GRUPPO PER LA TUTELA DEI DATI PERSONALI
(ARTICOLO 29)

12168/02/IT
WP 80

Documento di lavoro sulla biometria

Adottato il 1° agosto 2003

Il gruppo è stato istituito a norma dell'articolo 29 della direttiva 95/46/CE. Si tratta dell'organo consultivo indipendente dell'UE in tema di tutela dei dati e della vita privata. I compiti del gruppo sono definiti dall'articolo 30 della direttiva 95/46/CE e dall'articolo 14 della direttiva 97/66/CE. Segretariato:

Direzione E (Servizi, proprietà intellettuale e industriale, media e protezione dei dati) della Commissione europea, direzione generale "Mercato interno", B-1049 Bruxelles, Belgio, Ufficio n. C100-6/136.

Website: www.europa.eu.int/comm/privacy

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995[1],

visti gli articoli 29 e 30, paragrafi 1, lettera a) e 3, della direttiva,

visto il suo regolamento interno, in particolare gli articoli 12 e 14,

ha adottato il presente documento di lavoro.

1. INTRODUZIONE

Il rapido sviluppo delle tecnologie biometriche e l'estensione della loro applicazione nel corso degli ultimi anni rendono necessaria un'attenta analisi per quanto concerne l'aspetto della tutela dei dati[2]. L'uso generalizzato e incontrollato della biometria solleva preoccupazioni in relazione alla tutela dei diritti e delle libertà fondamentali degli individui. Si tratta di dati di carattere speciale in quanto riguardano le caratteristiche comportamentali e fisiologiche di un individuo e sono tali da consentirne l'identificazione univoca[3].

Attualmente si ricorre spesso al trattamento di dati biometrici nelle procedure automatizzate di autenticazione/verifica e di identificazione, in particolare per il controllo dell'accesso ad aree tanto fisiche quanto virtuali (accesso a determinati sistemi o servizi elettronici).

In precedenza l'impiego della biometria era limitato essenzialmente alle prove del DNA e al controllo delle impronte digitali. La rilevazione delle impronte digitali è stata utilizzata segnatamente a fini giudiziari (ad es. nell'ambito di indagini penali). Se la società incoraggia lo sviluppo di basi di dati contenenti impronte digitali o altri dati biometrici per altre applicazioni correnti le possibilità di un loro reimpiego da parte di terzi a scopo di confronto e ricerca per fini propri potrebbero aumentare, pur non essendo questo l'obiettivo inizialmente perseguito; tra questi terzi potrebbero figurare le autorità incaricate di applicare la legge.

Una preoccupazione specifica in relazione ai dati biometrici deriva dalla possibilità che, con l'uso generalizzato di tali dati, il pubblico diventi insensibile agli effetti che il loro

---

[1] Gazzetta ufficiale L 281 del 23/11/1995, pag. 31, disponibile in http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

[2] Dopo gli avvenimenti dell'11 settembre 2001 la biometria è stata spesso presentata come un valido strumento per migliorare la sicurezza pubblica. In sede di Unione europea sono in corso discussioni sulla possibilità di integrare elementi biometrici a livello di carte di identità, passaporti, documenti di viaggio e visti. Gli Stati Uniti richiederanno presto identificatori biometrici per gli stranieri in ingresso o in uscita dal paese. La Convenzione n.108 dell'OIL è stata modificata nel 2003 allo scopo di introdurre il ricorso obbligatorio alla biometria per i lavoratori marittimi. Sono in atto discussioni anche in altri forum internazionali quali il G8, l'OCSE ecc..

[3] L'identificazione univoca dipende tuttavia da numerosi fattori quali le dimensioni della base di dati e il tipo di elementi biometrici utilizzati.

trattamento può avere sulla vita quotidiana. L'uso di elementi biometrici nelle biblioteche scolastiche, ad esempio, può diminuire la consapevolezza dei bambini quanto ai rischi legati alla tutela dei dati e alle possibili ripercussioni sulla loro vita futura.

Il presente documento si prefigge di contribuire ad una applicazione efficace ed omogenea delle disposizioni nazionali in tema di protezione dei dati adottate conformemente alla direttiva 95/46/CE in relazione ai sistemi biometrici. Esso si concentra principalmente sulle applicazioni biometriche a fini di autenticazione e verifica. Il gruppo si propone di fornire linee guida uniformi a livello europeo, destinate in particolare all'industria dei sistemi biometrici ed agli utilizzatori di tali tecnologie.

