Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Incaricato federale della protezione dei dati e della trasparenza
IFPDT

Guida ai sistemi di riconoscimento biometrico

Versione 1.0
Settembre 2009

Il presente documento, destinato a chi sviluppa e utilizza i sistemi di riconoscimento biometrico, è stato redatto allo scopo di illustrare le sfide e le modalità di valutazione dei sistemi di riconoscimento biometrico nell'ottica della protezione dei dati personali tenendo conto delle disposizioni della legge federale sulla protezione dei dati, sia per i sistemi già sul mercato, sia per quelli futuri.

Il testo è suddiviso in tre parti: L'introduzione è dedicata in particolare alla **terminologia e alle definizioni** al fine di permettere di comprendere meglio un tema così complesso come la biometria. La seconda parte elenca i **criteri fondamentali** applicabili all'allestimento e all'impiego di un sistema di riconoscimento biometrico. Infine, la terza parte costituisce una **guida alla valutazione**: Si tratta di consigli pratici, suddivisi in quattro serie di argomenti che forniscono gli elementi chiave che consentono di mettere in luce le esigenze da rispettare nell'ambito della protezione dei dati. Fornendo una risposta a tutte queste domande per il vostro caso particolare, sarete dunque in grado di valutare il sistema di riconoscimento a disposizione o futuro tenendo conto degli elementi di protezione dei dati.

Feldeggweg 1, 3003 Berna
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

Indice

1. Introduzione

1.1 Preambolo

Utilizzati sempre più in ambito sia privato che pubblico, i sistemi di riconoscimento biometrico comportano numerosi vantaggi per le persone che li introducono, sia per le persone interessate. Tuttavia, l'uso di dati biometrici per l'identificazione o la verifica dell'identità dichiarata comporta anche rischi per il rispetto dei diritti individuali e delle libertà fondamentali.

Questi sistemi di riconoscimento si basano sull'analisi delle caratteristiche fisiologiche o comportamentali del corpo umano. L'uso di dati biometrici per il riconoscimento comporta alcuni rischi per le persone: in particolare il mancato rispetto del diritto all'autodeterminazione informativa, l'usurpazione dell'identità, la creazione di un identificatore unico globale, l'impiego di informazioni complementari sulla persona interessata (ad esempio, sulle sue malattie) contenute nei dati biometrici. Questa problematica è ancor più importante nell'ottica dei rischi connessi ai possibili usi futuri delle caratteristiche biometriche come identificatore unico globale, cioè per combinare dati che provengono da fonti diverse al fine di realizzare un profilo della personalità all'insaputa della persona interessata.

Le caratteristiche biometriche in genere sono permanenti (ogni individuo le mantiene per tutta la vita), uniche (proprie ad ogni individuo) e universali (propri a tutti gli individui). Tuttavia queste caratteristiche non sono assolute perché sottoposte a volte ad alterazione naturale, accidentale o volontaria nel tempo, l'esistenza di gemelli biometrici o la possibilità di insuccesso nella registrazione.

Lo scopo del presente documento è far luce su sfide e modalità di valutazione dei sistemi di riconoscimento biometrico nell'ambito della protezione dei dati.

L'architettura dei sistemi ha un impatto notevole sui rischi e sull'intensità di lesione della personalità, dell'integrità fisica o della dignità umana. Per limitare gli eventuali rischi di lesione, è necessario osservare i principi della protezione dei dati, in particolare i principi di liceità, trasparenza (buona fede, riconoscibilità o obbligo di informare), finalità, proporzionalità e sicurezza dei dati. Conformemente al principio della proporzionalità, i dati personali devono essere trattati con mezzi adeguati, necessari e non eccessivi rispetto alle finalità del trattamento. Perciò si dovrebbe far ricorso a sistemi di riconoscimento biometrico solo se non esistono altri mezzi meno intrusivi per raggiungere lo scopo prefisso. Se le circostanze giustificano l'introduzione di un sistema di riconoscimento biometrico, è necessario definire l'architettura del sistema (in particolare il processo di riconoscimento, le modalità di memorizzazione dei dati, le caratteristiche e i dati biometrici), in maniera da limitare al massimo il rischio di ledere le persone interessate. Inoltre, devono essere prese le misure tecniche e organizzative appropriate per garantire l'affidabilità dei sistemi e la sicurezza dei dati, in particolare al momento di memorizzarli e di trasmetterli. Inoltre le persone interessate devono essere debitamente informate sui loro diritti.

Il presente documento è suddiviso in tre parti. La prima riporta precisazioni terminologiche e illustra le principali tecnologie biometriche. La seconda comprende un elenco di principi fondamentali specifici ai sistemi di riconoscimento biometrico. Infine, la terza parte, consiste in una guida alla valutazione valida tanto per i sistemi già a disposizione quanto per quelli futuri. Nella misura in cui le scelte fatte divergono dalle raccomandazioni del presente documento, è necessario esporre i motivi del ricorso ad una soluzione più intrusiva.

Per concludere, il presente documento tiene conto dell'attuale livello raggiunto dalla tecnologia. Se necessario, l'IFPDT introdurrà adeguamenti tenendo conto dello sviluppo tecnologico e delle esperienze raccolte.

1.2 Terminologia e definizioni

1.2.1 Terminologia

La nozione di biometria e di processi di funzionamento dei sistemi di riconoscimento biometrico sono complessi.

Etimologicamente, il termine «biometria»[1] (*Biometrik – biometry*) si riferisce all'analisi delle caratteristiche fisiche (voce, tratti del viso, impronte digitali, …) di un individuo.

Da qualche tempo, il termine biometria viene utilizzato anche in senso più ristretto per riferirsi ai *sistemi di riconoscimento biometrico* (*Biometrie – biometrics*). Non esiste una definizione unanime o generalmente riconosciuta per la nozione di *sistema di riconoscimento biometrico automatizzato* (*Biometrie – biometrics*).

L'adozione di una terminologia e di definizioni uniformi è essenziale per la comprensione del funzionamento, dei vantaggi dei sistemi di riconoscimento biometrico e delle sfide che vi sono connesse.

Svariati progetti sono stati avviati, in particolare da parte dell'ISO, ma non sono riusciti a risolvere le divergenze e fino ad oggi non è stato possibile arrivare ad un consenso sull'armonizzazione della terminologia e delle definizioni nel settore dei sistemi di riconoscimento biometrico.

La seguente sezione riporta un elenco ragionato delle definizioni scelte dall'Incaricato federale per la protezione dei dati e della trasparenza (IFPDT).

1.2.2 Definizioni[2]

Caratteristiche biometriche: caratteristiche fisiologiche[3] o comportamentali[4] misurabili di un individuo.

Sistema di riconoscimento biometrico: sistema che permette di procedere al riconoscimento automatizzato o umano (verifica o identificazione) di una persona in base alle caratteristiche biometriche.

