GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

00720/12/IT

WP193

Parere 3/2012 sugli sviluppi nelle tecnologie biometriche

adottato il 27 aprile 2012

[NdT] Ai fini del presente parere, con "responsabile del trattamento" e con "incaricato del trattamento" si intendono rispettivamente il "titolare" e il "responsabile" di cui all'articolo 4, lettera f) e lettera g) del decreto legislativo 30 giugno 2003, n. 196 (codice in materia di protezione dei dati personali).

Sintesi

I sistemi biometrici sono strettamente legati all'individuo perché sono in grado di sfruttarne una caratteristica determinata e unica ai fini dell'identificazione e/o dell'autenticazione. Mentre i dati biometrici di una persona possono essere cancellati o modificati, la fonte da cui sono stati estratti non può di norma essere né modificata, né cancellata.

I dati biometrici sono usati con successo ed efficacia nella ricerca scientifica; essi rappresentano inoltre un elemento chiave della scienza forense e una valida componente dei sistemi di controllo dell'accesso. Questi dati sono in grado di aumentare il livello di sicurezza e facilitano le procedure di identificazione e autenticazione rendendole veloci e agevoli. In passato, l'impiego di questa tecnologia era economicamente dispendioso e, pertanto, l'impatto sui diritti delle persone fisiche in materia di protezione dei dati era limitato. Negli ultimi anni questa situazione è mutata sostanzialmente: l'analisi del DNA è divenuta più rapida e accessibile quasi per tutti, il progresso tecnologico ha fatto diminuire il costo dello spazio di archiviazione e della potenza di elaborazione, rendendo possibile la creazione di album di immagini online e di *social network* contenenti miliardi di fotografie. I lettori di impronte digitali e i dispositivi di videosorveglianza sono ormai un oggetto di consumo alla portata di tutti. Grazie al contributo fornito dallo sviluppo di queste tecnologie, molte operazioni sono più facilmente realizzabili, gli autori di numerosi reati sono stati individuati e i sistemi di controllo dell'accesso sono più affidabili; tuttavia, tale sviluppo ha anche introdotto nuove minacce ai diritti fondamentali. La discriminazione genetica è divenuta un problema concreto e il furto di identità un rischio non più teorico.

Se altre nuove tecnologie destinate al pubblico, che di recente hanno sollevato preoccupazioni riguardanti la protezione dei dati, non sono necessariamente incentrate sulla creazione di un legame diretto con un soggetto specifico oppure se la creazione di tale collegamento richiede un considerevole dispendio di tempo ed energie, i dati biometrici sono, proprio per la loro natura, direttamente collegati a una persona. Il che non è sempre un aspetto positivo, anzi comporta svariati svantaggi. Da un lato, per esempio, il fatto di dotare i sistemi di videosorveglianza e gli *smartphone* di sistemi di riconoscimento del volto basati su banche dati di *social network* potrebbe far venire meno l'anonimato e la circolazione non identificata delle persone; dall'altro, tuttavia, i lettori di impronte digitali, i lettori di vene o anche solo un sorriso in una videocamera possono sostituire carte, codici, *password* e firme.

Il presente parere affronta questi ed altri recenti sviluppi per sensibilizzare sia le persone coinvolte, sia gli organi legislativi. Le innovazioni tecniche, molto spesso presentate come tecnologie che servono soltanto a migliorare la capacità dell'utente e la fruibilità delle applicazioni, possono in realtà determinare, in assenza di adeguate garanzie, una graduale perdita di riservatezza. Pertanto, il parere individua misure tecniche e organizzative che mirano ad attenuare i rischi per la protezione dei dati e la vita privata, e che possono contribuire a evitare conseguenze negative sulla vita privata dei cittadini europei e sul loro diritto fondamentale alla protezione dei dati.

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,

visti l'articolo 29 e l'articolo 30, paragrafo 1, lettera a), e paragrafo 3, della suddetta direttiva,

visto il proprio regolamento interno,

HA ADOTTATO IL PRESENTE PARERE

1. Campo di applicazione del parere

Nel documento di lavoro sulla biometria del 2003 (WP80) il Gruppo di lavoro articolo 29 (in prosieguo: il "Gruppo di lavoro") ha preso in considerazione alcune problematiche in materia di protezione dei dati relative all'utilizzo di tecnologie emergenti in grado di leggere e di elaborare elettronicamente dati biometrici. Negli anni passati è stato fatto un ampio uso di questa tecnologia nei settori pubblico e privato ed è stata sviluppata una serie di nuovi servizi. Le tecnologie biometriche, che un tempo richiedevano l'investimento di importanti risorse finanziare o informatiche, sono divenute straordinariamente più rapide ed economiche e l'uso di lettori di impronte digitali è oggi una consuetudine diffusa. Alcuni computer portatili, per esempio, contengono un lettore di impronte digitali per il controllo biometrico dell'accesso. I progressi raggiunti nel campo dell'analisi del DNA consentono attualmente di ottenere risultati in pochi minuti. Fra le tecnologie di recente creazione ne esistono alcune, quali il riconoscimento del volto o dello schema delle vene, che hanno già raggiunto un livello ottimale di sviluppo e il cui impiego in svariate situazioni della vita quotidiana è ormai imminente. Le tecnologie biometriche sono strettamente connesse a talune caratteristiche personali degli individui e alcune possono essere utilizzate per rivelare dati sensibili. Inoltre, molte di queste tecnologie consentono il tracciamento automatizzato nonché la localizzazione o la profilazione delle persone, per cui il loro impatto potenziale sulla vita privata e sulla protezione dei dati delle persone è elevato. Tale impatto è direttamente proporzionale alla crescente diffusione di queste tecnologie: qualsiasi individuo potrebbe essere registrato in uno o più sistemi biometrici.

Scopo del parere è fornire un quadro rivisto e aggiornato di linee guida generali unificate e di raccomandazioni sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni biometriche. Esso è rivolto alle autorità legislative europee e nazionali, all'industria dei sistemi biometrici e agli utenti di tali tecnologie.

2. Definizioni

Le tecnologie biometriche non sono nuove e sono già state oggetto di vari pareri del Gruppo di lavoro. In questa sezione è riportato un elenco delle definizioni pertinenti, ove opportuno debitamente aggiornate.

Dati biometrici: come già osservato dal Gruppo di lavoro nel parere 4/2007 (WP136), i dati biometrici possono essere definiti come

> *proprietà biologiche, aspetti comportamentali, caratteristiche fisiologiche, tratti biologici o azioni ripetibili laddove tali caratteristiche e/o azioni sono tanto proprie di un certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità.*

I dati biometrici cambiano in maniera irreversibile la relazione tra corpo e identità, in quanto le caratteristiche del corpo umano possono essere "lette" da una macchina e sottoposte a un successivo trattamento.

I dati biometrici possono essere archiviati e trattati in vari modi. Talvolta le informazioni di natura biometrica ottenute da una persona sono archiviate e trattate in una forma grezza che permette di riconoscerne la fonte senza avere conoscenze specifiche (per esempio, la fotografia di un volto, l'immagine di un'impronta digitale o la registrazione della voce). Talaltra, le informazioni di natura biometrica ottenute in forma grezza vengono trattate in maniera da estrarre e salvare come modello biometrico soltanto determinate caratteristiche e/o aspetti.

Fonte dei dati biometrici: la fonte dei dati biometrici può essere estremamente varia ed essere costituita dagli elementi fisici, fisiologici, comportamentali o psicologici di una persona. Secondo il parere 4/2007 (WP136):

> *le fonti di dati biometrici (per esempio, i campioni di tessuti umani) non possono essere considerate dati biometrici di per sé ma possono essere usate per la raccolta di dati biometrici (mediante l'estrazione di informazioni dalle fonti stesse).*

Come indicato nel parere WP80, si distinguono due categorie principali di tecniche biometriche:

- esistono, in primo luogo, tecniche di tipo fisico e **fisiologico** che misurano le caratteristiche fisiche e 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, l'analisi dei pori della pelle, ecc.;
- 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, il modo di camminare o di muoversi, schemi che indicano percorsi mentali subconsci come il fatto di mentire ecc.

Occorre altresì tenere conto di un campo di tecniche emergente, basate sulla **psicologia**, in cui figura la misurazione della risposta a situazioni concrete o test specifici per l'eventuale corrispondenza a un determinato profilo psicologico.

Modello biometrico: dalla forma grezza dei dati biometrici è possibile estrarre caratteristiche principali (per esempio, misurazioni del volto da un'immagine) e conservarle per sottoporle a trattamento in un secondo tempo, al posto degli stessi dati grezzi. In tal caso si parla di

modello biometrico dei dati. La definizione delle dimensioni (la quantità di informazioni) del modello è una questione fondamentale. Da un lato le dimensioni devono essere sufficientemente ampie da permettere di gestire la sicurezza (evitando sovrapposizioni fra dati biometrici diversi o sostituzioni di identità); dall'altro lato, le dimensioni del modello non devono essere eccessivamente ampie, onde evitare il rischio di ricostruzione dei dati biometrici. La creazione del modello deve essere un processo univoco, nel senso che non dovrebbe essere possibile ricreare i dati biometrici grezzi a partire dal modello.

Sistemi biometrici: secondo il WP80 i sistemi biometrici sono:

> *applicazioni di tecnologie biometriche che permettono l'identificazione e/o l'autenticazione/verifica automatica di un individuo. Le applicazioni a fini di autenticazione/verifica sono spesso utilizzate per vari compiti in settori completamente differenti, a vari fini e sotto la responsabilità di numerose entità diverse.*

Grazie ai recenti sviluppi tecnologici, è inoltre possibile oggi servirsi dei sistemi biometrici per scopi di classificazione/separazione.

I rischi dei sistemi biometrici derivano dalla natura stessa dei dati biometrici utilizzati nel trattamento. Pertanto, una definizione più generica potrebbe essere quella di un sistema che estrae dati biometrici per sottoporli successivamente a trattamento.

Il trattamento di dati biometrici in un sistema biometrico comporta, di norma, l'esecuzione di processi differenti quali l'iscrizione, l'archiviazione e il confronto:

- iscrizione dei dati biometrici: comprende tutti i processi che hanno luogo all'interno di un sistema biometrico per estrarre dati biometrici da una fonte biometrica e per collegarli a una persona. La quantità e la qualità dei dati richiesti nel corso dell'iscrizione dev'essere sufficiente a consentire l'identificazione, l'autenticazione, la classificazione o la verifica corrette della persona senza ricorrere alla registrazione di una quantità eccessiva di dati. La quantità di dati estratti da una fonte biometrica durante la fase di iscrizione dev'essere adeguata alla finalità del trattamento, come pure al livello di rendimento del sistema biometrico.

La fase di iscrizione costituisce di norma il primo contatto che una persona ha con un sistema biometrico specifico. Nella maggior parte dei casi l'iscrizione richiede la partecipazione diretta dell'interessato (per esempio, nella rilevazione delle impronte digitali) e, pertanto, può offrire una valida opportunità per fornire informazioni e una corretta notificazione del trattamento. Tuttavia, l'iscrizione di una persona può altresì avvenire a sua insaputa o senza il suo consenso (per esempio, nel caso dei sistemi di televisione a circuito chiuso dotati di funzionalità di riconoscimento del volto). L'accuratezza e la sicurezza del processo di iscrizione è essenziale per la prestazione dell'intero sistema. Una persona potrebbe essere in grado di iscriversi nuovamente in un sistema biometrico per aggiornare i dati biometrici registrati.

- Conservazione dei dati biometrici: i dati ottenuti durante la fase di iscrizione possono essere conservati a livello locale nei centri operativi in cui è stata effettuata l'iscrizione (per esempio, in un lettore) per un utilizzo futuro, su un dispositivo in possesso dell'interessato (per esempio, una *smart card*) oppure possono essere inviati e archiviati in una banca dati a livello centrale, accessibile da uno o più sistemi biometrici.

- **Confronto dei dati biometrici**: si tratta del confronto dei dati/del modello biometrici (ottenuti durante l'iscrizione) con i dati/il modello biometrici raccolti da un nuovo campione ai fini dell'identificazione, della verifica/autenticazione o della classificazione.

Identificazione biometrica: l'identificazione di una persona con un sistema biometrico consiste solitamente nel confronto dei dati biometrici di tale persona (acquisiti al momento dell'identificazione) con una serie di modelli biometrici conservati in una banca dati (per esempio, un confronto di vari campioni).

Verifica/autenticazione biometrica: l'identificazione di una persona con un sistema biometrico consiste solitamente nel confronto dei dati biometrici di tale persona (acquisiti al momento dell'identificazione) con un unico modello biometrico conservato in un dispositivo (per esempio, un confronto di due campioni).

Classificazione/separazione biometrica: la classificazione/separazione biometrica di una persona mediante un sistema biometrico consiste solitamente nello stabilire se i dati biometrici di una persona appartengano a un gruppo dotato di alcune caratteristiche predefinite al fine di intraprendere un'azione specifica. In tal caso, non è importante identificare o verificare la persona, bensì inserirla automaticamente in una determinata categoria. Per esempio, una schermata pubblicitaria può mostrare messaggi pubblicitari diversi, in base all'età o al sesso della persona che la guarda.

Biometria multimodale: può essere definita come la combinazione di tecnologie biometriche diverse per migliorare l'accuratezza o il rendimento del sistema (nota anche come biometria multilivello). Durante il confronto i sistemi biometrici impiegano due o più tratti o modalità biometrici della stessa persona. Questi sistemi possono funzionare in maniera diversa: raccogliendo dati biometrici diversi con sensori altrettanto diversi oppure prelevando unità multiple dei medesimi dati biometrici. Alcuni studi inseriscono in questa categoria anche i sistemi che funzionano effettuando letture multiple degli stessi dati biometrici o quelli che utilizzano algoritmi multipli per l'estrazione di caratteristiche sul medesimo campione biometrico. Tra gli esempi di sistemi biometrici multimodali figurano il passaporto elettronico nell'UE e gli *US-VISIT Biometric Identification Services* (servizi di identificazione biometrica US-VISIT) negli Stati Uniti.