2. DESCRIZIONE DEI SISTEMI BIOMETRICI

Per sistemi biometrici si intendono le applicazioni di tecnologie biometriche che permettono l'identificazione e/o l'autenticazione/verifica automatica di un individuo[4]. Le applicazioni a fini di autenticazione/verifica sono spesso utilizzate per vari compiti in settori completamente differenti e sotto la responsabilità di numerose entità diverse.

Ogni tecnica biometrica, che sia utilizzata a scopo di autenticazione/verifica o di identificazione, dipende, in misura maggiore o minore, dall'elemento biometrico considerato:
- **universale:** l'elemento biometrico è presente in tutte le persone[5];
- **unico**: l'elemento biometrico deve essere distintivo per ogni persona;
- e **permanente:** ogni persona conserva il proprio elemento biometrico nel corso del tempo.

Si possono distinguere due categorie principali di tecniche biometriche a seconda che vengano utilizzati dati stabili o dati comportamentali dinamici[6].

Esistono, in primo luogo, tecniche di tipo fisico e **fisiologico** che misurano le caratteristiche fisiologiche di una persona. Esse comprendono: la verifica delle impronte digitali, l'analisi dell'immagine delle dita, il riconoscimento dell'iride, l'analisi della retina, 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 DNA[7], l'analisi dei pori della pelle ecc..

---

[4] La distinzione fra autenticazione (verifica) ed identificazione è importante. L'autenticazione risponde alla domanda: sono la persona che dichiaro di essere? Il sistema certifica l'identità della persona grazie all'elaborazione di dati biometrici che si riferiscono all'individuo autore della domanda e prende una decisione sì/no (confronto 1:1). L'identificazione risponde alla domanda: chi sono io? Il sistema riconosce l'individuo autore della domanda distinguendolo da altre persone i cui dati biometrici sono a loro volta registrati. In questo caso il sistema prende una decisione "1 su n" e risponde che la persona che pone la domanda è X.

[5] A questo proposito gli elementi biometrici non sono tutti equivalenti ed il tasso di differenziazione di una persona da un'altra può variare considerevolmente in funzione del tipo di dati biometrici utilizzati. Gli elementi biometrici maggiormente distintivi sembrano essere il DNA, la retina e le impronte digitali.

[6] Alcune tecniche possono fondarsi tanto sulla fisiologia quanto sul comportamento.

[7] Benché l'uso del DNA a fini di identificazione biometrica sollevi questioni specifiche queste non verranno discusse nel presente documento. Va detto comunque che attualmente non sembra possibile generare un profilo di DNA in tempo reale come strumento di autenticazione.

In secondo luogo esistono tecniche di tipo **comportamentale** che misurano il comportamento di una persona. Esse comprendono la verifica della firma manoscritta, l'analisi della battitura su tastiera, l'analisi dell'andatura ecc..

Tenendo conto dei rapidi progressi tecnici e della crescente preoccupazione in tema di sicurezza molti sistemi biometrici funzionano associando diverse modalità biometriche dell'utilizzatore ad altre tecnologie di identificazione o autenticazione. Alcuni sistemi, ad esempio, associano il riconoscimento del volto alla registrazione della voce. Per l'autenticazione si possono utilizzare contemporaneamente tre metodi, basandosi su qualcosa che l'individuo conosce (*password*, numero personale di identificazione (PIN), ecc.), qualcosa che egli possiede (dispositivo di autenticazione o *token*, CAD key, *smart card*, ecc.) e qualcosa che è proprio della sua persona (una caratteristica biometrica). Nel caso di un computer, ad esempio, una persona potrebbe inserire una *smart card*, digitare una *password* e presentare le proprie impronte digitali.

La raccolta di campioni biometrici, i cosiddetti dati biometrici (ad esempio, l'immagine dell'impronta digitale, l'immagine dell'iride o della retina, la registrazione della voce), viene effettuata nel corso della cosiddetta fase di "iscrizione" utilizzando un sensore specifico per ogni tipo di elemento biometrico. Il sistema biometrico estrae dai dati biometrici i tratti specifici dell'utilizzatore necessari per elaborare un "modello" biometrico. Il modello è una riduzione strutturata di un'immagine biometrica, ossia la misura biometrica registrata di un individuo. È tale modello, presentato in forma digitale, ad essere archiviato e non l'elemento biometrico in se stesso. I dati biometrici possono inoltre essere elaborati come dati grezzi (un'immagine) in funzione del sistema biometrico utilizzato[8].