Dato biometrico grezzo: rappresentazione fisica o numerica di una caratteristica biometrica, recepibile da un sistema di riconoscimento biometrico.

Dato biometrico elaborato o modello biometrico (biometric template)**:** rappresentazione numerica di un dato biometrico grezzo, recepibile da un sistema automatico di riconoscimento biometrico.

Dati biometrici: dati biometrici grezzi o elaborati.

---

1 Derivato da bio- (dal greco bios - «vita») e -metria (dal greco metron - «misura»).

2 La versione tedesca e inglese sono allegate al presente documento.

3 In particolare le impronte digitali, la conformazione dell'iride o l'immagine del viso, la sagoma della mano o la vascolarizzazione.

4 In particolare la firma, la voce o l'andatura.

Registrazione biometrica: processo iniziale di raccolta di un dato biometrico individuale e di memorizzazione come dato biometrico di riferimento.

Insuccesso nella registrazione (failure to enrol «*FT*»)**:** la proporzione di utenti per i quali il sistema di riconoscimento biometrico non è in grado di acquisire un dato biometrico di riferimento di qualità sufficiente.

Verifica biometrica: processo di confronto (1:1) di un dato biometrico di controllo con un dato biometrico di riferimento allo scopo di verificare se la persona in questione è effettivamente chi dice di essere.

Identificazione biometrica: processo di confronto (1:n) di un dato biometrico di controllo con una serie di dati biometrici di riferimento registrati nel database allo scopo di determinare chi sia la persona in questione.

Insuccesso nell'acquisizione (failure to acquire «FTA»)**:** la proporzione di tentativi in cui la qualità dell'immagine acquisita dal sistema di riconoscimento biometrico non è sufficiente.

Soglia di decisione (threshold)**:** il valore minimo necessario ad un confronto biometrico per poter essere considerato riuscito. Quando questo valore viene stabilito in modo da parificare la proporzione tra i tassi di falsa accettazione e quelli di falso rifiuto, la soglia viene chiamata «valore di errore uguale" (equal error rate «EER»).

Tasso di false accettazioni (false acceptance rate «FAR»)**:** la probabilità di errore di un sistema di riconoscimento biometrico nell'identificare un individuo o nell'autenticare un impostore.

Tasso di falsi rifiuti (false rejection rate «FRR»)**:** la probabilità di fallimento di un sistema di riconoscimento biometrico nell'identificare o nel verificare la persona registrata [per maggiori informazioni sui tassi di errore, in particolare «FMR» e «FMNR», vedi anche FIDIS D 3.10: Biometrics in identity management[5]].

Modello biometrico su carta (template on card): supporto di memoria sul quale si possono registrare i modelli biometrici di riferimento.

Confronto biometrico su carta (match on card)**:** una smartcard con microprocessore sulla quale si possono registrare i modelli biometrici di riferimento e confrontarli a modelli biometrici di controllo.

Sistema biometrico su carta (system on card / encapsulated biometrics)**:** una smartcard con microprocessore dotata di un lettore biometrico (allo stato attuale della tecnica disponibile solo per le impronte digitali), sulla quale è possibile acquisire, registrare e confrontare dati biometrici.

1.3 Le principali tecnologie biometriche

Il riconoscimento biometrico è un settore della ricerca in costante evoluzione. Le varie tecnologie utilizzate per identificare una persona o verificarne l'identità si basano sull'analisi delle **caratteristiche fisiologiche** (*something you are; passive biometrics*) o delle **caratteristiche comportamentali** (*something you do; active biometrics*).

Caratteristiche fisiologiche	**Caratteristiche comportamentali**

[5] http://www.fidis.net/resources/deliverables/hightechid/#c2057

- sagoma del viso	- autografo
- impronte digitali	- timbro vocale
- sagoma della mano	- andatura
- scansione dell'iride	- dinamica di battitura sulla tastiera (keystroke)
- vascolarizzazione della mano o del dito	- …
- …	

Le caratteristiche biometriche dovrebbero essere

- uniche (*distinctiveness*), diverse da una persona all'altra;
- universali (*universality*), tutti devono averle;
- permanenti (*permanence*), invariabili nel tempo – per ogni persona;
- collezionabili (*collectability*), devono poter essere acquisite.

Nel caso ideale, una caratteristica biometrica dovrebbe essere anche

- performante (*performance*), cioè stabile, esatta, adatta allo scopo e analizzabile in modo rapido;
- accettabile (*acceptance*), cioè che vengono raccolte senza forte opposizione;
- affidabile (*reliability*), cioè il cui rilascio è difficile da contraffare o da eludere.

2. Principi fondamentali per l'uso di sistemi di riconoscimento biometrico

Il presente capitolo elenca i principi fondamentali di cui tener conto nell'ideazione e nell'impiego dei sistemi di riconoscimento biometrico.

- I dati personali possono essere trattati solo in modo lecito (art. 4 cpv. 1 LPD) e trasparente (art. 4 cpv. 2 & 4 LPD).

- Le finalità del trattamento (art. 4 cpv. 3 LPD) devono essere rigorosamente rispettate. Dunque, i dati raccolti al fine di permettere un riconoscimento biometrico non devono essere trattati in maniera incompatibile con le finalità iniziali, eccezion fatta per ragioni legali (in particolare a scopo di proseguimento penale).

- Devono essere previste **alternative** per persone che non sono in grado di utilizzare un sistema di riconoscimento biometrico in modo da evitare qualsiasi discriminazione immotivata. Queste alternative devono inoltre essere proposte a chiunque non desideri che i propri dati biometrici vengano utilizzati per il riconoscimento, a patto di rispettare le finalità iniziali.

- L'**architettura dei sistemi di riconoscimento biometrico** influenza molto i rischi e l'intensità delle lesioni della personalità, dell'integrità fisica o della dignità umana. Le esigenze della protezione dei dati personali devono essere rispettate e integrate sin dalla fase di ideazione e durante la manutenzione dei sistemi.

- Si raccomanda di non sfruttare le **informazioni personali complementari** (in particolare su malattie, sull'origine) contenute nei dati biometrici.

- Il principio della **proporzionalità** (art. 4 cpv. 2 LPD) deve essere rigorosamente rispettato. In particolare, si farà ricorso alla biometria solo se **non esistono mezzi meno intrusivi** per raggiungere lo scopo desiderato o se la biometria costituisce uno degli elementi di protezione o di sicurezza dei dati. Conviene dunque adottare mezzi **adeguati, appropriati e non eccessivi** rispetto alle finalità del trattamento, al momento di scegliere **i sistemi di riconoscimento** (mezzi tradizionali e/o riconoscimento biometrico), **il procedimento di riconoscimento** (verifica o identificazione biometrica), **le modalità di archiviazione dei dati** (decentralizzazione o centralizzazione), **le caratteristiche biometriche** (che non lasciano tracce e la cui acquisizione non è percepibile o che lasciano tracce e la cui acquisizione non è percepibile) e **i dati biometrici** (elaborati o grezzi).

