

Le differenze tra approccio empiristico e ontologico all'identità personale implica rilevanti conseguenze anche in ambito giuridico e socio-politico.

L'approccio empiristico, ammettendo la variabilità dell'identità personale (in base alla presenza o all'assenza di qualità e comportamenti ritenuti rilevanti che possono comparire o scomparire nelle diverse fasi evolutive della vita), è l'orientamento che si appella alla neutralità del diritto, chiamato a garantire la libera espressione della volontà individuale e che deve astenersi dal prendere posizione rispetto alle diverse etiche nel contesto pluralistico sociale, divenendo o strumento formale della volontà o manifestazione della fattualità. In questa prospettiva, la dignità umana non è riconosciuta in sé, ma è attribuita estrinsecamente dal soggetto.

Di contro, l'approccio ontologico all'identità personale elabora una fondazione teoretica forte del concetto di "dignità umana" che, tematizzando concetti e categorie estranee alla dimensione giuridica, quali "sostanza" e "essenza", richiama alla originaria identificazione tra persona ed essere umano riaffermando il fondamento e il senso dei diritti umani¹¹³.

La filosofia ontologica della persona pretende di richiamare il diritto a quella che ritiene sia la sua originaria vocazione nella difesa di ogni persona secondo giustizia. Il riconoscimento della dignità intrinseca della persona umana costituisce il punto centrale del dibattito tra personalismo filosofico e diritto¹¹⁴ ed esige uno sforzo continuo per un efficace bilanciamento sul piano teoretico e sul piano analitico, dunque pratico.

2. *Biometria analitica*

Sul piano pratico e analitico l'identità biometrica avoca a sé, peculiarità, tratti e caratteristiche proprie, univoche e irripetibili di ogni essere vivente e si distinguono in:

- a. caratteristiche biometriche anatomiche o fisiologiche, basate su dati derivati da misurazioni effettuate su caratteristiche fisiche di ogni essere vivente (ad esempio negli umani sono l'impronta digitale, l'iride, la retina, la geometria della mano, i tratti somatici del volto, ecc.);
- b. caratteristiche biometriche comportamentali, ossia caratteristiche basate su dati che riguardano aspetti riconducibili a specifici "comportamenti" propri ed univoci di un essere vivente (ad esempio, negli umani troviamo il riconoscimento vocale, le dinamiche di apposizione della firma, l'andatura e la gestualità, le espressioni del viso, la postura, ecc.)¹¹⁵.

Nelle caratteristiche biometriche anatomiche rientra, per definizione, anche l'analisi del DNA, che non è inclusa tra le tecniche biometriche di riconoscimento previste dalle legislazioni vigenti, a causa della complessità intrinseca,

¹¹³ Sul punto si vedano: L. Palazzani, *Il concetto di persona tra bioetica e diritto*, Torino, Giappichelli, 1996; A. Pessina, *Bioetica. L'uomo sperimentale*, Milano, Mondadori, 1999; V. Possenti, *La bioetica alla ricerca dei principi: la persona*, in «Medicina e Morale», n. 6/1992, pp. 1075-1096.

¹¹⁴ F. D'Agostino, *La bioetica, le biotecnologie e il problema dell'identità della persona*, in A. Pavan (Ed.), *Dire persona. Luoghi critici e saggi di applicazione di un'idea*, Bologna, Il Mulino, 2003, p. 133.

¹¹⁵ G. Preite, *Politica e biometria. Nuove prospettive filosofiche delle scienze sociali*, cit., pp. 88-89.

dell'impossibilità di operare in tempo reale e, *in primis*, per i suoi livelli di invasività nella sfera più intima dell'individuo.

Tra le tecniche biometriche anatomiche la rilevazione delle impronte digitali è la tecnica più consolidata per il riconoscimento della persona¹¹⁶. I procedimenti di riconoscimento basati sulla biometria dell'impronta digitale sono tre:

- a. riconoscimento dell'immagine completa dell'impronta;
- b. riconoscimento delle *minutiae*, cioè le caratteristiche minori dell'impronta¹¹⁷;
- c. riconoscimento della corrispondenza tra aree di una stessa impronta.

