IL REGIME GIURIDICO
DEI SISTEMI DI RICONOSCIMENTO BIOMETRICO

di Luca Giacopuzzi*

I sistemi di rilevazione biometrica[1] hanno ad oggetto dati ricavati dalle caratteristiche fisiche o comportamentali di un individuo, risultanti in un modello di riferimento preordinato al riconoscimento della persona.

Se a tutti è noto che il dato biometrico è un dato personale[2], ai più, tuttavia, sfugge che esso è un dato assolutamente *sui generis*, e ciò tanto per la natura[3] dello stesso quanto per le implicazioni giuridiche del relativo trattamento. Basti considerare, in relazione a quest'ultimo profilo, che i dati biometrici – pur rappresentati in via normativa tra i dati cd. semi-sensibili – possono, in alcuni casi, rientrare nella categoria dei dati sensibili[4], con le conseguenze che ne derivano.

* Avvocato in Verona (www.lucagiacopuzzi.it), titolare dello Studio Legale Giacopuzzi (www.studiogiacopuzzi.it).

[1] Detti, pertanto, si fondano su:

i) dati (trattasi di valori numerici generati tramite funzioni matematiche), ottenuti da

ii) caratteristiche fisioniomiche (per esempio: rilevazione dell'impronta dattiloscopia o della geometria della mano, riconoscimento facciale o vocale, scannerizzazione della retina o dell'iride, analisi della cd. "dynamic signature", esame dell'andatura) risultanti in un

iii) modello di riferimento (cd. "template") deputato al riconoscimento dell'interessato (a mezzo di un processo informatico di identificazione o di autenticazione).

[2] La raccolta di dati biometrici e il successivo utilizzo degli stessi sono operazioni di trattamento di dati personali, alle quali trova applicazione la normativa di cui al D.Lgs. 196/03 (di seguito "il Codice"). Sul punto vedasi, anche, i seguenti interventi del Garante per la protezione dei dati personali: Provv. 19.11.1999, Provv. 21.07.2005, Provv. 23.11.2005, Provv. 01.02.2007.

[3] Come evidenziato dai Garanti europei nel "Documento di lavoro del 01.08.2003", il dato biometrico presenta tre caratteristiche del tutto peculiari: l'universalità, posto che l'elemento biometrico è presente in ciascun individuo; l'unicità, atteso che la componente biometrica è distintiva di ogni persona; la permanenza, dato che ognuno tendenzialmente conserva la propria caratteristica biometrica nel tempo.

[4] L'impiego di sistemi biometrici di riconoscimento facciale, per esempio, può comportare il trattamento di dati che rivelano l'origine etnica o razziale dell'interessato.

Il trattamento dei predetti dati richiede, quindi, elevate cautele per prevenire possibili pregiudizi a danno degli interessati (i quali, peraltro, avrebbero non poche difficoltà a dimostrare l'eventuale falsificazione della propria identità biometrica).

Proprio per le criticità che connotano il dato biometrico, il trattamento delle caratteristiche fisiche e comportamentali di una persona, ai fini del riconoscimento della stessa, costituisce oggetto di un vivace dibattito dottrinale, nell'ambito del quale, secondo molti, ad oggi non è possibile individuare soluzioni condivise, definitive ed appaganti.

Non si ritiene di condividere questa opinione, poiché, sebbene la materia sia complessa e di non immediata decifrazione, riteniamo raggiunte alcune certezze, di cui si dirà.

L'Autorità Garante per la protezione dei dati personali ha avuto modo di occuparsi della tematica in esame in diverse occasioni.

Con Comunicato del 09.05.2006, il Garante ha individuato una sorta di "decalogo" per il corretto utilizzo dei dati biometrici, nel quale spiccano anche prescrizioni di carattere tecnico, in parte riprese dalla successiva Deliberazione n.53 del 26.11.2006.

E'stato precisato, in particolare, che nei casi in cui sia possibile far ricorso a dati biometrici la centralizzazione delle informazioni in una banca dati non risulta consentita, in quanto, alla luce del principio di cui all'art. 3 del D.Lgs.196/03[5] (principio di necessità), i sistemi informativi devono essere configurati in modo da ridurre al minimo l'utilizzo di dati personali.