Accuratezza: difficilmente l'utilizzo di sistemi biometrici consente di ottenere risultati del tutto privi di errore; ciò a causa di differenze a livello ambientale al momento dell'acquisizione dei dati (illuminazione, temperatura, ecc.) e di differenze nelle apparecchiature usate (videocamere, dispositivi di scansione, ecc.). I parametri più comunemente usati per la valutazione dei risultati sono il *False Accept Rate* e il *False Reject Rate*, che possono essere adeguati al sistema in uso:

- *False Accept Rate* (FAR): consiste nella probabilità che un sistema biometrico identifichi in maniera errata una persona o che non respinga un impostore. Esso misura la percentuale di dati invalidi erroneamente accettati ed è altresì noto come falso positivo.

- *False Reject Rate* (FRR): consiste nella probabilità che il sistema non riconosca una persona. Ciò si verifica quando una persona non viene associata al suo modello biometrico. Il parametro è noto altresì come falso negativo.

Con un corretto aggiustamento del sistema e un'esatta regolazione delle impostazioni è possibile ridurre al minimo gli errori importanti dei sistemi biometrici fino al livello consentito per l'uso operativo, limitando il rischio di valutazioni inesatte. Un sistema perfetto sarà caratterizzato da valori FAR e FRR pari a zero, sebbene, più comunemente, tali parametri sono inversamente proporzionali, per cui l'incremento del parametro FAR spesso riduce il livello del parametro FRR.

Nel valutare se l'accuratezza di un determinato sistema biometrico sia o meno accettabile è importante esaminare la finalità del trattamento, come pure il FAR e il FRR e la dimensione della popolazione. Inoltre, la valutazione dell'accuratezza di un sistema biometrico può tener conto anche della capacità di individuare un campione dal vero. Per esempio, è possibile copiare impronte digitali latenti e utilizzarle per creare false impronte. In tal caso un lettore di impronte digitali non deve lasciarsi ingannare ma deve essere in grado di identificare correttamente la persona in questione.

3. Analisi giuridica

Il quadro giuridico pertinente è la direttiva sulla protezione dei dati (95/46/CE). Il Gruppo di lavoro ha già affermato, nel suo parere WP80, che nella maggior parte dei casi i dati biometrici sono dati personali. Pertanto, essi possono essere oggetto di trattamento soltanto in presenza di una base giuridica e se il trattamento è adeguato, pertinente e non eccedente rispetto alle finalità per le quali vengono rilevati e/o successivamente trattati.

Finalità

Un requisito fondamentale per il ricorso alla biometria consiste nella chiara definizione delle finalità per le quali vengono raccolti e trattati i dati, tenendo conto dei rischi per la protezione dei diritti fondamentali e delle libertà delle persone.

Per esempio, i dati biometrici possono essere raccolti per garantire o aumentare la sicurezza dei sistemi di trattamento attuando misure appropriate per proteggere i dati personali dall'accesso non autorizzato. In linea di principio, non esistono ostacoli all'attuazione di misure di sicurezza appropriate basate su caratteristiche biometriche dei soggetti incaricati del trattamento al fine di garantire un livello di sicurezza adeguato, in relazione ai rischi che il trattamento comporta e alla natura dei dati personali da proteggere. Tuttavia, non bisogna dimenticare che l'utilizzo della biometria non garantisce di per sé una maggiore sicurezza, in quanto molti dati biometrici sono rilevabili all'insaputa della persona interessata. Maggiore è il livello di sicurezza previsto, minore è la capacità dei dati biometrici di soddisfare da soli tale obiettivo.

Il principio di limitazione delle finalità dev'essere rispettato unitamente agli altri principi sulla protezione dei dati; nello specifico, occorre tenere presenti i principi della proporzionalità, della necessità e della minimizzazione dei dati allorché vengono definite le diverse finalità di un'applicazione. Quando è possibile, l'interessato deve poter scegliere fra le varie finalità di un'applicazione con molteplici funzionalità, soprattutto se una o più di esse richiedono il trattamento di dati biometrici.

Esempio:
è stato consigliato l'uso di dispositivi elettronici che offrono procedure di autenticazione specifiche basate su dati biometrici in relazione alle misure di sicurezza da adottare in caso di:

- trattamento di dati personali raccolti da operatori di telefonia durante intercettazioni autorizzate da un giudice;
- accesso ai dati relativi al traffico e all'ubicazione conservati per finalità giudiziarie da fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione e accesso alle strutture pertinenti ove sono conservati tali dati;
- raccolta e archiviazione di dati genetici e di campioni biologici.

Le **fotografie** su internet, nei media sociali, nelle applicazioni on-line per la gestione o la condivisione di fotografie non possono essere oggetto di ulteriori trattamenti al fine dell'estrazione di modelli biometrici o dell'iscrizione in un sistema biometrico per il riconoscimento automatico delle persone basato sulle immagini (riconoscimento del volto) in assenza di una specifica base giuridica (il consenso, per esempio) per questa nuova finalità. In presenza di una base giuridica per tale finalità accessoria, il trattamento dev'essere inoltre adeguato, pertinente e non eccedente rispetto a tale finalità. Qualora una persona interessata abbia fornito il proprio consenso al trattamento delle fotografie in cui essa compare per essere automaticamente associata a un album di fotografie online con un algoritmo per il riconoscimento del volto, questo trattamento dev'essere effettuato in un modo che tenga conto della protezione dei dati: una volta che nome, pseudonimo o altro testo specificato dall'interessato sono stati associati alle immagini, i dati biometrici non più necessari vanno cancellati. La creazione di una banca di dati biometrici permanente non è necessaria a priori per questa finalità.

Proporzionalità

L'uso della biometria pone il problema della proporzionalità di ogni categoria di dati trattati alla luce delle finalità del trattamento. Il fatto che i dati biometrici possano essere usati soltanto se adeguati, pertinenti e non eccessivi comporta una rigorosa valutazione della necessità e della proporzionalità dei dati trattati e se sia possibile raggiungere la finalità perseguita in maniera meno invasiva.

Nell'analisi della proporzionalità di un sistema biometrico proposto, la prima considerazione fondamentale è se il sistema sia inevitabile per soddisfare la necessità accertata, ossia se è essenziale per soddisfare tale necessità o, piuttosto, è il più conveniente o quello più efficace sotto il profilo dei costi. Il secondo fattore di cui tener conto è la potenziale efficacia del sistema riguardo al soddisfacimento di tale necessità alla luce delle peculiarità della tecnologia biometrica di cui si prevede l'uso[1]. Il terzo aspetto da soppesare è se la conseguente perdita di riservatezza sia proporzionata al vantaggio previsto. Nel caso in cui il vantaggio sia relativamente minore, come una maggiore comodità o un esiguo risparmio, la perdita di riservatezza non sarà ritenuta opportuna. Il quarto aspetto da tenere in

[1] Biometria per finalità di verifica o di identificazione: un identificatore biometrico può essere ritenuto idoneo sotto il profilo tecnico per una finalità e non per l'altra (per esempio, si devono preferire le tecnologie caratterizzate da basse percentuali di falsi negativi in sistemi pensati per finalità di identificazione nell'ambito di attività di contrasto).

considerazione nella valutazione dell'adeguatezza di un sistema biometrico è osservare se un mezzo meno invasivo della riservatezza possa raggiungere lo scopo desiderato[2].

Esempio:
In un centro fitness e salute viene installato un sistema biometrico centralizzato basato sul rilevamento delle impronte digitali per consentire l'accesso al centro e ai servizi da esso offerti soltanto ai clienti che hanno pagato l'ingresso.
Per il funzionamento del sistema sarebbe necessario conservare le impronte digitali di tutti i clienti e dei membri del personale. Questa applicazione appare sproporzionata alla necessità di controllare l'accesso al centro e di facilitare la gestione degli abbonamenti. Non è impossibile prevedere altre misure ugualmente applicabili ed efficaci quali una semplice lista di controllo, l'utilizzo di etichette RFID o di un tesserino magnetico, che non richiedono il trattamento di dati biometrici.

Il Gruppo di lavoro mette in guardia contro i rischi che comporta l'uso di dati biometrici per finalità di identificazione in grandi banche dati centralizzate, considerate le conseguenze potenzialmente pregiudizievoli per le persone interessate.

Si deve tenere conto dell'enorme impatto sulla dignità umana degli interessati e delle implicazioni di tali sistemi per i diritti fondamentali. Alla luce della convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, nonché della giurisprudenza della Corte europea dei diritti dell'uomo sull'articolo 8 della convenzione, il Gruppo di lavoro sottolinea che qualsiasi ingerenza nel diritto alla protezione dei dati dev'essere consentita unicamente a condizione che sia prevista dalla legge e che sia necessaria in una società democratica per proteggere un interesse pubblico importante[3].

Per garantire il rispetto di queste condizioni è necessario specificare l'obiettivo perseguito dal sistema ed esaminare la proporzionalità dei dati da inserirvi con riferimento a tale obiettivo.

A tal fine, il responsabile del trattamento è tenuto a dimostrare se il trattamento e i meccanismi ad esso relativi, le categorie dei dati da raccogliere e da trattare, nonché il trasferimento di informazioni contenute nella banca dati siano necessari e indispensabili. Le misure di sicurezza adottate devono essere adeguate ed efficaci. Il responsabile del trattamento deve tener conto dei diritti delle persone cui si riferiscono i dati personali e garantire che l'applicazione contenga un meccanismo adeguato per l'esercizio di tali diritti.

---

2 Per esempio, *smart card* o alri metodi che non raccolgono o centralizzano informazioni biometriche per finalità di autenticazione.

3 Cfr. Corte di giustizia dell'Unione europea, sentenza del 20 maggio 2003 nelle cause riunite C-465/00, C-138/01 e C-139/01, *Rechnungshof/Österreichischer Rundfunk e a.*, Corte europea dei diritti dell'uomo, sentenza del 4 dicembre 2008, ricorsi 30562/04 e 30566/04, *S. e Marper/ Regno Unito* nonché sentenza del 19 luglio 2011, ricorsi 30089/04, 14449/06, 24968/07, 13870/08, 36363/08, 23499/09, 43852/09 e 64027/09 *Goggins e a./Regno Unito*.

Esempio:
Uso di dati biometrici per finalità di identificazione. I sistemi che analizzano il volto di una persona, nonché quelli che ne analizzano il DNA, possono contribuire in maniera molto significativa alla lotta contro la criminalità e a rivelare in modo efficace l'identità di sconosciuti sospettati di aver commesso un reato grave. Tuttavia, se usati su larga scala, questi sistemi producono gravi effetti collaterali. Nel caso del riconoscimento del volto in cui i dati biometrici sono facilmente ottenibili all'insaputa dell'interessato, un utilizzo indiscriminato metterebbe fine all'anonimato nelle aree pubbliche e consentirebbe la localizzazione continua di persone. Nel caso dei dati riguardanti il DNA, l'uso della tecnologia si accompagna al rischio della potenziale divulgazione di dati sensibili sulla salute di un individuo.

Accuratezza

I dati biometrici trattati devono essere accurati e pertinenti rispetto alle finalità per le quali vengono rilevati. I dati devono essere accurati al momento dell'iscrizione e nel momento in cui si stabilisce il legame fra la persona e i dati biometrici. L'accuratezza al momento dell'iscrizione è inoltre importante per prevenire il furto d'identità.

I dati biometrici sono unici e la maggior parte di essi genera un solo campione o una sola immagine. Se impiegati su larga scala, in particolare con riferimento a una fascia importante di popolazione, i dati biometrici possono essere considerati alla stregua di un mezzo identificativo di portata generale ai sensi della direttiva 95/46/CE. L'articolo 8, paragrafo 7, della suddetta direttiva è pertanto applicabile e gli Stati membri sono tenuti a determinare le condizioni del relativo trattamento.

Minimizzazione dei dati

Potrebbe sorgere una difficoltà specifica, in quanto i dati biometrici contengono spesso più informazioni di quelle richieste per il confronto delle funzioni. Il responsabile del trattamento è tenuto all'applicazione del principio della minimizzazione dei dati e questo significa, in primo luogo, che soltanto le informazioni richieste devono essere trattate, trasmesse o conservate – non tutte quelle disponibili. In secondo luogo, il responsabile del trattamento dei dati deve garantire che la configurazione di default agevoli la protezione dei dati senza doverla attuare.

Periodo di conservazione

Il responsabile del trattamento è tenuto a determinare un periodo di conservazione per i dati biometrici che non dev'essere superiore a quello necessario al conseguimento delle finalità per le quali essi sono rilevati o sono successivamente trattati. Il responsabile del trattamento deve garantire che i dati o i profili derivati da tali dati siano cancellati definitivamente al termine del suddetto periodo.

Dev'essere chiara la differenza fra dati personali generici eventualmente necessari per un periodo di tempo più lungo e dati biometrici ormai inutili, per esempio quando l'interessato non ha più accesso a un'area specifica.

Esempio:
Un datore di lavoro utilizza un sistema biometrico per controllare l'accesso a un'area riservata. Le mansioni di un lavoratore non prevedono più l'accesso all'area riservata (per esempio a causa di mutate responsabilità o lavoro). In questo caso i suoi dati biometrici devono essere cancellati, essendo venuta meno la finalità per la quale essi sono stati raccolti.

3.1. Motivo di liceità

Il trattamento dei dati biometrici si deve fondare su uno dei motivi di liceità di cui all'articolo 7 della direttiva 95/46/CE.

3.1.1. Consenso, articolo 7, lettera a)

Il primo motivo di liceità indicato all'articolo 7, lettera a), è che l'interessato abbia manifestato il proprio consenso al trattamento. Secondo l'articolo 2, lettera h), della direttiva sulla protezione dei dati, il consenso dev'essere una manifestazione di volontà libera, specifica e informata della persona interessata. Dev'essere chiaro che tale consenso non può essere formulato in maniera libera con l'accettazione obbligatoria di termini e condizioni generali oppure mediante possibilità di optare per l'esclusione. Inoltre, il consenso dev'essere revocabile. In proposito, nel suo parere sulla definizione di consenso, il Gruppo di lavoro sottolinea diversi aspetti importanti della nozione: la validità del consenso, il diritto dei singoli alla revoca del proprio consenso, il consenso rilasciato prima dell'inizio del trattamento e i requisiti sulla qualità e l'accessibilità dell'informazione[4].

In molti casi di trattamento di dati biometrici, senza una valida alternativa come una *password* o un tesserino magnetico il consenso non può considerarsi fornito in maniera libera. Per esempio, un sistema che ne scoraggi l'uso da parte degli interessati (perché fa perdere troppo tempo o è troppo complicato) non può essere considerato una valida alternativa e non comporta, dunque, un consenso valido.

