CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

# LINEE GUIDA PER LE TECNOLOGIE BIOMETRICHE

Versione del 8-10-2004

Il presente documento è stato elaborato da un gruppo di lavoro, costituito dal Cnipa (Centro nazionale per l'informatica nella pubblica amministrazione) nel marzo 2004 con durata 12 mesi, al cui interno sono rappresentate amministrazioni pubbliche, esponenti del mondo universitario e della ricerca e le associazioni dei fornitori.

Il gruppo di lavoro ha l'obiettivo di predisporre e di aggiornare periodicamente un documento di linee guida sulle tecnologie biometriche in grado di fornire delle indicazioni a supporto delle pubbliche amministrazioni per progetti che prevedano il ricorso a tali tecnologie.

Fanno parte del gruppo di lavoro:
Alessandro Alessandroni, *Cnipa*;
Stefano Aprile, *Ministero della Giustizia*;
Elvio Baldracco, *Stato Maggiore della Difesa*;
Antonello Busetto *Federcomin*;
Giovanni Fattorini, *Stato Maggiore della* Difesa;
Francesco Giuffrè, *Anie*;
Massimo Gneo, *Ministero dell'Interno;*
Maurizio Leoni, Sta*t*o *Maggiore della Difesa*;
Dario Maio, *Università di Bologna*;
Davide Maltoni, *Università di Bologna*;
Giovanni Manca, *Cnipa*;
Luca Merlini, *Assintel*;
Valeria Mirabella, *Cnipa*;
Roberto Muscillo, *Ministero della Giustizia* ;
Giuseppe Neri *Assinform*;
Stefano Petecchia, *Ministero dell'Interno*;
Giovanni Rellini Lerz, *Cnipa*;
Roberto Romano *Anasin*;
Adriano Santoni, *Assocertificator*i;
Mario Savastano, *CNR Napoli*;
Stefano Venanzi, *Cnipa*.

Si ringrazia inoltre Gianfranco Pontevolpe (*Cnipa*) che ha fornito il suo prezioso contribuito.

Ai lavori del Gruppo assiste Cosimo Comella rappresentante dell'Ufficio del Garante per la protezione dei dati personali nel quadro della cooperazione istituzionale sugli argomenti da trattare.

Sommario

*Capitolo 1*

# Obiettivi documento

## 1.1 Premessa

La difficile situazione internazionale ha indotto un sensibile rafforzamento dei controlli atti a garantire la sicurezza dei cittadini e, negli ultimi anni i governi di tutto il mondo hanno promosso il potenziamento delle azioni di controllo del territorio e delle frontiere nell'ambito delle quali sono spesso emerse difficoltà legate alla identificazione certa degli individui.
In questo contesto l'interesse verso le tecnologie biometriche è rapidamente cresciuto grazie alla possibilità di basare il riconoscimento degli individui su dati certi quali caratteristiche fisiche e comportamentali, ragionevolmente uniche e non riproducibili.
L'impiego della biometria a rafforzamento della sicurezza è testimoniato da iniziative internazionali, quali il nuovo passaporto europeo ed il permesso di soggiorno elettronico e, per ciò che attiene all'Italia, dalla nuova Carta d'Identità Elettronica (CIE), che avranno come denominatore comune l'uso di identificatori biometrici a sostegno dell'autenticità. Ulteriori investimenti sono inoltre previsti per il potenziamento dei sistemi AFIS (Automated Fingerprint Identification Systems) [1], basati sull'utilizzo di impronte digitali e da anni impiegati dagli organi investigativi internazionali per l'identificazione degli individui.
L'uso delle tecnologie biometriche non si limita comunque agli ambienti investigativi o di controllo delle frontiere, ma registra una rapida diffusione anche in altri importanti settori privati e pubblici. Con riferimento alla Pubblica Amministrazione, la diffusione della biometria si intreccia strettamente con un processo di informatizzazione e di centralizzazione della figura del cittadino nei processi amministrativi che il Governo ha da anni avviato con impegno. Il massiccio ricorso a canali innovativi, quali ad esempio Internet, nell'attuazione dell'e-government, sta rendendo sempre più evidente la necessità di soluzioni ottimali per l'autenticazione e la sicurezza nell'accesso ai dati ed ai servizi on-line quali importanti presupposti del nuovo rapporto cittadino-istituzioni.
Come è noto i metodi basati sull'uso di password, attualmente i più diffusi, non sempre sono in grado assicurare una adeguata garanzia; per queste ragioni molte amministrazioni stanno decisamente procedendo verso l'uso di tecniche di tipo biometrico.
L'interesse diffuso intorno alle tecnologie biometriche e la necessità di guidare le Pubbliche Amministrazioni in un mercato in rapida evoluzione ha portato alcuni governi, fra i quali quelli statunitense, britannico e tedesco, alla costituzione di gruppi di lavoro con l'obiettivo di fornire indicazioni e chiarimenti. Inoltre un considerevole numero di forum internazionali analizza la biometria sia per gli aspetti più propriamente tecnici che per quelli sociali, etici ed inerenti il delicato tema della privacy.