La fase di iscrizione svolge un ruolo essenziale dato che è l'unica in cui sono presenti contemporaneamente dati grezzi, algoritmi di estrazione e protezione (crittografia, *hashing* ecc.) e modelli. A questo proposito va sottolineato che se i dati grezzi rivelano informazioni che possono essere considerate di natura delicata a termini dell'articolo 8 della direttiva 95/46/CE il processo di iscrizione di tali dati va allora effettuato conformemente a tale disposizione (vedi nel seguito punto 3.7).

Un'altra questione importante in relazione alla tutela dei dati riguarda la forma in cui vengono conservati i modelli relativi agli utilizzatori, che dipende dal tipo di applicazione per cui verrà utilizzato il dispositivo biometrico nonché dalle dimensioni dei modelli stessi. I modelli possono essere archiviati secondo una delle seguenti modalità:

a) - nella memoria di un dispositivo biometrico;
b) - in una base di dati centrale;
c) - in tessere plastificate, schede ottiche o *smart card*. Questo metodo di conservazione consente agli utilizzatori di portare con sé i propri modelli come dispositivi di identificazione.

In teoria, ai fini dell'autenticazione/verifica, non è necessario memorizzare i dati di riferimento in una base di dati; è sufficiente archiviare i dati personali in un sistema decentralizzato. L'identificazione invece è possibile solo memorizzando i dati di riferimento in una base di dati centralizzata dato che, per accertare l'identità della persona interessata, il

---

[8] Il presente documento si riferisce principalmente ai sistemi biometrici basati sui modelli, ma può essere applicato anche in caso di dati grezzi. La specificità dei dati grezzi tuttavia può rendere necessario l'adattamento delle prescrizioni in tema di tutela dei dati.

sistema deve confrontare i suoi modelli o i suoi dati grezzi (immagine) con i modelli o i dati grezzi di tutte le persone i cui dati sono già registrati a livello centrale.

Un altro punto essenziale in relazione alla tutela dei dati è rappresentato dal fatto che taluni sistemi biometrici si basano su informazioni, quali i campioni di DNA o le impronte digitali, che possono essere raccolte all'insaputa della persona interessata, che può inconsapevolmente lasciare tracce. Applicando un algoritmo biometrico alle impronte digitali trovate su un bicchiere può essere possibile[9] determinare se la persona è registrata in una base di dati contenente dati biometrici e, in caso affermativo, scoprire la sua identità confrontando i due modelli. Questo si applica inoltre ad altri sistemi biometrici quali quelli basati sull'analisi della battitura su tastiera o sul riconoscimento a distanza del volto a causa delle caratteristiche specifiche della tecnologia adottata[10]. L'aspetto problematico è rappresentato dal fatto che, da un lato, questa raccolta e questo trattamento di dati possono essere effettuati all'insaputa della persona interessata e, dall'altro, che indipendentemente dalla loro attuale affidabilità tali tecnologie biometriche si prestano ad un uso generalizzato a causa del loro "basso livello di intrusività". È quindi necessario stabilire garanzie specifiche in materia.

3. APPLICAZIONE DEI PRINCIPI DELLA DIRETTIVA 95/46/CE

3.1. Applicazione della direttiva 95/46/CE

L'articolo 2, lettera a) della direttiva 95/46/CE definisce i "dati personali" come "qualsiasi informazione concernente una persona fisica identificata o identificabile (…); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica (…)". La considerazione preliminare 26 aggiunge che "per determinare se una persona è identificabile, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona".

Conformemente a tale definizione le misure di identificazione biometrica o la loro traduzione digitale in un modello sono, nella maggior parte dei casi, dati a carattere personale[11]. I dati biometrici possono sempre essere considerati come "informazione concernente una persona fisica" in quanto sono dati che, per la loro stessa natura, forniscono informazioni su una determinata persona. Nell'ambito dell'identificazione biometrica la persona è generalmente identificabile in quanto i dati biometrici sono

---

9 Sono tuttavia necessari alcuni elementi quali la capacità di raccogliere l'impronta digitale dal bicchiere senza danneggiarla, l'attrezzatura tecnica necessaria per elaborare i dati a partire dalle impronte digitali, l'accesso all'algoritmo del costruttore e/o alla base di dati contenente le impronte digitali.