Esempi:
In mancanza di altri motivi di liceità, un sistema biometrico di autenticazione potrebbe essere usato per controllare l'accesso a un video club soltanto se i clienti sono liberi di decidere se avvalersi o meno di tale sistema. Ciò significa che il proprietario del video club deve offrire meccanismi alternativi e meno invasivi della vita privata. Tale sistema dovrà permettere al cliente che, per motivi personali, non desidera o non è in grado di sottoporsi alla rilevazione delle impronte digitali, di opporvisi. La semplice scelta tra non usare un servizio e fornire i propri dati biometrici prova chiaramente che il consenso non è stato fornito in maniera libera e che non può essere considerato un motivo di liceità.

In una scuola materna è installato uno *scanner* rilevatore dello schema delle vene per verificare che gli adulti (genitori e membri del personale) che vi accedono siano autorizzati a farlo. Per il funzionamento di tale sistema sarebbe necessario conservare le impronte digitali di tutti i genitori e dei membri del personale. In mancanza di una modalità alternativa di accesso alla scuola materna, il consenso rappresenterebbe una base giuridica discutibile, soprattutto per i lavoratori, che potrebbero non disporre di un'opportunità di scelta concreta di opporsi all'uso di tale sistema, ma anche per i genitori.

[4] WP 187, parere 15/2011 sulla definizione di consenso.

Benché possa sussistere il forte sospetto che il consenso fornito sia debole alla luce della naturale posizione di squilibrio tra lavoratore e datore di lavoro, il Gruppo di lavoro non lo esclude del tutto "*purché vi siano garanzie sufficienti che si tratti veramente di una manifestazione di volontà libera*"[5].

Pertanto, il consenso nell'ambito del lavoro subordinato dev'essere analizzato e debitamente dimostrato. Invece di richiedere il consenso, i datori di lavoro potrebbero occuparsi di verificare se è necessario usare i dati biometrici dei lavoratori per finalità legittime e ponderare tale necessità con i diritti e le libertà fondamentali dei lavoratori medesimi. Laddove la necessità sia adeguatamente dimostrabile, la base giuridica di tale trattamento può fondarsi sull'interesse legittimo del responsabile del trattamento come definito all'articolo 7, lettera f), della direttiva 95/46/CE. Il datore di lavoro è sempre tenuto a cercare i mezzi meno invasivi scegliendo, se possibile, un procedimento non biometrico.

Tuttavia, come descritto al punto 3.1.3, possono esistere casi in cui un sistema biometrico potrebbe essere nell'interesse legittimo del responsabile del trattamento. In questi casi il consenso non è necessario.

Il consenso è valido soltanto quando vengono fornite informazioni sufficienti sull'uso dei dati biometrici e, poiché questi ultimi possono essere usati come identificatori unici e universali, fornendo informazioni chiare e facilmente accessibili circa le modalità di utilizzo dei dati specifici, la garanzia di un trattamento equo dev'essere ritenuta assolutamente necessaria. Ciò è pertanto un requisito fondamentale per un consenso valido nell'impiego dei dati biometrici.

Esempi:
Un consenso valido per un sistema di controllo dell'accesso che utilizza le impronte digitali richiede informazioni sul fatto se il sistema biometrico crei o meno un modello unico per quel sistema. In presenza di un algoritmo che genera il medesimo modello biometrico in sistemi biometrici differenti, l'interessato deve sapere che potrebbe essere riconosciuto in più sistemi biometrici differenti.

Qualcuno carica la propria immagine in un album fotografico su internet. L'iscrizione di questa immagine in un sistema biometrico richiede un consenso esplicito basato su informazioni esaustive in merito all'attività svolta con i dati biometrici, al lasso di tempo e alle finalità per cui essi saranno oggetto di trattamento.

Posto che il consenso è sempre revocabile, i responsabili del trattamento devono attuare mezzi tecnici che possano invertire l'uso di dati biometrici nei rispettivi sistemi. Un sistema biometrico che funziona sulla base del consenso dev'essere pertanto in grado di eliminare in maniera efficace tutti i collegamenti all'identità da esso creati.

3.1.2. Contratto, articolo 7, lettera b)

Il trattamento dei dati biometrici può rivelarsi necessario all'esecuzione del contratto concluso con l'interessato o all'esecuzione di misure precontrattuali prese su sua richiesta. Occorre tuttavia rilevare che ciò si applica in generale soltanto quando vengono forniti servizi puramente biometrici. Questa base giuridica non vale per legittimare un servizio accessorio consistente nell'iscrivere una persona in un sistema biometrico. Se tale servizio può essere distinto dal servizio principale, il contratto per quest'ultimo non può legittimare il trattamento dei dati biometrici. I dati personali non sono beni che si possono chiedere quale contropartita di un servizio; pertanto, i contratti che prevedono oppure che offrono un servizio unicamente

[5] WP 187, parere 15/2011 sulla definizione di consenso.

a condizione che qualcuno acconsenta al trattamento dei propri dati biometrici per un altro servizio non possono fungere da base giuridica per tale trattamento.

Esempi:
a) Due fratelli sottopongono alcuni campioni di capelli a un laboratorio per l'effettuazione di un test del DNA finalizzato a scoprire se sono realmente fratelli. Il contratto stipulato con il laboratorio per l'effettuazione di questo test è una base giuridica sufficiente per l'iscrizione e per il trattamento di dati biometrici.

b) Una persona inserisce una foto da mostrare ai suoi amici nel proprio album fotografico in un *social network*. Nel caso in cui il contratto (condizioni di servizio) preveda che l'uso del servizio sia vincolato all'iscrizione dell'utente in un sistema biometrico, quest'ultima disposizione non costituirebbe una base giuridica sufficiente per l'iscrizione.

3.1.3. Obbligo legale, articolo 7, lettera c)

Un altro motivo di liceità per il trattamento dei dati personali è che il detto trattamento sia necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento. Ciò si verifica, per esempio, in alcuni paesi nel momento in cui vengono rilasciati e/o usati passaporti[6] e visti[7].

3.1.4. Interessi legittimi del responsabile del trattamento, articolo 7, lettera f)

In base all'articolo 7 della direttiva 95/46/CE, il trattamento dei dati personali biometrici è inoltre giustificabile se è "necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure di terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata".

Ciò significa che esistono casi in cui l'uso di sistemi biometrici è nell'interesse legittimo del responsabile del trattamento. Tuttavia, siffatto interesse è legittimo soltanto se il rappresentante può dimostrare che il suo interesse prevale in maniera obiettiva sul diritto degli interessati a non essere iscritti in un sistema biometrico. Per esempio, quando la sicurezza di aree a rischio elevato dev'essere garantita in maniera specifica da un meccanismo che possa verificare con precisione se le persone sono autorizzate ad accedervi, un sistema biometrico può essere usato nell'interesse legittimo del responsabile del trattamento. Nell'esempio seguente riguardante un sistema biometrico di controllo dell'accesso a un laboratorio, il

---

[6] Le impronte digitali sono state inserite nei passaporti in ottemperanza al regolamento (CE) n. 2252/2004 del Consiglio, del 13 dicembre 2004, e nei permessi di soggiorno, in base al regolamento (CE) n. 1030/2002 del Consiglio, del 13 giugno 2002.

[7] La registrazione degli identificatori biometrici nel sistema di informazione visti (VIS) è stabilita dal regolamento (CE) n. 767/2008, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (regolamento VIS). Cfr. anche il parere 3/2007 sulla proposta di regolamento del Parlamento europeo e del Consiglio recante modifica dell'Istruzione consolare comune diretta alle rappresentanze diplomatiche e consolari di prima categoria in relazione all'introduzione di elementi biometrici e comprendente norme sull'organizzazione del ricevimento e del trattamento delle domande di visto (COM(2006)269 definitivo), WP134; il parere 2/2005 sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (COM (2004) 835 def.), WP 110; nonché il parere 7/2004 sull'inserimento di elementi biometrici nei permessi di soggiorno e nei visti tenuto conto della creazione del sistema di informazione visti (VIS), WP 96.

responsabile del trattamento non può offrire al lavoratore un meccanismo alternativo senza influire direttamente sulla sicurezza dell'area riservata, in quanto non esistono altre misure meno invasive idonee a raggiungere un livello adeguato di sicurezza per quest'area. È pertanto nel suo interesse legittimo attuare il sistema e iscrivere un numero limitato di lavoratori senza doverne ottenere il consenso. Tuttavia, nel caso in cui l'interesse legittimo del responsabile del trattamento costituisca un valido motivo di liceità per il trattamento, si applicheranno, come di consueto, tutti gli altri principi in materia di protezione dei dati, segnatamente il principio della proporzionalità e quello della minimizzazione dei dati.

Esempio:
In una società che si occupa di ricerca su virus pericolosi, un laboratorio è protetto da porte che si aprono soltanto una volta verificate con successo le impronte digitali e una volta effettuata la scansione dell'iride. Questo sistema è stato attuato per garantire che solo le persone cui sono noti i rischi specifici, che sono state formate sulle procedure da seguire e che l'azienda ritiene affidabili possano eseguire esperimenti con questi materiali pericolosi. L'interesse legittimo dell'azienda di accertarsi che unicamente le persone pertinenti sono autorizzate ad accedere a un'area riservata, per assicurare che i rischi per la sicurezza connessi all'accesso a quell'area specifica possano essere ridotti in maniera significativa, supera la volontà delle persone di non sottoporre a trattamento i propri dati biometrici.

Di norma, l'uso della biometria per necessità generiche di sicurezza di beni e persone non può essere considerato un interesse legittimo superiore agli interessi o ai diritti e alle libertà fondamentali dell'interessato. Al contrario, il trattamento di dati biometrici è giustificabile unicamente quale strumento necessario per la sicurezza di beni e/o persone laddove è dimostrata l'effettiva esistenza di un rischio considerevole sulla base di circostanze obiettive e documentate. A tal fine, il responsabile del trattamento deve dimostrare che le circostanze specifiche pongono un rischio concreto e considerevole, che egli è tenuto a valutare molto attentamente. Allo scopo di uniformarsi al principio di proporzionalità, in presenza di siffatte situazioni di rischio elevato il responsabile del trattamento è tenuto a verificare se eventuali misure alternative potrebbero essere ugualmente efficaci ma meno invasive rispetto agli obiettivi perseguiti e optare per esse.
È inoltre necessario riesaminare periodicamente l'esistenza delle circostanze in questione e, sulla base dei risultati di tale riesame, dev'essere terminata o interrotta ogni operazione di trattamento dei dati ormai ingiustificata.

3.2. Responsabile e incaricato del trattamento

La direttiva 95/46/CE pone alcuni obblighi agli incaricati del trattamento riguardo al trattamento dei dati personali. Nell'ambito della biometria varie tipologie di persone possono essere nominate "incaricato del trattamento", per esempio i lavoratori, le autorità di polizia o quelle competenti per l'immigrazione.

Il Gruppo di lavoro desidera richiamare gli orientamenti forniti nel suo parere sui concetti di responsabile del trattamento e di incaricato del trattamento[8], che contiene utili chiarimenti sulle modalità di interpretazione di queste definizioni chiave della direttiva.

[8] WP169, parere1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento".

3.3. Trattamento automatizzato (articolo 15 della direttiva)

L'uso di sistemi basati sul trattamento di dati biometrici richiede un'attenzione particolare per quanto concerne le conseguenze della potenziale discriminazione per le persone escluse dal sistema. Inoltre, al fine di proteggere il diritto delle persone di non essere oggetto di misure che abbiano effetti nei loro confronti e fondate esclusivamente su un trattamento automatizzato di dati, è necessario introdurre adeguate garanzie come interventi, rimedi o meccanismi umani, che consentano all'interessato di esprimere il suo punto di vista.

Secondo l'articolo 15 della direttiva 95/46/CE, "[g]*li Stati membri riconoscono a qualsiasi persona il diritto di non essere sottoposta ad una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento, ecc.*"

3.4. Trasparenza e informazione dell'interessato

In base al principio del trattamento leale, gli interessati devono essere a conoscenza della raccolta e/o dell'uso dei loro dati biometrici (articolo 6 della direttiva 95/46/CE). Vanno evitati i sistemi che raccolgono questi dati all'insaputa dell'interessato.

Il responsabile del trattamento deve accertarsi che gli interessati siano adeguatamente informati sugli elementi fondamentali del trattamento, in conformità con l'articolo 10 della direttiva sulla protezione dei dati, quali l'identità del responsabile, le finalità del trattamento, il tipo di dati, la durata del trattamento, i diritti degli interessati di accesso ai dati e di rettifica oppure di cancellare i propri dati e il diritto di revocare il consenso nonché le informazioni sui destinatari o le categorie di destinatari cui sono comunicati i dati. Posto che il responsabile del trattamento di un sistema biometrico è obbligato a informare l'interessato, nessuno deve raccogliere i dati biometrici all'insaputa dell'interessato.

3.5. Diritto di accesso ai dati biometrici

Gli interessati hanno il diritto di ottenere dagli incaricati del trattamento l'accesso ai propri dati, di norma anche a quelli biometrici. Gli interessati hanno altresì il diritto di accedere agli eventuali profili basati su questi dati biometrici. Nel caso in cui il responsabile del trattamento debba verificare l'identità degli interessati prima di consentire loro l'accesso, è fondamentale che quest'ultimo sia fornito senza procedere al trattamento di ulteriori dati personali.

3.6. Sicurezza dei dati

I responsabili del trattamento devono attuare misure tecniche ed organizzative appropriate 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, o da qualsiasi altra forma illecita di trattamento di dati personali.[9]

I dati raccolti e conservati devono essere adeguatamente protetti. Gli ideatori di sistemi sono tenuti a rivolgersi a idonei esperti della sicurezza per garantire che i punti deboli della sicurezza vengano affrontati in maniera adeguata, soprattutto in caso di migrazione su internet di sistemi esistenti.

[9] Articolo 17, paragrafo 1, della direttiva 95/46/CE.