In luogo, quindi, di modalità centralizzate di trattamento dei dati biometrici devono adottarsi soluzioni di riconoscimento biometrico basate su modelli, protetti con chiave crittografica, residenti in supporti posti nell'esclusiva disponibilità dell'interessato e privi dell'immagine[6] o di indicazioni nominative riferibili a quest'ultimo, sì che siano remote le possibilità di abuso dei dispositivi in caso di smarrimento degli stessi.

[5] Trattasi del Codice per la protezione dei dati personali, di seguito "il Codice".

[6] Indicazione aggiunta con Provv. 01.02.2007.

Per disposto dell'Autorità Garante, inoltre, i dati raccolti non possono di regola essere conservati per oltre sette giorni e, anche quando detto arco temporale possa essere protratto, vanno assicurati idonei meccanismi di cancellazione automatica dei dati.

In via di estrema sintesi, si rileva che l'Autorità, con particolare riguardo all'ambito lavorativo, ha ritenuto illecito l'utilizzo generalizzato e incontrollato dei dati biometrici, in quanto detto può essere giustificato solo in casi specifici, in relazione alle finalità perseguite e al contesto in cui essi sono trattati (per esempio, accesso ad aree dell'azienda per le quali debbano essere adottati livelli di sicurezza particolarmente elevati in ragione di specifiche circostanze o delle attività ivi svolte).

Nella maggioranza delle occasioni in cui tratta del tema, peraltro, il Garante sembra non distinguere il concetto di autenticazione e quello di identificazione; concetti che, come insegnano (anche) i Garanti europei nel "Documento di lavoro del 01.08.2003", devono essere tenuti, invece, ben differenziati.

Per autenticazione si intende quel processo finalizzato a verificare che l'incaricato che chiede di accedere ad un determinato sistema sia effettivamente colui che dichiara di essere, attraverso la verifica della sua identità basata sull'elaborazione di dati che si riferiscono all'incaricato medesimo. L'autenticazione, dunque, risponde alla domanda: "Tizio è la persona che dichiara di essere?", e il sistema prende una decisione 1:1 (sì/no).

L'identificazione, invece, consiste in quel processo in forza del quale un sistema riconosce un individuo, e ne accerta l'identità, confrontando i dati del medesimo con quelli di una molteplicità di soggetti, i cui dati sono a loro volta registrati, dando, quindi, risposta alla domanda: "Chi è Tizio?"; il sistema, in tal caso, prende una decisione 1:n.

Ciò premesso, va osservato che l'utilizzo di elementi biometrici come credenziali di autenticazione al fine di trattare i dati con strumenti elettronici è espressamente contemplato dalla Regola 2 del Disciplinare tecnico in materia di sicurezza , Allegato B al Codice.

A mente di detta Regola, infatti, "le credenziali di autenticazione consistono", tra l'altro, "in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave".

Tenuto conto del chiaro dettato normativo che precede, l'autenticazione informatica è misura di sicurezza che pare legittimare "*in re ipsa*" l'utilizzo di dati biometrici, a prescindere dalla sussistenza di ulteriori particolari finalità.

A tale conclusione sembra pervenire, del resto, lo stesso Garante, il quale, nel Provvedimento 21.07.2005, individua la finalità di sicurezza del trattamento dei dati personali quale autonoma causa di giustificazione per il trattamento dei dati biometrici, accanto a quella, più generica, che rimanda alle finalità perseguite e al contesto in cui essi sono trattati, da valutarsi caso per caso.

Non tragga in inganno la vicenda oggetto del Provv. 17.11.2010; detto riguarda una fattispecie che l'Autorità Garante qualifica come sistema di autenticazione su base biometrica volto a verificare la presenza in servizio del personale (finalità, quindi, che presuppone la previa identificazione dell'interessato). In verità, all'esito di un'attenta lettura del Provvedimento, si evince che il fine ivi descritto viene raggiunto non già mediante l'impiego del dato biometrico, bensì attraverso la (mera) lettura di un codice identificativo. Riportiamo, al proposito, un passo del Provvedimento (nostra la sottolineatura, n.d.a.): "I dipendenti sottoposti al rilevamento biometrico inserirebbero la card in un'apposita fessura, poggiando l'indice in un alloggio predisposto dell'apparecchio. Il dispositivo rileverebbe la corrispondenza dei dati contenuti nella card con quelli dell'indice e conseguentemente, poiché ad essa sarebbe associato un numero di identificazione del dipendente, ne rileverebbe la presenza al lavoro". Va da sé che il dato biometrico risulta impiegato a fini di sicurezza (*id est* autenticazione informatica), restando detto estraneo al processo di identificazione cui il sistema è altresì preordinato.