## 1.2 Le iniziative del CNIPA

Tenuto conto dell'importanza che le tecniche biometriche stanno assumendo nel contesto del settore pubblico, il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA) ha ritenuto opportuno approfondire gli aspetti tecnici e normativi della biometria. A tal fine, nel luglio del 2003, il CNIPA ha costituito un gruppo di studio sulle tecnologie

biometriche e successivamente, sulla base delle proposte formulate da tale gruppo, ha avviato una linea di attività dedicata al tema dell'impiego delle tecnologie biometriche nella Pubblica Amministrazione. Nel marzo del 2004 è stato costituito un Gruppo di lavoro incaricato della redazione delle linee guida sulle tecnologie biometriche.
Il CNIPA ha inoltre costituito un "Centro di competenza sulla biometria" per dare supporto alle amministrazioni pubbliche per esigenze connesse alla conoscenza, sperimentazione ed utilizzo delle tecnologie biometriche mirando a garantire:

- la messa a fattor comune di conoscenze ed esperienze tecnologiche e organizzative;
- una maggiore efficacia degli interventi, in termini di competenze e di assistenza alle pubbliche amministrazioni;
- l'allineamento a progetti internazionali con obiettivi simili.

Il CNIPA non intende quindi limitarsi ad una attività informativa e di indirizzo, ma vuole anche offrire un supporto tangibile ai progetti delle pubbliche amministrazioni dalla fase di analisi e di sperimentazione fino alla messa in esercizio delle soluzioni biometriche. E' inoltre prevista una attività di comunicazione attraverso l'organizzazione di convegni e seminari di studio.
Infine, attraverso il centro di competenza, il CNIPA partecipa a eventi nazionali ed internazionali di particolare rilevanza.

## 1.3 La biometria nella Pubblica Amministrazione

Nella Pubblica Amministrazione italiana, fino a qualche anno fa, escludendo le applicazioni AFIS, le tecnologie biometriche avevano trovato un utilizzo limitato per lo più ad applicazioni finalizzate al controllo dell'accesso fisico del personale a luoghi sensibili (ad es. siti militari). Recentemente sta crescendo l'interesse da parte di amministrazioni pubbliche verso l'utilizzo di tecnologie biometriche per il controllo dell'accesso fisico a edifici e aree riservate o per l'accesso logico ad applicazioni informatiche critiche.
La notevole diffusione delle carte di accesso ai servizi in rete della pubblica amministrazione, sta suscitando un notevole interesse verso l'utilizzo combinato di dati biometrici, certificati di autenticazione e smart card.
L'uso combinato di più tecnologie consente infatti di associare al livello di sicurezza offerto da una carta firmata elettronicamente la certezza che il possessore della carta sia il titolare degli accessi su una base più affidabile dell'usuale PIN. Inoltre, l'utilizzo di una carta custodita dall'utente per la memorizzazione del dato biometrico soddisfa quei requisiti in tema di privacy che sono indifferibili in ogni applicazione biometrica[1].