3.7. Garanzie per persone con necessità particolari

L'uso della biometria potrebbe avere importanti ripercussioni sulla dignità, sulla vita privata e sul diritto alla protezione dei dati di persone vulnerabili come i minori, gli anziani e le persone che non sono fisicamente in grado di ultimare correttamente la procedura di iscrizione. Considerate le conseguenze potenzialmente dannose per le persone interessate, perché una misura possa essere ritenuta ammissibile dovranno essere soddisfatti requisiti più rigorosi nel processo di valutazione delle ripercussioni di misure che interferiscono con la dignità del singolo, interrogandosi sulla necessità e la proporzionalità nonché sulle possibilità del singolo di esercitare il suo diritto alla protezione dei dati. Devono essere presenti garanzie idonee contro i rischi di stigmatizzazione o discriminazione delle suddette categorie di persone a motivo dell'età o dell'incapacità di registrarsi.

Riguardo all'introduzione di un obbligo giuridico generico di raccolta di identificatori biometrici per questi gruppi, segnatamente per minori e anziani ai controlli alle frontiere ai fini di identificazione, il Gruppo di lavoro è dell'idea che "*– per rispetto della dignità umana e perché la procedura sia affidabile – sarebbe opportuno limitare, per i minori e gli anziani, il rilevamento e il trattamento delle impronte digitali e stabilire limiti d'età che siano coerenti con i limiti introdotti per altre grandi banche dati dell'Unione (Eurodac, per esempio*)"[10].

In ogni caso, devono essere attuate garanzie specifiche (idonee procedure di ripiego, per esempio) per garantire il rispetto della dignità umana e delle libertà fondamentali di chiunque non sia in grado di portare a termine correttamente la procedura di iscrizione, evitando in tal modo di far subire all'interessato le imperfezioni del sistema tecnico[11].

3.8. Dati sensibili

Alcuni dati biometrici potrebbero essere considerati sensibili ai sensi dell'articolo 8 della direttiva 95/46/CE, soprattutto i dati che rivelano l'origine razziale o etnica, ovvero i dati relativi alla salute. Per esempio, i dati sul DNA di una persona contengono sovente dati relativi alla salute o possono rivelarne l'origine razziale o etnica. In questo caso, i dati sul DNA sono sensibili e le garanzie particolari di cui all'articolo 8 devono applicarsi in aggiunta ai principi generali di protezione dei dati di cui alla suddetta direttiva. Va altresì tenuto conto del contesto del trattamento per valutare la sensibilità dei dati sottoposti a trattamento da un sistema biometrico[12].

3.9. Ruolo delle autorità nazionali garanti della protezione dei dati

Tenendo conto della crescente standardizzazione delle tecnologie biometriche di interoperabilità, in linea generale è pacifico che l'archiviazione centralizzata di dati biometrici accresce sia il rischio dell'utilizzo di tali dati quale chiave di connessione di banche dati multiple (il che potrebbe comportare la creazione di profili dettagliati di una persona), sia i pericoli specifici del riutilizzo di tali dati per finalità incompatibili, soprattutto nel caso di accesso non autorizzato.

Il Gruppo di lavoro raccomanda che i sistemi che utilizzano dati biometrici come chiave per connettere banche dati multiple prevedano ulteriori garanzie, in quanto questo tipo di

---

[10] WP134 – Parere 3/2007 sulla proposta di regolamento del Parlamento europeo e del Consiglio recante modifica dell'Istruzione consolare comune diretta alle rappresentanze diplomatiche e consolari di prima categoria in relazione all'introduzione di elementi biometrici e comprendente norme sull'organizzazione del ricevimento e del trattamento delle domande di visti (COM(2006)269 definitivo).

[11] Cfr. WP134 – Parere n. 3/2007, pag. 8.

[12] Cfr. WP 29 - Documento di consulenza su categorie speciali di dati ("dati sensibili") Ref. Ares (2011)444105 - 20/4/2011.

trattamento presenta potenzialmente rischi specifici per i diritti e le libertà degli interessati (articolo 20 della direttiva 95/46/CE). Allo scopo di assicurare la presenza di idonee garanzie e, in particolare, per attenuare i rischi per gli interessati, prima di introdurre tali misure il responsabile del trattamento deve consultare la competente autorità nazionale per il controllo della protezione dei dati.

4. Nuovi sviluppi e tendenze tecnologiche, nuovi scenari

4.1. Introduzione

Le tecnologie biometriche sono state a lungo usate principalmente dalle autorità pubbliche, ma di recente la situazione si è gradualmente modificata, nel senso che le organizzazioni commerciali svolgono oggi un ruolo primario nell'utilizzo di queste tecnologie e nello sviluppo di nuovi prodotti.

Uno dei motivi principali di questa situazione è che la tecnologia è progredita in maniera tale per cui i sistemi biometrici che funzionavano bene soltanto in condizioni controllate sono stati perfezionati e oggi sono adatti a un uso esteso in una serie di ambienti diversi. Al riguardo, in alcuni casi la biometria sta sostituendo o migliorando i tradizionali metodi di identificazione, segnatamente quelli basati su fattori multipli di identificazione, necessari per sistemi di autenticazione forte. Cresce inoltre l'uso di tecnologie biometriche in applicazioni che, al prezzo di un minor livello di precisione, sono in grado di identificare una persona in maniera rapida e agevole.

Anche l'uso di tecnologie biometriche è in graduale espansione rispetto alla sfera di applicazione originale: le tecniche di identificazione e autenticazione sono usate anche per l'analisi comportamentale, la sorveglianza e la prevenzione delle frodi.

I progressi ottenuti nel campo delle tecnologie informatiche e nelle reti stanno anch'essi conducendo alla nascita di quella che si definisce "biometria di seconda generazione", basata sull'utilizzo di caratteristiche comportamentali e psicologiche considerate da sole o combinate con altri sistemi tradizionali nell'ambito di sistemi multimodali. A completare il quadro, si osserva una graduale tendenza verso l'uso della biometria negli sviluppi dell'intelligenza ambientale diffusa e dell'informatica pervasiva.

4.2. Nuove tendenze riguardo alla biometria

Esistono varie tecnologie biometriche che possono essere ritenute mature, con svariate applicazioni nei sistemi di contrasto, di governo elettronico e commerciali, tra cui, a titolo meramente indicativo, impronte digitali, geometria della mano, scansione dell'iride e alcuni tipi di riconoscimento del volto. Si rileva altresì la presenza di alcune tecnologie biometriche emergenti dedicate all'analisi delle caratteristiche del corpo umano. Sebbene alcune di esse siano nuove, altre tecnologie biometriche tradizionali ricavano nuovi impulsi da altrettanto nuove capacità di elaborazione.

Elementi tipici di questi nuovi sistemi sono l'uso di caratteristiche del corpo umano che consentono la categorizzazione/identificazione di persone e la raccolta a distanza di tali caratteristiche. I dati rilevati vengono usati per la profilazione, per la sorveglianza a distanza o per compiti ancora più complessi come l'intelligenza ambientale.

Ciò è divenuto possibile grazie ai progressi continui nel campo dei sensori, che consentono la rilevazione di nuove caratteristiche fisiologiche, come pure di nuovi modi di trattare i dati biometrici tradizionali.

Occorre anche evidenziare l'utilizzo della cosiddetta *soft biometrics* (biometria "leggera"), che si identifica con l'uso di caratteristiche molto comuni, non idonee a distinguere o a identificare con chiarezza una persona, ma che consentono di migliorare il risultato di altri sistemi di identificazione.

Un altro elemento essenziale dei nuovi sistemi biometrici è la potenziale capacità di raccogliere informazioni a distanza o in movimento senza la collaborazione o l'intervento dell'interessato. Sebbene si tratti di una tecnologia non ancora pienamente sviluppata, l'impegno profuso è enorme, soprattutto ai fini delle attività di contrasto.

Ciò che progredisce rapidamente è l'uso di sistemi multimodali che impiegano biometrie diverse simultaneamente oppure letture/unità multiple della stessa biometria, che possono essere rettificate per ottimizzare lo scambio di sicurezza/facilità d'uso dei sistemi biometrici. In tal modo è possibile ridurre la percentuale di falsi positivi, migliorare i risultati di un sistema di riconoscimento oppure facilitare la raccolta di dati di un maggior numero di persone bilanciando la non universalità di una fonte di dati biometrici combinandola con un'altra.

Cresce sempre più l'utilizzo dei sistemi biometrici presso enti pubblici e privati; di norma, nel settore pubblico delle attività di contrasto i dati biometrici sono utilizzati con regolarità; si espande rapidamente l'uso della biometria anche nel settore della finanza, in quello bancario e dei servizi sanitari online, nonché in altri settori come quello dell'istruzione, del commercio al dettaglio e delle telecomunicazioni. Questo sviluppo sarà alimentato dalle nuove caratteristiche derivate dalla convergenza/fusione di tecnologie esistenti. Ne costituisce un esempio l'impiego dei sistemi di TV a circuito chiuso, che consentono la rilevazione e l'analisi di dati biometrici e di tracce comportamentali umane.

Quanto osservato può inoltre essere visto come un cambiamento di interesse per lo sviluppo dei sistemi biometrici dagli strumenti di identificazione verso finalità di riconoscimento blande, in altre parole, dall'identificazione alla rilevazione del comportamento o di necessità specifiche delle persone. Ciò fornisce nuove opportunità per usi di gran lunga diversi rispetto alle applicazioni di sicurezza su larga scala: sicurezza personale, gioco d'azzardo e commercio al dettaglio beneficeranno di una migliore interazione uomo-macchina, che andrà oltre l'identificazione o la categorizzazione delle persone.

4.3. Impatto sulla vita privata e sulla protezione di dati

Fin dall'inizio della loro attuazione si è confermata la capacità dei sistemi informatici di far sorgere seri motivi di preoccupazione in svariati settori, fra cui quello della vita privata e della protezione dei dati, che ne hanno senza dubbio influenzato l'accettazione sociale, alimentando il dibattito sulla legittimità e sui limiti del relativo utilizzo come pure sulle garanzie necessarie per attenuare i rischi individuati.

La tipica riluttanza nei confronti dei sistemi biometrici è stata, ed è tuttora, connessa alla protezione dei diritti dei singoli. Nondimeno, i nuovi sistemi e gli sviluppi di quelli esistenti fanno sorgere una serie di preoccupazioni, fra cui la possibilità di nascondere la raccolta, l'archiviazione e il trattamento, come pure la raccolta di materiali con informazioni particolarmente sensibili che possono invadere la sfera più intima del singolo.

Gli utilizzi deviati rappresentavano un problema già agli albori delle tecnologie e dei sistemi biometrici; sebbene questi costituiscano un rischio ben noto e già affrontato nella biometria tradizionale, è indubbiamente palese che le maggiori potenzialità tecniche dei nuovi sistemi informatici fanno sorgere il rischio che i dati vengano usati in maniera opposta alla loro finalità originaria.

Le tecniche di occultamento consentono l'identificazione all'insaputa degli interessati, comportando una seria minaccia per la vita privata e una perdita di controllo sui dati personali. Questo produce gravi conseguenze sulla capacità di esercitare liberamente il proprio consenso o, semplicemente, di ottenere informazioni sul trattamento. Inoltre, alcuni sistemi possono raccogliere segretamente informazioni connesse agli stati emozionali o alle caratteristiche corporee e rivelare informazioni riguardanti la salute che determinano un trattamento dei dati non proporzionale, nonché il trattamento dei dati sensibili ai sensi dell'articolo 8 della direttiva 95/46/CE.

Tenendo conto del fatto che le tecnologie biometriche non possono garantire un'accuratezza assoluta, esiste sempre un rischio implicito che deriva dalle identificazioni inesatte. I falsi positivi comportano decisioni che influiscono sui diritti dei singoli. Il furto di identità basato sull'uso di fonti biometriche falsificate o rubate può causare danni gravi. Diversamente da altri sistemi di identificazione, non si può semplicemente fornire una nuova identificazione al singolo soltanto perché è stata compromessa.

È opportuno menzionare la profilazione nell'ambito dell'adozione di decisioni automatizzate o per prevedere un comportamento o le preferenze in una situazione specifica Alcuni dati biometrici possono rivelare informazioni fisiche su una persona, le quali possono essere usate per individuare e definire finalità, come pure culminare nella discriminazione, nella stigmatizzazione o nel confronto non voluto con informazioni non previste/indesiderate.

4.4. Riferimento a tecnologie e sistemi biometrici specifici

4.4.1. Schema delle vene e usi combinati

Due principali tecnologie in uso si basano sul riconoscimento del percorso delle vene: il riconoscimento attraverso le vene del palmo della mano e il riconoscimento attraverso le vene delle dita, entrambe attualmente molto diffuse soprattutto in Giappone.

Dal punto di vista tecnico il riconoscimento attraverso il percorso delle vene si basa sul modello di vene ottenuto con una fotocamera a infrarossi quando il dito o la mano sono illuminati da una luce nel vicino infrarosso. L'immagine acquisita viene trattata per evidenziare le caratteristiche dello schema delle vene, creando in tal modo una nuova immagine della rete vascolare. Il vantaggio principale di questa tecnologia è che nessuno lascia traccia delle proprie caratteristiche biometriche[13] non essendo necessario "toccare" il lettore. Ad oggi è inoltre difficile rilevare dati biometrici senza il consenso dell'interessato. Infine, questa tecnica è altresì utilizzabile per scoprire se il soggetto presentato al sistema è vivo o morto, in base alla presenza della circolazione sanguigna.

[13] Alcuni autori sostengono che le tecnologie associate al riconoscimento dello schema delle vene possono rivelare malattie come l'ipertensione o talune anomalie vascolari.

Il riconoscimento attraverso lo schema delle vene è utilizzabile per applicazioni di accesso logico e per l'accesso fisico a strutture. I costruttori offrono anche la possibilità di inserire il sensore in altri prodotti, soprattutto per finalità legate alle attività bancarie.

I rischi per la protezione dei dati connessi all'uso di sistemi basati sullo schema delle vene possono essere illustrati come segue:

- accuratezza: il livello del risultato ottenibile dal percorso delle vene è elevato, poiché questa tecnologia è considerata come una valida alternativa alle impronte digitali. Il riconoscimento attraverso lo schema delle vene offre inoltre un basso "*Failure to Enrol Rate*" (FER), non essendo soggetto a deterioramento del dito o della mano. Queste tecnologie non sono ancora state sperimentate/usate presso il grande pubblico (in Giappone il modello è confrontato con quello conservato nella *smart card*). In alcuni casi questa tecnologia può essere influenzata anche da condizioni climatiche che si ripercuotono sul sistema vascolare (calore, pressione, ecc.).