- **La giornalizzazione dei processi biometrici** (registrazione e/o riconoscimento) in particolare deve tener conto dei principi di finalità e proporzionalità. La creazione di schede, la durata di archiviazione, l'anonimizzazione o la distruzione devono essere fissate in base a questi due principi.

- Per i processi di **verifica biometrica**, bisogna optare per **tecnologie che non implicano la memorizzazione in una banca di dati centrale** e che permettono alle persone interessate di controllare in parte (modello o confronto biometrico su carta) o per intero (sistema su carta) l'uso dei propri dati biometrici. La creazione di una banca di dati centralizzata è tuttavia adeguata, quando soddisfa un'esigenza preminente per la sicurezza.

- Se i dati biometrici sono archiviati in modo centralizzato, si deve prevedere una procedura di **cancellazione dei dati** per il momento in cui questi non saranno più necessari al raggiungimento delle finalità indicate al momento della raccolta o nella legge oppure per quando non corrisponderanno più alle circostanze.

- I sistemi di riconoscimento biometrico devono essere ideati e adattati in modo da garantire **l'esattezza e la qualità dei dati biometrici** (art. 5 cpv. 1 LPD). A tale scopo è opportuno definire il numero minimo di tratti biometrici distintivi che permettono di garantire un livello di riconoscimento (verifica/identificazione) adeguato alla finalità. D'altra parte, si tratta di scegliere in particolare una soglia di accettazione in funzione della percentuale ammissibile di false accettazioni (FAR). Si tratta di tenere inoltre in considerazione le conseguenze negative che i falsi rifiuti (FRR) possono causare alle persone interessate. Lo scopo di queste scelte è garantire l'affidabilità e l'efficacia del sistema di riconoscimento in relazione alle finalità dell'operazione.

- Per garantire la **sicurezza dei dati** (art. 7 cpv. 1 LPD), in particolare al momento della loro archiviazione e comunicazione, devono essere prese misure tecniche e organizzative (commisurate alla sensibilità dei dati biometrici trattati).

- Devono essere garantiti i **diritti delle persone interessate** (art. 8 LPD). Anche le persone interessate devono avere la possibilità di controllare come vengono usati i propri dati biometrici. Devono inoltre essere debitamente informate e associate all'elaborazione (raccolta presso la persona interessata o almeno non a sua insaputa) a meno che la legge non preveda espressamente un trattamento riservato. Devono infine avere accesso ai propri dati biometrici e ottenerne la rettifica o la cancellazione, se necessario.

- Il detentore della collezione di dati deve, se necessario, **notificare le collezioni di dati biometriche** all'IFPDT (art. 11*a* cpv. 2 & 3 LPD).

3. Guida alla valutazione

3.1 Introduzione

L'uso di sistemi di riconoscimento biometrico comporta rischi per quel che concerne il rispetto dei diritti e delle libertà fondamentali. Per questa ragione, è essenziale rispettare il principio della proporzionalità al momento di scegliere il sistema più adeguato (mezzi tradizionali o biometrici), la procedura di riconoscimento (verifica o identificazione), le modalità di archiviazione (decentralizzazione o centralizzazione), le caratteristiche biometriche, i dati biometrici (grezzi o elaborati) e le misure atte a garantire la sicurezza dei dati nonché il grado di affidabilità del sistema. L'elaborazione dei trattamenti di dati personali deve essere svolta con il sostegno di mezzi adeguati e necessari che non oltrepassino le finalità del trattamento.

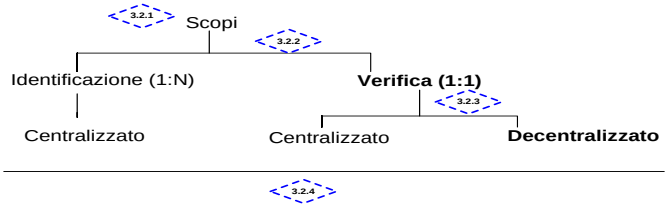
La presente guida è suddivisa in quattro parti: finalità, liceità e trasparenza (3.2); i mezzi di riconoscimento (3.3); la sicurezza dei dati e l'affidabilità del sistema (3.4); i diritti delle persone interessate (3.5).

La guida verte sulle considerazioni di cui tener conto nell'analisi dei sistemi di riconoscimento biometrico in materia di diritto alla protezione dei dati e offre un commento per ogni considerazione. Uno schema sintetico delle considerazioni precede le prime tre parti.

3.2 Finalità, liceità e trasparenza

I dati personali devono essere trattati per finalità chiaramente definite, lecite e comprensibili per le persone interessate. Inoltre, i trattamenti successivi devono essere compatibili con le finalità iniziali.

Finalità, liceità e trasparenza (le soluzioni raccomandate sono indicate **in grassetto**)



3.2.1 A quale scopi viene introdotto il sistema di riconoscimento biometrico?

3.2.2 Di quale processo di riconoscimento si tratta, di indificazione o di verifica?

3.2.3 I dati biometrici sono memorizzati in modo centralizzato o decentralizzato (modalità di memorizzazione)?

3.2.4 Quali sono i motivi giustificativi per il trattamento?

3.2.1 A quale scopo viene introdotto il sistema di riconoscimento biometrico?

Gli scopi del trattamento di dati biometrici devono essere definiti chiaramente ed essere comprensibili per le persone interessate.

3.2.2 Di quale processo di riconoscimento si tratta, di identificazione o di verifica?

Se lo scopo è verificare l'identità dichiarata (claimed identity), è opportuno seguire una procedura di verifica biometrica. La verifica biometrica soddisfa le esigenze di autenticazione forte cui i mezzi tradizionali di autenticazione (ad es. parole chiave o gettoni d'accesso, i cosiddetti «token») non rispondono in modo adeguato.

L'identificazione biometrica comporta rischi maggiori e dunque l'implementazione di un tale processo si può prendere in considerazione solo quando è indispensabile per raggiungere lo scopo scelto, in questo caso per *sapere chi sia la persona interessata*. A questo proposito è necessario stabilire se il processo di identificazione scelto debba essere automatizzata completamente o solo in parte (cfr. 0).

