BIOMETRIA TRA PRIVACY E SICUREZZA

Di Telesio Perfetti – www.computerlaw.it

1. Considerazioni di ordine generale e aspetti tecnici

In data 21 Luglio 2005 l'Autorità Garante per la protezione dei dati personali (di seguito indicata come Garante Privacy) ha emanato un interessante ed importante provvedimento in materia di uso, da parte di una s.p.a., di dati personali biometrici (nel caso di specie trattavasi di impronte digitali) con finalità di verifica della presenza in azienda dei dipendenti. Orbene, il Garante Privacy ha stabilito il principio in base al quale non può ritenersi lecito un uso generalizzato ed incontrollato dei dati biometrici nei luoghi di lavoro. In tali ambienti l'utilizzo dei suddetti dati può esser giustificato solo in casi particolari, in relazione alle finalità e al contesto in cui essi sono trattati (ad es., accessi a determinate aree dell'azienda, per le quali debbano essere adottati livelli di sicurezza elevati in ragione di specifiche circostanze o attività ivi svolte), oppure per le finalità di sicurezza del trattamento di dati personali. Alla base del ragionamento fatto dal Garante v'è indubbiamente la costatazione che, per quel che concerne l'accertamento dell'identità personale all'interno del luogo di lavoro, sono utilizzabili modalità alternative, altrettanto rigorose, ma meno problematiche per la dignità dei lavoratori interessati (art. 2 Codice Privacy)[1].

Viene così raccomandata la massima cautela nell'uso di dati delicati come quelli biometrici, considerata la loro stretta implicazione con la persona e con il di lei corpo, tanto da poterne permettere una identificazione o riconoscimento univoco. Ed infatti la "biometria"[2] nell'odierna accezione informatica è da intendersi quale **tecnica di identificazione automatica o di verifica dell'identità di un soggetto sulla base di caratteristiche fisiche e/o comportamentali**[3]. Pertanto, nell'ambito del trattamento dei dati personali con strumenti elettronici[4] le credenziali di autenticazione[5] biometriche costituiscono valido strumento per farsi riconoscere da un sistema informatico, id est da un computer, P.C., terminale, portatile etc., e per poter conseguentemente accedere alle risorse dello stesso. In sostanza la verifica dell'identità di un incaricato del trattamento di dati personali, anziché avvenire, come di norma avviene, attraverso la digitazione di un codice identificativo (*user-id*) e di una parola-chiave (*password*)[6] ad esso associata, è resa possibile tramite il raffronto tra una caratteristica fisica o comportamentale di un determinato soggetto con uno o più campioni della stessa precedentemente registrati. Il processo di registrazione è chiamato *enrollment* e per mezzo di esso la persona fornisce al sistema elettronico una sua caratteristica fisica o comportamentale per mezzo di un dispositivo di acquisizione, che può variare a seconda del dato biometrico utilizzato (ad es. uno scanner per le impronte digitali o per la retina ovvero una video-camera per il riconoscimento facciale). Il dato o campione di dato viene analizzato dal sistema, "processato" (usando un termine tecnico), onde estrarre da esso informazioni caratteristiche distintive. Tali informazioni andranno poi a formare il cd. *template*, che altro non è se non una rappresentazione o ricostruzione in termini matematici, numerici, "digitali" dei dati biometrici acquisiti. Concluso il processo di enrollment, il template viene archiviato o registrato su di un database centralizzato ovvero su di un dispositivo quale una smart-card, una tessera plastificata o una scheda ottica (supporti dunque "decentralizzati" e che l'utilizzatore può recar via seco).

