile il ciclo delle rinascite è che i segni sulla pelle (cicatrici e rughe) ed i segni nella mente (ricordi) siano cancellati (Ps. Plato *Axiach*. 366 C). La tensione contenuta nell'agnizione di Ulisse ha quindi anche un valore religioso. Non solo Ulisse è un re “marchiato”, ma è un re che parla attraverso il proprio marchio. In effetti poco dopo l'episodio di Euriclea, nel canto XX, è Ulisse stesso ad utilizzare coscientemente il proprio corpo come “carta di identità”. Dovendo cercare un aiuto per vendicarsi dei pretendenti, l'eroe mostra la cicatrice a due servi, un porcaio e un bovaro, da cui si fa riconoscere. Come i *kóroi* arcaici anche l'eroe omerico parla attraverso la propria nudità, ma la sua non è la pelle liscia dei giovinetti dai sorrisi enigmatici che recano doni al dio, al contrario è la pelle-*semeion* della divinità infernale che sta per offrire i propri nemici in olocausto all'Ade.

Questa lunga introduzione sui segni del corpo deve servire ora ad accompagnarci in un excursus attraverso le tecnologie di identificazione biometrica. Per parlare di biometria, i mezzi di comunicazione di massa sono spesso ri-

corsi all'immagine del “corpo passaporto”. Vedremo in che misura questo è vero e quali conseguenze etiche ed antropologiche se ne potranno trarre. Il nostro non sarà un percorso né lineare né esaustivo, sia perché il campo è vasto sia perché la materia è ancora mal definita. L'argomento centrale sarà, comunque, quello già contenuto in nuce nell'introduzione: la rivoluzione biometrica è una rivoluzione che riguarda non solo l'*identificazione* ma le *identità* e, più in generale, il senso della corporeità. In ultimo, riprendendo riflessioni già sviluppate da alcuni studiosi a partire da Michel Foucault, sosteneremo che la biometria fa parte di una più vasta tendenza che mira a fondare la cittadinanza sulla biologia.

DEFINIZIONI

In senso generale, il termine biometria indica un insieme di tecniche di ricerca e di logiche interpretative applicate ai più diversi campi di indagine scientifica su fenomeni quantitativi della vita.

La parola fu coniata verso la fine dell'Ottocento da Francis Galton (1822-1911), geografo, antropologo, naturalista e fondatore dell'eugenica. Le ricerche scientifiche di Galton furono molte e di varia natura, accomunate tuttavia dalla forte insistenza sull'aspetto quantitativo. *L'Origine delle specie* di Darwin lo stimolò a concentrarsi sulla misurazione delle differenze individuali negli organismi viventi. In particolare, numerose sue ricerche furono volte a cercare di capire se le caratteristiche fisiche e mentali degli uomini, variabili da persona a persona, dipendano dalla sola eredità biologica o anche dalle condizioni ambientali di sviluppo, e in che misura.

La biometria quindi comprende vari metodi di misurazione di caratteristiche legate alle proprietà anatomiche e di comportamento di un individuo; questi metodi servono a:

1. studiare la dipendenza di queste caratteristiche da fattori ereditari e ambientali;
2. studiare la loro costanza/variabilità nel tempo;
3. studiare la loro eventuale associazione con determinate condizioni fisiologiche e patologiche;
4. studiare il loro grado di unicità relativamente ad ogni individuo.

Sino all'introduzione delle moderne tecnologie di identificazione, le applicazioni della biometria sono state essenzialmente quattro:

5. *Applicazioni mediche*: ogni medico usa quotidianamente la biometria quando rileva, ad esempio, il peso, l'altezza, i diametri corporei, la pressione arteriosa, ecc. Questi dati sono normalmente usati per scopi clinici. Attraverso una comparazione con dati (statisticamente) normali e uno studio della loro variabi-

lità nel tempo si inferiscono informazioni sullo stato di salute del soggetto esaminato o anche di interi gruppi umani.

6. *Applicazioni a scopo di ricerca scientifica*: lo studio quantitativo delle collettività viventi - umane, animali, vegetali - e dei caratteri somatici, fisiologici e patologici, individuali serve a comprendere i problemi dell'eredità, della trasformazione delle specie e dell'evoluzione; si sono formate quindi una biometria umana, animale, botanica, e così via, con il puro scopo di studiare statisticamente i caratteri misurabili.
7. *Applicazioni in ambito sociale e antropologico*: l'identificazione di caratteristiche comuni ad una determinata popolazione non è solo servita a fondare la genetica delle popolazioni, ma ha anche conferito uno statuto scientifico all'antropologia delle razze umane, e ad alcune sue applicazioni tra cui il razzismo.
8. *Applicazioni legali*: l'unicità, o la quasi unicità, di alcune caratteristiche fa sì che la loro misurazione costituisca un elemento di identificazione; sin dal 1902, grazie al piemontese Giovanni Gasti, le impronte digitali sono state usate a questo scopo.

LE TECNOLOGIE DI IDENTIFICAZIONE BIOMETRICHE

La moderna biometria fa parte di quelle tecnologie complessivamente chiamate AIDC (Automatic Identification and Data Capture), che comprendono, oltre la biometria, le smart card, i codici a barre, i dispositivi RFID, le carte magnetiche e OCR, i microchip impiantabili, i MEMS, ecc. Si tratta di tecnologie che hanno in comune la capacità di estrarre dati attraverso un meccanismo elettronico automatizzato e quindi di processarli in sistemi controllati da microprocessori, quali, ad esempio, computer. Queste tecnologie sono spesso coniugate tra loro, tanto che spesso non è possibile distinguerle realmente nelle loro applicazioni. Ad esempio i dispositivi a emissione di radiofrequenze (RFID) furono inizialmente utilizzati soltanto per identificare e tracciare merci nella catena di distribuzione militare e quindi anche civile. Via, via però che si affermò l'idea e si sperimentò l'uso di dispositivi RFID anche nell'identificazione umana si fece strada la convinzione che il chip potesse contenere anche dati biometrici. Oggi gran parte delle targhette RFID usate in ambito umano contengono anche i dati biometrici del soggetto. Ad esempio l'uso di RFID impiantabili sotto pelle contenenti le informazioni sanitarie e i dati biometrici di un paziente è stato approvato negli anni scorsi dalla FDA negli Stati Uniti e sperimentato negli Usa e in numerosi altri paesi, tra cui l'Italia. Un simile sistema è stato proposto, ma ancora non adottato su vasta scala, per il controllo dei lavoratori trans-

frontalieri e degli immigrati stagionali. Vale la pena, comunque, di conservare una distinzione tra biometria e tutte le altre forme di AIDC. Infatti ciò che distingue la biometria da tutte le altre tecnologie è che la biometria misura una caratteristica corporea (fisica o comportamentale).

Già alla fine degli anni 1960 la nascente industria informatica aveva cercato di automatizzare le tecniche di rilevazione di alcuni dati biometrici caratterizzati dalla loro relativa unicità e costanza nel tempo (impronte digitali, forma dell'iride, geometria dei vasi sanguigni in alcuni distretti corporei, ecc.) e quindi tali da poter essere usati a scopi identificativi. Queste tecnologie erano però poco affidabili, ingombranti e costose. La situazione sta oggi cambiando rapidamente e radicalmente. Lo stimolo principale allo sviluppo della biometria negli ultimi anni viene dall'emergenza terrorismo. Dopo l'undici settembre, il governo americano ha investito circa tre miliardi di dollari per dotarsi di un sistema di controllo biometrico alle proprie frontiere e il costo di mantenimento di questo sistema è stato calcolato essere di circa un altro miliardo e mezzo di dollari l'anno (<http://www.nature.com/embor/journal/v5/n2/full/7400085.html>). Spinta dalle commesse militari e di sicurezza interna, l'industria biometrica ha progredito rapidamente coinvolgendo anche il settore civile.