3.2.3 I dati biometrici sono memorizzati in modo centralizzato o decentralizzato (modalità di memorizzazione)?

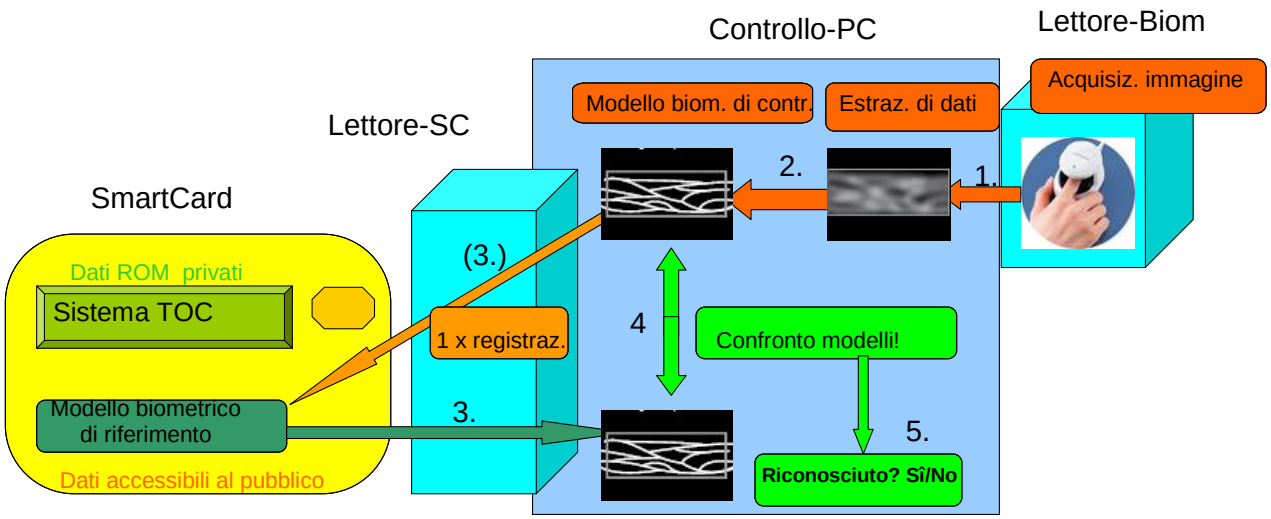
Se l'archiviazione dei dati è centralizzata, misura evidentemente necessaria per la procedura di identificazione biometrica, le esigenze relative alla protezione dei dati sono più rigorose. In particolare, il detentore della collezione deve fare attenzione nel rispettare le finalità del trattamento, non utilizzare i dati biometrici come identificatore unico, garantire l'esattezza dei dati e il diritto di accesso alle persone interessate, rendere sicuri i dati con misure tecniche e organizzative adeguate (cifratura, backup etc.).

Se lo scopo del trattamento di dati biometrici è la verifica dell'identità dichiarata, ogni dato biometrico di riferimento deve essere memorizzato integralmente (o parzialmente[6]) in maniera decentralizzata su un supporto personale. Esistono diversi tipi di supporto che permettono alle persone interessate di controllare in parte (modello biometrico su carta - *template on card* o confronto biometrico su carta - *match on card*) o integralmente (sistema biometrico su carta - *system on card*) l'uso fatto dei propri dati biometrici. La completa autodeterminazione informativa implica che i dati biometrici siano sempre sotto il controllo delle persone interessate; al momento attuale, questa possibilità è garantita solo dalla soluzione più avanzata (sistema biometrico su carta - *system on card / encapsulated biometrics*).

Le soluzioni di base (modello biometrico su carta - *template on card*) permettono solo di archiviare i dati biometrici di riferimento su un supporto personale. Le soluzioni intermedie (confronto biometrico su carta - *match on card*) permettono in più di svolgere la procedura di confronto su carta. Infine, le soluzioni presentate (sistema biometrico su carta - *system on card / encapsulated biometrics*), applicabili in pratica solo con le impronte digitali, permettono di memorizzare i dati biometrici di riferimento, di svolgere la procedura di confronto e di prendere una decisione su carta (successo o fallimento della verifica biometrica).

[6] Alcuni recenti sviluppi cercano di *spartire il riferimento biometrico* in due elementi, uno decentralizzato e l'altro centralizzato; quindi il confronto è possibile solo con tutti e due gli elementi!

Modello biometrico su carta



A) Registrazione:

1) Acquisizione di dati biometrici di riferimento (dati grezzi) per mezzo di un supporto di controllo (PC)
2) Estrazione di tratti distintivi di riferimento per mezzo di un supporto di controllo (PC) e invio del modello biometrico di riferimento alla carta.
3) Memorizzazione del modello biometrico di riferimento su carta.

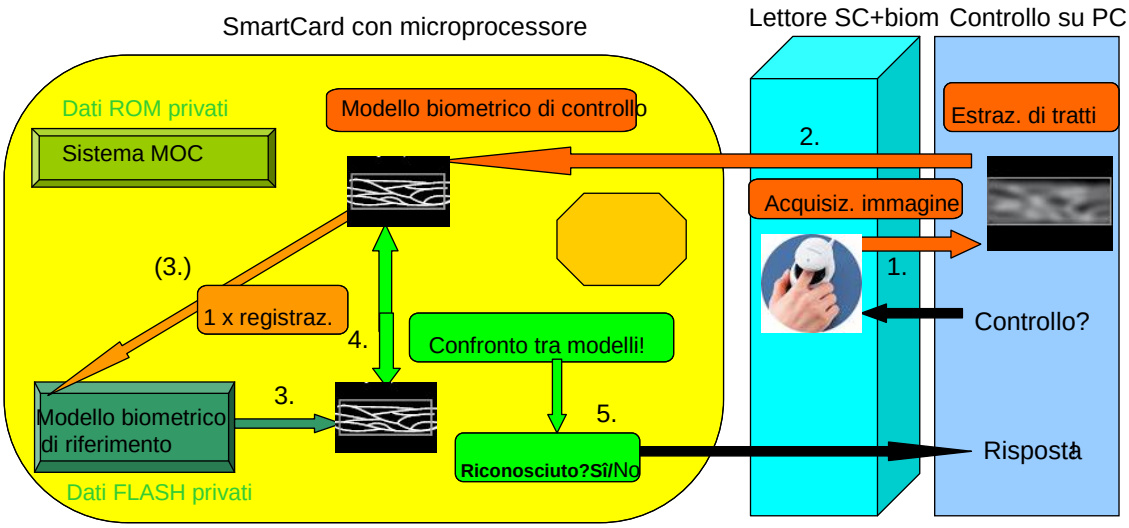
B) Verifica:

1) Acquisizione di dati biometrici (dati grezzi) per mezzo di un supporto di controllo (PC)
2) Estrazione di tratti distintivi (=> modello biometrico di controllo)
3) Invio del modello biometrico di riferimento al supporto di controllo (PC)
4) Confronto sul supporto di controllo tra i dati di riferimento e quelli di controllo
5) Riconoscimento: positivo/negativo sul supporto di controllo (PC).

In questa situazione, le persone interessate mantengono il controllo parziale dell'uso fatto dei propri dati biometrici di riferimento memorizzati su carta.

Al momento della verifica, i dati biometrici necessari vengono letti dal lettore per smartcard e trasmessi al sistema di riconoscimento. In questa occasione non è escluso che, a questo momento, venga fatta una copia non autorizzata dei dati biometrici.