Si è parlato peraltro di "caratteristiche fisiche" e di "caratteristiche comportamentali". Ebbene tra le tecniche di tipo fisico e fisiologico sono da menzionare la verifica delle impronte digitali, l'analisi dell'immagine delle dita, il riconoscimento dell'iride, la scansione retinica, il riconoscimento del volto, la geometria della mano, il riconoscimento della forma dell'orecchio, il rilevamento dell'odore del corpo, il riconoscimento vocale, l'analisi della struttura del D.N.A., l'analisi dei pori della pelle o della struttura delle vene etc. Ma esistono anche tecniche di tipo comportamentale, come nel caso di verifica della firma autografa, la misurazione del tempo di

battitura della tastiera, l'analisi dell'andatura etc[7]. Tali tecniche possono anche combinarsi in vario modo (verifica di una caratteristica fisica con verifica di un'altra caratteristica fisica ovvero con quella di una caratteristica comportamentale, ovvero di più comportamentali tra loro). Più spesso le caratteristiche biometriche vengono associate ad un codice identificativo (ad es., un P.I.N.) o, in alternativa, ad una parola-chiave (v. Punto 2 del Disciplinare tecnico in materia di misure minime di sicurezza o Allegato B).

2. Normativa di riferimento nell'ordinamento italiano

Come si è detto, dunque, i dati biometrici possono essere utilizzati come strumento di autenticazione (informatica), rectius di identificazione[8]. Tali dati presentano qualità affatto peculiari, e precisamente:

- l'**universalità**: l'elemento biometrico è presente in ogni persona
- l'**esclusività**: l'elemento biometrico è unico, assolutamente inequivoco e distintivo di ogni persona
- la **permanenza**: ogni persona conserva i propri elementi biometrici nel corso del tempo (salvo lesioni dell'integrità fisica)

Le credenziali biometriche, come pure si è visto, consentono così di accedere ad un sistema per procedere a determinate operazioni, tra le quali per l'appunto quelle di trattamento dei dati personali. Ma gli stessi dati biometrici sono dati personali (per la definizione v. art.4, co.1 lett.b) Codice Privacy) e come tali sono soggetti, quanto a tutela, garanzie, modalità e finalità di trattamento, alle disposizioni del "Codice in materia di protezione dei dati personali", Codice Privacy per l'appunto. Segnatamente, le più significative norme del Cod.Priv. in materia di trattamento dei dati biometrici sono le seguenti:

- art.2: il trattamento deve svolgersi nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
- art.3: rispetto del principio di necessità del trattamento, in base al quale i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
- art.11: qualità dei dati. I dati vanno trattati secondo liceità e correttezza e nel rispetto dei principi di finalità e proporzionalità del trattamento: i dati possono essere cioè utilizzati per scopi determinati (specifici), espliciti (trasparenti) e legittimi (non contrastanti con le leggi e con l'ordinamento giuridico) e devono essere pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati. Vanno inoltre conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario alle finalità suddette. Ogni violazione di siffatta disciplina comporta l'inutilizzabilità dei dati stessi.
- art.13: completezza e chiarezza dell'informativa, soprattutto in relazione alle finalità ed alle modalità (ivi incluso il profilo della sicurezza) del trattamento dei dati biometrici, nonché alla possibilità da parte dell'interessato di esercitare i propri diritti ex art. 7 Cod.Priv., in modo altresì che possa essere prestato, qualora dovesse esser richiesto e salve dunque le eccezioni espressamente e specificamente previste ex lege, il consenso al trattamento (art. 23 per i dati biometrici meramente identificativi, e art. 26, in caso di dati biometrici "sensibili"[9]), consenso che così può essere effettivo, reale, fermo e ribadito, in quanto informato, pienamente consapevole, libero, spontaneo, espresso, personale, sempre revocabile e, se necessario, formale (art.26 Cod. Priv.).
- art.17: osservanza delle prescrizioni ulteriori dettate dal Garante Privacy per il trattamento di quei dati, che presentano rischi specifici[10], come per l'appunto i dati biometrici.