- Impatto: l'impatto dei sistemi basati sugli schemi delle vene sulla protezione dei dati è limitato, in quanto i dati biometrici non si raccolgono facilmente e l'uso del percorso delle vene è attualmente limitato ad applicazioni nel settore privato.

- Consenso e trasparenza: poiché i dati relativi allo schema delle vene possono essere rilevati soltanto con l'impiego di illuminazione e fotocamere nel vicino infrarosso, si può ritenere che l'interessato sia a conoscenza del trattamento e, appoggiando il dito o la mano sul lettore, trasmetta il consenso. Tuttavia, come per tutti i sistemi biometrici, questa presunzione andrebbe ridimensionata in alcuni ambiti specifici, per esempio quando l'interessato è un lavoratore subordinato del responsabile del trattamento.

- Ulteriore finalità o ulteriori finalità di trattamento: ad oggi i dati relativi allo schema delle vene presentano rischi limitati riguardo all'utilizzo per ulteriori finalità. Il rischio può aumentare se il trattamento è generalizzato e se la falsificazione dell'identità è resa più agevole.

- Capacità di collegamento: i dati relativi allo schema delle vene non forniscono informazioni collegabili con altri dati, salvo con dati dello stesso tipo provenienti da un altro trattamento.

- Individuazione/profilazione: finché questo tipo di tecnica biometrica rimarrà poco usata, per esempio in una banca dati centrale per carte di pagamento, il rischio di individuazione/profilazione con dati relativi allo schema delle vene sarà limitato.

- Trattamento di dati sensibili: gli unici dati sensibili che potrebbero derivare dai dati sullo schema delle vene riguardano lo stato di salute, ma finora non è stata condotta alcuna valutazione formale sull'argomento.

- Revocabilità: i dati relativi allo schema delle vene sembrano essere molto stabili nel tempo, ma questa affermazione richiede una conferma empirica (i sistemi basati sullo schema delle vene sono troppo recenti per fornire risultati confermati). I suddetti dati vanno pertanto considerati irreversibili.

- Protezione antifalsificazione dell'identità: la falsificazione dell'identità dei dati relativi allo schema delle vene non è stata ancora diffusamente esplorata ma i risultati di una ricerca recente hanno indicato che è possibile falsificare un lettore di vene del palmo della mano[14]. La difficoltà principale per la falsificazione di questi dati consiste nella raccolta di un campione dei dati biometrici.

4.4.2. Impronte digitali e usi combinati

Il riconoscimento delle impronte digitali è uno dei sistemi biometrici più antichi e diffusamente studiati, nonché uno fra i più utilizzati su larga scala. Da oltre un secolo le forze di contrasto si servono dell'identificazione attraverso le impronte digitali sia per la verifica, sia per l'identificazione delle persone. Essa si basa sul fatto che le impronte digitali sono uniche per ciascuna persona e che esse contengono caratteristiche misurabili per poter decidere se un'impronta combacia con un campione già rilevato.

La registrazione delle impronte digitali richiede la presenza fisica della persona nonché, a seconda del caso previsto, di personale adeguatamente formato per garantire una buona qualità dei dati. Il rilevamento delle impronte digitali non è un compito da poco, nel senso che l'accuratezza del confronto dipende dalla qualità dell'immagine rispetto alla tecnica di quest'ultima. Le tecniche di acquisizione possono variare dalla pressione di una o due dita fino a tutte e dieci le dita, con modalità piana o rollata. A seconda del sistema impiegato, le impronte digitali possono essere usate soltanto per la verifica (1:1) o per l'identificazione e il confronto con tracce (1: n). Tuttavia, come risulta da alcuni studi, una parte della popolazione non è in grado di registrarsi per svariati motivi, ponendo un problema che richiede l'esistenza di adeguate procedure di ripiego, soprattutto per grossi sistemi, per evitare di privare i singoli di qualcosa cui hanno diritto.

Sebbene, in linea di principio, questo non sia un metodo troppo invasivo, in ogni caso può essere percepito come tale poiché si accompagna all'immagine negativa associata al trattamento di una persona come sospettata, ciò a causa dell'uso comune che se ne fa nell'ambito delle attività di contrasto.

Le impronte digitali indicano varie caratteristiche utilizzabili per finalità di verifica/identificazione anche se l'analisi dei minimi particolari è tuttora la tecnica più usata. Lo sviluppo di nuove tecniche (ossia gli scanner ad alta risoluzione) consentirà l'uso di altre caratteristiche. Lo sviluppo tecnologico ha altresì riguardato le capacità di identificazione consentendo l'uso di grosse banche dati per finalità di identificazione.

In proposito, i sistemi più avanzati sono i noti sistemi automatizzati d'identificazione dattiloscopica (AFIS) impiegati per finalità di contrasto e utilizzabili per lo scambio di dati attraverso la ricerca in vari archivi posti in siti transfrontalieri. Lo scambio di dati affronta problemi connessi a siti, a formati e a livelli di qualità differenti.

Esempi di AFIS in Europa sono l'Eurodac e il sistema di informazione visti che, secondo le previsioni, saranno fra le banche dati più grandi a livello mondiale, considerando che vi saranno conservate circa 70 milioni di impronte digitali. Nei suoi precedenti pareri il Gruppo di lavoro ha sollevato svariate questioni in merito all'utilizzo di banche dati su vasta scala, rilevando la necessità di garantire proporzionalità. Occorre soprattutto affrontare problemi di

[14] Cfr.: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf.

affidabilità in termini di risultati falsi positivi e falsi negativi, di efficace controllo dell'accesso a tali banche dati, come pure i problemi connessi all'uso di impronte digitali di minori e di anziani.

Nei sistemi biometrici basati sulle impronte digitali vengono normalmente usati dei modelli, solitamente considerati dai fornitori di sistemi come un modo per proteggere il singolo. Tuttavia, a seconda del sistema/algoritmo usato per creare il modello, esistono alcuni rischi potenziali connessi alla possibilità di collegare modelli con altre banche dati di impronte digitali per l'identificazione delle persone.

Riveste una certa importanza anche la questione dell'impiego di tecniche per eludere i sistemi di riconoscimento delle impronte digitali attraverso l'uso di dita artificiali o di impronte create da materiale artificiale, che consente pratiche legate al furto di identità. Esistono approcci diversi per ridurre la vulnerabilità di questi sistemi come la rilevazione dal vivo, i sistemi basati sul riconoscimento di più dita e anche l'uso di un appropriato controllo umano per i compiti di iscrizione e identificazione/verifica.

Le preoccupazioni per la protezione dei dati connesse all'uso delle impronte digitali possono essere così descritte in breve:

- Accuratezza: anche se, dopotutto, le impronte digitali presentano un'elevata percentuale di accuratezza, quest'ultima può essere messa in discussione dai limiti relativi a questioni riguardanti le informazioni – scarsa qualità dei dati o procedura di acquisizione incompatibile – o la dichiarazione – caratteristiche selezionate o qualità degli algoritmi di estrazione. Ciò può comportare falsi negativi o falsi positivi.

- Impatto: l'irreversibilità del processo può ridurre la capacità del singolo di esercitare i propri diritti o di riformare decisioni adottate sulla base di indicazioni false. Basarsi sull'accuratezza delle impronte digitali può rendere più difficile rettificare eventuali errori, comportando conseguenze di ampia portata per i singoli. Ciò dev'essere tenuto in considerazione in sede di valutazione della proporzionalità del trattamento in relazione alla decisione specifica da adottare sulle impronte digitali. Va altresì detto che la mancanza di misure di sicurezza può essere la causa del furto di identità, con un potenziale forte impatto sul singolo.

- Capacità di collegamento: le impronte digitali possono essere utilizzate in maniera illecita in quanto i dati ad esse relativi sono collegabili con altre banche dati. Questa possibilità di collegamento ad altre banche dati può condurre a usi non compatibili con le finalità originarie; per ridurne il rischio è possibile avvalersi di tecniche come i dati biometrici convertibili oppure la criptazione di questi ultimi.

- Trattamento di dati sensibili: secondo alcuni studi, le immagini delle impronte digitali possono rivelare informazioni sull'etnia dell'interessato[15].

- Ulteriore finalità o ulteriori finalità di trattamento: la conservazione centralizzata di dati, soprattutto in grosse banche dati, implica rischi connessi alla sicurezza dei dati, alla possibilità di collegamento e agli utilizzi deviati. In assenza di garanzie, ciò

[15] http://www.handresearch.com/news/fingerprints-world-map-whorls-loops-arches.htm and http://www.crime-scene-investigator.net/fingerprintpatterns.html

consente l'uso di impronte digitali per finalità diverse da quelle inizialmente poste alla base del trattamento.

- Consenso e trasparenza: il consenso è una questione essenziale per quanto riguarda l'uso delle impronte digitali per scopi diversi da quelli di contrasto. Le impronte digitali sono facilmente riproducibili da impronte latenti e perfino da fotografie, all'insaputa dell'interessato. Altre questioni che riguardano il consenso sono quelle legate all'ottenimento del consenso del minore e al ruolo svolto in proposito dai genitori (per esempio, la rilevazione di impronte digitali a scuola), nonché quelle connesse alla validità del consenso per fornire impronte digitali in ambito lavorativo.

- Revocabilità: i dati relativi alle impronte digitali sono molto stabili nel tempo e devono essere considerati irreversibili. A determinate condizioni è possibile revocare un modello di impronta digitale.

- Protezione anti-falsificazione dell'identità: le impronte digitali sono facilmente rilevabili grazie alle molteplici tracce di impronte che ciascun individuo lascia. Inoltre, con diversi sistemi e sensori è possibile utilizzare false impronte digitali, soprattutto quando in tali sistemi non figura una specifica protezione anti-falsificazione dell'identità. La riuscita di un'aggressione dipende in larga misura dal tipo di sensore (ottico, capacitivo, ecc.) e dal materiale usato dall'aggressore.

Esempio:
Un ospedale utilizza impronte digitali in una banca dati centrale per autenticare i pazienti in un servizio di radioterapia, onde accertarsi che ogni paziente riceva il trattamento corretto. Le impronte digitali sono preferibili al riconoscimento mediante lettura delle vene in quanto il trattamento altera il sistema vascolare. Inoltre, viene utilizzata una banca dati centrale perché le condizioni dei pazienti (età, patologia) comportano un rischio elevato di perdita dei badge, il che impedirebbe l'accesso al trattamento. In tal caso l'uso delle impronte digitali è una soluzione adeguata.

4.4.3. Riconoscimento del volto e usi combinati

Il volto, alla stregua delle impronte digitali, è usato da molto tempo e in maniera diffusa come fonte di dati biometrici. Ultimamente, dal volto non soltanto è possibile determinare l'identità ma anche caratteristiche fisiologiche e psicologiche come l'origine etnica, l'emozione e il benessere. La capacità di estrarre questo volume di dati da un'immagine e il fatto che sia possibile scattare una fotografia da una certa distanza all'insaputa dell'interessato dimostra il livello dei problemi in materia di protezione dei dati che queste tecnologie possono far sorgere.

Il riconoscimento del volto quale mezzo per l'identificazione e la verifica non è passato inosservato agli occhi delle autorità di contrasto, di altre autorità pubbliche e perfino di organizzazioni private. Da molti anni le fotografie compaiono su passaporti, patenti di guida, carte di identità e foto segnaletiche e non è insolita la presenza di una fotografia stampata su una tessera di controllo dell'accesso o su altra carta di identità aziendale. Tali immagini si ottengono di norma con un'illuminazione controllata e si limitano a una visione frontale o di profilo dell'interessato. L'uso di questa serie controllata di immagini è stata una logica base di partenza per il trattamento automatico e il riconoscimento delle persone. Tale capacità è stata nel frattempo superata e la tecnologia è arrivata al punto in cui è possibile giungere all'identificazione partendo da immagini tratte da una molteplicità di fotocamere, di punti di

vista e di condizioni di luce. Esiste inoltre una quantità enorme di immagini pubblicamente disponibili su internet, come quelle che vengono caricate nei social network e in altre gallerie altrettanto pubblicamente disponibili. I rischi non si limitano alle immagini tradizionali, in quanto il riconoscimento del volto è stato inserito con successo nei *video feed* in tempo reale. Il responsabile del trattamento deve riconoscere che l'aggiunta di nuove capacità di trattamento in un sistema già esistente (per esempio il riconoscimento del volto nelle TV a circuito chiuso) può modificare la finalità specifica del sistema originario ed è tenuto a rivalutare l'impatto di questa modifica sulla vita privata.

Segue una descrizione dei rischi per la protezione dei dati connessi all'uso dei sistemi di riconoscimento del volto:

- Accuratezza: se non è possibile garantire la qualità delle immagini, esiste il rischio di compromettere l'accuratezza. È evidente che, se il volto non viene svelato (perché è celato dai capelli o da un cappello, per esempio), il confronto o la categorizzazione avverrà con un elevato margine di errore. Le variazioni di posa e di illuminazione rimangono una sfida importante per il riconoscimento del volto, che influenzano in maniera significativa l'accuratezza.

- Impatto: l'impatto specifico sulla protezione dei dati di un particolare sistema di riconoscimento del volto dipenderà dalle sue finalità e dalle circostanze specifiche. Un sistema di categorizzazione pensato per contare i dati statistico-demografici dei visitatori di un luogo di attrazione privo di capacità di registrazione avrà un impatto diverso sulla protezione dei dati rispetto a quello di un sistema usato per nascondere la sorveglianza delle autorità di contrasto finalizzata a identificare potenziali agitatori.

- Consenso e trasparenza: un rischio per la protezione dei dati non insito in molti altri tipi di trattamento di dati biometrici consiste nel fatto che è possibile ottenere e sottoporre a trattamento immagini provenienti da una serie di punti di vista, di condizioni ambientali e all'insaputa dell'interessato. Nel parere 15/2011 sulla definizione del consenso, il Gruppo di lavoro specifica che, per poter essere considerato quale base giuridica per il trattamento, il consenso dev'essere "informato". Ciò non accade nel caso in cui l'interessato ignori che le immagini raccolte sono finalizzate al trattamento per il riconoscimento del volto. Sebbene l'interessato sia a conoscenza della presenza di una videocamera in funzione, potrebbero non esservi tracce visive per distinguere un sistema di TV a circuito chiuso *live* o per registrazioni da una lente che cattura immagini per il riconoscimento del volto.