[1] Occorre comunque tenere conto della responsabilità del titolare (vedi capitolo 5)

## 1.4 Contenuti del documento

Questo documento rappresenta la prima versione delle linee guida per le tecnologie biometriche in ambito Pubblica Amministrazione. Il documento fornisce delle indicazioni di carattere generale che rappresentino un supporto valido alle amministrazioni nella fase di progettazione di interventi che prevedono il ricorso a tecnologie biometriche. Viene offerta una panoramica sulle tecnologie disponibili e vengono esaminate le principali questioni legate agli aspetti tecnologici. Vengono infine offerti elementi utili per la valutazione delle alternative ed affrontate le tematiche legate agli ambiti sociali e normativi, con particolare riferimento alla tutela dei dati personali. Un secondo documento avrà lo scopo di fornire indicazioni operative alle pubbliche amministrazioni per le attività di progettazione, acquisizione, valutazione e gestione dei sistemi biometrici facendo riferimento anche all'esito di sperimentazioni e progetti avviati dalle pubbliche amministrazioni.
Per ciò che attiene alla struttura del documento, dopo la breve introduzione del capitolo 1, il capitolo 2 riporta le definizioni principali della biometria e le fasi del processo biometrico; il capitolo 3 descrive le varie tecniche utilizzando uno schema comune che prevede, per le tecniche principali, una descrizione generalizzata, i punti di forza e debolezza, i settori applicativi e il mercato. Eccezione viene fatta per le caratteristiche delle impronte digitali che, rappresentando il più diffuso metodo biometrico, sono descritte più in particolare; il capitolo 4 illustra i principali campi di applicazione; il capitolo 5 è incentrato sugli aspetti normativi connessi alla tutela dei dati personali; il capitolo 6 mette in evidenza gli aspetti non tecnici della biometria con particolare riferimento alla considerazione dei fattori etici e sociali; i capitoli 7 e 8 forniscono indicazioni per la progettazione di una soluzione biometrica e la valutazione delle prestazioni riportando, allo stesso tempo, esempi di implementazione di sistemi biometrici a livello sia nazionale, sia internazionale; infine, il capitolo 9, appendice, riporta utili informazioni sui laboratori di ricerca, gli standard correnti e alcuni approfondimenti tecnici sulla valutazione delle prestazioni dei sistemi biometrici. Il glossario chiude il documento.

## 1.5 Destinatari del documento

Il documento si rivolge alle amministrazioni pubbliche aventi le esigenze già esposte, ma per alcuni contenuti di carattere generale può anche essere un utile panorama sull'argomento.

*Capitolo 2*

# Il processo biometrico

## 2.1 Premessa

Il presente capitolo intende offrire una prima descrizione del processo biometrico con particolare riferimento agli aspetti tassonomici. Molti dei temi trattati saranno discussi in dettaglio nel prosieguo del documento.

## 2.2 Definizioni

Il termine "riconoscimento biometrico"[2] [3] fa riferimento all'identificazione o alla verifica automatica di identità degli individui attraverso la valutazione di caratteristiche fisiche e comportamentali [4].

I due distinti obiettivi di un processo biometrico sono quindi:

- verifica della dichiarazione di identità di un soggetto;
- attribuzione di una identità ad un soggetto.

### 2.2.1 Accesso fisico e accesso logico

In biometria due termini ricorrenti sono:

- accesso fisico (controllo biometrico dell'), procedura di accertamento della titolarità del soggetto all' ingresso in un locale, edificio, comprensorio o area;
- accesso logico (controllo biometrico dell'), procedura di accertamento della titolarità del soggetto ad usufruire di una risorsa informatica.