- art. 31 e ss.: adeguata protezione dei dati biometrici, ergo adozione di tutte le misure di sicurezza idonee e preventive (non solo minime dunque), in modo da garantire la riservatezza, l'integrità e la disponibilità dei dati. In caso di mancata, insufficiente, inadeguata protezione, oltre alle eventuali responsabilità penali (art.169 Cod.Priv., nel caso di misure "minime"), il Titolare del trattamento potrebbe essere esposto anche a responsabilità civili (art.15 Cod.Priv., che richiama l'art. 2050 c.c., dacché l'attività di trattamento dei dati personali è definita ex lege come attività pericolosa, con quel che ne consegue in termini di inversione dell'onere probatorio)[11]. Il profilo della sicurezza è particolarmente importante in caso di trattamento di dati biometrici. Infatti il sistema informatico che li tratta deve essere altamente affidabile, soggetto a verifiche periodiche e periodicamente testato. Inoltre sarebbero opportune certificazioni e omologazioni dei dispositivi hardware e software, che tengano eventualmente conto delle valutazioni espresse da comitati tecnici indipendenti. I rischi di trattamento illecito e/o non conforme, di accesso non autorizzato o abusivo al sistema o alla rete, di perdita, cancellazione e distruzione, nonché di "sottrazione" o indebita appropriazione("*identity theft*" o "furto di identità") e indebito uso dei dati sono maggiori per quei dati biometrici che lasciano tracce. Ad es. si pensi alle impronte digitali che restino impresse su un determinato oggetto (penna, bicchiere, pezzo di carta…). Esse potrebbero essere raccolte all'insaputa dell'interessato e, applicando un algoritmo alle impronte stesse così reperite, sarebbe possibile (anche se non di facile attuazione) determinare se la persona è registrata in un database ed in caso affermativo scoprire la sua identità confrontando i due modelli[12]. Ergo si necessita, in tale campo, di un livello elevato di sicurezza.
- art.37 lett.a): obbligo di notificazione al Garante Privacy prima di procedere al trattamento, rispettando le modalità di cui al successivo art.38 (in particolare la notificazione è valida solo se è trasmessa per via telematica utilizzando il modello predisposto dal Garante e osservando le prescrizioni da questi impartite, anche per quanto riguarda le modalità di sottoscrizione con firma digitale e di conferma del ricevimento della notificazione).

Alla luce della ricognizione di tale suddetta disciplina si può meglio comprendere la decisione del Garante Privacy assunta col provvedimento del 21 Luglio 2005. Il Garante infatti ha ritenuto che l'utilizzazione delle impronte digitali allo scopo di verificare la presenza dei dipendenti in azienda fosse senza dubbio una forma di trattamento non necessario, non proporzionato (eccedente), non finalisticamente giustificabile e non corretto, anzi inadeguato, sotto il profilo della qualità. E a ben vedere l'uso delle tecniche biometriche può trovare spazio solo in determinate circostanze, id est laddove esse vengano utilizzate come misure minime di sicurezza (art.34, lett. a) e b) Cod.Priv. in combinato disposto con i Punti 1 e 2 dell'All.B), ovvero quale strumento di accesso (limitato e controllato, nonché autorizzato) in particolari aree o locali, che devono restare sicuri e riservati in vista di particolari finalità e attività (ad es. custodia, protezione e ricovero di back-up, di database contenenti dati genetici o di archivi militari e/o industriali contenenti formule, know-how, documenti che interessino la difesa e la sicurezza nazionale…). Non potrebbero al contrario esser adottate per esigenze meramente organizzative, economiche e aziendali (stante anche il limite di cui all'art. 41, co.2 Cost.).

Concludendo, il trattamento di dati biometrici è consentito solo ottemperando a rigorosi obblighi (artt.13, 17, 31 e ss. e 37 Cod.Priv.), entro stretti limiti (ex artt. 2, 23, 26 Cod.Priv.; per le P.A. v. gli artt. 18, 19, 20 e 22 Cod.Priv.) e osservando i principi di necessità, correttezza, finalità, proporzionalità (pertinenza e non eccedenza) e qualità dei dati (artt. 3 e 11 Cod.Priv.).

"_____"

(*"L'uomo è misura di tutte le cose"*, Protagora di Abdera, filosofo sofista del V sec. A.C.)