Gli aeroporti di Schiphol ad Amsterdam e Ben Gurion di Tel Aviv utilizzano lettori dell'iride per l'identificazione di gruppi selezionati di passeggeri in transito. Sistemi biometrici sono utilizzati in molti altri aeroporti per controllare l'accesso del personale. Microsoft ha appena commercializzato un lettore di impronte digitali che dovrebbe aiutare nella gestione delle password dei personal computer¹. Sistemi di identificazione biometrica affiancheranno presto il PIN delle maggiori carte di credito, con l'obiettivo di ridurre le frodi. Alcune case produttrici di autoveicoli stanno già dotando le loro vetture con antifurti provvisti di lettori di impronte digitali (è del marzo 2005 la notizia che, in Malesia, un paese dove la moda degli antifurti biometrici sta prendendo piede, un malcapitato automobilista ha avuto il dito indice mozzato da una banda di ladri d'auto). L'accesso a mense scolastiche e aziendali è regolato da sistemi di identificazione biometrica in numerose aziende e scuole negli USA, in Francia, e Inghilterra (e in Italia è stato recentemente proibito dall'autorità garante per il trattamento dei dati personali). Sistemi biometrici sono im-

¹ Tra la fine del 2004 e l'inizio del 2005 Microsoft ha commercializzato vari sistemi - complessivamente denominati Fingerprint Reader - basati sul riconoscimento dell'impronta digitale, che consentono di "loggarci" ad accensione computer e accedere a pagine web dove è necessario digitare un user ID e una password. I sistemi sono abbastanza imprecisi ma sono soddisfacenti per un utente medio che non abbia particolari problemi di sicurezza.

piegati in Olanda per evitare l'uso illecito dei servizi di assistenza sociale e nei programmi di somministrazione controllata di metadone per tossicodipendenti (in entrambi i casi l'obiettivo è quello di impedire accessi abusivi). Sistemi basati sulla geometria facciale sono diffusi in molte case da gioco e casinò per bloccare l'accesso a bari e giocatori professionisti. Sistemi simili sono usati per identificare teppisti e hooligans negli stadi. Molti governi stanno inoltre studiando la possibilità di utilizzare la biometria nelle procedure di voto elettronico e per validare l'accesso ad applicazioni informatiche critiche ed a dati sensibili da parte del personale della pubblica amministrazione o di utenti online (ad esempio in Italia il CNIPA, Centro Nazionale per l'Informatica nella Pubblica Amministrazione, ha costituito un centro di competenza sulla biometria).

I più diffusi sistemi biometrici sono oggi basati sulle impronte digitali, sulla geometria dei vasi sanguigni della mano, sulla geometria del volto, sulla struttura dell'iride, sulla dinamica della firma (cioè sulla pressione esercitata dalla mano durante la firma), sulla dinamica della scrittura su tastiera (cioè sul modo in cui ciascuno batte un testo su una tastiera di pc), sul riconoscimento vocale, sul riconoscimento dell'odore del corpo, sulla geometria delle orecchie. Questi sistemi – isolatamente o, più spesso, variamente incrociati – sono tutti già in uso. Altri sistemi sono in fase avanzata di studio: alcuni basati sulla luminescenza della pelle, altri sul riconoscimento del profilo genetico (attraverso, ad esempio, l'analisi di frammenti di DNA presenti nel fiato emesso) altri sulle onde cerebrali (ad esempio i sistemi basati sulla NWA, *neural wave analysis interface*, un sistema di interfaccia cervello computer).

Tutti i sistemi biometrici sono fondamentalmente costruiti a partire da un lettore (scanner) che riproduce su un supporto elettronico i dati biometrici della persona (forma dell'iride, impronte digitali, geometria del volto, ecc.) e un software che li converte in forma digitale attraverso un algoritmo². Poiché gli algoritmi usati sono diversi, ogni sistema biometrico creerà diversi modelli (*template*) della stessa caratteristica fisica. Questo fatto pone sia un problema di interoperabilità (un'impronta digitale letta da una macchina dell'industria X genererà un *template* diverso dal *template* generato dalla macchina dell'industria Y) sia un problema di banca immagini (l'unica garanzia che sia possibile passare da un sistema operativo all'altro è, ovviamente, conservare banche delle immagini vere e proprie e

non solo dei *template*). I sistemi biometrici possono essere usati per l'identificazione (quando i dati di una persona vengono confrontati con una banca dati in cui ad ogni profilo biometrico corrisponde un'informazione anagrafica) oppure per la verifica (quando vengono confrontati con il documento di cui la persona è in possesso). In questo ultimo caso possono anche non entrare in gioco i dati anagrafici poiché il sistema non certifica l'identità ma solo l'autenticità: la persona che usa quel documento è per davvero la persona che ha il diritto di usare quel documento (se poi il documento non contiene dati anagrafici ma solo un identificatore generico, ecco che l'anonimato è preservato, pur con la garanzia che non si è di fronte ad una falsa identità).

CAMPI DI APPLICAZIONE

I campi di applicazione delle tecnologie biometriche sono convenzionalmente classificati in:

- 1) *Identificazione civile*, che comprende l'uso della biometria in tutte le forme *e-government* (ad esempio per l'identificazione degli elettori durante le procedure di voto) e in tutte le transazioni tra cittadino e istituzioni, comprese le istituzioni sanitarie (per esempio per regolare l'accesso alle cartelle cliniche), e per il controllo alle frontiere (ad esempio il passaporto biometrico);
- 2) *Identificazione commerciale*, che comprende il settore dei trasporti (accesso a aerei, metropolitane, bus, ecc.), il settore ricreativo e alberghiero (ad esempio Disneyland in Florida rilascia già da qualche anno dei pass biometrici), e tutti gli altri possibili settori merceologici e in ambito bancario (ad esempio l'*e-banking*, i bancomat, e il riconoscimento dei possessori di carte di credito); la biometria vocale, inoltre, può costituire un elemento importante di innovazione per tutti i sistemi di assistenza al cliente basati su *call center*;
- 3) *Identificazione a scopi militari e di sicurezza*³, che comprende sia il controllo dell'accesso fisico e logico a settori delicati per la sicurezza, sia la possibilità di coniugare i sistemi biometrici ai sistemi d'arma più disparati (rendendoli così più sicuri), sia la possibilità di identificare a distanza il nemico ed altri obiettivi umani;

² Nella sua definizione più semplice ed intuitiva un algoritmo è una procedura di calcolo o, più in generale, l'elenco delle operazioni necessarie per risolvere un problema in un numero finito di operazioni. In altri termini, un algoritmo è l'insieme delle operazioni, logiche di calcolo, la cui sequenza porta con certezza ad un determinato risultato (ad es. gli algoritmi di generazione chiavi di cifratura).

³ Tutte le applicazioni militari elencate fanno parte del programma DARPA sulle guerre asimmetriche lanciato dal Pentagono all'indomani dell'11 settembre. Sebbene il programma sia stato ufficialmente sospeso a causa dei suoi costi eccessivi, le singole sue parti costituiscono ancora un obiettivo del governo americano.