Confronto biometrico su carta



A) Registrazione:

1) Acquisizione di dati biometrici di riferimento (dati grezzi) per mezzo di un supporto di controllo (PC).
2) Estrazione di tratti distintivi di riferimento per mezzo di un supporto di controllo (PC) e invio del modello biometrico di riferimento alla carta.
3) Memorizzazione del modello biometrico di riferimento su carta.

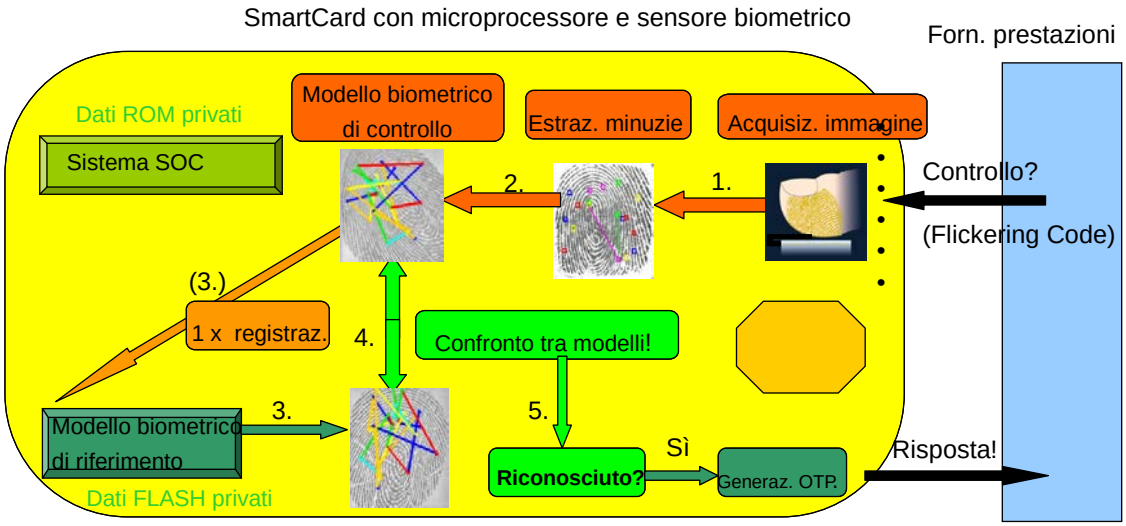
B) Verifica:

1) Acquisizione di dati biometrici (dati grezzi) per mezzo di un supporto di controllo (PC).
2) Estrazione dei tratti distintivi di controllo (=> modello biometrico di controllo).
3) Invio del modello biometrico di riferimento alla carta.
4) Confronto su carta tra i dati di riferimento e quelli di controllo.
5) Riconoscimento: positivo/negativo trasmesso al supporto di controllo (PC).

Una smartcard con confronto biometrico su carta dispone di un'unità di calcolo autonoma: cioè, il confronto tra le caratteristiche biometriche (modello biometrico di controllo) e i dati biometrici memorizzati localmente (modello biometrico di riferimento) si svolge sulla carta. Il sistema di controllo all'accesso riceve unicamente l'accettazione o il rifiuto della carta, senza che gli siano inviati dati biometrici. In questo modo, le persone interessate mantengono il controllo dei propri dati biometrici e delle transazioni relative al processo di confronto. Invece, non sono in grado di controllare l'uso dei dati della transazione scambiati tra il lettore e la carta.

Sistema biometrico su carta

(System on card – encapsulated biometrics)



A) Registrazione:

1) Acquisizione su carta delle impronte digitali di riferimento.
2) Estrazione su carta delle minuzie di riferimento.
3) Memorizzazione su carta del modello biometrico di riferimento.

B) Verifica:

1) Acquisizione su carta delle impronte digitali.
2) Estrazione delle minuzie di controllo e creazione di un modello biometrico di controllo.
3) Lettura su carta dei dati di riferimento.
4) Confronto su carta tra il modello di riferimento e quello di controllo.
5) Riconoscimento: se riuscito, generazione di una «password monouso» (One Time Password) per il fornitore di prestazioni.

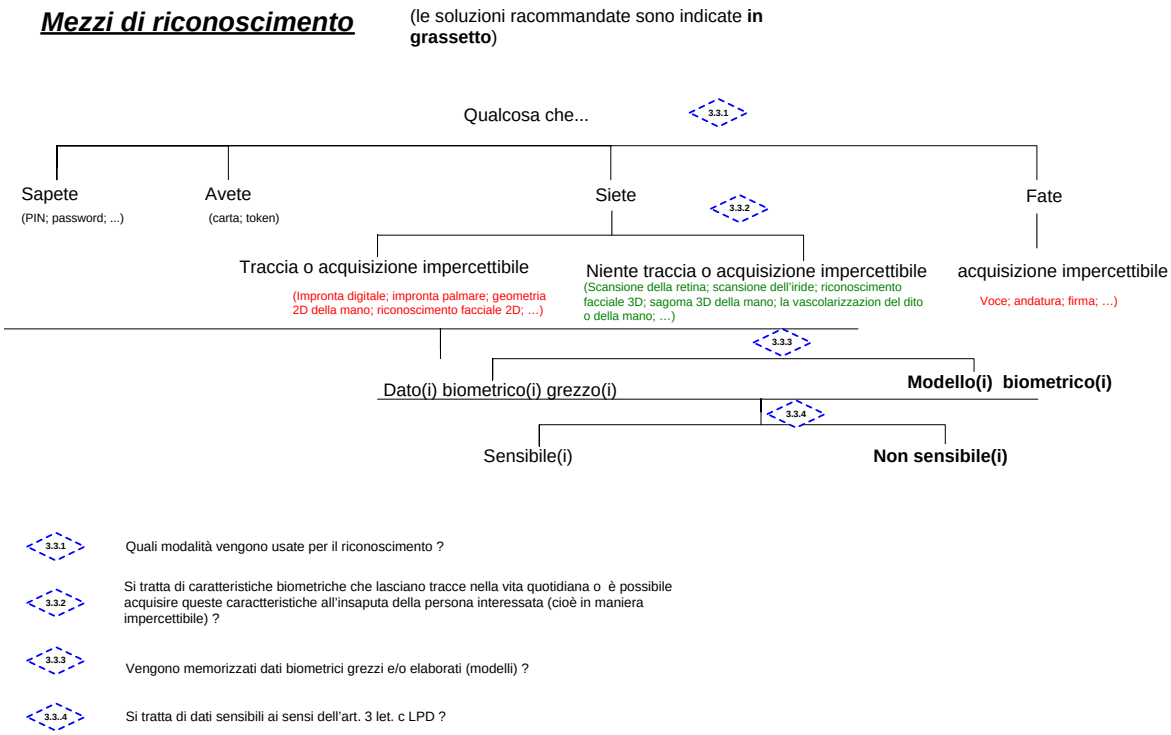
Le persone interessate mantengono il completo controllo dell'uso fatto dei propri dati biometrici memorizzati su carta poiché in quest'ultima sono incorporati un'unità di calcolo e un lettore biometrico. Dunque non c'è scambio di dati biometrici di riferimento o di dati di trasmissione tra la carta ed il sistema di controllo dell'accesso. Il fornitore di prestazioni riceve dal sistema biometrico su carta solo una «password monouso» che può essere generata e in seguito utilizzata solo da una persona autenticata.