10 Si veda il punto 3 sull'applicazione della direttiva 95/46/CE e in particolare il punto 3.3 sull'obbligo di informare la persona interessata.

11 Qualora i dati biometrici, quali ad esempio un modello, vengano registrati in modo tale che non esistano mezzi che possono essere ragionevolmente usati dal responsabile del trattamento o da altri per identificare la persona interessata tali dati non possono essere considerati come dati personali.

utilizzati per l'identificazione o l'autenticazione/verifica almeno nel senso di distinguere la persona interessata da tutte le altre[12].

L'articolo 3, paragrafo 1 della direttiva 95/46/CE stabilisce che il principio della tutela dei dati si applica al trattamento di dati personali interamente o parzialmente automatizzato nonché al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi. Le disposizioni delle direttiva non si applicano se il trattamento dei dati viene effettuato da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico. Molte applicazioni biometriche ad uso domestico rientrano in questa categoria.

Oltre a tali esclusioni specifiche il trattamento dei dati biometrici può essere considerato lecito solo se tutte le procedure utilizzate, a partire dall'iscrizione, vengono effettuate conformemente alle disposizioni della direttiva 95/46/CE.

Il presente documento non si occupa di tutte le questioni sollevate dall'applicazione della direttiva 95/46/CE ai dati biometrici. Esso tratta unicamente delle questioni più importanti e non offre quindi una panoramica esauriente delle conseguenze dell'applicazione della direttiva 95/46/CE.

3.2. Principio della finalità e della proporzionalità

L'articolo 6 della direttiva 95/46/CE stabilisce che i dati personali devono essere rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. I dati personali inoltre devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e successivamente trattati (principio della finalità).

Il rispetto di tale principio implica in primo luogo che venga determinata con chiarezza la finalità per la quale i dati biometrici sono rilevati e trattati. È necessario altresì valutare il rispetto della proporzionalità e della liceità, considerando i rischi per la tutela dei diritti e delle libertà fondamentali degli individui e in particolare la possibilità o meno di perseguire la medesima finalità in modo meno intrusivo. La proporzionalità è stata il principale criterio alla base di quasi tutte le decisioni in tema di trattamento dei dati biometrici prese fino a questo momento dalle autorità incaricate della protezione dei dati.[13]

Ai fini di controllo dell'accesso (autenticazione/verifica) il gruppo ritiene che i sistemi biometrici fondati sulle caratteristiche fisiche che non lasciano tracce (ad esempio, la forma della mano, ma non le impronte digitali) o i sistemi biometrici fondati sulle caratteristiche fisiche che lasciano tracce, ma i cui dati non vengono registrati in una memoria appartenente ad una persona diversa dalla persona interessata (in altre parole, i dati non vengono memorizzati nel dispositivo di controllo d'accesso o in una base di dati centrale) comportino un numero minore di rischi per la protezione dei diritti e delle

---

[12] L'identificabilità della persona dipende anche dalla disponibilità di altri dati i quali, insieme o separatamente, consentono alla persona in questione di essere appunto identificata. La possibilità di un'identificazione diretta mediante "uno o più elementi specifici caratteristici della sua identità fisica" è citata espressamente nella definizione di dati personali di cui all'articolo 2, lettera a) della direttiva 95/46/CE.

[13] Decisioni, ad esempio, delle autorità olandesi, francesi, tedesche, italiane e greche.

libertà fondamentali degli individui[14]. Numerose autorità di protezione dei dati hanno sottoscritto tale opinione dichiarando che i dati biometrici andrebbero preferibilmente memorizzati non in una base di dati, bensì su un oggetto accessibile unicamente all'utilizzatore, quale una tessera microchip, un telefono mobile o una carta bancaria[15]. In altri termini, le procedure di autenticazione/verifica che possono essere realizzate senza ricorrere ad una memoria centrale dei dati biometrici non dovrebbero applicare tecniche di identificazione eccessive.

Il gruppo ritiene pertanto che prima di introdurre altri tipi di applicazioni (basate sulla memorizzazione di modelli numerici di impronte digitali nei terminali o in una base di dati centrale) il loro impiego andrebbe sottoposto ad un'attenta valutazione. Qualora tuttavia si adotti questo tipo di sistema, ad esempio nel caso di impianti di alta sicurezza[16], esso potrebbe essere considerato come un trattamento di dati che presenta rischi a termini dell'articolo 20 della direttiva 95/46/CE e potrebbe quindi dover subire un controllo preventivo da parte delle autorità di protezione dei dati conformemente alla legislazione nazionale (vedi il punto 3.5).