NOTE

[1] E' appena il caso di dire che già la nostra Costituzione, pur se garantisce e tutela la libertà di iniziativa economica privata come diritto fondamentale della persona (art. 41, co.1 Cost.), prevede altresì quale limite invalicabile al suo esercizio il rispetto della libertà, della sicurezza e della dignità umana (art.41, co.2 Cost.). Inoltre la Carta dei diritti fondamentali dell'U.E., detta anche "Carta di Nizza" (parte peraltro integrante del Trattato che istituisce una Costituzione per l'Europa), riconosce ex art.1 la dignità umana quale diritto inviolabile e fondante della stessa persona, quale valore assoluto e irriducibile, posto al vertice della gerarchia dei diritti umani, dal quale essi discendono e nel quale tutti si integrano, si completano, si rafforzano, si consolidano, si esaltano. La dignità dunque come valore profondo, intimo, intangibile, indisponibile dell'essere umano; essa lo caratterizza e differenzia da tutti gli altri esseri viventi, sostanziandone la superiorità e la qualità di individuo, id est entità unica, indivisibile, irriproducibile, non strumentalizzabile, non degradabile a grandezza fungibile. L'uomo dunque come essere vivente capace di intendere e di volere e di orientare la propria vita verso un fine, ed egli stesso si pone come fine nei riguardi degli altri uomini e mai come mezzo (kantianamente parlando). V'è da notare che l'art.1 della carta di Nizza coincide sostanzialmente con l'art.1 dell'attuale Costituzione tedesca.

[2] Il termine "biometria" è etimologicamente di origine greca, essendo
misura.

[3] Cfr. la definizione in *"Brevi note sulle tecnologie biometriche in un contesto ICT"*, a cura del Gruppo di studio per la definizione di iniziative nel campo della biometria istituito dal C.N.I.P.A. Il documento è del Gennaio del 2004 ed è reperibile all'url http://www.cnipa.gov.it/site/_files/Note%20tecnologie%20biometriche%20nell'ICT.pdf.

[4] Per "strumenti elettronici" sono da intendersi *"gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento"* (art.4, co.3, lett.b) del Codice Privacy).

[5] A norma dell'art.4, co.3, lett.d) del Codice Privacy le cd. "credenziali di autenticazione" sono *"i dati ed i dispositivi in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica"*. L'autenticazione informatica è a sua volta *"l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità"*. Si ricordi che l'autenticazione informatica è presupposto necessario per procedere al trattamento di dati personali e costituisce anche il primo anello della catena di sicurezza logica all'interno di una determinata struttura. Gli altri due anelli sono costituiti dall'*autorizzazione* e dall'*accounting* o *auditing* (cd. *"sistemi AAA"*) . Per una definizione e distinzione tra le varie fasi, v. C.Giustozzi,*"Giuristi e informatici divisi da una lingua comune: autenticazione?"*, reperibile all'url http://www.interlex.it/forum10/relazioni/24giustozzi.htm.

Il Codice Privacy (art.34, lett.a) e b) Codice Privacy) prescrive, tra le altre, quali misure minime di sicurezza (la cui mancata adozione cioè è sanzionata penalmente: v. art.169 Codice Privacy) sia l'autenticazione informatica sia l'adozione di procedure di gestione delle credenziali di autenticazione. D'altro canto l'Allegato B, contenente il Disciplinare tecnico in materia di misure minime di sicurezza, si occupa specificamente del sistema di autenticazione informatica nei Punti da 1 a 11.

[6] La PW costituisce l'elemento riservato dell'associazione logica "identificativo/parola-chiave". Essa deve esser dunque nota al solo titolare, deve avere un numero minimo di caratteri (il Punto 5 dell'Allegato B ne prevede un minimo di 8, ma maggior lunghezza è sinonimo di maggior sicurezza) e deve essere non banale, non ovvia in un duplice senso:

- soggettivo: non devono né possono essere usate PW che contengano riferimenti anche indiretti all'incaricato
- oggettivo: è sconsigliabile l'uso di PW recanti espressioni o parole di uso comune

Altra importante prescrizione, di cui al Punto 5, è quella in base alla quale la PW va aggiornata periodicamente (ogni 6 mesi per i dati comuni, ogni 3 per quelli sensibili e giudiziari).