3.2.4 Quali sono i motivi giustificativi per il trattamento?

Ogni trattamento di dati personali da parte di organi federali necessita una base legale. Inoltre i dati sensibili o i profili di personalità possono essere trattati solo se una legge in senso formale lo prevede espressamente. Invece, i motivi che giustificano il trattamento di dati personali da parte di persone private sono: il consenso della persona interessata, oppure un interesse pubblico o privato preponderante, o la legge. Il consenso deve essere rilasciato liberamente, in base ad un motivo specifico e dopo aver ricevuto informazioni. Questo presuppone che le persone interessate siano debitamente informate e che sia stata messa a loro disposizione un'alternativa al riconoscimento biometrico, a patto che le finalità iniziali non siano compromesse.

3.3 I mezzi di riconoscimento

È essenziale che al momento di scegliere i mezzi di riconoscimento venga rispettato il principio della proporzionalità. Quindi, al momento di decidere le modalità di riconoscimento biometrico (verifica o identificazione), le caratteristiche biometriche, i dati biometrici memorizzati e il tipo di dati (sensibili o meno) è opportuno scegliere i mezzi adeguati, necessari e non eccessivi rispetto alle finalità del trattamento; in altre parole, le tecnologie biometriche meno intrusive tra quelle atte a raggiungere le finalità scelte.



3.3.1 Quali modalità vengono usate per il riconoscimento ?

3.3.2 Si tratta di caratteristiche biometriche che lasciano tracce nella vita quotidiana o è possibile acquisire queste caractteristiche all'insaputa della persona interessata (cioè in maniera impercettibile) ?

3.3.3 Vengono memorizzati dati biometrici grezzi e/o elaborati (modelli) ?

3.3.4 Si tratta di dati sensibili ai sensi dell'art. 3 let. c LPD ?

3.3.1 Quali modalità vengono usate per il riconoscimento?

A parte le modalità biometriche, qualcosa che siete – *something you are*, o qualcosa che fate – *something you do*, esistono i mezzi tradizionali di autenticazione, cioè un'informazione di cui si è a conoscenza – *something you know* (NIP, parola chiave, …) o un oggetto che si possiede – *something you have* (carte, token, chiavi, badge, …) con o senza contatto.

Per quanto possibile, la procedura di verifica biometrica deve aver luogo partendo da un dato biometrico (o più d'uno, a seconda delle circostanze); eventualmente deve essere completata dai tradizionali mezzi di autenticazione.

Per le procedure di identificazione biometrica, un solo campione in genere porta ad un gruppo di persone più o meno folto. Perciò l'identificazione individuale è possibile solo in presenza di dati complementari, in particolare campioni biometrici supplementari o indizi pertinenti.

La questione della compatibilità delle finalità genera anche problemi di interoperabilità tra i differenti sistemi che si fondano sulla biometria. La standardizzazione imposta dall'interoperabilità comporta un aumento della gamma di possibilità d'interconnessione tra le banche di dati.

3.3.2 Si tratta di caratteristiche biometriche che lasciano tracce nella vita quotidiana o è possibile acquisire queste caratteristiche all'insaputa della persona interessata (cioè in maniera impercettibile)?

Determinate caratteristiche biometriche possono essere acquisite e utilizzate all'insaputa delle persone interessate. Ogni giorno tutti noi lasciamo tracce più o meno utilizzabili delle diverse caratteristiche biometriche. Inoltre alcuni dati biometrici possono essere acquisiti senza che la persona interessata lo venga a sapere.

È necessario dunque privilegiare[7] le tecnologie che sfruttano dati biometrici che non lasciano tracce o ne lasciano poche e non permettono la registrazione dei dati all'insaputa delle persone interessate.

3.3.3 Vengono memorizzati dati biometrici grezzi o elaborati (modelli)?

L'uso di dati elaborati deve essere privilegiato, poiché questi contengono meno informazioni sulle persone interessate. Il fine consiste nell'estrarre un numero di caratteristiche distintive sufficiente a raggiungere gli scopi previsti.

Inoltre, se dati grezzi sono memorizzati, conviene specificare i motivi giustificativi di questo trattamento.

[7] Come precisato dal gruppo per la tutela dei dati personali (articolo 29) nel Documento di lavoro sulla biometria, n. 80 del 1° agosto 2003, «*Ai fini di controllo dell'accesso (autenticazione/verifica) il gruppo ritiene che i sistemi biometrici fondati sulle caratteristiche fisiche che non lasciano tracce (ad esempio, la forma della mano, ma non le impronte digitali) o i sistemi biometrici fondati sulle caratteristiche fisiche che lasciano tracce, ma i cui dati non vengono registrati in una memoria appartenente ad una persona diversa dalla persona interessata (in altre parole, i dati non vengono memorizzati nel dispositivo di controllo d'accesso o in una base di dati centrale) comportino un numero minore di rischi per la protezione dei diritti e delle libertà fondamentali degli individui*».

3.3.4 Si tratta di dati sensibili ai sensi dell’art. 3 let. c LPD?

I dati biometrici sono dei dati personali. Secondo le caratteristiche ritenute, i dati biometrici possono contenere informazioni complementari sull’origine o sulla salute; in tal caso si tratta di dati sensibili ai sensi dell’art. 3 let. c LPD. Alla luce delle ricerche scientifiche svolte fino ad oggi, l'impronta digitale, la sagoma della mano e i tratti del viso, la scansione dell'iride ed il riconoscimento vocale contengono informazioni complementari sull’origine o sulla salute.