Sotto il profilo della vulnerabilità, gli attuali sistemi tecnologici e informatici, basati sul riconoscimento delle impronte digitali, sono a tal punto efficaci da verificare se l'impronta biometrica digitale corrisponde ad una persona viva o meno (attraverso la lettura di impulsi elettrici). La gestione di un sistema biometrico di autenticazione basato sulla lettura delle impronte digitali presenta notevoli vantaggi in termini di efficacia, efficienza ed economicità in considerazione dei bassi costi di creazione, implementazione e gestione di tali sistemi; infatti, la registrazione delle impronte digitali in database è agevole, come anche la sua conservazione nel tempo, le impronte restano invariate per tutta la durata della vita di una persona, tranne che non subentrino eventi straordinari o incidenti che causano l'alterazione dei dati registrati (ad esempio: forti bruciate, abrasioni, amputazioni, ecc.). Tuttavia, a fronte di tali vantaggi occorre considerare la resistenza psicologica che i soggetti manifestano verso questa tecnica biometrica, poiché storicamente associata al settore investigativo e giudiziario per censire, individuare e catalogare i criminali. Nonostante tali riserve, la rilevazione dell'impronta digitale, a parità di altre tecniche, è ora la più indicata per le verifiche di accesso logico in spazi, aree e contesti (aree militari, zone protette, tribunali, aeroporti, specifici settori ospedalieri, ecc.) in cui l'accesso fisico del soggetto deve essere motivato e autorizzato.

Anche la rilevazione delle caratteristiche dell'iride è una tecnica precisa d'identificazione che si colloca tra le meno invasive. La tecnica si basa sull'iridologia, scienza che studia la lettura della morfologia e del cromatismo dell'iride come fonte d'informazione sugli aspetti costituzionali, fisici, psichici, patologici, ereditari dell'intero organismo e che rendono ogni individuo unico, differente da ogni altro. Più complicata e invasiva della precedente è, invece, la tecnica per il riconoscimento della retina, il cui impiego comporta difficoltà di rilevazione di non poco conto, si pensi ai portatori di occhiali o di altri correttivi del campo visivo, ed elevati costi legati alle apparecchiature; ne deriva che il suo impiego è confinato a particolari necessità di sicurezza¹¹⁸.

Tra le tecniche biometriche comportamentali, la rilevazione dei tratti somatici del volto (geometria del volto) è molto efficace. Tale tecnica si basa sulla misurazione delle caratteristiche olistiche, ossia sull'analisi di ogni singolo tratto che

¹¹⁶ Nel 1902 Vucetich elaborò il primo metodo di classificazione per il riconoscimento dei criminali, anche se la tecnica per la raccolta delle impronte era ancora imperfetta e poco attendibile; il metodo fu ripreso e perfezionato nel 1907 da Gasti per la Scuola Italiana di Polizia Scientifica. Nel 1950 in America si svilupparono i primi sistemi automatici per il riconoscimento delle impronte digitali grazie agli studi portati avanti dall'F.B.I. in collaborazione con il N.B.S. e con la Rockwell International Corporation.

¹¹⁷ Le *minutiae* sono delle minuscole linee presenti sull'epidermide e che formano dei vortici. Ogni impronta di un dito comprende fino a cento *minutiae* che hanno la caratteristica di essere uniche per ogni individuo. Vengono denominate dagli esperti del settore anche "dermatoglifo" (firma della pelle).

¹¹⁸ G. Preite, *Politica e biometria. Nuove prospettive filosofiche delle scienze sociali*, cit., p. 90.

caratterizza il volto nell'insieme. Le foto o i video consentono, infatti, di identificare una o più persone utilizzando dei database in cui sono immagazzinati i volti¹¹⁹.

Negli ultimi anni, a seguito degli avvenimenti terroristici internazionali, si sono diffusi sistemi alquanto sofisticati di rilevazione dei tratti somatici con lo scopo di identificare (riconoscere) una classe di individui ritenuti pericolosi¹²⁰.

La rilevazione della geometria della mano è molto più semplice poiché consiste nella verifica delle misure e della conformazione dell'arto, combinata spesso con la rilevazione di conduzione elettrica al fine di garantire l'effettivo contatto della mano sulla superficie del rilevatore. Tale tecnica è utilizzata in molti progetti che prevedono l'autenticazione biometrica nel caso di accessi frequenti con un basso livello di sicurezza. La ricerca di modelli innovativi di riconoscimento basati su peculiarità fisiche e comportamentali sta affermando a livello sperimentale altre chiavi biometriche, prima ignorate dalla scienza tecnologica e che riguardano la fisionomia del corpo umano, in particolare le caratteristiche dell'orecchio, delle labbra e dell'impronta non solo delle dita, ma anche della mano e ancora lo stesso odore emanato dalla cute del corpo. In particolare, il filone che si riferisce alla individuazione, analisi e codifica delle emanazioni corporee ipotizza la possibilità di utilizzare uno strumento basato su speciali sensori capaci sia di assorbire gli odori, sia di convertirli in corrispondenti dati informatici; mentre, le caratteristiche biometriche dell'orecchio e delle labbra, appaiono meno interessanti dal punto di vista pratico, essendo preferibile il riconoscimento automatico dell'impronta della mano, infatti, la rilevazione delle "linee" della mano, come in precedenza detto, è sicuramente la tecnica più diffusa e psicologicamente più tollerata dall'utente¹²¹. In generale le tecniche di riconoscimento biometrico che si basano sulle caratteristiche comportamentali hanno trovato spazio applicativo in tutti i progetti che prevedono l'autenticazione biometrica mista o multipla.