La direttiva 95/46/CE vieta l'ulteriore trattamento dei dati qualora questo sia incompatibile con la finalità per la quale i dati erano stati raccolti. Quando, ad esempio, i dati biometrici vengono sottoposti a trattamento a fini di controllo dell'accesso l'uso di tali dati per valutare lo stato emotivo della persona interessata o a fini di sorveglianza sul luogo di lavoro non sarebbe compatibile con la finalità originaria della rilevazione. Occorre prendere tutti i provvedimenti necessari per evitare questo tipo di riutilizzo incompatibile[17]. La direttiva 95/46/CE prevede deroghe al divieto di trattare ulteriormente i dati per finalità ritenute incompatibili, ma solo quando si applicano condizioni specifiche.

In linea generale si riconosce che il rischio che dati biometrici ottenuti da tracce fisiche lasciate da un individuo a sua insaputa (impronte digitali) siano riutilizzati per finalità incompatibili è relativamente inferiore se i dati, invece di essere memorizzati in basi di dati centralizzate, restano con la persona stessa senza essere accessibili a terzi. L'archiviazione centralizzata dei dati biometrici aumenta altresì il rischio che tali dati vengano utilizzati come chiave per collegare basi di dati distinte ed ottenere così profili dettagliati delle abitudini della persona interessata tanto nel settore pubblico quanto in quello privato. La questione della finalità compatibile solleva inoltre il problema della interoperabilità di sistemi diversi che utilizzano la biometria. La normalizzazione

---

[14] Si può distinguere il caso in cui i dati biometrici vengono trattati a livello centrale da quello in cui i dati biometrici di riferimento vengono registrati su un dispositivo mobile e in cui il processo di abbinamento viene effettuato sulla carta, ma non sul sensore o anche in cui il sensore fa parte del dispositivo mobile.

[15] È necessario tenere conto dei sistemi adottati per risolvere i problemi derivanti dalla perdita, dal furto o dal danneggiamento delle carte e promuovere gli strumenti che non comportano la memorizzazione dei dati biometrici. Per quanto possibile i dati andrebbero rilevati ancora una volta direttamente presso la persona interessata.

[16] Lo stato attuale della tecnologia biometrica è tale che non esistono ancora soluzioni affidabili per una identificazione in tempo reale di una popolazione di qualsiasi dimensioni reale ed è altrettanto improbabile che possano essere disponibili in un prossimo futuro.

[17] Come sottolineato sopra, tale finalità deve essere chiaramente definita.

necessaria per conseguire l'interoperabilità potrebbe favorire una maggiore interconnessione fra le basi di dati.

L'impiego della biometria solleva inoltre la questione della proporzionalità di ogni categoria di dati trattati alla luce della finalità per la quale vengono trattati. I dati biometrici possono essere utilizzati solo se adeguati, pertinenti e non eccessivi. Questo implica una valutazione accurata della necessità e della proporzionalità dei dati trattati[18]. In Francia, ad esempio, il CNIL ha rifiutato l'uso delle impronte digitali per controllare l'accesso dei bambini ad una mensa scolastica,[19] ma ha accettato per la medesima finalità l'uso della geometria della mano. In Portogallo l'autorità di protezione dei dati ha emesso di recente una decisione sfavorevole in merito all'uso da parte di un'università di un sistema biometrico (impronte digitali) per controllare l'assiduità e la puntualità del personale non docente[20]. In Germania l'autorità incaricata della protezione dei dati ha emesso una decisione favorevole all'introduzione delle caratteristiche biometriche nei documenti di identità allo scopo di evitarne la falsificazione a condizione che, per il confronto con le impronte digitali del proprietario, i dati siano memorizzati nel microchip della carta e non in una base di dati.

Una difficoltà specifica può derivare dal fatto che spesso i dati biometrici contengono più informazioni di quante siano necessarie per l'identificazione o l'autenticazione/verifica. Questo è più probabile nel caso dell'immagine originale (dati grezzi) dato che il modello può e dovrebbe essere costruito tecnicamente in modo tale da rendere impossibile il trattamento di dati non necessari. I dati non necessari dovrebbero essere distrutti quanto prima possibile[21]. Taluni dati biometrici inoltre possono rivelare l'origine razziale o riguardare la salute (vedi nel seguito punto 3.7).