- Ulteriore finalità o ulteriori finalità di trattamento: una volta ottenute, lecitamente o illecitamente, le immagini digitali possono essere facilmente condivise o riprodotte per divenire oggetto di trattamento in sistemi diversi da quelli cui erano state originariamente destinate. Questo fenomeno è evidente nell'ambito dei media sociali, in cui gli utenti caricano le fotografie personali da condividere con la famiglia, con gli amici e con i colleghi. Non appena presenti sulla piattaforma del medium sociale, le immagini sono a disposizione per essere riutilizzate dalla medesima piattaforma per svariate finalità, alcune delle quali possono essere inserite nella piattaforma talvolta anche dopo che l'immagine è stata ottenuta e/o caricata.

- Capacità di collegamento: un ampio numero di servizi online consente agli utenti di caricare un'immagine da collegare al profilo dell'utente. Il riconoscimento del volto

può essere utilizzato per collegare i profili di vari servizi online (attraverso l'immagine del profilo) ma anche tra la realtà online e il mondo reale esterno. Non è impossibile fotografare una persona per strada e determinarne in tempo reale l'identità attraverso una ricerca compiuta fra le immagini contenute nei profili pubblici. Esistono servizi offerti da terzi che sono anche in grado di setacciare le fotografie dei profili e altri contenuti pubblicamente disponibili per creare immense collezioni di immagini al fine di associarvi un'identità vera.

- Individuazione / profilazione: potrebbe essere possibile servirsi di un sistema di identificazione anche se non si conosce la vera identità di una persona. Un sistema per il riconoscimento del volto posto all'interno di un centro commerciale o di un'area pubblica analoga è potenzialmente utilizzabile per individuare percorsi e abitudini dei singoli clienti; la finalità potrebbe essere quella di gestire in modo efficace le code o il posizionamento dei prodotti, al fine di migliorare la permanenza della clientela nel centro. Tuttavia, la capacità di individuare o di localizzare una persona va di pari passo con la possibilità di tracciarne il profilo e di distribuire pubblicità mirata o altri servizi specifici.

- Trattamento dei dati sensibili: come si è detto, il trattamento dei dati biometrici potrebbe essere usato per determinare dati sensibili, in particolare quelli contenenti indizi visivi quali razza, gruppo etnico o magari una condizione clinica.

- Revocabilità: una persona può facilmente modificare l'immagine del proprio volto (barba, occhiali, cappello, ecc.) in maniera sufficiente da ingannare i sistemi di riconoscimento del volto, soprattutto se funzionano in un ambiente non controllato. Tuttavia, le principali caratteristiche del viso di una persona sono stabili nel tempo e i sistemi possono anche migliorare il riconoscimento, raccogliendo e associando più "volti" noti di una persona.

- Protezione anti-falsificazione dell'identità: molti sistemi di riconoscimento del volto sono facilmente falsificabili ma i produttori stanno cercando di migliorare la protezione anti-falsificazione con tecniche quali la scansione in 3D o la registrazione di video. Tuttavia, la maggior parte dei sistemi di base utilizzati in applicazioni pubbliche non contiene questo tipo di protezione.

Esempio:
Un esempio estremamente irreale è quello di un sistema di sorveglianza video di prossima generazione, pensato per centri commerciali, in grado di riconoscere le persone, individuare i movimenti in maniera automatica e distinguere caratteristiche del volto quali il sorriso o la rabbia. Esso potrebbe riconoscere i clienti abituali già all'ingresso del parcheggio riservato e guidarli verso i loro posti preferiti. Nel momento in cui i clienti entrano nel centro commerciale, il sistema potrebbe identificarne l'abbigliamento per suggerire i negozi da visitare in base alle offerte disponibili, ciò a fronte di dati raccolti sui precedenti acquisti o di una serie prevista di indicatori. Potrebbe inoltre essere organizzata una pubblicità su misura nelle vetrine o potrebbe essere posto un divieto di accesso automatico a negozi, ristoranti e altri luoghi. Potenziali ladri di automobili potrebbero essere identificati prima ancora che tocchino un'automobile. Se necessario, la presenza di velivoli telecomandati (droni) con videocamere e altri sensori potrebbe essere utile a conservare le tracce dei sospettati fino alla

smentita o alla conferma del sospetto. Potrebbe essere rilevata la presenza di oggetti nascosti negli indumenti (coltelli o articoli rubati nei negozi). Questa tecnologia non si basa unicamente sui nuovi sistemi biometrici ma combina ed elabora informazioni già disponibili con altri dati raccolti da una serie di sistemi diversi.

Un'applicazione analoga è stata ideata nel progetto INDECT (*Intelligent information system supporting observation, searching and detection for security of citizens in urban environment* — sistema intelligente di informazione a sostegno dell'osservazione, della ricerca e della rilevazione per la sicurezza dei cittadini in contesti urbani), nell'ambito del quale varie tecnologie sono combinate per prevenire potenziali azioni di terrorismo e criminalità. Il Gruppo di lavoro sottolinea con vigore che siffatto uso della biometria richiede un'adeguata base giuridica unitamente a considerazioni rigorose sulla necessità e la proporzionalità di tali misure.

4.4.4. Riconoscimento vocale e usi combinati

Un utilizzo relativamente comune del riconoscimento vocale, oltre a quello di dato biometrico per l'identificazione, comporta l'identificazione di elementi specifici dell'impronta vocale per classificare il parlatore. Un esempio è l'analisi delle risposte di una persona durante una conversazione telefonica per identificare la presenza di stress e di irregolarità nell'eloquio che evidenzino potenziali casi di frode.

Testimonianze rese note dai produttori riferiscono che, grazie all'impiego di questa tecnologia, le società di servizi finanziari hanno incrementato le percentuali di rilevamento di frodi e consentito un servizio più rapido per la risoluzione dei reclami autentici.

Se usati in un sistema di classificazione, i rischi per la protezione dei dati sono leggermente diversi rispetto a un sistema biometrico di identificazione, nel senso che non è richiesta una fase d'iscrizione e non è necessaria la conservazione del modello biometrico per lungo tempo. Tuttavia, in caso di conversazione telefonica registrata, come di norma accade con le istituzioni finanziarie, devono essere attuati controlli adeguati per garantire la sicurezza di questi dati.

- Accuratezza: uno dei rischi relativi alla protezione dei dati di questo sistema sta nelle percentuali di rilevazione, soprattutto nei falsi positivi e nei falsi negativi, ossia nel numero di persone erroneamente identificate come responsabili di comportamenti fraudolenti oppure nel numero di richieste basate sull'uso intenzionale di informazioni false, non identificate. Sebbene un sistema di classificazione possa essere in grado di tollerare percentuali più elevate di errori rispetto alla verifica o all'identificazione, devono essere ancora attuate procedure adeguate per gestire tempestivamente i casi che possono essere classificati in modo errato.

- Consenso e trasparenza: un approccio rispettoso della vita privata da applicare a queste tecnologie può essere quello di farsi carico di garantire che le chiamate siano controllate per verificarne l'idoneità e che gli interessati siano informati delle procedure avviate. In un caso di studio le persone sono state ritenute inadatte all'esperimento se non di madrelingua inglese o se portatori di disabilità uditive o intellettive oppure se prive di accesso a un telefono. I partecipanti erano liberi di rifiutarsi di rispondere alla chiamata e di fornire informazioni in maniera tradizionale ma anche, per gli interessati dissenzienti o disabili, di partecipare a tale sistema senza subirne uno svantaggio.

- Ulteriore finalità o ulteriori finalità di trattamento: nonostante la stragrande maggioranza delle ipotesi relative a questa tecnologia richieda modifiche strutturali specifiche per essere attuate, in quanto i settori pubblico e privato consolidano le loro infrastrutture IT in maniera da comprendervi tecnologie quali la *Voice over IP* (voce tramite protocollo internet), le tecnologie di riconoscimento vocale possono divenire più facilmente integrabili senza tener conto degli obblighi di protezione dei dati del responsabile del trattamento.

- Revocabilità: se è vero che una persona può volontariamente modificare la propria voce, le impronte vocali sono piuttosto stabili e possono essere validamente usate per identificare in maniera inconfondibile una persona, soprattutto se questa non è informata (e dunque non propensa a modificare la voce).

- Protezione anti-falsificazione dell'identità: le voci registrate sono utilizzabili per beffare i sistemi di riconoscimento vocale. Le tecniche anti-falsificazione dell'identità prevedono domande/risposte su argomenti contestuali (chiedere la data del giorno o ripetere parole di uso non comune).

4.4.5. DNA

I migliori dispositivi impiegati per il sequenziamento e il confronto del DNA e la disponibilità di attrezzature che ne consentano l'analisi a prezzi abbordabili rendono necessario riconsiderare alcune affermazioni contenute nel precedente documento di lavoro sulla biometria (WP80).

Uno dei principali cambiamenti intervenuti nel settore delle tecnologie sull'analisi del profilo del DNA è la riduzione del tempo necessario per le operazioni di sequenziamento e confronto. I continui progressi compiuti nel corso degli anni dagli studiosi e dall'industria delle biotecnologie hanno ridotto il tempo necessario per la creazione di un profilo di DNA dall'ordine di giorni all'ordine di ore e perfino di minuti.

Il lancio di un mercato di servizi online basati sull'analisi del DNA costituisce una minaccia per i diritti delle persone alla protezione dei dati, soprattutto quando il servizio richiede il trasferimento di campioni e di dati biometrici tra paesi diversi (compresi i paesi terzi), la presenza di più titolari del trattamento e la mancanza di adeguate garanzie per il trattamento di dati genetici o riguardanti la salute.

È altamente probabile che nel prossimo futuro sarà possibile eseguire analisi del profilo del DNA e confronti di campioni in tempo reale (o quasi) con dispositivi portatili, il che costituirà il punto di partenza per lo sviluppo di sistemi di autenticazione/identificazione biometrica dotati di maggiori livelli di accuratezza rispetto all'autenticazione attraverso le impronte digitali, il riconoscimento vocale oppure quello del volto.

I progressi nell'analisi del profilo del DNA sono inoltre dovuti al crescente interesse dei governi, dei giudici e delle autorità di contrasto riguardo alle biotecnologie da applicare nelle indagini penali. Grazie all'affidabilità del confronto del DNA e al fatto che è possibile raccogliere campioni di DNA all'insaputa dell'interessato, nel tempo svariati Stati membri hanno creato o avviato iniziative per creare banche dati centralizzate di profili di DNA di persone condannate e di campioni trovati nei luoghi in cui sono stati commessi reati.

Nel maggio 2005 sette Stati membri dell'UE hanno firmato l'accordo denominato "Trattato di Prüm" allo scopo di migliorare la collaborazione nelle indagini penali transnazionali e in tema

di giustizia attraverso lo scambio di informazioni. L'accordo definisce nuove basi di collaborazione fornendo ai firmatari determinati diritti di accesso alle banche dati nazionali di DNA unicamente nell'ambito della repressione (azione penale), come pure in quello dei dati su impronte digitali, dei dati anche personali e dei dati sulla registrazione di veicoli. A partire dalla data sopra indicata, altri Stati membri sono divenuti firmatari del trattato, i cui elementi essenziali sono racchiusi nella decisione del Consiglio 2008/615/GAI.

In forza del presente quadro giuridico, svariati Stati membri dell'UE possiedono o possiederanno a breve una banca dati nazionale funzionale contenente i profili del DNA delle persone condannate e le prove raccolte sui luoghi del reato, il che solleva preoccupazioni riguardo a tale specifico trattamento di dati.

Uno dei problemi principali connessi alla creazione di banche dati sul DNA consiste nel fatto che i dati genetici provenienti da campioni di DNA (loci) possono rivelare – non immediatamente durante la fase di rilevazione – informazioni correlate con lo stato di salute, la predisposizione a patologie o l'origine etnica. Per questo motivo la creazione di banche dati sul DNA pone un rischio importante per la dignità umana e i diritti fondamentali, rischio che è stato considerato nella risoluzione del Consiglio 2009/C 296/01. Sono previste disposizioni specifiche per limitare l'analisi del DNA a zone cromosomiche prive di espressione genetica attraverso una determinata serie di marcatori del DNA che notoriamente non fornisce informazioni su specifiche caratteristiche ereditarie (conosciuta anche come la "ESS" – Serie europea standard).

Tuttavia, la possibilità che uno dei marcatori estratti contenuto in una banca dati sul DNA nazionale possa in futuro rivelare caratteristiche ereditarie o altre informazioni sensibili richiede un'attenzione continua riguardo ai progressi nell'ambito della biologia con la conseguenza che, se ciò malauguratamente dovesse accadere, alcune informazioni della banca dati dovrebbero essere immediatamente cancellate. Inoltre, poiché tali banche dati sul DNA raccolgono profili di persone condannate, l'analisi statistica dei dati dev'essere rigidamente limitata per evitare la profilazione in base al sesso o alla razza.

Per quanto riguarda le banche dati sul DNA per finalità di polizia e di giustizia penale, la Corte europea dei diritti dell'uomo ha ritenuto che occorre distinguere fra il trattamento dei dati personali e i profili genetici dei sospettati e quelli delle persone condannate per aver commesso un reato[16].

Esiste inoltre un rischio potenziale che l'analisi del DNA possa essere usata per identificare familiari o parenti collegati a un delitto irrisolto oppure a persone condannate, essendo possibile cercare i profili di DNA nella banca dati con serie parziali di marcatori o caratteri jolly. Questa funzionalità solleva il problema delle implicazioni dei successivi controlli effettuati in base alle informazioni scaturite da una ricerca basata su caratteristiche familiari.

Va pure rilevata la presenza di rischi specifici connessi all'uso di serie di dati di genomi nell'ambito della ricerca. Il Gruppo di lavoro ritiene che l'accesso ai campioni e ai dati debba essere rigorosamente limitato alla ricerca e consentito esclusivamente per finalità di ricerca; inoltre, è necessario chiarire in base a quali circostanze i dati e i risultati delle ricerche saranno divulgati alle persone (tenendo altresì conto del diritto di non essere informati) o inseriti in documentazione di natura medica.