Il riconoscimento biometrico fa riferimento all'identificazione della persona attraverso l'utilizzo di caratteristiche sue proprie. Gli obiettivi che il riconoscimento biometrico si propone sono due:

- A. verificare la dichiarazione di identità della persona;
- B. associare identità ad un soggetto utilizzando differenti modalità di accesso.

Nel caso di accesso fisico, il controllo biometrico si realizza attraverso una procedura di accertamento della titolarità personale all'ingresso di una zona o un'area riservata, un edificio protetto, ecc.

Nel caso di accesso logico, il controllo biometrico è effettuato tramite una procedura di accertamento circa la titolarità della persona interessata (utente) a usufruire di una determinata risorsa informatica.

Un'ulteriore distinzione riguarda le modalità di verifica e le modalità di identificazione.

¹¹⁹ I sistemi per il riconoscimento facciale più utilizzati sono: il PCA (Principal Component Analysis), che interpreta il volto come un punto in uno spazio delle immagini e lo proietta su un nuovo spazio attraverso una trasformazione lineare che massimizza la varianza dei volti; l'LCA (Local Component Analysis), con il quale si cerca di operare il riconoscimento automatico dei volti in immagine sia statiche che in movimento.

¹²⁰ Cfr. G. Iovane, M. Gaeta, S. Salerno, *Bio-Face system*, Paper in *Atti del Convegno NIWeek*, Austin, 2004.

¹²¹ Cfr. M. C. Siddi, *Chiavi biometriche e impatto sulla Pubblica Amministrazione*, in *Atti del Convegno Firma digitale o garanzie biometriche?*, 2006, in <http://spol.unica.it/teleamm/>.

Nel primo caso, quando si parla di processo di verifica, è da intendersi un processo in cui i dati acquisiti in un determinato momento dal sensore biometrico sono comparati con un unico dato depositato dall'utente nella fase di registrazione e custodito su un dispositivo sicuro o in un archivio magnetico indicizzato, esempio un codice identificativo.

Nel secondo caso i dati acquisiti in un determinato momento dal sensore biometrico sono comparati con un insieme di dati contenuti in un archivio. Dal punto di vista prettamente tassonomico il riconoscimento biometrico include entrambe le fasi.

Un sistema biometrico è, inoltre, caratterizzato da due differenti tipi d'identificazione: positiva e negativa.

L'identificazione positiva si ha quando la persona interessata dichiara (anche implicitamente) di appartenere al gruppo di utenti noti al sistema, in tal caso assume rilevanza il legame tra la persona esaminata e l'identità memorizzata in precedenza nel sistema; la persona chiede, in questo caso, un'identificazione in positivo che si traduce nella verifica della propria identità tramite un confronto automatico tra il campione presentato e uno o più dati biometrici memorizzati. Se il sistema d'identificazione positiva non riesce a trovare un grado di coincidenza tra il campione in esame e tutti i campioni registrati superiore ad una soglia prefissata, l'esito è un rifiuto; in caso contrario, la corrispondenza tra il campione in esame e uno dei campioni registrati comporta una accettazione. In tale procedura possono essere utilizzate entrambe le modalità operative di confronto basate sulla verifica dell'identità e sull'identificazione¹²².

Con il sistema d'identificazione negativa, invece, la persona dichiara (anche implicitamente) di non appartenere al gruppo di utenti noti al sistema. Il procedimento, dunque, stabilisce e verifica che una determinata persona da identificare non risulti tra un gruppo di persone (utenti) inclusi e riconosciuti dal sistema. Se il sistema d'identificazione non riesce a trovare un grado di coincidenza (superiore a una soglia prefissata tra il dato campione preso in esame e tutti i dati biometrici registrati) il risultato dell'operazione si traduce in una accettazione, nel caso contrario si genera un rifiuto.

Per questo procedimento può essere utilizzata soltanto la modalità di confronto/identificazione "1 : n", dove "n" rappresenta l'intera popolazione interessata, frequentemente inclusa in liste ristrette accessibili da un numero limitato di utenti: le *check list* (oppure le *short list* per i casi critici)¹²³.