### 2.2.2 Verifica ed identificazione

Una prima cruciale distinzione nell'ambito del processo biometrico, approfonditamente messa in evidenza nei prossimi capitoli, è quella tra le modalità di ***verifica*** o ***identificazione***.

In un processo di ***verifica***, detto anche "uno a uno", i dati acquisiti, sul momento, dal sensore biometrico vengono comparati con un unico dato biometrico depositato dall'utente nella fase

[2] Dal greco bios (vita) e metros (misura)

[3] Il termine "biometria", ha inteso negli anni passati lo studio e l'uso di metodi matematici e statistici applicati alla biologia, alle scienze agrarie e forestali, alla medicina, alla genetica, alle scienze ambientali e a settori affini. Per i dovuti riferimenti può risultare utile consultare il sito della Società Italiana di Biometria (http://axp.mat.uniroma2.it/~sib/newsta.htm)

[4] National Biometric Test Center Collected Works, 1997-2000, Edited by James L. Wayman, Director, Version 1.3, August, 2000, Prepared under DoD Contract MDA904-97-C-03 and FAA Award DTFA0300P10092

di registrazione (enrollment) e residente, ad esempio, su un dispositivo sicuro o in un archivio magnetico, indicizzato, in questo caso, ad esempio, da un codice identificativo.
In un processo di ***identificazione*** i dati acquisiti sul momento dal sensore biometrico vengono comparati con un insieme di dati biometrici contenuti in un archivio
Dal punto di vista tassonomico, in ambito biometrico, oltre a "verifica" ed "identificazione", compare spesso il termine "riconoscimento biometrico" usato in generale quando non si vuole specificare se verifica o identificazione. Infine, il vocabolo "autenticazione", che in ambito ICT [5] intende l'operazione di provare genericamente a un sistema informatico l'identità di un utente, nella biometria fa quasi sempre riferimento ad un processo di verifica.

### 2.2.3 Biometria fisica e comportamentale

Con riferimento alla definizione di riconoscimento biometrico, si opera una distinzione di massima fra:

- biometria "fisica" e cioè basata su dati derivati da caratteristiche fisiche dell'individuo quali ad esempio impronte digitali, caratteristiche del viso, dell'iride o della mano;
- biometria "comportamentale" e cioè basata sulla valutazione di caratteristiche comportamentali dell'individuo quali, ad esempio, la dinamica di apposizione della firma, il tipo di andatura o anche, per alcuni aspetti, l'emissione della voce.

### 2.2.4 Biometria interattiva e passiva

Sebbene la maggior parte dei processi biometrici di pertinenza della Pubblica Amministrazione siano realizzati con utenti a conoscenza della operatività del sistema (biometria interattiva) e cooperativi, alcune applicazioni di puro carattere investigativo e governativo [6] potrebbero prevedere l'uso di sistemi biometrici senza che l'utente ne sia a conoscenza (biometria passiva). Tipica è la discussa applicazione della sorveglianza nei luoghi caratterizzati da un largo afflusso di pubblico i cui aspetti verranno esaminati nel paragrafo dedicato al riconoscimento biometrico del volto.

### 2.2.5 Identificazione positiva e negativa

Un sistema biometrico può operare in identificazione positiva o negativa; nel primo caso l'individuo dichiara (anche implicitamente) di appartenerne al gruppo di utenti noti al sistema, nel secondo caso l'individuo dichiara (anche implicitamente) di non appartenere al gruppo di utenti noti al sistema.

[5] Information Communication Technology

[6] La natura strettamente governativa della sorveglianza non si applica alla lettera agli Stati Uniti dove è possibile anche per i privati implementare applicazioni di biometria passiva. Classico è il caso della ricerca dei giocatori professionisti, cui non è permesso giocare all'interno dei casinò, implementato da organizzazioni di security private.