- 4) *Identificazione a scopi legali*, che comprende sia l'uso della biometria per sostituire le tecniche tradizionali di controllo di detenuti in libertà provvisoria o sottoposti a speciali regimi di sorveglianza, sia il controllo dell'accesso a carceri e tribunali, sia l'identificazione di sospetti;
- 5) *Sorveglianza e screening* comprendono tutti quegli usi in cui la biometria viene applicata a larghe masse di persone con l'obiettivo di identificare precocemente persone da inserire in gruppi precedentemente *profiled*⁴, se questa attività avviene in modo scoperto si parla di *screening* (ad esempio un controllo all'ingresso degli stadi per impedire l'accesso a potenziali teppisti), se avviene in modo coperto si parla di *sorveglianza* (ad esempio se si usano le telecamere a circuito chiuso di una banca per identificare potenziali rapinatori senza che i clienti sappiano che le telecamere sono dotate di sistemi di identificazione biometrica).

Se si sommano tutte questi campi applicativi e si considerano tutte le tecnologie già in uso e quelle che presto lo saranno, è difficile non farsi cogliere da una vertigine. Naturalmente come in tutti i settori tecnologici è pressoché impossibile predire quali tecnologie prenderanno veramente piede e quali soccomberanno. Ad esempio gli esperti ritengono che difficilmente la biometria riuscirà a sostituire un sistema ben collaudato ed affidabile come quello del PIN per l'autenticazione del prelievo di contante dai dispensatori automatici di banconote (bancomat). Al contrario molti esperti pensano che il tempo delle tessere magnetiche per l'accesso a camere d'albergo, parcheggi, palestre e simili sia destinato a finire presto, soppiantato da sistemi di riconoscimento biometrico.

C'è infine un settore che è solo agli inizi, in fase ancora di sperimentazione, la cui importanza futura è ben difficile da valutare. Si tratta delle applicazioni della biometria alla robotica avanzata e all'*ambient intelligence*. La robotica avanzata comprende forme di robotica che possono sostituire o coadiuvare gli esseri umani in procedure particolarmente complesse, sia in ambito produttivo industriale, sia in ambito dei servizi sociali. L'*ambient intelligence* riguarda la costruzione di ambienti altamente tecnologici (domotica, *home hospital*, *smart house*, ecc.) che interagiscono in modo intelligente con gli esseri umani. Sia robotica avanzata, sia *ambient intelligence* possono essere ul-

teriormente sviluppati dotandosi di sistemi di riconoscimento biometrici. Ad esempio un home hospital potrà distinguere e riconoscere i pazienti, o un robot potrà identificare con certezza e senza errore le persone da cui "prendere ordini".

Persino lo scenario fantascientifico di un'identificatore unico per tutta la popolazione del pianeta (la "carta di identità biometrica universale") sarebbe in linea di principio già tecnologicamente fattibile. Infatti se si calcolano una media di cento identificazioni giornaliere per cittadino telematico (comprese quelle per l'accesso ad aree ristrette, luoghi di lavoro, acquisti online e con carte di credito, uso di telefoni cellulari, ecc.), e presumendo una popolazione mondiale di circa dieci miliardi di persone, avremo circa di 10¹² identificazioni al giorno. Se consideriamo attorno ai 100 kB lo spazio medio per immagazzinare l'informazione biometrica, significa che già oggi 2000 hard disk da 500 GB l'uno sarebbero in grado di contenere il traffico dati necessario ad identificare tutti i cittadini del mondo⁵!

In definitiva se è difficile indovinare come sarà la "società biometrica" futura, ci sono pochi dubbi però che le tecnologie di identificazione biometriche siano qui per rimanere.

FATTORI NON TECNICI DELLA BIOMETRIA

Con la generica denominazione di "fattori non tecnici" vengono in genere considerati tutti quegli aspetti che condizionano lo sviluppo e l'accettazione delle tecniche di identificazione biometriche ma non dipendono direttamente dallo sviluppo tecnologico. In un rapporto del 2001 il RAND Institute (RAND, 2001) classificava i fattori non tecnici in tre grandi categorie: *informational privacy*, *physical privacy* e obiezione religiosa.

Informational privacy

Con il termine *informational privacy* il rapporto comprende tutte le preoccupazioni che riguardano il trattamento e la protezione dei dati personali. La diffusione della biometria ha sollevato numerose obiezioni e preoccupazioni. Le principali riguardano l'intrusività di questi sistemi e il rischio che la creazione di grandi banche dati biometriche possa costituire una minaccia per la privacy. Ad esempio 30 maggio 2006 la Corte Europea di Giustizia ha

⁴ Il termine *profiled* è difficilmente traducibile, riferendosi non solo alla semplice costruzione di categorie entro cui inserire i soggetti sorvegliati, ma ad una complessa attività di analisi comunemente chiamata "data mining" che sfrutta la capacità dei sistemi informatici di processare una grande mole di informazioni in tempi ridotti.

⁵ Ovviamente questo scenario *orwelliano* non considera la possibilità di errore contenuta in ogni identificazione biometrica (che è, ricordiamo, di tipo probabilistico). Ad esempio un sistema che avesse un margine di mancati riconoscimenti dello 0,01%, applicato all'intera popolazione del pianeta produrrebbe ogni giorno circa 100 milioni di falsi riconoscimenti.

abrogato gli accordi sul trasferimento di dati personali di passeggeri aerei, ivi compresi i dati dei passaporti biometrici (Passenger Name Record – PNR) tra Commissione Europea e il Bureau of Customs and Border Protection degli Stati Uniti. La sentenza ha riguardato due casi che hanno visto opposti il Parlamento Europeo e il Consiglio dell'Unione Europea (Caso C-317/04) e il Parlamento Europeo e la Commissione Europea (Caso C-318/04). In entrambi i casi⁶ la Corte ha dato ragione al Parlamento Europeo ed ha cancellato gli accordi in essere.

Il tema biometria e *privacy* è, indubbiamente, uno dei temi "caldi" nel dibattito politico ed etico e ad esso sono stati dedicati gran parte dei documenti internazionali sulla biometria, da quello dell'OECD a quello del Gruppo di Lavoro sull'Art.29 che raggruppa tutte le autorità garanti della *privacy* dei 25 paesi europei. Ovviamente in questa sede non è nemmeno pensabile di poter dare conto anche sommariamente di questi documenti a cui, quindi, si rimanda direttamente il lettore. Tuttavia vi sono due punti che preme segnalare. Il primo, ed indubbiamente più importante, riguarda un'ambiguità di fondo che nessuno di questi documenti risolve, lo status cioè da accordare ai dati biometrici. I dati biometrici devono essere considerati alla stregua di immagini estratte dal corpo umano in modo banale e pubblicamente disponibili (come, per intendersi, immagini fotografiche) oppure devono essere considerati dati sensibili, soggetti a particolare protezione (come, ad esempio, le immagini ottenute nel corso di indagini di risonanza magnetica nucleare o altre tecnologie mediche)? La risposta ha delle importanti conseguenze giuridiche e, probabilmente, dovrebbe essere articolata ulteriormente (è intuitivo che la biometria del volto, ad esempio, non possa essere comparata alla biometria dell'iride. Tuttavia cosa dire di tecnologie che misurano dati "pubblici", come l'odore del corpo o le intonazioni della voce, ma in qualche modo più "intimi"?)

Un secondo elemento che emerge da un'analisi comparata dei vari documenti internazionali dedicati alla *privacy* è quello che definisce un parametro per valutare la liceità dell'utilizzazione della biometria, cioè il cosiddetto principio di "proporzionalità". Da tutti i documenti appare chiaro che un'applicazione biometrica può essere conside-

rata eticamente e politicamente legittima solo se il grado di identificazione che assicura è proporzionato agli scopi dell'applicazione stessa. Un esempio chiarirà l'argomento: se lo scopo di un sistema biometrico è quello di identificare coloro che accedono ad una centrale atomica e di assicurare che nessun individuo non autorizzato possa giungere sino ai reattori nucleari, sarà più che accettabile usare una combinazione di biometrie che, seppur meno rispettose della *privacy* individuale, assicurino un livello di sicurezza elevato. Se invece l'applicazione biometrica serve a controllare l'accesso dei dipendenti ad una mensa aziendale (ed il caso su cui si è recentemente pronunciato il garante della *privacy* italiano), o può essere considerata *tout court* sproporzionata, oppure dovrà comunque essere adeguata agli obiettivi (ad esempio non si useranno tecnologie ad alto impatto come quelle basate sullo scanner dell'iride ma si preferiranno metodi meno sicuri ma di più facile accettazione come la lettura della geometria della mano).