Va infine ricordato che i sistemi biometrici possono essere concepiti in modo tale da poter essere considerati, *inter alia*, come tecnologie a difesa della vita privata in quanto possono diminuire il trattamento di altri dati personali quali il nome, l'indirizzo, la residenza ecc..

3.3. Rilevazione leale ed informazione della persona interessata

I dati biometrici devono essere trattati e soprattutto rilevati in modo leale[22]. Il responsabile del trattamento deve informare la persona interessata conformemente agli

---

[18] In determinate circostanze deve inoltre essere possibile ricorrere all'anonimato o all'uso di pseudonimi. È necessario tenere conto dei sistemi adottati per risolvere i problemi derivanti dalla perdita, dal furto o dal danneggiamento delle carte e promuovere gli strumenti che non comportano la memorizzazione dei dati biometrici. Per quanto possibile i dati andrebbero rilevati ancora una volta direttamente presso la persona interessata.

[19] Sembra tuttavia che nel Regno Unito l'autorità di protezione dei dati abbia accettato l'uso delle impronte digitali in circostanze analoghe a condizione che vengano adottate adeguate precauzioni.

[20] L'autorità portoghese di protezione dei dati ha ritenuto che l'applicazione di sistemi del genere fosse sproporzionata ed eccessiva rispetto alla finalità del trattamento dei dati. Il sistema avrebbe memorizzato i dati in un dispositivo biometrico e le persone da controllare sarebbero state circa 140.

[21] A sostegno di questa soppressione si veda anche l'articolo 6, paragrafo 1, lettera e) della direttiva 95/46/CE che stabilisce che i dati personali vanno conservati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali sono trattati.

[22] Articolo 6, lettera a) della direttiva 95/46/CE.

articoli 10 e 11 della direttiva 95/46/CE[23]. Questo prevede in particolare la definizione esatta della finalità e l'identità del responsabile dell'archivio (che spesso coinciderà con la persona che gestisce il sistema biometrico o che applica la tecnica biometrica).

Vanno evitati i sistemi che raccolgono dati biometrici all'insaputa dei soggetti interessati. Alcuni sistemi biometrici quali il riconoscimento a distanza del volto, la rilevazione delle impronte digitali, la registrazione della voce presentano maggiori rischi da questo punto di vista.

3.4. Criteri per la legittimazione del trattamento dei dati

Il trattamento dei dati biometrici deve fondarsi su una delle basi di legittimazione di cui all'articolo 7 della direttiva 95/46/CE. Se il responsabile del trattamento dell'archivio utilizza il consenso come base di legittimazione il gruppo sottolinea che vanno rispettate le condizioni stabilite dall'articolo 2 della direttiva 95/46/CE (qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento).

3.5. Controllo preliminare - notifica

Come indicato sopra, il gruppo appoggia l'uso di sistemi biometrici che non memorizzano le tracce in un terminale di accesso né le archiviano in una base di dati centrale (cfr. punto 3.2). Se tuttavia è stato previsto di utilizzare tali sistemi ed alla luce del rischio di riutilizzo per finalità diverse nonché dei pericoli specifici derivanti dall'accesso non autorizzato il gruppo raccomanda agli Stati membri di prendere in considerazione la possibilità di sottoporli ad un controllo preliminare da parte delle autorità di protezione dei dati conformemente all'articolo 20 della direttiva 95/46/CE, poiché tale tipo di trattamento presenta potenzialmente rischi specifici per i diritti e le libertà delle persone interessate. Se gli Stati membri intendono introdurre il controllo preliminare in relazione al trattamento dei dati biometrici le autorità nazionali incaricate della protezione dei dati vanno debitamente consultate prima dell'introduzione di tali misure.

3.6. Misure di sicurezza

Conformemente all'articolo 17 della direttiva 95/46/CE il responsabile del trattamento deve attuare le misure tecniche ed organizzative appropriate in tema di sicurezza al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete. Le misure di sicurezza vanno adottate quando i dati biometrici sono sottoposti a trattamento (archiviazione, trasmissione, estrazione delle caratteristiche e confronto ecc.) ed in particolare se il responsabile del trattamento trasmette tali dati via Internet. Le misure di sicurezza possono prevedere, ad esempio, la cifratura dei modelli e la

---

[23] Le deroghe all'obbligo di informare le persone interessate di cui agli articoli 10 e 11 della direttiva 95/46/CE dovrebbero basarsi su misure legislative e costituire una misura necessaria per limitare il campo d'applicazione dell'obbligo di informazione allo scopo di salvaguardare gli interessi elencati nell'articolo 13 della direttiva 95/46/CE (pubblica sicurezza, prevenzione, ricerca, accertamento e perseguimento di infrazioni penali ecc.).

protezione delle chiavi di cifratura oltre al controllo ed alla protezione dell'accesso, rendendo così virtualmente impossibile la ricostruzione dei dati originali a partire dai modelli.