In un processo di identificazione positiva si ha evidenza del legame tra la persona in esame con una identità in precedenza memorizzata nel sistema e l'utente richiede una identificazione in positivo, cioè la verifica della propria identità tramite un confronto automatico tra il campione presentato e uno o più template memorizzati[7]. Se il sistema di identificazione positiva non riesce a trovare un grado di coincidenza tra il campione in esame e tutti i campioni registrati superiore ad una soglia prefissata, l'esito è un "rifiuto". D'altro canto, la corrispondenza tra il campione in esame e uno dei campioni registrati comporta una "accettazione". In tale procedura possono essere utilizzate entrambe le modalità operative di confronto (verifica d'identità e identificazione). Esempi di identificazione positiva sono il controllo degli accessi fisici e degli accessi logici, l'accesso a risorse in genere.
L'identificazione negativa provvede a stabilire che il soggetto da identificare non risulti tra un gruppo di persone già conosciute al sistema (es. non abbia più di una patente, non sia presente in una lista di segnalazioni giudiziarie, ecc…). Tale procedura è stata quella più utilizzata sino ad oggi in ambito governativo negli U.S.A. Lo scopo di questo sistema di identificazione è di impedire l'uso di più identità da parte di una singola persona. Se il sistema di identificazione non riesce a trovare un grado di coincidenza superiore ad una soglia prefissata, tra il campione in esame e tutti i template registrati, ciò si traduce in una "accettazione", nel caso contrario si genera un "rifiuto". Si noti che, mentre un riconoscimento positivo può essere eseguito anche con tecniche non biometriche, un riconoscimento negativo, che stabilisce che un soggetto non è chi dice di non essere, può essere compiuto soltanto con l'impiego di tecniche biometriche. Per l'identificazione negativa può essere utilizzata soltanto la modalità operativa di confronto tramite identificazione 1:N, dove N è l'intera popolazione di interesse talvolta ristretta a una "check list" o "short list" che contempla i casi maggiormente critici.
Esempi di identificazione negativa sono le procedure di controllo per evitare la concessione multipla di benefici assistenziali sotto false identità, i controlli per evitare di emissione documenti a persone che dichiarano falsa identità, il controllo dell'immigrazione, la sorveglianza.

## 2.3 Le fasi del processo biometrico

Le fasi di un processo biometrico, dalla fase di registrazione (enrollment) alla "verifica di identità" o "identificazione", sono schematizzate in Figura 2.1.

[7] Ovviamente, la vera identità dell'utente deve essere accuratamente stabilita durante la registrazione ricorrendo a documenti e processi esterni al sistema biometrico vero e proprio