Tuttavia l'impatto più profondo che la biometria ha, e promette di avere, sui dati personali riguarda probabilmente il mondo della biomedicina. La biometria sarà sempre più usata sia per limitare la consultazione di dati sensibili medici. Un cittadino comune difficilmente può immaginare quale massa di dati venga ogni giorno raccolta, immagazzinata e scambiata a scopo di ricerca, epidemiologico e per la produzione di applicazioni biomediche. La diffusione di cartelle cliniche elettroniche e di *smart card* contenenti informazioni mediche sta ponendo sempre maggiori sfide al rispetto della *privacy* ma questa è solo la punta dell'iceberg. In realtà il sistema biomedico nel suo complesso è stato travolto dalla rivoluzione informatica. Per esempio in tutto il mondo migliaia di banche di organi, di tessuto e di DNA raccolgono campioni biologici dalle più diverse provenienze (volontari sani, pazienti ospedalizzati, pezzi operatori ed autoptici), li catalogano e li studiano, ricavandone le più disparate informazioni che vengono raccolte in sistemi informatici in rete. Anche le banche di organi e tessuto a scopo di trapianto si avvalgono di sistemi informatici che permettono ai diversi centri di scambiarsi informazioni in tempo reale. I sistemi internazionali di sorveglianza delle malattie infettive - massimamente potenziati in conseguenza dell'allarme bioterrorismo e dal diffondersi di nuove malattie emergenti - stanno raggiungendo livelli di sofisticatezza prima inimmaginabili, come ha dimostrato la mobilitazione per l'epidemia di SARS del 2003 e quella per l'influenza aviaria nel 2006. La stessa ricerca farmacologica è poi ormai largamente un'impresa internazionale. Gran parte delle sperimentazioni su nuovi vaccini e nuovi medicinali avvengono in studi multicentrici che coinvolgono numerose nazioni. Tutti questi centri si scambiano informazioni e dati utilizzando il *world wide web*. Per non citare infine il campo in continua espansione della telemedicina che consente di effettuare a distanza dif-

⁶ La Corte Europea di Giustizia ha ritenuto che nel primo caso (C-317/04) il trasferimento di dati personali dei passeggeri dalle compagnie aeree alle autorità di frontiera statunitensi, in quanto giustificato da ragioni di sicurezza e militari, non rientrasse nelle competenze dell'Unione ma fosse riservato ai singoli stati nazionali. Nel secondo caso (C-318/04) la Corte ha ritenuto che la Commissione avesse applicato erroneamente l'articolo 95 del Trattato dell'Unione Europea, quello relativo alle misure da adottare per favorire lo stabilimento del mercato interno e rimuovere le barriere al libero movimento beni e di persone.

facili indagini diagnostiche e, talvolta, impegnative procedure chirurgiche. Lungo i canali elettronici – a volte dedicati, altre volte gli stessi di internet – viaggiano così ogni giorno milioni di informazioni di natura biomedica. La questione è duplice: non solo bisogna garantire che l'accesso a queste informazioni sia riservato solamente a chi ne ha diritto, ma bisogna anche impedire che diverse banche si interconnettano tra loro in assenza di una previa ed esplicita autorizzazione dei cittadini coinvolti⁷. L'interconnessione di banche dati non è infatti una procedura innocua priva di effetti, al contrario essa genera un surplus di informazione che non è facilmente prevedibile. La biometria potrebbe sia offrire uno strumento di controllo all'accesso di dati sensibili sia permettere ai cittadini di rintracciare e mantenere il dominio sui dati che li riguardano. In effetti molti ospedali e strutture sanitarie si stanno dotando di identificatori biometrici per controllare il flusso informatico di dati medici. Tuttavia i sistemi biometrici danno origine essi stessi a nuove banche dati contenenti informazioni sensibili (ad esempio caratteristiche fisiche e comportamentali delle persone inserite nell'archivio) il che imbroglia ulteriormente il problema, ricordando inevitabilmente il quesito scherzoso dei chierici medioevali: *Christophorus Christum, sed Christus sustulit orbem: Constitit pedibus dic ubi Christophorus? A rendere ancora più complesso il tutto, stanno infine le diverse normative nazionali che difficilmente si possono applicare alla proteiforme realtà di banche dati virtuali, prive di una localizzazione fisica unica, che si espandono a rizoma su diversi paesi e nazioni.*

La biometria però non è solo una minaccia alla privacy ma può anche essere una sua alleata. Sempre in ambito biomedico ci sono state varie esperienze di utilizzazione dell'identificazione biometrica per consentire procedimenti di autenticazione in grado di preservare l'anonimato degli utenti. La città di New York, ad esempio, ha avviato un programma di assistenza a pazienti sieropositivi, infetti dal virus HIV dell'AIDS, che si avvale di una carta di identità biometrica anonima. Il paziente, presentando una tessera anonima contenente i suoi dati biometrici, viene riconosciuto come legittimo possessore della tessera e quindi au-

torizzato ad usufruire del programma di assistenza senza che egli debba rivelare il suo nome o presentare un documento anagrafico. Sistemi simili sono stati proposti per l'autenticazione di particolari categorie di pazienti, spesso caratterizzate da una richiesta di anonimato (tossicodipendenti, prostitute, immigrati clandestini). Più in generale, quindi, si può dire che mentre i processi di identificazione – che si affidano a banche dati centralizzate – sono una minaccia per la privacy, i sistemi di autenticazione – dove i dati personali sono contenuti in carte magnetiche di cui rimane possessore il singolo cittadino – possono essere addirittura una *privacy enhancing technology*.

Physical privacy

Il rapporto RAND riserva il termine *physical privacy* a tutte le forme di possibile intrusività fisica della biometria.

Alcune tecnologie biometriche, pur estremamente efficienti, sono state abbandonate proprio a causa della loro elevata intrusività, ad esempio la biometria della retina, ormai caduta completamente in disuso. Al di là degli aspetti più irrazionali della questione (ad esempio la paura che tutte le biometrie basate su una forma di contatto fisico con l'apparecchio possano trasmettere malattie infettive), le preoccupazioni per la intrusività della biometria hanno spesso riguardato i rischi di stigmatizzazione che essa comporta. Ad esempio la maggior parte dei sistemi basati sulla lettura dell'iride richiedono al soggetto di accostare l'occhio ad un lettore posto ad un'altezza media dal suolo. Persone con un'altezza inferiore alla media hanno la necessità di chiedere assistenza e vengono quindi identificate previamente. In un mondo ideale tutto ciò creerebbe pochi problemi, ma nel nostro mondo – così complesso e lontano dall'ideale – è facile temere che tutto ciò possa creare forme di discriminazione. Basti pensare che dopo i sessant'anni le impronte digitali stesse diventano meno affidabili e leggibili, con la conseguenza che, in mondo in cui i passaporti fossero tutti basati sulla lettura automatica delle impronte digitali, i cittadini *seniores* incontrerebbero parecchie difficoltà ad essere identificati.