Numerosi sono gli esempi riguardanti la procedura d'identificazione negativa, come i controlli effettuati al fine di evitare l'emissione di documenti a coloro che dichiarano una identità falsa, i controlli per evitare la concessione multipla di benefici assistenziali sotto false identità, i controlli sull'immigrazione e i controlli inerenti la sorveglianza.

Questa procedura è largamente utilizzata negli Stati Uniti con lo scopo di impedire l'uso di più identità da parte di una singola persona.

In generale i sistemi biometrici sono impiegati dagli apparati pubblici con il consenso degli interessati o in regime di biometria interattiva. Tuttavia, in molte applicazioni di carattere investigativo, giudiziario, governativo, militare, è

¹²² G. Preite, *Politica e biometria. Nuove prospettive filosofiche delle scienze sociali*, cit., p. 92.

¹²³ Ivi, p. 93.

previsto l'utilizzo di sistemi biometrici senza che le persone esposte ne siano a conoscenza. Si tratta di biometria passiva, tipico esempio sono i sistemi di sorveglianza installati nei porti, stazioni, aeroporti, ossia in quei luoghi caratterizzati da un largo afflusso di pubblico e quindi definiti "aree a rischio".

3. Etica e metodo biometrico

In scienza, è definito universo l'insieme di elementi di cui è negata una conoscenza esaustiva e integrale anche per uno solo dei caratteri propri e comuni. Caratteristica dell'universo non è dunque l'infinita, ma l'eccedenza della sua misura rispetto a quella del nostro dispositivo di conoscenza¹²⁴. Il problema della misurazione degli elementi allora è risolto prelevando dall'universo un frammento che sia, da una parte, sufficientemente piccolo per consentirne l'intera esplorazione e dall'altra sufficientemente grande e composito per riprodurre, pur in scala ridotta, l'immagine rappresentativa dell'universo.

Questo frammento si chiama campione e il campionamento è, di fatto, come teoria e come pratica, la più importante tecnica della metodologia statistica, preliminare e pregiudiziale a tutte le altre tecniche del ramo. Inoltre, per descrivere il campione bisogna produrre delle statistiche che arrivino a dire cose credibili sull'universo e che consentano di raggiungere la prova di significatività o saggio dell'ipotesi che è, in modo implicito o esplicito, il *primum movens* di ogni esperimento e che realizza insieme con la stima fiduciale l'ulteriore e fondamentale compito della statistica: essere una metodologia per decidere¹²⁵.

È a questo livello che gli esiti generano una problematizzazione rilevante sul piano filosofico-politico e sociologico, dando evidenza all'elevata complessità che caratterizza il rapporto tra etica e metodo biometrico¹²⁶.

La stessa neutralità assiologia del metodo è messa in discussione quando è applicata alla tassonomia, alla misurazione della vita, alla misurazione nell'uomo: «All'interno di un ambito positivo di eticità, è etico sperimentare con il maggiore rigore biometrico; ritenendo che il rigore etico ed il rigore metodologico sono ortogonali cioè possono darsi l'uno o l'altro o entrambi o nessuno¹²⁷».

Nell'ambito metodologico statistico è comunemente condiviso porre il rapporto di osservazione (osservatore/osservato), in termini "catalettici", cioè di assunzione di tutta la soggettività al polo attivo dell'indagine e di riduzione totale all'oggettività del polo passivo dell'indagine stessa.

L'assunzione di soggettività da una sola parte del rapporto, significa l'esercitato diritto di programmare, descrivere e decidere le condizioni dell'oggetto. Qui si coglie uno degli aspetti fondamentali della metodologia statistica quale metodologia per lo studio delle cose, dove la definizione più comprensiva e più corretta di "cosa" è quella di "non persona".

¹²⁴ Ad esempio, il numero dei granelli di sabbia presenti sul pianeta non è infinito, ma rappresenta la parte di un universo del quale vogliamo conoscere solo alcune caratteristiche (peso, dimensione, forma, ecc.) di ogni granello di sabbia senza doverli misurare tutti; tuttavia, lo stesso universo dei granelli di sabbia può risultare infinito riguardo a tutte le pesate o a tutte le determinazioni del diametro dei granelli esistenti. Sul tema cfr. G.A. Maccacaro, *Biometria, Principi e metodi*. Padova, Piccin, 1978, p. XXIII.

¹²⁵ *Ibidem*.

¹²⁶ G. Preite, *Politica e biometria. Nuove prospettive filosofiche delle scienze sociali*, cit., p. 94 e ss.

¹²⁷ G. A. Maccacaro, *Introduzione*, in F. Salvi, B. Chiandotto (Eds.), *Biometria, Principi e metodi*, cit., pp. XXV e ss.