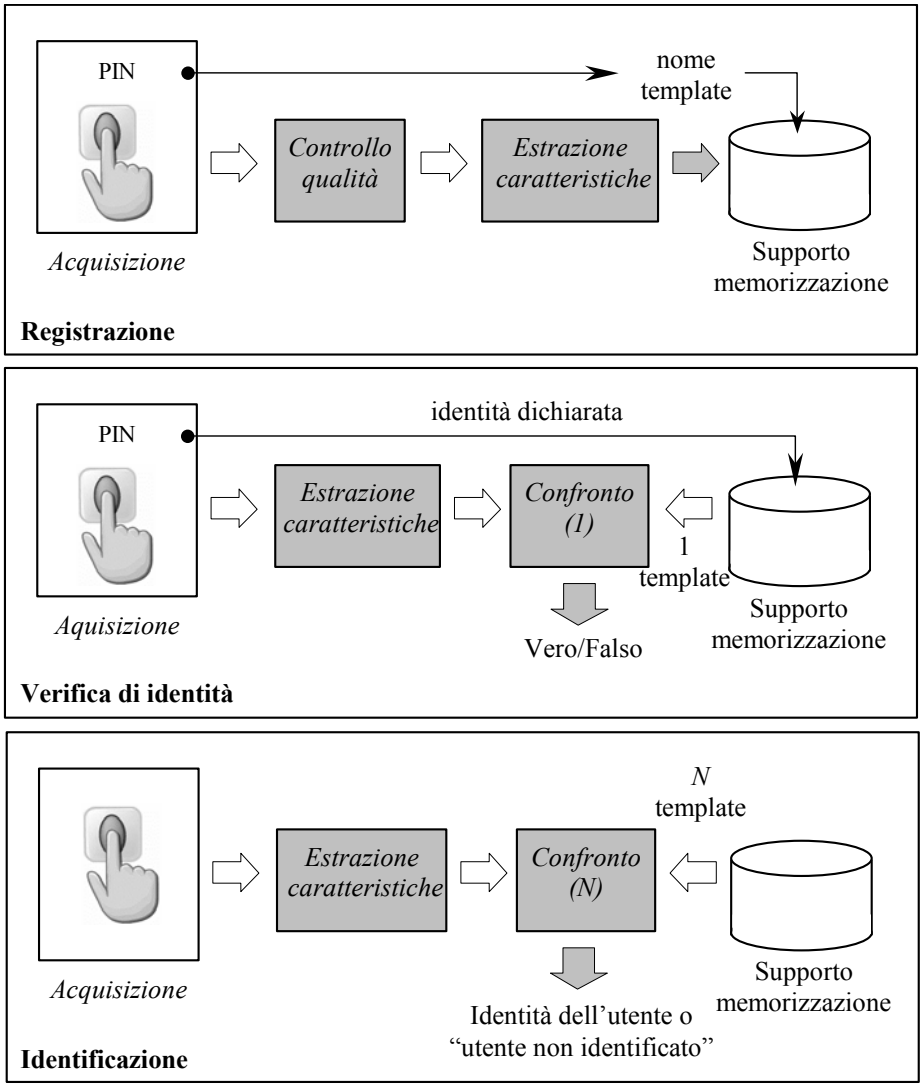


*Figura 2.1: schemi a blocchi di registrazione, verifica di identità e identificazione nei sistemi biometrici basati su impronte digitali.*

### 2.3.1 Registrazione (enrollment)

La registrazione dell'utente (enrollment) è la prima fase di un processo biometrico e consiste nell'acquisizione da parte del sensore della caratteristica biometrica dell'individuo. Del campione ottenuto viene generalmente controllata la qualità e se essa non è soddisfacente il processo di registrazione viene reiterato. Generalmente segue una procedura nota come "estrazione delle caratteristiche", che si fonda sulla derivazione, dal campione acquisito, di alcune caratteristiche numeriche il cui insieme prende il nome di "template". La fase di registrazione si conclude con la memorizzazione del template su un supporto di memorizzazione che è, in generale, un dispositivo sicuro. Talvolta, come può accadere ad esempio nel caso delle impronte digitali, il processo biometrico può fare riferimento alla immagine della caratteristica biometrica e non ad una estrazione di caratteristiche. La comparazione con le altre immagini può allora avvenire sulla base di tecniche di correlazione di tipo ottico o numerico. Per tenere conto di questa duplice possibilità, nel presente

documento si farà talvolta riferimento al termine "identificativo biometrico" per indicare sia l'immagine che il template della caratteristica biometrica.

### 2.3.2 Fase di verifica

Durante la verifica di identità, il sensore acquisisce il campione biometrico dell'utente, dal quale, come accade nel processo di enrollment, vengono estratte le caratteristiche e calcolato il template. Quest'ultimo viene comparato con quello precedentemente memorizzato nella fase di enrollment e residente, ad esempio, sul dispositivo sicuro in possesso dell'utente o sul supporto di memoria di una risorsa informatica, in questo caso indicizzato, ad esempio, da un PIN a conoscenza dell'utente.
L'esito del confronto è vero/falso a conferma o rifiuto della dichiarazione di identità dell'utente in funzione del superamento di una soglia prefissata da parte del grado di coincidenza (matching score) tra il template presentato e quello precedentemente memorizzato.