---

[16] Corte europea dei diritti dell'uomo, sentenza del 4.12.2008, *S. e Marper /Regno Unito* (ricorsi 30562/04 e 30566/04) in particolare, punto 125.

Segue una descrizione dei rischi per la protezione dei dati connessi con l'utilizzo del DNA quale dato biometrico:

- Accuratezza: sebbene il DNA presenti un elevatissimo grado di accuratezza, occorre prendere in considerazione il fatto che ciò dipenderà dal numero di marcatori (loci) analizzati. I sistemi di analisi devono garantire il massimo livello di accuratezza.

- Impatto: l'uso del DNA può essere ritenuto estremamente intrusivo per la persona. I dati genetici possono rivelare informazioni sensibili. L'analisi statistica dei dati è utilizzabile anche per la profilazione e può comportare effetti discriminatori per le persone interessate.

- Ulteriore finalità o ulteriori finalità di trattamento: le nuove tecnologie consentono al giorno d'oggi di aumentare la quantità di scambio di dati. Per questo motivo dev'essere chiaro chi è il soggetto che può accedere alle informazioni di una banca dati sul DNA. La ricerca familiare e la ricerca mirata al contesto razziale (*racial targeting*) possono essere ritenute una nuova tecnologia, che mette in discussione la finalità originaria del trattamento nelle banche dati sul DNA attualmente disponibili.

- Consenso e trasparenza: oggi vengono offerti servizi per eseguire analisi del DNA su campioni biologici (la saliva, per esempio) inviati mediante posta ordinaria e i cui risultati sono resi disponibili attraverso internet. Controlli insufficienti sull'identità potrebbero consentire a singoli o ad organizzazioni di sottoporre campioni di altre persone ottenendo dati personali riservati di terzi.

- Possibilità di collegamento: considerata la quantità e la varietà di informazioni ricavabili dal sequenziamento del DNA, quest'ultimo presenta un rischio elevato di un uso improprio in quanto i dati estratti sono facilmente collegabili con altre banche dati che consentono l'analisi del profilo della persona. Anche una ricerca basata sulla familiarità consente la creazione di collegamenti con parenti.

- Trattamento di dati sensibili: il DNA può rivelare informazioni associate allo stato di salute, alla predisposizione a patologie o all'origine razziale dell'interessato. È pertanto estremamente importante applicare il principio della minimizzazione dei dati al momento della scelta dei loci. Le informazioni sul DNA possono essere estratte da diversi campioni per un periodo di tempo più lungo: è dunque consigliabile garantire che l'accesso ai campioni sia strettamente riservato a utilizzatori autorizzati e soltanto per usi consentiti.

- Revocabilità: il DNA è irreversibile.

- Protezione anti-falsificazione dell'identità: il DNA è a priori assai difficile da falsificare. Tuttavia, in molti casi è facile raccogliere campioni del DNA (capelli, per esempio) all'insaputa del soggetto interessato.

4.4.6. Biometria della firma

La biometria della firma può essere considerata un esempio dei nuovi impieghi delle tecnologie biometriche tradizionali. Si tratta di tecniche biometriche basate sul comportamento che misurano la condotta di una persona secondo le dinamiche della firma manoscritta. Il tradizionale riconoscimento della firma si fonda sull'analisi di caratteristiche statiche o geometriche dell'immagine visiva della firma (come appare), la biometria della

firma, invece, si riferisce all'analisi delle caratteristiche dinamiche della firma (come è stata fatta) e ciò fa sì che queste tecniche siano spesso indicate come "firma dinamica".

Le tipiche caratteristiche dinamiche misurate da un sistema biometrico della firma (come una tavoletta grafica) sono la pressione, l'angolo di scrittura, la velocità e l'accelerazione della penna, la forma delle lettere, la direzione dei tratti della firma e altri tratti dinamici unici. Queste caratteristiche variano a seconda dell'utilizzo e dell'importanza fra un distributore e un altro e vengono di norma rilevate con dispositivi sensibili al contatto. Alcuni dispositivi di riconoscimento della firma sono in grado di eseguire la verifica combinando l'analisi delle caratteristiche statiche (immagine visiva) e di quelle dinamiche (pressione, angolazione, velocità, ecc.) di una firma.

Segue una descrizione dei rischi relativi alla protezione dei dati connessi all'uso della biometria della firma:

- Accuratezza: poiché le persone non firmano sempre allo stesso modo, possono sorgere problemi durante la procedura di iscrizione, come pure al momento della verifica dell'identità.

- Impatto: la biometrica basata sulle caratteristiche comportamentali come la firma può non essere unica nel tempo ed è modificabile dall'interessato. Una firma diversa dal solito può celare un motivo psicologico e il cambiamento può precludere una verifica positiva, comportando la necessità di un'altra procedura di verifica dell'identità degli interessati.

- Anti-falsificazione dell'identità: l'immagine grafica di una firma tradizionale è facilmente replicabile e falsificabile da un esperto, con una fotocopia oppure con un software di grafica, mentre una firma dinamica è più sicura in quanto la procedura di verifica controlla anche le caratteristiche dinamiche, che sono complesse e uniche rispetto alla calligrafia di una persona.

5. Orientamenti generali, raccomandazioni per il settore specifico e misure tecniche e organizzative.

Lo sviluppo di un sistema biometrico si basa sulla collaborazione delle varie parti coinvolte:

- produttori: progettano e testano sensori biometrici e definiscono i risultati delle tecnologie biometriche;
- integratori: progettano il prodotto finale che sarà venduto ai clienti: essi scelgono la tecnologia biometrica e definiscono parzialmente le finalità del sistema (scegliendo il pubblico a cui rivolgersi);
- rivenditori: vendono il prodotto finale al cliente; di norma informano il cliente sui risultati, sui rischi ed eventualmente sul relativo quadro giuridico;
- installatori: installano il prodotto presso i locali del cliente;
- clienti: scelgono di acquistare un sistema biometrico, definiscono la finalità e i mezzi del trattamento e, pertanto, sono responsabili del trattamento;
- interessati: forniscono dati biometrici usati dal sistema.

Alcune parti coinvolte svolgono anche più di un ruolo tra quelli sopra descritti, ciascuno dei quali deve garantire un utilizzo dei sistemi biometrici che sia rispettoso della vita privata. L'installatore, per esempio, non può attivare una caratteristica di sicurezza definita dall'integratore.

5.1. Principi generali.

Riguardo ai dati biometrici, la sicurezza dev'essere una delle preoccupazioni principali, considerata l'irreversibilità di tale tipo di dati. Pertanto, una violazione di questi dati pregiudica l'ulteriore uso sicuro della biometria come identificatore e il diritto alla protezione dei dati delle persone interessate, per le quali non è possibile ridurre gli effetti della violazione.

I rischi aumentano con il numero di applicazioni che impiegano questo tipo di dati (soprattutto il rischio di violazioni e di utilizzi deviati). Il maggior uso di dati biometrici ne accresce la probabilità di furto.

Il Gruppo di lavoro riconosce l'attuale tendenza a consentire l'accesso a distanza ai sistemi biometrici, per esempio interfacce consegnate via internet. Tale tendenza introduce una nuova serie di problemi relativi alla sicurezza, molti dei quali sono già noti al settore informatico. Sin dall'inizio, a partire dalla fase di progettazione, l'utilizzo di tale sistema deve richiedere il coinvolgimento di tecnici idonei addetti alla sicurezza provenienti dal settore informatico.

Il Gruppo di lavoro raccomanda un livello elevato di protezione tecnica per il trattamento dei dati biometrici attraverso l'uso delle ultime tecnologie. Al riguardo, il Gruppo di lavoro invita ad attenersi alle norme del settore per la protezione dei sistemi in cui vengono trattate le informazioni biometriche.

5.2. Tutela della vita privata fin dalla progettazione (*privacy by design*)

La tutela della vita privata fin dalla progettazione è il concetto secondo cui la vita privata dev'essere integrata in maniera proattiva nella tecnologia stessa.

Riguardo ai sistemi biometrici, la tutela della vita privata fin dalla progettazione concerne l'intera catena di valore dei sistemi biometrici:

- i produttori sono tenuti ad attuare i principi della tutela della vita privata fin dalla progettazione nel momento in cui progettano nuove tecnologie e sensori: in quest'obbligo può rientrare la cancellazione automatica dei dati grezzi dopo il calcolo del modello o la criptazione per la conservazione di dati biometrici (in una banca dati centrale o su una *smart card*). I produttori devono inoltre concentrarsi sullo sviluppo di tecnologie biometriche che siano rispettose della vita privata;
- gli integratori e i rivenditori devono anch'essi attuare i principi della tutela della vita privata fin dalla progettazione nel momento in cui definiscono il prodotto definitivo che sarà messo in vendita, scegliendo tecnologie rispettose della vita privata e aggiungendo misure di sicurezza al prodotto definitivo quali la decentralizzazione della banca dati;
- i clienti (i futuri responsabili del trattamento) sono tenuti ad applicare i principi della tutela della vita privata fin dalla progettazione ogni volta che chiedono un sistema biometrico specifico o ne definiscono le caratteristiche tecniche. In questo caso, i produttori e gli integratori devono offrire un determinato livello di flessibilità nei loro prodotti al fine di rispettare i principi di proporzionalità, limitazione delle finalità, minimizzazione dei dati e sicurezza.

Questi principi hanno già trovato attuazione in alcuni dispositivi biometrici; in uno specifico lettore biometrico alcuni produttori hanno infatti inserito parametri di criptazione e commutatori *anti-pulling* (anti-rimozione) e *anti-tamper* (anti-manomissione) per impedire l'accesso non autorizzato a dati biometrici.

Il Gruppo di lavoro raccomanda che i sistemi biometrici siano progettati secondo "cicli di vita dello sviluppo" formali, che contemplino le seguenti fasi:

1. specifica di requisiti basati su un'analisi dei rischi e/o una valutazione dell'impatto sulla vita privata (PIA, *Privacy Impact Assessment*);
2. descrizione e dimostrazione delle modalità secondo cui il progetto soddisfa i requisiti;
3. convalida con verifiche funzionali e di sicurezza;
4. verifica della conformità del progetto definitivo con il quadro normativo.

Il Gruppo di lavoro promuove la definizione di schemi di certificazione che potrebbero garantire l'attuazione della tutela della vita privata fin dalla progettazione e aumentare le informazioni dei responsabili del trattamento dei dati circa i rischi relativi alla protezione dei dati associati ai sistemi biometrici.

5.3. Quadro di valutazione dell'impatto sulla vita privata

5.3.1. Principi generali

La valutazione dell'impatto sulla vita privata è un processo in cui un'entità compie una valutazione dei rischi associati a un trattamento di dati personali, unitamente a una definizione di ulteriori misure pensate per attenuare tali rischi. Per esempio, con riferimento alla tecnologia RFID, il Gruppo di lavoro ha stabilito che l'entità che definisce l'applicazione è responsabile della realizzazione della suddetta valutazione e che tale entità può essere il responsabile del trattamento o il fornitore che progetta l'applicazione RFID.

A causa dei rischi specifici che accompagnano l'uso dei dati biometrici, il Gruppo di lavoro chiede che la persona (il produttore, l'integratore o il cliente finale) che definisce la finalità e i mezzi del dispositivo compia anche le valutazioni dell'impatto sulla vita privata quale parte integrante della fase di progettazione dei sistemi che trattano questo tipo di dati.

La PIA deve tener conto di quanto segue:

- natura delle informazioni raccolte;
- finalità delle informazioni raccolte;
- accuratezza del sistema, posto che da una corrispondenza/non corrispondenza di un campione biometrico potrebbero derivare decisioni importanti per una persona;
- base giuridica e conformità giuridica; necessità o meno del consenso;
- accesso al dispositivo e condivisione interna ed esterna di informazioni presso il responsabile del trattamento, il che comporterà tecniche e procedure di sicurezza per proteggere l'accesso non autorizzato ai dati;
- misure in assoluto meno pregiudizievoli della vita privata già adottate; eventuale esistenza di una procedura alternativa al dispositivo biometrico (come la richiesta della carta di identità);
- decisioni prese in merito al periodo di conservazione e alla cancellazione di dati; quale sia il periodo di tempo pertinente; se i dati siano stati tutti raccolti per lo stesso periodo di tempo e se esistono un meccanismo di decisione automatico e un processo di ripiego appropriato;
- diritti dell'interessato.

Le valutazioni dell'impatto sulla vita privata non devono focalizzarsi unicamente sull'identificazione dei rischi, dovendo altresì fornire adeguate misure di protezione dei dati e

indicare il modo in cui il responsabile del trattamento è riuscito a trovare soluzioni idonee per attenuare i rischi relativi alla protezione dei dati individuati nella sezione precedente.

Qualora la PIA sia stata condotta dal produttore o dall'integratore, lo sviluppo del sistema biometrico potrebbe anche richiedere un'ulteriore valutazione, per tenere conto delle peculiarità del responsabile del trattamento. Nel caso in cui un sistema biometrico sia inserito nel sistema di informazioni del cliente, per esempio, quest'ultimo deve effettuare un'altra PIA che consideri le proprie misure e procedure di sicurezza informatiche.

5.3.2. La specificità dei dati biometrici

I dati biometrici richiedono un'attenzione specifica in quanto identificano una persona in modo inequivocabile mediante le caratteristiche comportamentali o psicologiche che le sono tipiche.

Per questo motivo, lo scopo delle valutazioni dell'impatto sulla vita privata dev'essere la valutazione del modo in cui è possibile evitare o limitare sostanzialmente i seguenti tre rischi attraverso il sistema oggetto dell'analisi.

Il primo rischio è l'usurpazione di identità, soprattutto in caso di identificazione e di autenticazione. Il dispositivo biometrico non dev'essere ingannato da un attacco di falsificazione (*spoofing*) e deve garantire che la persona che sta tentando di eseguire il confronto sia realmente quella registrata nel sistema. Tale minaccia sembra meno significativa per i dati biometrici che non possono essere rilevati all'insaputa dell'interessato, come lo schema delle vene[17], ma rappresenta, invece, uno dei problemi principali per i dispositivi di riconoscimento del volto o delle impronte digitali. Queste ultime sono lasciate ovunque semplicemente toccando un oggetto e l'immagine del volto può anche essere ottenuta con una fotografia senza che il soggetto se ne accorga.