Ciò precisato, a parere di chi scrive l'adozione di un sistema di autenticazione biometrica, quale misura di sicurezza espressamente contemplata dalla Regola 2 del Disciplinare tecnico, non richiede l'adempimento dell'onere di verifica preliminare

da parte dell'Autorità Garante, prevista dall'art. 17 del Codice. E ciò sebbene ci sia noto che la prassi è improntata a maggior cautela: cfr., ad esempio, il Provv. 28.02.2008, le cui indicazioni sono dettate in relazione ad un dispositivo di rilevamento delle impronte vocali quale misura di autenticazione, sottoposto al vaglio del Garante da Michelin Italiana Spa.

Come ogni sistema di autenticazione informatica, anche un dispositivo basato su credenziali biometriche dovrà, comunque, essere conforme alle Regole 1-11 del Disciplinare tecnico, ove compatibili. In particolare:

- nelle istruzioni impartite ad ogni incaricato dovrà essere prescritta l'adozione delle cautele necessarie ad assicurare la diligente custodia dei dispositivi in possesso ed uso esclusivi (Regola 4);
- le credenziali di autenticazione dovranno essere disattivate se non utilizzate da almeno sei mesi (Regola 7) ovvero nel caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali (Regola 8).

In via prudenziale, inoltre, sempre in quanto compatibili, andranno osservate anche le prescrizioni di cui al Decalogo del Garante del 09.05.2006 che, seppure più propriamente dettate con riferimento a sistemi di "identificazione" per l'accesso a determinati locali o aree aziendali, sono precetti ispirati a criteri generali in materia di trattamento di dati personali, il cui rispetto, pertanto, si impone ogni qualvolta vi sia un'operazione qualificabile come tale.

Alla luce di quanto precede, pare poter affermare che, ferma l'ammissibilità dell'autenticazione biometrica per fini di sicurezza, l'identificazione biometrica è giustificata solo in casi particolari, tenuto conto delle finalità e del contesto in cui i dati biometrici sono trattati; in relazione ai luoghi di lavoro per presidiare accessi ad "aree sensibili", considerata la natura delle attività ivi svolte: si pensi, per esempio, a processi produttivi pericolosi (cfr. Provv. 15.06.2006) o sottoposti a segreti di varia natura (cfr. Provv. 23.11.2005) o al fatto che particolari locali siano destinati alla custodia di beni, documenti segreti o riservati o oggetti di valore (cfr. Provv. 15.06.2006), oppure per tutelare la sicurezza di terzi (cfr. Provv. 26.07.2006).

In ogni caso, a prescindere dal sistema adottato e dal processo cui detto è preordinato (autenticazione ovvero identificazione) va tenuto conto che la raccolta e la registrazione dei dati biometrici per l'autenticazione o per l'identificazione degli interessati sono, a tutti gli effetti, operazioni di trattamento di dati personali, rispetto alle quali trovano applicazione la normativa di cui al Codice e le indicazioni dell'Autorità Garante (specie se rese ai sensi dell'art. 154, 1 comma, lett.c) del Codice).