### 2.3.3 Fase di identificazione

In fase di identificazione l'utente non usa supporti di memorizzazione con la caratteristica biometrica o non inserisce un codice identificativo e il sistema confronta il template estratto dalla caratteristica biometrica con tutti i template presenti in archivio, al fine di trovare tutti quelli caratterizzati da un grado di coincidenza superiore ad una soglia prefissata. L'output del sistema è l'identità associata all'utente con il migliore grado di coincidenza oppure una segnalazione "utente non identificato". In realtà in diversi sistemi la procedura di identificazione viene interrotta non appena si trova un utente la cui similarità è maggiore della soglia.
Sebbene operare in modalità identificazione possa risultare molto utile, è anche piuttosto rischioso specie se l'archivio contiene molti utenti (si veda § 7.2.1).
Indipendentemente dal modo di operare (verifica o identificazione) la fase di confronto delle caratteristiche con il template non è banale come un semplice confronto di password e può dar origine a errori quali falsi rifiuti e false accettazioni.

## 2.4 Classificazione delle applicazioni

In letteratura sono riportate numerose classificazioni delle applicazioni biometriche [1], [2]. Una sintetica distinzione dovrebbe distinguere una biometria:

| | |
|---|---|
| Governativa | Privata |
| Manifesta | Non manifesta |
| Operata da utenti abituati | Operata da utenti non abituati |

| | |
|---|---|
| Supervisionata | Non supervisionata |
| Operata in un ambiente standard [8] | Operata in un ambiente non standard |
| Aperta [9] | Chiusa |

## 2.5 Dispositivi di acquisizione

Alcuni comuni dispositivi di acquisizione delle caratteristiche biometriche sono:

- lettori di impronta digitale connessi ad hardware proprietari o a una delle porte di un personal computer (seriale, parallela, USB), dispositivi inglobati in schede di tipo PCMCIA o in mouse o anche inseriti nella tastiera di personal computer.
- videocamere, macchine fotografiche digitali o scanner fotografici per il riconoscimento biometrico del viso;
- particolari videocamere sensibili alla luce visibile e all'infrarosso e dotate di led emettitori di luce infrarossa per l'iride;
- dispositivi proprietari per la geometria della mano;
- microfoni o apparecchi telefonici per le caratteristiche della voce;
- tavolette elettroniche o penne elettroniche per il riconoscimento biometrico della firma.

## 2.6 Bibliografia/Riferimenti in rete

[1]. National Biometric Test Center Collected Works 1997-2000, edited by James L. Wayman, Director, August, 2000

[2] W. Saito, "Installing and Integrating Biometric Systems into your exixting Systems", presentation at 22th NISS (National Institute of Statistic Sciences) Conference, 1999.

[8] Una applicazione implementata non alle condizioni climatiche e di temperatura esterne, in un ambiente caratterizzato da una temperatura intorno ai 20°, alla pressione di circa 1 Atm ed in condizioni di illuminazione controllata potrebbe considerarsi operante in un ambiente standard.

[9] Applicazione i cui dati non vengono esportati verso altri sistemi biometrici, ad esempio gestiti da un soggetto giuridico differente

*Capitolo 3*

# Le tecnologie biometriche

## 3.1 Premessa

Il presente capitolo descrive le più importanti tecniche biometriche con un ordine che riflette le quote di mercato attribuite dagli esperti.