Tuttavia questi esempi non entrano ancora nel cuore del problema etico sollevato dalla biometria. La questione più complessa riguarda infatti la natura stessa delle informazioni raccolte con la biometria. Nel febbraio 2005 un'azienda israeliana, i-Mature Inc, (<http://i-mature.net/index.php>) ha commercializzato un sistema biometrico di verifica dell'età (AGR – Age Group Recognition). Un piccolo dispositivo – dal costo estremamente contenuto, 25 USD – può essere collegato a qualsiasi computer e determinare l'età ossea del soggetto che chiede di accedere a determinati contenuti *online* o intranet. Il dispositivo è tarato su diverse classi d'età (ovviamente non è in grado di determi-

⁷ Si entra qui nel delicato campo della cosiddetta *mission creep*, cioè di un uso non autorizzato di una data tecnologia. Normalmente tecnologi e ricercatori non amano discutere questi temi e ricorrono al tradizionale esempio del cacciavite (un cacciavite serve per svitare le viti, se poi qualcuno lo usa impropriamente per ferire un altro essere umano, non può esserne fatta colpa allo strumento). L'argomento però non esime dalle responsabilità, infatti chi sviluppa una tecnologia deve sempre prevederne anche un possibile uso "maligno", l'esperienza insegna che prima o poi esso si verificherà. Il problema della *mission creep* diventa poi cruciale nelle applicazioni "coperte" della biometria, ad esempio negli usi a scopo di sorveglianza e sicurezza.

nare con precisione l'età anagrafica, ma è in grado di differenziare tra bambini, adolescenti e adulti). A seconda della classe d'età il soggetto viene abilitato o inabilitato ad alcuni accessi logici. Il sistema viene venduto come dispositivo anti-pedofilia (ad esempio bloccare ad adulti l'accesso a *chat room* per ragazzi e adolescenti) e anti pornografia (ad esempio bloccare a bambini l'accesso a siti pornografici). Il sistema può essere associato a un sistema di riconoscimento delle impronte digitali (l'apparecchio misura l'età ossea sulle falangi della mano) costituendo così una soluzione integrata ai problemi di verifica età-identità via internet. Si tratta solo di un esempio. I sistemi biometrici sono in grado già ora – e lo saranno sempre più in futuro – di rivelare ben più che la semplice identità di una persona. In origine la biometria è nata come tecnica medica: cosa altro sono tutte le tecniche di indagine strumentale medica se non infatti forme di biometria? Anche semplicemente facendo una comparazione tra i dati biometrici di un individuo archiviati e quelli ottenuti nel momento dell'autenticazione o dell'identificazione si possono trarre numerose informazioni (ad esempio la geometria facciale può rivelare un intervento di chirurgia plastica o una patologia che alteri i lineamenti, come alcune endocrinopatie). Tutti i sistemi biometrici, poi, tendono anche a verificare che la fonte dei dati sia "vivente". Sarebbe infatti relativamente facile ingannare un sistema utilizzando protesi in plastica o maschere. Verificare che la fonte dei dati sia vivente implica però testare la sua reattività. Ad esempio un lettore dell'iride potrà testare simultaneamente la risposta pupillare, oppure un lettore di geometria facciale potrà anche testare l'irrorazione sanguigna del volto. Ma, per restare anche solo a questi due esempi, noi sappiamo che la risposta pupillare dipende da numerosi fattori, tra cui l'assunzione di determinati farmaci, alcune droghe ed alcool, nonché, nelle donne, da una gravidanza in corso; non diversamente lo stato di vasodilatazione o vasocostrizione dei vasi sanguigni del volto dipende da fattori emozionali, farmacologici, dalla temperatura corporea, ecc. Insomma, utilizzando un sistema di identificazione biometrico si potranno raccogliere e sommare informazioni di ogni tipo sulla salute del soggetto, sull'eventuale uso di sostanze e sul suo stato emozionale. Del resto anche la macchina della verità – un poligrafo che misura tre risposte fisiologiche: il respiro, la pressione del sangue e la capacità della pelle di condurre elettricità – non è che un sistema biometrico primitivo. La preoccupazione aumenta se si considera che le popolazioni bersaglio dei sistemi biometrici saranno inizialmente i gruppi più deboli e meno in grado di difendersi. In ambito medico sono stati già proposti come soggetti in cui utilizzare l'identificazione biometrica gli anziani non autosufficienti, i bambini e i disabili psichici (tutte categorie nelle quali si presume sia più difficile l'identificazione anagrafica tradizionale). In ambito sociale sono gli immi-

grati clandestini, i rifugiati politici, i drop out di ogni tipo, spesso provvisti di documenti validi, a costituire il target naturale della biometria.

Obiezione religiosa alla biometria

Per quanto la cosa possa apparire bizzarra, esistono anche obiezioni religiose alla biometria. Al di là di quelle relative a fattori più culturali che religiosi (l'opposizione all'uso degli stessi sistemi per maschi e femmine in alcuni paesi islamici, il rifiuto di sottoporsi allo scanner dell'iride in alcuni paesi africani, la difficoltà ad utilizzare le impronte digitali in alcuni paesi asiatici) è difficile parlare di questioni religiose sollevate dalla biometria, tranne che in un caso. Una vera obiezione religiosa si è infatti verificata soltanto negli Stati Uniti dove alcuni gruppi evangelici hanno interpretato la biometria come una tecnica per la ricerca del "marchio della bestia", cioè del segno numerico impresso dall'Anticristo sui suoi seguaci secondo la loro lettura dell'Apocalisse di Giovanni. Ancora oggi in Arizona è possibile sottrarsi all'obbligo di patenti di guida con identificativi biometrici, adducendo ragioni di fede.

BIOMETRIA E IDENTIFICAZIONE

La biometria può sembrare a prima vista una tecnologia fra le tante, forse provvista di qualche maggiore pericolosità per la *privacy*, ma sostanzialmente con minore impatto etico e sociale di altre tecnologie, in particolare quelle nate in ambito biomedico (biotecnologie, tecnologie di *imaging*, neurorobotica, ecc.). Non è così. In realtà la biometria è probabilmente una delle tecnologie con maggiori probabilità di cambiare le nostre vite nel prossimo futuro: tutto dipenderà se si svilupperà una massa critica di applicazioni sufficiente da imporla come *standard* identificativo. Se così fosse – e al momento, come si è visto, appare difficile fare previsioni in un senso o nell'altro - nulla sarà più uguale. Cercheremo ora di spiegare perché.

Identità

Il cuore della "questione biometrica" sta nel problema dell'identificazione. I tecnologi e gli ingegneri che lavorano sulla biometria tendono spesso a banalizzare questo fatto, sostenendo che la biometria non rappresenta null'altro se non una soluzione tecnica ad una questione pratica creata dalla crescente interconnessione del mondo. Proprio questa considerazione dovrebbe, invece, avvertire della centralità del tema. Mentre la questione dell'identità personale è per unanime consenso uno dei temi fondamentali della nostra epoca, non altrettanto però si può dire per l'identificazione, che appare anzi un tema negletto.

In seno alla filosofia si parla del problema della “identità personale” per riferirsi al problema di comprendere e spiegare come una persona possa rimanere la stessa, pur attraverso i cambiamenti fisici, psichici, esistenziali cui va incontro nell’arco della propria vita. Si tratta di un problema che risale all’origine stessa del filosofare e che torna ciclicamente “di moda”. Il problema ontologico sfuma nel problema psicologico e questo in quello più propriamente sociologico. Indubbiamente ogni essere umano ha bisogno di “conoscere la propria identità”, ossia di possedere di se stesso un’immagine unitaria – una narrazione biografica – che possa dare un senso alle sue azioni e alla sua vita. L’immagine di sé, però, non si radica soltanto in una memoria individuale, in una dimensione psicologica, ma trova linfa anche nella memoria collettiva del gruppo e dei gruppi di appartenenza. Così identità personale, memoria individuale e collettiva – incarnata dalla tradizione e dalle varie forme di trasmissione conscie ed inconscie della cultura – costituiscono un intreccio ricco e complesso. Diversamente dall’identità, l’identificazione descrive un processo più che una condizione, cioè si occupa dei modi in cui le identità vengono attribuite. L’identificazione presume quindi almeno due poli: un soggetto sconosciuto (privo di identità) e un soggetto, o un gruppo, conosciuti (con una identità). Se il soggetto sconosciuto verrà considerato uguale ad un soggetto conosciuto, o se verrà compreso come parte del gruppo conosciuto, saremo dinanzi ad un’identificazione positiva, al contrario si parlerà di identificazione negativa.