In tale contesto occorre tenere conto di alcune nuove tecnologie. Uno sviluppo interessante è offerto dalla possibilità di utilizzare i dati biometrici come chiavi di cifratura. A priori questo comporterebbe un minor rischio per la persona interessata in quanto la decodificazione è possibile solo grazie ad una nuova rilevazione dei dati biometrici presso la persona interessata, il che eviterebbe la creazione di basi di dati contenenti modelli di dati biometrici che potrebbero venire riutilizzati a fini totalmente diversi.

Le necessarie misure di sicurezza dovrebbero essere adottate fin dall'inizio del trattamento, soprattutto nel corso della fase di "iscrizione", quando i dati biometrici vengono trasformati in modelli o immagini. Deve essere chiaro che qualsiasi perdita delle caratteristiche di integrità, riservatezza e disponibilità a livello di basi di dati danneggerebbe tutte le future applicazioni basate sulle informazioni contenute in tali basi di dati e comporterebbe altresì danni irreparabili per le persone interessate. Se, ad esempio, le impronte digitali di un individuo autorizzato fossero associate all'identità di un individuo non autorizzato, quest'ultimo potrebbe avere accesso, senza averne diritto, ai servizi a disposizione del proprietario delle impronte digitali. Il risultato sarebbe una sottrazione di identità che, indipendentemente dal fatto di essere scoperta o meno, renderebbe le impronte digitali della persona inattendibili per future applicazioni, limitandone così la libertà.

Gli errori dei sistemi biometrici possono avere pesanti conseguenze per le persone interessate: in particolare il rifiuto erroneo di persone autorizzate e l'accettazione indebita di persone non autorizzate possono dar luogo a gravi problemi a diversi livelli. A priori l'uso di dati biometrici dovrebbe ridurre il rischio di errori del genere, ma esso potrebbe anche creare l'illusione che l'identificazione o l'autenticazione/verifica della persona interessata sia sempre corretta. Può essere difficile o addirittura impossibile per la persona interessata provare il contrario. Un sistema, ad esempio, potrebbe erroneamente identificare una persona come un individuo che non deve essere autorizzato a prendere un aereo o ad entrare nel territorio di un determinato paese: la persona disporrebbe allora di scarsi mezzi per risolvere il problema di fronte a tali prove "irrefutabili" a suo sfavore. Va sottolineato ancora una volta che in casi del genere qualsiasi decisione che produca effetti giuridici su un individuo va presa solo dopo aver riconfermato il risultato del trattamento automatizzato, conformemente all'articolo 15 della direttiva 95/46/CE.

Occorre infine ricordare che l'uso della biometria potrebbe migliorare le procedure di controllo nel caso di accesso ai dati personali relativi a terzi, ad esempio in caso di furto e di uso improprio (procedure di autorizzazione).

3.7. Dati di natura delicata

Alcuni dati biometrici possono essere considerati di natura delicata a termini dell'articolo 8 della direttiva 95/46/CE, segnatamente i dati che rivelano l'origine razziale o etnica o i dati relativi alla salute. Nei sistemi biometrici basati sul riconoscimento del volto, ad esempio, possono essere trattati dati che rivelano l'origine razziale o etnica. In tali circostanze si applicano le speciali garanzie di cui all'articolo 8 oltre ai principi generali di protezione previsti dalla direttiva.

Questo non significa che qualsiasi trattamento di dati biometrici debba includere necessariamente dati di natura delicata. Stabilire se un trattamento comprende dati di natura delicata è una questione di valutazione legata alle caratteristiche biometriche specifiche utilizzate nonché all'applicazione biometrica stessa. È maggiormente probabile che sia il caso quando vengono trattati dati biometrici sotto forma di immagini dato che in linea di massima i dati grezzi non possono essere ricostruiti a partire dal modello.