[7] Le tecniche biometriche sono state oggetto di attenta analisi da parte del Gruppo per la tutela dei dati personali (istituito a norma dell'art.29 della dir. 1995/46/CE e i cui compiti sono definiti dall'art.30 della stessa e dall'art.14 della dir. 1997/66/CE). Tale organo consultivo indipendente dell'U.E. ha adottato, in data 1 Agosto 2003, un *"Documento di lavoro sulla biometria"* , in cui vengono affrontate le questioni inerenti alla descrizione e classificazione delle tecniche biometriche, alle caratteristiche precipue delle stesse e all'applicazione dei principi della dir. 1995/46/CE in tale materia. Tra l'altro nel Documento si pone in evidenza il fatto che gli elementi biometrici non sono tutti equivalenti ed il tasso di identificazione di una persona può variare considerevolmente in funzione del tipo di dati utilizzati; e comunque gli elementi biometrici maggiormente distintivi sembrano essere il D.N.A., la retina, le impronte digitali. Quanto al D.N.A., nel Documento è poi fatto presente che, al di là di specifiche questioni che può sollevare l'uso di tale dato, allo stato attuale non sembra possibile generare un profilo di D.N.A. in tempo reale come strumento di autenticazione.

[8] La distinzione tra "autenticazione" e "identificazione" è importante. Infatti con il procedimento di autenticazione (ad es., associazione logica user-id/PW) l'utilizzatore risponde alla domanda *"sei tu la persona che dichiari di essere?"*. Il

sistema certifica in tal modo l'identità della persona tramite un raffronto 1:1. Con il procedimento di identificazione si risponde invece alla domanda *"chi sei tu?"*, laddove il sistema riconosce l'individuo distinguendolo da altre persone, dopo aver proceduto ad un raffronto stavolta 1:n. Probabilmente è preferibile parlare di autenticazione in relazione ai procedimenti di associazione logica user-id/PW, mentre alle tecniche biometriche sembra attagliarsi di più l'espressione identificazione, per le caratteristiche che esse presentano: v. ancora C.Giustozzi cit.

[9] Alcuni dati biometrici sono da considerarsi "dati sensibili" ex art.4, co.1, lett.d) Cod.Priv., in quanto idonei (aventi cioè semplicemente l'attitudine) a rivelare l'origine etnica o razziale dell'interessato (ad es. il riconoscimento del volto) ovvero lo stato di salute (ad es. il D.N.A.). In tali casi, se il trattamento è operato da privati, si applicano, oltre ai principi generali di protezione previsti dal Codice, le garanzie speciali previste dall'art.26 del Codice Privacy (consenso scritto *ad substantiam*, autorizzazione del Garante, divieto di diffusione dei dati sulla salute). Per le pubbliche amministrazioni si applicano, quanto ai dati biometrici sensibili, gli artt. 20 e 22 Cod.Priv. (da notare che non è necessario il consenso, ma sono prescritte altre garanzie e misure di tutela; è inoltre ribadito il divieto di diffusione dei dati sulla salute).

[10] Si parla in tali casi di "dati semisensibili".

[11] Ed i rischi aumentano sol se si consideri che la responsabilità civile non verrebbe meno neppure in caso di distruzione o perdita, anche accidentale, dei dati.

[12] Tali preoccupazioni sono state fatte proprie dal Gruppo per la tutela dei dati personali nel Documento cit., laddove si consiglia di registrare i dati non su di una banca-dati centralizzata (id est su di una memoria appartenente ad una persona diversa dall'interessato), bensì su un oggetto accessibile unicamente all'utilizzatore, come una tessera microchip, un telefono mobile o una carta bancaria, metodi questi comunque meno eccessivi rispetto ad una memoria centrale e comportanti rischi minori.

Uno dei motivi per i quali il Garante Privacy non ha dato parere favorevole nel Provvedimento del 21 Luglio 2005 consisteva proprio nel fatto che la società, che voleva utilizzare le impronte digitali per rilevare le presenze dei dipendenti sul posto di lavoro, aveva centralizzato i codici identificativi derivati dal dato biometrico. Ergo tali modalità tecniche sono state considerate sproporzionate, ergo ancora potevano e dovevano esser adottate misure tecnologiche meno invasive, come per l'appunto la memorizzazione dei codici su un supporto che restasse nell'esclusiva disponibilità dell'interessato.