I processi di identificazione sono in definitiva processi di inclusione/esclusione durante i quali alcune qualità di un oggetto vengono alternativamente affermate o negate. Il meccanismo di identificazione elementare è quindi sempre del tipo: “*X è a,b,c. Ogni oggetto che sia a,b,c, è un Y (dove Y può essere un insieme con un solo membro o un insieme a più membri). Dunque X è Y*”. Questo schema funziona sia a livello psicologico – nel corso dei processi di interiorizzazione che costruiscono la personalità di ciascuno di noi – sia a livello sociale nei processi di attribuzioni di identità (identità civili, culturali, professionali, ecc.). Non considerando qui i meccanismi di costruzione delle identità psicologiche, le identificazioni sociali si costruiscono attraverso segni dello stesso tipo di quelli di cui parlava Aristotele nella Poetica e citati all’inizio di questo scritto: segni fisici, eventi storici e memorie personali, miti, ragionamenti che scaturiscono dall’azione (Arist., *Poetica* 16). In altre parole i metodi di identificazione personale sono sostanzialmente rimasti gli stessi dalla società omerica sino agli albori della civiltà moderna. L’inizio dell’epoca moderna – da metà del 1500 sino a tutto il 1600 – corrisponde al consolidarsi di nuovi metodi di identificazione (Benoist JM, 1983). Nella seconda metà del 1400, l’intensificarsi di rapporti commerciali ed economici tra le varie

città e regioni europee, aveva portato ad un incremento rapido e drammatico della corrispondenza scritta ufficiale, fenomeno soprattutto evidente nell’Europa continentale (Bely L, 1997). L’incremento della corrispondenza scritta comportò di necessità un incremento nel numero di messi che circolavano per l’Europa. Si trattava di persone che ricavavano informazioni di natura militare ed economica spesso vitali, proprio per questo era cruciale la loro corretta identificazione. Daniel Nordman ha dimostrato come in Europa, tra la fine del 1400 e l’inizio del 1500, si sviluppò un sistema di lascia-passare e passaporti ad uso di questi messi (Nordman D, 1988) e come questo sistema funga da modello per lo sviluppo successivo dei documenti di identità. È tuttavia con le guerre di religione del Seicento, con il grande movimento di truppe e comunità civili che esse comportarono, e con il consolidarsi di stati nazionali ristretti in ben definiti confini territoriali, che la necessità di accertare l’identità degli individui divenne cruciale (Groebner V, 2001). Per secoli, infatti, la comunità locale era stata la principale garante dell’identificazione personale. Le identità erano certificate dalla testimonianza diretta. Agli inizi del 1500 la trasmissione del patronimico trovò una sua prima stabilizzazione nei registri parrocchiali di nascita, che vennero appunto introdotti in questo periodo. La certificazione ecclesiastica di nascita fu utilizzata anche come prova della raggiunta maggiore età a fini ereditari e di usufrutto di benefici. Questo nascente sistema subì una grave crisi con la rottura provocata dalla Riforma. I protestanti – come prima gli ebrei – non comparivano nei registri parrocchiali cattolici e in molti paesi dell’Europa continentale si interruppe la rete di registrazione civile basata sulle strutture ecclesiastiche.

Non avrebbe senso in questa sede dilungarsi oltre sulla nascita del sistema dei documenti di identità se non per evidenziarne la struttura. A tal fine si può ricordare la descrizione che ne fece il filosofo tedesco J.G.Fichte nei “*Fondamenti del diritto naturale secondo i principi della dottrina della scienza*” del 1796, in un momento in cui, cioè, il processo di costruzione dell’identità civile è ormai giunto al suo compimento: “Il principio cardine di uno stato ben regolato dalla polizia è questo: ogni cittadino dovrà essere in ogni momento ed in ogni posto [...] riconoscibile come questa o quella persona. Nessuno deve rimanere sconosciuto alla polizia. Questo può essere ottenuto con certezza solo nel seguente modo. Ciascuno deve sempre portare con sé un documento firmato dal rappresentante del governo a lui più vicino in cui la sua persona è descritta con accuratezza [...] Nessuno quindi dovrebbe essere accolto in nessun luogo se non rendendo noto tramite il suo documento il proprio ultimo luogo di residenza e il suo nome” (citato da Caplan J, 2001). Il fondamento dell’identificazione personale, la sua fonte di legittimità, risiede quindi nello stato: è lo stato, tramite un suo funzionario, che as-

sicura il legame certo tra un documento e colui che lo possiede. In altri termini è lo stato che risponde alla domanda "Chi è la persona con cui io debbo trattare?". Anche oggi l'addetto al controllo alla frontiera accerta solamente che un governo riconosciuto attesti l'esistenza di un cittadino di quella nazionalità, con quel nome, nato quel giorno di quel mese di quell'anno, e residente in quel luogo. La foto, non diversamente da un PIN o una password, serve unicamente a verificare che colui che porta il documento ne sia il legittimo possessore, ma chi certifica l'identità è lo stato che ha emesso il documento. Tanto è vero che se lo stato certifica una nuova identità (come nei casi di collaboratori di giustizia inseriti in un programma di protezione o di persone che hanno cambiato sesso), questa diventa l'unica vera identità.

L'identificazione in un mondo globalizzato

Non è dunque per caso che i processi di globalizzazione che hanno investito il mondo nella seconda metà del 1900 abbiano messo in crisi anche la pretesa che le identità siano certificate dagli stati nazionali. La società globale è innanzitutto una società in movimento. Ogni giorno circa 8 milioni di persone si spostano utilizzando vettori aerei e la popolazione totale in movimento sul nostro pianeta (comprendente migranti per ragioni economiche, rifugiati politici, vittime di disastri naturali e di guerre, turisti, personale di organizzazioni internazionali e umanitarie) è stata calcolata attorno ad un miliardo di persone. A questo miliardo di esseri umani in movimento fisico si aggiunge almeno un altro miliardo in movimento virtuale, tanti erano già nel 2004 gli accessi alla rete internet nel mondo. Questo universo in movimento ha una necessità crescente, quella di identità certe. Organizzazioni internazionali come le Nazioni Unite, organizzazioni non governative, rifugiati politici, persone espulse dai territori d'origine da disastri naturali, apolidi provenienti da regioni occupate o teatro di guerra, cartelli mafiosi di vario tipo, reti terroristiche internazionali: sono tutti esempi di questo magma eterogeneo di persone in movimento attraverso le frontiere che sfuggono in buona parte ai controlli degli stati nazionali. La maggior parte della popolazione proveniente dai paesi in via di sviluppo non possiede documenti di identità affidabili. Ancora oggi ci sono Stati che non hanno reso obbligatoria la registrazione dei bambini alla nascita e l'Unicef ha calcolato che ogni anno nascono circa 50 milioni di bambini privi di identità civile. Quando i cittadini occidentali si preoccupano dei loro diritti alla privacy e persino all'anonimato, non ci si dovrebbe scordare che questi diritti, così come ogni altro diritto, si fondano innanzitutto sul diritto ad avere un'identità. Non c'è garanzia di legge, non c'è diritto politico, civile, sociale od economico senza identità sicure e riconosciute. In un mon-

do sempre più interconnesso non è nemmeno pensabile dividere l'umanità tra cittadini (pochi) dotati di identità certe ed affidabili, garantite da Stati "sicuri", ed una massa crescente di *sans papiers* su scala mondiale. Ma se la certificazione degli stati non possiede più un grado di sicurezza sufficiente, dove radicare i processi di identificazione? La risposta giunge quasi scontata: nel corpo.