3.8. Identificatore univoco

I dati biometrici sono unici e la maggior parte di loro genera un modello (o immagine) unico. Se utilizzati su vasta scala, in particolare per una parte importante di popolazione, i dati biometrici possono essere considerati come un mezzo identificativo di portata generale a termini della direttiva 95/46/CE. In tal caso si applicherebbe l'articolo 8, paragrafo 7 della direttiva 95/46/CE e gli Stati membri dovrebbero determinare le condizioni che regolano il trattamento dei dati.

Se i dati biometrici sono destinati ad essere utilizzati come chiave per collegare basi di dati contenenti dati personali[24], problemi particolarmente seri possono presentarsi qualora la persona interessata non possa opporsi al trattamento dei dati biometrici. Questa situazione può verificarsi frequentemente nei rapporti fra cittadini ed autorità pubbliche.

Da questo punto di vista sarebbe auspicabile che i modelli e le loro rappresentazioni digitali venissero trattati tramite manipolazioni matematiche (cifratura, algoritmi o funzioni di *hashing),* usando diversi parametri per ogni prodotto biometrico utilizzato, al fine di evitare la combinazione di dati personali provenienti da diverse basi di dati grazie al confronto di modelli o di rappresentazioni digitali.

3.9. Codice di condotta e uso della tecnologia a difesa della vita privata

Il gruppo incoraggia l'industria a produrre sistemi biometrici che facilitino l'attuazione delle raccomandazioni contenute nel presente documento di lavoro e se dovessero essere elaborate norme europee o internazionali in questo settore tale lavoro andrebbe svolto in collaborazione con le autorità di protezione dei dati onde promuovere sistemi biometrici progettati in modo da rispettare la protezione dei dati, minimizzare i rischi sociali ed evitare l'uso improprio dei dati biometrici. Il gruppo sottolinea l'importanza in tale contesto delle tecnologie a difesa della vita privata (*Privacy Enhancing Technologies* - PETS) allo scopo di ridurre la rilevazione dei dati ed impedirne il trattamento illecito.

Il gruppo pone inoltre l'accento sull'importanza dei codici di condotta destinati a contribuire alla corretta applicazione dei principi di protezione dei dati tenendo conto delle caratteristiche specifiche dei diversi settori, conformemente all'articolo 27 della direttiva 95/46/CE. I codici comunitari possono essere presentati al gruppo, che determinerà, tra l'altro, se i progetti ad esso presentati sono conformi alle disposizioni nazionali in tema di protezione dei dati adottate in applicazione della direttiva 95/46/CE.

---

[24] Vedi anche il punto 3.2 sopra sul riutilizzo compatibile.

CONCLUSIONI

Il gruppo ritiene che la maggior parte dei dati biometrici comporti il trattamento di dati personali. Al momento di sviluppare sistemi biometrici è necessario pertanto rispettare pienamente i principi di protezione dei dati di cui alla direttiva 95/46/CE considerando la natura specifica della biometria, fra cui la possibilità di rilevare dati biometrici all'insaputa della persona interessata e la quasi certezza del legame con detta persona.

Il rispetto del principio di proporzionalità, che costituisce l'elemento centrale della protezione garantita dalla direttiva 95/46/CE, impone, soprattutto nell'ambito dell'autenticazione/verifica, una netta preferenza per le applicazioni biometriche che non trattano dati ottenuti a partire da tracce lasciate inconsapevolmente dagli individui o che non rientrano in un sistema centrale. Questo permette alla persona interessata di esercitare un migliore controllo sul trattamento dei dati personali che la riguardano.

Il gruppo intende rivedere il presente documento di lavoro alla luce dell'esperienza delle autorità incaricate della protezione dei dati nonché degli sviluppi tecnologici legati alle applicazioni biometriche. Poiché attualmente i dati biometrici vengono introdotti per vari usi in una serie di diversi contesti sarà necessario proseguire il lavoro senza indugio, in particolare nel settore dell'occupazione, dei visti, dell'immigrazione e della sicurezza nell'ambito dei viaggi.

Benché spetti all'industria sviluppare sistemi biometrici conformi ai principi di protezione dei dati, un dialogo costruttivo tra tutte le parti interessate, comprese le autorità di tutela dei dati, basato in particolare su un progetto di codice di condotta, si rivelerebbe assai utile da tutti i punti di vista.

Bruxelles, 13 giugno 2003
Per il gruppo
Il Presidente
Stefano RODOTÀ