3.4 La sicurezza dei dati e l'affidabilità del sistema

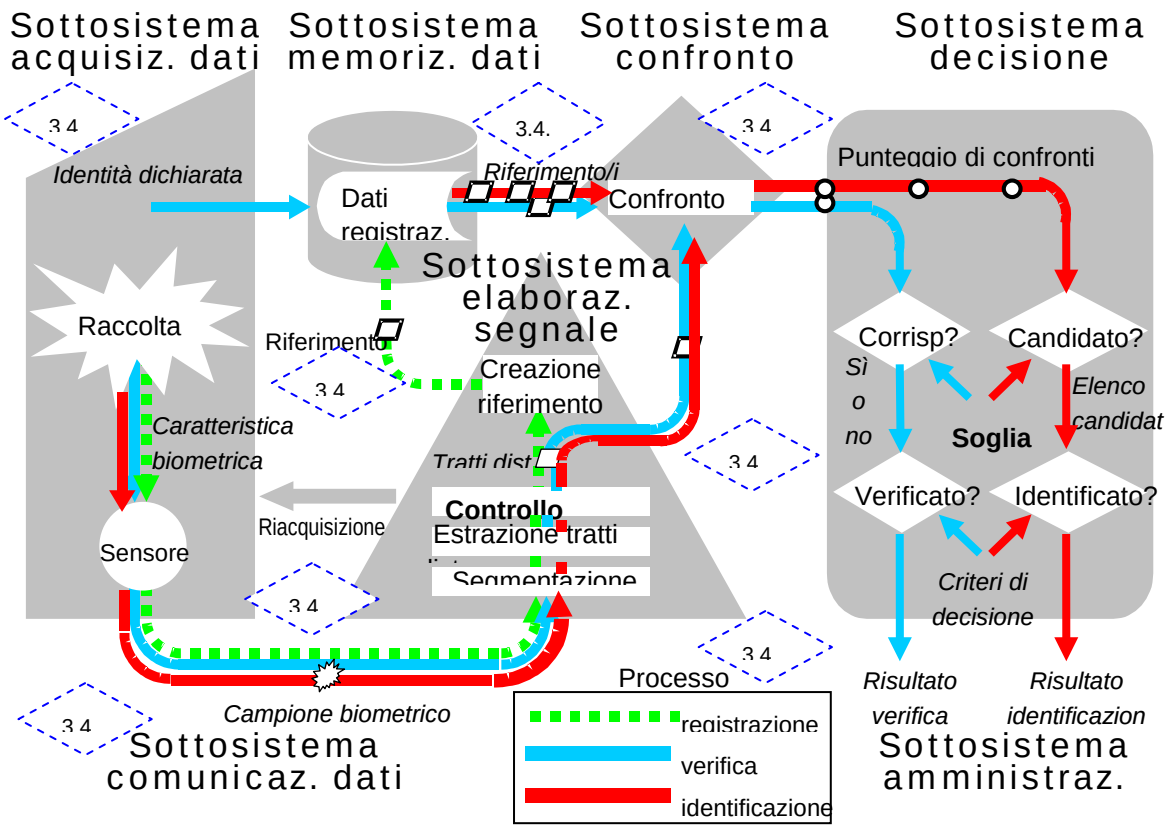
3.4.1 Qual è l'architettura del sistema di riconoscimento biometrico?

I sistemi di riconoscimento prevedono tre fasi essenziali: la registrazione, le verifiche o le identificazioni successive, il controllo dei diritti di accesso accordati alla persona riconosciuta (autenticata). Nel nostro contesto, la fase di registrazione prevede in primo luogo l'identificazione formale della persona interessata, seguita dalla registrazione biometrica.

Nonostante la diversità degli scopi e delle applicazioni dei sistemi di riconoscimento biometrico, questi ultimi hanno comunque un buon numero di elementi in comune che ne permettono una descrizione generale.

In linea di massima, un sistema di riconoscimento biometrico comprende i sottosistemi di acquisizione dei dati, di comunicazione dei dati, di trattamento del segnale, di memorizzazione dei dati, di confronto, di decisione e di amministrazione.

Rappresentazione concettuale di un sistema di riconoscimento biometrico:



3.4.1 Qual è l'architettura del sistema di riconoscimento biometrico ?

3.4.2 Quali misure di sicurezza sono attuate ?

3.4.3 Qual è il processo di registrazione biometrica ?

3.4.4 Qual è la proporzione d'insuccesso nella registrazione (FTE) ?

3.4.5 Qual è il numero previsto di persone registrate ?

3.4.6 Come funziona il processo di riconoscimento biometrico ?

3.4.7 Qual è la soglia di accettazione scelta, un funzione della percentuale di false accettazioni ? Qual è di conseguenza la percentuale di falsi rifiuti ?

3.4.8 Esiste una giornalizzazione dei processi biometrici (registrazione e riconoscimento) ? In caso di risposta affermativa, quali sono ?

I campioni biometrici acquisiti vengono prelevati con un sensore che trasmette i dati ad un processore il quale a sua volta ne estrae in maniera riproducibile misure distintive (tratti) eliminando tutti gli altri elementi. I tratti che ne risultano possono essere memorizzati in una banca di dati come riferimento, chiamato a volte riferimento o modello biometrico. In alcuni casi, il campione grezzo (senza estrazione di tratti) può essere memorizzato come riferimento biometrico. Un nuovo campione può essere confrontato ad un riferimento specifico, a vari riferimenti o a tutti i riferimenti presenti nella banca di dati, al fine di stabilire se vi è corrispondenza. Una decisione su una identità dichiarata o cercata è rilasciata in base alla similitudine tra i tratti del campione e quelli del/i riferimento/i confrontato/i.

I **sottosistemi** di un sistema di riconoscimento biometrico funzionano come segue:

- Acquisizione di dati: raccolta di un'immagine o di un segnale tratti dalla caratteristica biometrica presentata da un individuo a un sensore biometrico che restituisce l'immagine o il segnale sotto forma di campione biometrico acquisito. È importante che il sensore riprenda il carattere "vivo" della caratteristica presentata (affidabilità) ed è preferibile che non ci sia bisogno di contatto fisico (accettabilità, sicurezza).

- Comunicazione dei dati: garantisce la trasmissione di campioni, tratti, riferimenti, risultati e decisioni tra i diversi sottosistemi, eventualmente con l'aiuto di formati standard di scambio di dati biometrici. Il campione biometrico acquisito può essere compresso e/o criptato prima di essere trasmesso e decompresso e/o decriptato prima dell'uso. La cifratura è raccomandata in particolare per garantire la segretezza e l'integrità dei dati trasmessi.

- L'elaborazione del segnale: comprende in linea di massima un processo di segmentazione al fine di localizzare il segnale della caratteristica del soggetto nel campione biometrico acquisito, un processo di estrazione dei tratti che permette di estrarre in maniera riproducibile i tratti distintivi del campione biometrico acquisito e un processo di controllo della qualità che valuta la validità dei campioni, dei tratti, dei riferimenti ecc. con la possibilità di rimandare il controllo al sottosistema di acquisizione per raccogliere altri campioni o modificare i parametri di segmentazione o di estrazione.

- Memorizzazione dei dati: l'insieme dei riferimenti memorizzati costituisce una «base di dati di registrazione» che comprende eventualmente altri particolari sulla persona registrata o sul processo di registrazione. I riferimenti possono essere memorizzati nell'apparecchio di acquisizione, su un sistema portatile (smartcard), su un PC o su un server locale oppure in una banca di dati centrale.