LA CITTADINANZA BIOLOGICA

La prima globalizzazione – quella tra il 1600 e il 1800 – aveva avuto necessità di creare lo standard aureo per fondare le transazioni economiche su un valore riconosciuto internazionalmente; la globalizzazione contemporanea ha la necessità di trovare uno standard comune per fondare le transazioni elettroniche. Le transazioni elettroniche, a differenza di quelle monetarie, sono volatili, difficili da cristallizzare. Eppure la mobilità di persone e merci richiede transazioni sicure e certe. Dal turista che usa una stessa carta di credito in ogni parte del globo, dall'immigrato regolare che vuole usufruire dei benefici dello stato sociale che lo ospita, sino al finanziere che muove in tempo reale ingenti capitali da una nazione all'altra, l'esigenza è la medesima: assicurare l'accesso logico o fisico al sistema solo a coloro che ne hanno diritto. Lo sviluppo delle tecnologie di *Automatic Identification and Data Capture* risponde essenzialmente a questa esigenza. La maggior parte di queste tecnologie ripete lo schema tradizionale dei documenti di identità, seppure in modo tecnicamente più sofisticato. Si tratta di sistemi basati sul possesso di qualcosa. Così come nel sistema tradizionale l'identità è certificata dal possesso di un documento rilasciato da un'autorità statale – "tu sei colui che porta legittimamente quel documento che attesta chi tu sei" – le identità elettroniche sono certificate dalla corrispondenza tra i dati contenuti in un oggetto (carta di credito, RFID, smart card, microchip, ecc.) e la conoscenza che ciascuno ha di un determinato codice (PIN, password, firme elettroniche). La conoscenza di quel codice identifica perché un'autorità (banca che emesso la carta di credito, sistema sanitario nazionale, sistema di certificazione elettorale, ecc.) certifica che colui che conosce quel determinato codice è colui che afferma di essere. Questo sistema presenta numerose falle perché password, PIN, firme elettroniche possono essere, con diversi gradi di difficoltà "rubate", permettendo automaticamente di "rubare le identità". Ad esempio la scarsa sicurezza delle transazioni economiche via internet costituisce ancora oggi il fattore limitante principale allo sviluppo dell'*e-commerce*.

Se password e PIN non cambiano sostanzialmente lo scenario, non si può dire lo stesso per la biometria. La biometria è la risposta al problema della verifica dell'identità così come è posto in modo originale dalla network society

(Nanavati S, Thieme M, Nanavati R, 2002), cioè da una società che, nella definizione che ne dà Manuel Castells, è principalmente caratterizzata dalla crisi dello stato-nazione. 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 è indipendente da ogni stato, autorità o altra istituzione: sul proprio corpo. Questa soluzione è solo a prima vista scontata: in realtà, rappresenta una vera rivoluzione. Alcuni studiosi hanno obiettato che si tratterebbe di una novità relativa: infatti spetterebbe sempre agli stati certificare alla fine l'associazione tra una determinata caratteristica biometrica e l'identità di una persona. Non è vero. Certo, sino a che la biometria non si sarà affermata come standard - e nel caso che non si affermi - il sistema di riconoscimento anagrafico rimarrà centrale. Ma già adesso, per citare un esempio sufficientemente evocativo, è accaduto che una corte inglese accettasse di emettere una sentenza nei confronti di un frammento di DNA. In un caso di stupro, infatti, pur non essendo stato identificato lo stupratore, è stato possibile tracciarne il profilo genetico a partire dai resti organici lasciati sulla vittima. La sentenza è stata dunque emessa nei confronti di un profilo genetico, e sarà eseguita quando e se si identificherà colui che lo possiede. (Williams R, 2005) In modo meno suggestivo, ma sostanzialmente analogo, l'Unione Europea si è dotata di una banca dati centralizzata che raccoglie le impronte digitali - e nel futuro anche altri dati biometrici - dei richiedenti asilo respinti da uno dei paesi dell'Unione in modo tale che nessuno di questi si possa ripresentare sotto diversa identità alle frontiere di un altro paese. Anche in questo caso i dati fisici non sono collegati in modo significativo a nessun elemento anagrafico, e gli individui sono identificati solo tramite le proprie impronte digitali. Se la biometria diventa lo standard, il concetto stesso di identificazione è destinato a cambiare. Non importerà collegare l'individuo ad un nome e ad un cognome, ad una città ed una nazione, a una data e un luogo di nascita, e nemmeno ad un sesso o una professione: tutti questi dati diventeranno inessenziali. Basterà collegarlo ad una sua caratteristica fisica immutabile, unica e non riproducibile, che possa essere estratta tramite un algoritmo e collezionata in una banca dati. Se si presta attenzione, questo processo rivoluziona non solo il sistema di documenti di identità basato sull'autorità degli stati nazionali, ma anche ogni precedente sistema di identificazione e persino il nostro rapporto con la corporeità.

Un nuovo genere di cittadinanza sta nascendo nell'età della genomica, della biotecnologia e della biometria. Chirurgia cosmetica, chirurgia per la rettificazione del sesso, protesica, impianti di *biochips*, tatuaggi, *piercing*, scarnificazioni, *body art*, trapianti di organi: non si può credere che il concentrarsi di tante diverse pratiche - però con una

simile *ratio* - sia casuale e priva di effetti antropologici. Seguendo altri autori (Nikolas Rose, 2003) chiamiamo questa nuova forma di cittadinanza "la cittadinanza biologica". Ci sono state molte discussioni sull'importanza delle conoscenze biologiche nella politica e nella storia dei diciannovesimo e ventesimo secolo, ma il tema della biologizzazione della politica è stato esplorato raramente dalla prospettiva della cittadinanza. Le diverse pratiche di cittadinanza possono essere lette come pratiche che coinvolgono direttamente la dimensione della corporeità. In altri termini il corpo a diversi livelli, dai più superficiali (chirurgia estetica) sino a quelli molecolari (terapia genica), diventa l'origine dei processi di cittadinanza, cioè i cittadini non sono più definiti dal *genos* o dalla polis (cioè dall'insieme dei rapporti umani che intrattengono) ma dalla loro costituzione biologica. Il "cittadino biologico" sta all'intersezione tra politica e biopolitica. Il suo corpo è di nuovo un corpo nudo davanti al potere, come quello dei *kúroi* greci e come quello di Ulisse.

Giorgio Agamben paragona tutti noi, nel momento in cui presentiamo un passaporto biometrico che ci permette di varcare una frontiera, ai prigionieri di Guantanamo: corpi nudi, privi di storia e di identità che non sia la pura appartenenza biologica. Come i corpi dei prigionieri di Auschwitz-Birkenau, il nostro corpo tatuato, letto dalla biometria, serve a ricordarci il nostro essere fuori dall'ordine delle famiglie, dall'ordine del *genos*, e di appartenere per sempre al mondo della *ph?sis*.