E, dunque, oltre a quanto sin qui esposto:

- l'art. 2, il quale garantisce che il trattamento si svolga nel rispetto della dignità dell'interessato (detto principio, in particolare, fa emergere la necessità di rispettare l'autonomia delle persone di fronte a particolari raccolte di dati);
- l'art. 3, che introduce, e disciplina, il principio di necessità; principio che impone di accertare se la finalità perseguita non possa essere raggiunta con l'impiego di dati che non coinvolgano il corpo;
- l'art. 11, secondo cui i dati devono essere trattati secondo liceità e correttezza; raccolti e registrati per scopi determinati, espliciti e legittimi; esatti e, se necessario, aggiornati; pertinenti e non eccedenti rispetto alle finalità della raccolta e del successivo trattamento; conservati in una forma che consenta l'identificazione dell'interessato per un tempo non superiore a quello necessario agli scopi del trattamento;
- l'art. 13, che prevede l'obbligo di informativa, da rendere, chiaramente e senza formule ambigue, a tutti gli interessati; precisa, a tal fine, l'Autorità Garante che nella predetta il Titolare del trattamento dovrà aver cura di indicare, altresì, l'esistenza di pratiche alternative di autenticazione ovvero di identificazione "in relazione all'eventualità che taluno non possa o non intenda aderire alla rilevazione biometrica[7]";

[7] In questi termini il Provv. 01.02.2007.

- l'art. 17, che, per fattispecie particolari o non considerate[8] dal Garante, introduce l'onere di sottoporre il sistema biometrico a verifica preliminare dell'Autorità. Giova precisare, a riguardo, che non può desumersi alcuna approvazione implicita dal semplice inoltro al Garante di note relative a progetti cui non segua un esplicito riscontro dell'Autorità, in quanto il principio del silenzio-assenso non trova applicazione;
- l'art. 23, che prescrive al Titolare di acquisire, precedentemente all'inizio delle operazioni di trattamento, il consenso degli interessati; con la conseguenza che, qualora un soggetto non possa o non voglia sottoporsi alla rilevazione biometrica, deve essere predisposto un sistema alternativo di autenticazione ovvero di identificazione;
- artt. 29 e 30, che disciplinano l'obbligo di designazione per iscritto del personale preposto alla raccolta dei dati biometrici, cui impartire idonee istruzioni operative cui attenersi in veste di incaricato o di responsabile del trattamento;
- gli artt. 31 e 33, unitamente al Disciplinare tecnico di cui all'Allegato B; trattasi di precetti che impongono l'adozione di misure minime ed idonee a presidio della sicurezza del sistema[9]. Tra le predette si segnala come idonea la predisposizione di un programma di formazione degli incaricati, cui segua la consegna agli stessi di apposite istruzioni scritte alle quali attenersi, con particolare riguardo all'ipotesi di smarrimento o sottrazione del dispositivo loro affidato;
- l'art. 37, che onera il Titolare della notificazione preventiva del trattamento biometrico che intende porre in essere;

[8] Come è stato efficacemente rilevato dall'Autorità Garante, ancorché in relazione ad ambiti differenti da quello in esame (cfr., per esempio, il Provvedimento dell'08.04.2010 in tema di videosorveglianza), il Titolare è espressamente esonerato dal cd. prior checking qualora il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti.

[9] Si noti che, a mente della Regola 25 del Disciplinare tecnico, il Titolare che adotti misure minime di sicurezza si avvalendosi di soggetti esterni alla propria struttura deve ricevere dai predetti una dichiarazione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del Disciplinare.

- le prescrizioni dell'Autorità Garante di cui al Provvedimento del 27.11.2008[10], atteso che, secondo la nozione di amministratore di sistema ivi fornita, anche coloro che presidiano un sistema di rilevazione biometrica rientrano nella predetta categoria.

Resta ferma, peraltro, la necessità che, ove il caso concreto lo richieda, l'installazione di un sistema di riconoscimento biometrico avvenga nel rispetto delle garanzie procedurali previste dall'art.4, 2 comma, della L.20.05.1970 n.300 (Statuto dei lavoratori), richiamata dall'art. 114 del Codice.

Atteso quanto si è detto, appare di tutta evidenza che, a monte di ogni progetto di rilevazione di dati biometrici, la regola tecnica deve essere posta al vaglio del precetto giuridico. Ed invero molti processi sottoposti a verifica preliminare, ancorché aderenti alle prescrizioni tecniche indicate dall'Autorità Garante, non hanno ottenuto il *placet* della medesima, in quanto non conformi alle indicazioni di legge in tema di privacy, per contrasto, anzitutto, con i principi di necessità e di proporzionalità tra lo strumento impiegato e le finalità prospettate.

[10] Come successivamente modificato.