Il secondo rischio è lo sviamento delle finalità sia da parte del responsabile del trattamento, sia da parte di terzi, autorità di contrasto comprese. Questo pericolo comune per i dati personali diventa importante con l'uso dei dati biometrici. I produttori devono adottare tutte le misure di sicurezza per evitare ogni uso improprio dei dati e accertarsi che i dati non più necessari ai fini del trattamento vengano cancellati immediatamente.

Analogamente a qualsiasi altro dato, i dati biometrici legittimamente trattati o conservati, come pure le fonti di dati biometrici, non possono essere trattati o iscritti dal responsabile del trattamento per finalità nuove o diverse, salvo trattarsi di un nuovo motivo legittimo per l'altrettanto nuovo trattamento di questi dati.

Il terzo rischio è la violazione dei dati che, nell'ambito dei dati biometrici, richiede azioni specifiche in base al tipo di dati compromessi. Nel caso in cui si utilizzi un sistema che crea dati biometrici su base di un algoritmo che converte un campione biometrico in un determinato codice e il dato biometrico o l'algoritmo venga rubato o compromesso, questi devono essere sostituiti. Quando la violazione comporta la perdita di dati biometrici direttamente identificati e molto prossimi alla fonte di dati biometrici, quali immagini di volti o impronte digitali, la persona interessata dev'esserne informata con precisione affinché possa difendersi in un possibile e futuro caso in cui i dati biometrici compromessi potrebbero essere usati come prova contro di essa.

[17] Sebbene sia difficile prevedere quali potrebbero essere, nei prossimi anni, le aggressioni alla tecnologia che riguarda lo schema delle vene se il loro utilizzo sarà più diffuso.

5.4. Misure tecniche e organizzative

Proprio in virtù della loro natura, il trattamento dei dati biometrici richiede misure tecniche e organizzative specifiche, nonché precauzioni atte ad evitare gli effetti negativi per l'interessato in caso di violazione dei dati – soprattutto a causa dei rischi del comportamento illecito all'origine della "ricostruzione" non autorizzata di una caratteristica biometrica da un modello biometrico, il relativo collegamento con banche dati diverse e l'ulteriore "uso" all'insaputa degli interessati, per finalità non compatibili con quelle originarie e/o la possibilità che alcuni dati biometrici possano essere usati per rivelare informazioni sulla razza o sulla salute delle persone.

5.4.1. Misure tecniche

- *Uso di modelli biometrici*

Quando è possibile, i dati biometrici devono essere conservati come modelli biometrici.

Il modello va estratto con modalità tipiche per quel determinato sistema biometrico e non usate da altri responsabili del trattamento di sistemi analoghi, al fine di garantire che una persona sia identificabile soltanto in quei sistemi biometrici che possiedono una base giuridica per questa operazione.

- *Conservazione su dispositivo personale rispetto a conservazione su dispositivo centralizzato*

È preferibile evitare la conservazione centralizzata delle informazioni biometriche personali ogni qual volta è consentito sottoporre a trattamento i dati biometrici.

Soprattutto ai fini della verifica, il Gruppo di lavoro ritiene opportuno che i sistemi biometrici si basino sulla lettura di dati biometrici conservati come modelli criptati su media esclusivamente in possesso dei relativi interessati (per esempio: *smart card* o dispositivi simili). Le loro caratteristiche biometriche sono confrontabili con il modello o i modelli conservati sulla *card* e/o sul dispositivo mediante procedure di confronto standard direttamente attuate sulla *card* e/o sul dispositivo in questione, mediante le quali – in generale e se possibile – la creazione di una banca dati contenente informazioni biometriche dev'essere evitata. Effettivamente, in caso di perdita o di smarrimento della carta e/o del dispositivo, esistono attualmente rischi limitati di uso improprio delle informazioni biometriche in essi contenute. Per diminuire il rischio di furto di identità, in tali dispositivi occorre memorizzare pochi dati identificativi relativi all'interessato.

Tuttavia, per scopi specifici e in presenza di necessità oggettive, si possono ritenere ammissibili le banche dati centralizzate che contengono informazioni biometriche e/o modelli. Il sistema biometrico usato e le misure di sicurezza prescelte devono limitare i rischi summenzionati e garantire che il riutilizzo dei dati biometrici in questione per ulteriori finalità sia impossibile o almeno rintracciabile. Per evitare la lettura, la riproduzione, la modifica o la cancellazione di dati biometrici vanno usati meccanismi basati su tecnologie crittografiche.

In caso di conservazione di dati biometrici su un dispositivo fisicamente controllato dall'interessato, occorre usare una specifica chiave di criptazione per i dispositivi di lettura, come pure un'efficace garanzia per proteggere questi dati dall'accesso non autorizzato. Inoltre, questi sistemi decentralizzati offrono una protezione migliore dei dati biometrici fin dalla progettazione, in quanto l'interessato continua a controllare fisicamente i propri dati biometrici e nessun elemento può essere oggetto di interesse, né utilizzato.

Il Gruppo di lavoro sottolinea inoltre che l'idea della banca dati centralizzata racchiude un'ampia gamma di attuazioni tecniche dalla conservazione nel lettore a una banca dati ospitata all'interno di una rete.

- *Rinnovabilità e revocabilità*

Posto che la fonte dei dati biometrici non può essere modificata, i sistemi biometrici destinati a stabilire un legame di identità devono essere ideati in modo che il processo di registrazione e il trattamento di dati biometrici consentano l'estrazione di più modelli biometrici indipendenti dalla medesima fonte, per poterli sostituire in caso di violazione di dati o di evoluzione tecnologica.

I sistemi biometrici vanno progettati in maniera da consentire la revoca del collegamento di identità, per rinnovarlo oppure per cancellarlo definitivamente, per esempio in caso di revoca del consenso[18].

- *Forma criptata*

Per quanto riguarda il problema della sicurezza, occorre adottare misure adeguate per proteggere i dati conservati e trattati dal sistema biometrico: le informazioni biometriche devono sempre essere conservate in forma criptata. Occorre definire un quadro di gestione della chiave per garantire che le chiavi di criptazione siano accessibili unicamente in casi di effettiva necessità.

Considerato l'uso ampiamente diffuso di banche dati pubbliche e private contenenti informazioni biometriche, così come l'aumentata interoperabilità di diversi sistemi che impiegano la biometria, va privilegiato l'utilizzo di tecnologie specifiche o di formati di dati che rendano impossibili le connessioni di banche di dati biometrici e le divulgazioni non controllate di dati.

- *Anti-falsificazione dell'identità*

Il produttore deve attuare sistemi che determinino se i dati biometrici sono genuini e sempre relativi a una persona fisica, per conservare l'affidabilità di un sistema biometrico ed evitare il furto d'identità. Riguardo al riconoscimento del volto, potrebbe essere importante garantire che il volto sia autentico e non, per esempio, un'immagine incollata sul vero volto di un impostore.

- *Criptazione e decriptazione dei dati biometrici*

La criptazione dei dati biometrici è una tecnica che inserisce caratteristiche biometriche nell'algoritmo di criptazione e di decriptazione. In questo caso si usa di norma una parte di un dato biometrico come chiave per criptare un identificatore necessario per il servizio.

Questo sistema presenta numerosi vantaggi[19] e con esso non esiste alcuna conservazione dell'elemento identificatore o dei dati biometrici in quanto viene conservato unicamente il

---

[18] Per esempio, la tecnologia TURBINE, pensata per proteggere il modello biometrico mediante trasformazione crittografica delle informazioni relative alle impronte digitali in una chiave non invertibile che consente il raffronto mediante confronto diretto. I dati biometrici trasformati si considerano irreversibili rispetto ai campioni biometrici e ai modelli originali. Inoltre, per promuovere la fiducia dell'utente, questa chiave sarà anche reversibile, ossia sarà possibile creare una nuova chiave indipendente per emettere nuovamente identità biometriche. Cfr. anche: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf

[19] http://www.ipc.on.ca/images/resources/bio-encryp.pdf.

risultato dell'identificatore criptato con i dati biometrici. Inoltre, i dati personali sono revocabili perché è possibile creare un altro elemento identificatore che può essere anch'esso protetto con la criptazione di dati biometrici. Infine, risolvendo il problema di ricordare password lunghe e complesse, questo sistema è più sicuro e facile da usare.

Tuttavia, non è facile risolvere il problema crittografico che si pone in quanto criptazione e decriptazione non tollerano alcuna modifica della chiave, mentre i dati biometrici offrono un modello diverso che può dar luogo a modifiche nella chiave estratta. Il sistema deve pertanto essere in grado di calcolare la medesima chiave da dati biometrici leggermente diversi senza per questo aumentare i falsi positivi.

Il Gruppo di lavoro concorda sul fatto che la tecnologia di criptazione di dati biometrici offra vantaggiose possibilità alla ricerca e sia divenuta sufficientemente matura per essere maggiormente considerata a livello di ordine pubblico, di sviluppo di prototipi e di esame delle applicazioni.

- *Meccanismi di cancellazione automatizzata dei dati*

Per evitare che le informazioni biometriche siano conservate più a lungo di quanto necessario al conseguimento delle finalità per le quali esse sono state rilevate o successivamente trattate, occorre attuare idonei meccanismi di cancellazione automatizzata dei dati anche in caso di periodo di conservazione lecitamente prorogato, garantendo la tempestiva cancellazione di dati personali divenuti inutili per il funzionamento del sistema biometrico.

Se decidono di usare la memoria integrata sul lettore, i produttori possono anche attuare la conservazione dei modelli biometrici su memoria volatile, che garantisce la cancellazione dei dati una volta rimosso il lettore; in tal modo non rimane quindi alcun dato biometrico se il lettore viene venduto o disinstallato. È inoltre possibile usare commutatori *anti-pulling* per la cancellazione automatica dei dati in caso di tentativo di furto del lettore.

- *Grosse banche dati contenenti dati biometrici e banche dati "weak link" (anello debole)*

Alcuni paesi si servono di grosse banche dati contenenti dati biometrici principalmente per due scopi: facilitare le indagini penali e garantire il rilascio di documenti di identità (passaporti, carte di identità e patenti di guida). Di norma, le banche dati usate per le indagini penali raccolgono informazioni sui criminali e sui sospettati e devono essere progettate per identificare una persona attraverso i dati biometrici. Al contrario, le banche dati usate per contrastare l'usurpazione di identità comprendono dati biometrici di tutta la popolazione e devono essere usate soltanto per autenticare una persona (per esempio se questa ha perso i suoi documenti o ha distrutto il chip elettronico del passaporto in cui sono conservati i dati biometrici).

Il Gruppo di lavoro ritiene che si debbano attuare misure tecniche per evitare ogni sviamento della finalità in caso di utilizzo di una banca dati centrale per finalità di contrasto contro l'usurpazione di identità. Innanzitutto, il principio di minimizzazione dei dati richiede che si debbano raccogliere soltanto i dati necessari all'autenticazione della persona. Si ritiene, per esempio, che il confronto delle impronte digitali di due dita sia abbastanza preciso per autenticare una persona.

Inoltre, i responsabili del trattamento dei dati possono usare banche dati "*weak link*" in cui l'identità di una persona non è collegata a un'unica serie di dati biometrici, bensì a un gruppo di serie di dati biometrici. Il modo in cui la banca dati è concepita deve garantire l'autenticazione della persona con un'elevata probabilità di corrispondenza (per esempio

il 99,9%, che è sufficiente a dissuadere gli autori di frodi) e garantire che essa non possa essere usata per l'identificazione (in quanto una serie di dati biometrici corrisponde a una notevole quantità di persone).

Il Gruppo di lavoro incoraggia l'utilizzo di questi sistemi laddove sono in uso grosse banche dati contenenti dati biometrici per finalità di contrasto all'usurpazione di identità.

Esempio: misure tecniche per sistemi di autenticazione.
La fonte di dati biometrici è unica e potenzialmente collegata con l'interessato per tutta la vita. Occorre tenere a mente che, nel caso in cui questa fonte venga usata come base per sistemi di autenticazione, essa non potrà essere modificata, laddove nelle tecnologie di autenticazione comuni, che solitamente richiedono "la conoscenza o il possesso" di credenziali (per esempio *user ID* e *password*), queste ultime possono sempre essere modificate. Pertanto, i sistemi che impiegano l'autenticazione biometrica devono attuare garanzie specifiche per proteggere il collegamento fra il dato biometrico e altri dati relativi all'identità:
- i dati del modello non devono essere conservati a livello centrale in quanto la sicurezza dei dati biometrici è essenziale per la sicurezza complessiva del sistema biometrico. Occorre privilegiare una conservazione distribuita (per esempio su una *smart card*). In tal caso, la fonte dei dati e il modello sono trasmessi dall'interessato.
- la conservazione e la trasmissione di dati biometrici vanno protette contro l'intercettazione, la divulgazione non autorizzata e la modifica attraverso l'uso di appropriate tecnologie crittografiche.
- Alcuni tipi di dati biometrici non sono segreti (il volto, per esempio) e non possono essere resi inaccessibili, bloccati o modificati dopo la violazione di dati o in casi di uso improprio. Pertanto, l'autenticazione dev'essere combinata con altre credenziali inaccessibili o modificabili.

5.4.2. Misure organizzative

È necessario pianificare e approntare misure organizzative per garantire la protezione dei dati. Il responsabile del trattamento, per esempio, deve stabilire una procedura chiara riguardo al soggetto che può accedere alle informazioni sul sistema, se l'accesso è parziale, e ai motivi dell'accesso. Tutte le azioni devono essere rintracciate.

Il Gruppo di lavoro ritiene che sia possibile ricorrere all'*outsourcing* a fornitori esterni di servizi, anche per le richieste di visto (articolo 13 e articolo 43 del regolamento (CE) n. 810/2009 del 13 luglio 2009 che istituisce un codice comunitario dei visti), fenomeno sempre più comune a causa del crescente utilizzo del *cloud storage* (archiviazione remota).

In tal caso, il responsabile del trattamento deve stabilire una politica dettagliata sulle modalità di controllo dei propri fornitori, come ispezioni improvvise, e imporre garanzie per i lavoratori subordinati, nonché procedure in materia di diritti dei singoli, ecc.

Fatto a Bruxelles, il 27 aprile 2012

Per il Gruppo di lavoro
Il presidente
Jacob KOHNSTAMM