IL VOLTO E IL NOME

Tutto ciò ci riporta all'inizio del nostro percorso, alla storia di un uomo che per dieci lunghi anni vagò come straniero prima di giungere alla propria patria. Ulisse appare ai servi che lo accolgono, alla sua stessa moglie, come *aprosopon*, senza volto. Nell'antichità sono gli schiavi ad essere senza volto ed è interessante notare come la parola che in greco designa il volto, *prosopon*, sia la stessa da cui probabilmente origina anche il termine latino *persona*. La persona, potremmo dire, è un volto.

Il volto è il punto di incontro tra biologia e storia, tra *nomos* e *ph?sis*. Secondo i padri orientali il volto è il centro del corpo e il centro dell'icona. Domina tutto perché è il luogo della presenza di Dio. L'attenzione è attratta dallo sguardo, dagli occhi che irradiano il fascino del divino. Gli occhi sono talmente il centro dell'icona che il volto è detto "sguardo" o "sembianza" (*link*). La biometria si colloca in questa doppia polarità, la stessa che avevamo trovato nella cicatrice di Ulisse: da un lato la biometria riduce la cittadinanza ai suoi costituenti biologici elementari, dall'altra è una tecnologia che estrae (letteralmente) ciò che vi è di umano dalla pura naturalità, che trasforma il dato fi-

sico ('immagine di un volto, le tracce lasciate da una mano, l'odore di un corpo, il colore di un occhio) in una sequenza matematica e in uno schema geometrico.

Questa tensione si ritrova anche nelle diverse politiche: da un lato coloro che vogliono una biometria sempre più focalizzata sulla sicurezza e l'accertamento di identità sicure, dall'altra coloro che pensano che la biometria sia una grande opportunità per dare un'identità ai milioni di abitanti del mondo che non la posseggono.

Lo status morale, culturale e giuridico del corpo umano è cambiato nei secoli e nelle varie culture umane. 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'essere 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. Si apre un orizzonte postumano, l'orizzonte del cyber-Golem. La società contemporanea – postmoderna o della tarda modernità – si caratterizza per una percezione schizofrenica del corpo. Da un lato la corporeità è esaltata e presentata come fonte della stessa dignità umana. Da un altro lato, però, mai il corpo è stato così martoriato e vilipeso: un corpo reificato, trasformato in oggetto da modificare a piacimento con interventi protesici e di chirurgia cosmetica, sino ad arrivare al vero e proprio delirio del corpo "sostituibile" *ad libitum* tramite la clonazione.

Un segno evidente di questo approccio paradossale al corpo è il modo in cui la pelle (che del corpo è limite e contenitore) è nel contempo venerata (mai tante cure dagli antichi greci ad oggi erano state dedicate alla pelle umana e mai tanto orrore avevano sollevato i segni del tempo, rughe e cicatrici) e martoriata (la nostra è anche l'epoca del tatuaggio di massa, della moda del *piercing*, dei microchip impiantabili).

La biometria rivela l'ultima trasformazione del corpo, la sua "digitalizzazione", la sua trasformazione in corpo virtuale contenuto in banche dati elettroniche. Il corpo digitale è, per un verso, un corpo disperso, contenuto nei mille rivoli elettronici della rete; per un altro verso è invece un corpo quanto mai compatto. Per anni sociologi, filosofi, tecnoscienziati ci avevano assicurato che la nostra società si stava dirigendo verso un mondo fatto da identità multiple e cangianti. Ci ritroviamo invece in un mondo sempre più simile a quello in cui lo schiavo che cercava di fuggire veniva marchiato a fuoco per essere riconosciuto da chiunque. La biometria può esser quel marchio, ma può anche essere il volto che da un nome, il gesto che trasforma la folla anonima del mondo globalizzato in un insieme di persone. Dipenderà da noi scegliere l'uno o l'altro percorso.

Ringraziamenti: *Questo lavoro è stato supportato da un contratto di ricerca con la Commissione Europea, relativo al progetto BITE (contract nr SAS6-2004-006093)*

Bibliografia

- Bely L, ed., 1997, *L'invention de la diplomacie: Moyen Age*, PUF, Paris
- Benoist JM, ed., 1983, *Figures du Baroque*, PUF, Paris
- BIOVISION, 2003, Roadmap for Biometrics in Europe to 2010, available <http://www.eubiometricsforum.com/dmdocuments/BIOVISION-Roadmap.pdf>
- Bulmer M, 2003, *Francis Galton: Pioneer of Heredity and Biometry*, Johns Hopkins University Press
- Caplan J, 2001, This or that particular person; protocols of identification in Nineteenth-Century Europe, in Caplan J, Torpy J, eds. "Documenting Individual Identity", Princeton University Press
- Clarke R, 1994, The Digital Persona and Its Application to Data Surveillance, *The Information Society*, 10: 77-92.
- Data Protection Working Party of the European Commission, 2003, Biometrics, WP 80, 12168/02/EN, available www.europa.eu.int/comm/privacy
- Davies S, 1994, Touching Big Brother: How Biometric Technology Will Fuse Flesh and Machine, *Information Technology & People*, Vol. 7, (4):7
- Dery M, 2000, *Ritual Mechanics: Cybernetic Body Art*, in Bell D, Kennedy B (eds), 2000, *The Cybercultures Reader*, Routledge, London
- EC-DG JRC-IPTS, 2005, *Biometrics at the Frontiers: Assessing the impact on Society*, available www.jrc.cec.eu.int
- Giddens A, 1991, *Modernity and Self Identity*, Polity Press, Cambridge UK
- Groebner V, 2001, Describing the Person, Reading the Signs in late medieval And Renaissance Europe: Identity Papers, vested figures, and the limits of identification, in Caplan J, Torpy J, eds. "Documenting Individual Identity", Princeton University Press
- Haraway D, 1991, A Cyborg Manifesto: Science, Technology and Socialist Feminism in the late 20th century, in Bell D, Kennedy B (eds), 2000, *The Cybercultures Reader*, Routledge, London
- International Biometrics Group, 2005, BITE Global Biometric Market and Industry Report, available <http://www.bioethics.it>
- Mordini E, 2004b, Global Governance of the Technological Revolution, in Jacquart R. (ed): *Building the Information Society*, Kluwer Academic Publishers, Boston/London: 585-592
- Mordini E, 2005, Biowarfare as a Biopolitical Icon, *Poiesis & Praxis*, Vol 4, 1: in press
- Mordini E, Ottolini C., 2005, Implicazioni etiche e sociali della biometria, *L'Arco di Giano*, 45:53-72
- Munroy BJ, 2004, A coalition to drive personalised medicine forward, *Personalised Med.*, 1(1),9-13
- Nanavati S, Thieme M, Nanavati R, 2002, *Biometrics: Identity Verification in a Networked World*, J.Wiley & Sons
- Nikolas Rose, 2003, *Biological Citizenship*, in Ong A., Collier S., (eds.) *Global Anthropology*, Blackwell, 2003
- Nordman D, 1988, Sauf-conduits et passports en France, à la Renaissance, in Caerd J, Margoli JC, eds: "Voyager à la Renaissance", Seuil, 145-58
- Piccaluga G., 1988, Potmos impara a scrivere, *Scrittura e Civiltà* 12: 5-46
- Van der Ploeg I, 1999, The illegal body: 'Eurodac' and the politics of biometric identification, *Ethics and Information Technology* 1: 295-302
- Williams R, 2005, Genetic Identification and Criminal Investigation: Making and Using Forensic DNA Databases, paper presented in the 2nd BITE Project Meeting, Lancaster, 24th January 2005
- Woodward J D Jr, Webb K W, Newton E M, Bradley M, Rubenson D, 2001, *Army Biometric Applications: Identifying and Addressing Socio-cultural Concerns*, Rand Publications available <http://www.rand.org/pubs/publications/MR/MR1237/>