- Confronto: i tratti sono paragonati ad uno (in caso di verifica) o a vari (in caso di identificazione) riferimenti e i risultati del confronto (grado di corrispondenza) sono trasmessi al sottosistema di decisione.

- Decisione: il confronto è considerato come riuscito quando il risultato del confronto è superiore o uguale ad una soglia di accettazione (threshold) predefinita, in caso contrario come fallito. Nell'ambito di un'identificazione, la riuscita comporta un elenco di eventuali candidati.

- Amministrazione: pilota l'insieme del sistema biometrico, permettendo ad esempio di informare il soggetto durante o dopo l'acquisizione, di definire la soglia di accettazione o un altro parametro che influenza il comportamento globale del sistema, di giornalizzare o meno (logfiles) gli avvenimenti sopraggiunti nel sistema o ancora di fungere da interfaccia per l'applicazione principale sfruttando il sistema biometrico.

Data la complessità di un sistema di questo tipo, è chiaro che la sicurezza dipende da ciascun sottosistema, di modo che la disponibilità di soluzioni o di prodotti a favore di una certificazione in materia di protezione dei dati (art. 5 OCPD a partire dal 01.01.2010) potrebbe rappresentare un

vantaggio. Ciononostante, la realizzazione di un tale sistema, anche se con prodotti certificati, resta un compito complicato che richiede un'attenzione accurata e costante (al momento della creazione e della manutenzione dei sistemi di riconoscimento) al fine di rispettare nel migliore dei modi le esigenze di protezione dei dati.

3.4.2 Quali misure di sicurezza sono attuate?

È necessario applicare misure tecniche ed organizzative adatte alla sensibilità dei dati biometrici e che permettano di impedire l'accesso abusivo. I controlli dell'accesso possono essere fisici o logici (cioè connessi al sistema o ai dati).

Ciò vale soprattutto per i sottosistemi di memorizzazione e di comunicazione dei dati.

3.4.3 Come funziona il processo di registrazione biometrica?

Al momento della registrazione, un dato biometrico grezzo viene in un primo tempo acquisito per mezzo di un sensore, e poi l'immagine viene analizzata e se ne estrae un modello biometrico. In tale ottica, come vengono estratti i punti caratteristici (*features*) e quanti di questi vengono registrati per costituire il modello biometrico (è possibile modulare, ridurre il numero di punti caratteristici)?

3.4.4 Qual è la proporzione d'insuccesso nella registrazione (FTE)?

La proporzione di errori di registrazione evidenzia le difficoltà che le persone interessate possono incontrare durante questo processo; questo fattore dipende in larga misura dalla caratteristica biometrica scelta. Dunque è necessario prevedere un'alternativa al riconoscimento biometrico (principio di non discriminazione).

3.4.5 Qual è il numero previsto di persone registrate?

Il numero di persone registrate è particolarmente importante nell'ambito di un processo di identificazione, dato che questo condiziona la dimensione della banca di dati centrale e de facto le dimensioni dell'elenco dei candidati prodotto dal confronto 1-N. A tale riguardo, è necessario sottolineare che in pratica è possibile realizzare un'identificazione completamente automatizzata solo se l'elenco non comprende mai più di un candidato. Invece, quando l'elenco presenta più di un candidato, l'identificazione deve essere portata a termine, in generale «manualmente», in base a criteri supplementari.

3.4.6 Come funziona il processo di riconoscimento biometrico?

Il processo di riconoscimento biometrico consiste nel verificare l'identità dichiarata o nell'identificare una persona confrontando un dato biometrico di riferimento (memorizzato al momento della registrazione biometrica) con il dato biometrico attuale (registrato durante la procedura di riconoscimento). È importante sottolineare il carattere probabilistico del riconoscimento biometrico. In realtà, grazie al confronto tra dati biometrici, si ottiene una percentuale di similitudine. Il sistema biometrico «riconosce» la persona in questione se questa percentuale raggiunge o supera la soglia di accettazione prefissata.

3.4.7 Qual è la soglia di accettazione scelta, in funzione della percentuale tollerabile di false accettazioni? Qual è di conseguenza la percentuale di falsi rifiuti?

Più la soglia di accettazione è stabilita in alto, più aumenta il tasso di falsi rifiuti (*FRR*), cioè è possibile che persone registrate non vengano riconosciute. Abbassare la soglia di accettazione permette di ridurre il tasso di falsi rifiuti, ma a prezzo di un aumento proporzionale del tasso di false accettazioni (*FAR*): questo implica l'aumento del rischio di usurpazione d'identità.

3.4.8 Esiste una giornalizzazione dei processi biometrici (registrazione e riconoscimento)? In caso di risposta affermativa, come si svolge?

Questo trattamento di dati (creazione, memorizzazione, distruzione o anonimizzazione di file giornale) deve rispondere ai principi di finalità e proporzionalità.

3.5 I diritti delle persone interessate

3.5.1 Quali sono le misure attuate per garantire i diritti delle persone interessate?

Le persone interessate devono poter far valere i propri diritti di accesso e, se necessario, chiedere che i dati personali che li riguardano vengano rettificati, distrutti o segnalati come controversi se non è possibile stabilirne l'imprecisione.

Inoltre, se vengono trattati dati personali sensibili o compilati profili di personalità, le persone interessate devono essere debitamente informate. Cioè devono conoscere almeno l'identità del detentore della banca di dati, le finalità del trattamento per il quale i dati vengono raccolti e le categorie di destinatari di dati, se si intende comunicare i dati a terzi.

Per concludere, è necessario prevedere un'alternativa al riconoscimento biometrico in modo da evitare discriminazioni nei confronti di coloro che non sono in grado di utilizzare il sistema di riconoscimento biometrico (poiché non possiedono i dati biometrici richiesti o perché la qualità dei dati non è sufficiente). Inoltre, è necessario mettere a disposizione un'alternativa per quanti non desiderano che i propri dati biometrici vengano utilizzati a scopo di riconoscimento, a patto che le finalità iniziali non siano compromesse.

3.5.2 L'IFPDT è a conoscenza della banca di dati?

Le collezioni di dati devono essere notificate all'Incaricato federale alla protezione dei dati e della trasparenza (IFPDT). Quest’ultimo deve tenere un registro di dati accessibili online: lo scopo è, da una parte, garantire alle persone interessate la trasparenza e la facilità nell'esercizio dei propri diritti, dall’altra permettere all'IFPDT di svolgere il proprio compito di sorveglianza.

Gli organi federali ed i privati che trattano regolarmente dati sensibili e profili di personalità o che comunicano regolarmente dati personali a terzi sono tenuti a notificare le loro collezioni di dati all'IFPDT fatte salve le eccezioni previste all’art. 11a cpv. 5 LPD. Maggiori informazioni sulle modalità di notifica delle collezioni di dati sono disponibili sul sito internet dell'IFPDT (www.edoeb.admin.ch).