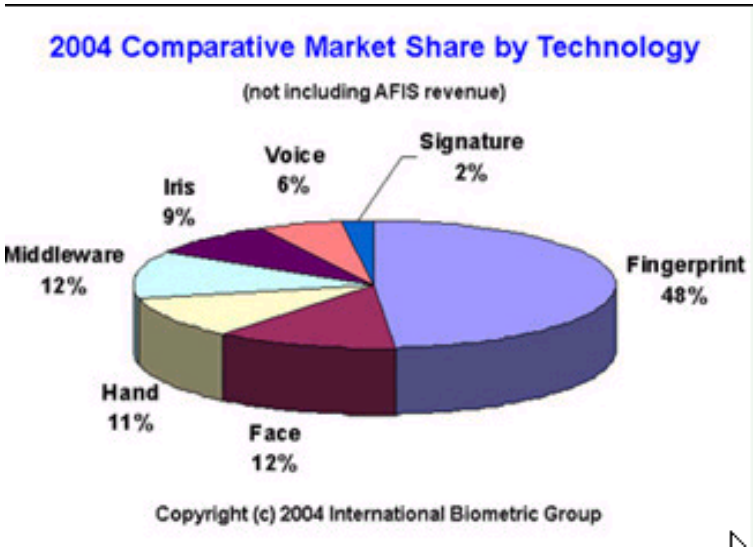


*Figura 3.1*

Tutte le tecniche saranno descritte, più o meno estensivamente, cercando di rispettare uno schema comune di esposizione. Per alcune tecniche biometriche è stato ritenuto opportuno aggiungere, alla fine del paragrafo, una sezione di approfondimento destinata agli utenti che desiderano analizzare in dettaglio alcuni aspetti tecnici.

## 3.2 Impronte digitali

La stabilità e l'unicità delle impronte digitali sono da tempo universalmente riconosciute, tanto che i sistemi giuridici, in vigore in quasi tutti i paesi del mondo, conferiscono alle impronte digitali valore probatorio nei processi. Le basi della moderna metodologia di analisi delle impronte digitali, pur esistendo testimonianze della conoscenza dell'unicità delle loro caratteristiche fin dal sedicesimo secolo, risalgono di fatto alla fine del XIX secolo, quando Henry Faulds introdusse un sistema di classificazione che consentiva di applicare per la prima volta il riconoscimento delle impronte digitali in ambito criminale. Contemporaneamente altri studiosi, tra cui l'ungherese Juan Vucetich e successivamente l'italiano Giovanni Gasti, proposero metodi di classificazione più accurati, associando a ciascuna delle dieci impronte digitali di un individuo un valore numerico e costruendo con questi valori un codice di dieci cifre che consente l'individuazione di un soggetto in un archivio di grandi dimensioni. Nel

1888, l'Inglese Francis Galton, condusse uno studio esteso sulle impronte digitali e riconobbe nelle impronte le più importanti micro-caratteristiche peculiari (ancora oggi utilizzate dalla maggior parte dei sistemi di riconoscimento), che da quel momento in poi presero il nome di "caratteristiche di Galton" o "minuzie". I primi sistemi automatici per il riconoscimento di impronte digitali (AFIS - Automated Fingerprint Identification System) furono sviluppati nel 1950 dall'F.B.I. (Federal Bureau of Investigation) in collaborazione con il National Bureau of Standard, Cornell Aeronautical Laboratory, e Rockwell International Corp. Dieci anni dopo NEC Technologies Inc. (Tokyo), Printrack Inc. (Anaheim, California), e Morpho System (Parigi) fecero il loro ingresso in campo basandosi sul lavoro e sui risultati ottenuti dall'FBI. I sistemi sviluppati furono adottati in diversi contesti, e le agenzie di polizia, affiancate da enti governativi e privati, persero la prerogativa di unico destinatario di queste tecnologie. Il primo sistema biometrico commerciale (a basso costo) per la verifica di identità fu ideato a partire dal 1971 da Randall Fowler e commercializzato solo 12 anni dopo da Identix Inc. Sunnyvale, California. Oggigiorno diverse società sviluppano e commercializzano sistemi di riconoscimento basati su impronte digitali.

### 3.2.1 Descrizione

Un'impronta digitale è la riproduzione dell'epidermide del polpastrello di una delle dita della mano ottenuta quando il dito è premuto contro una superficie levigata. Le più evidenti caratteristiche strutturali sono le creste e le valli epidermiche che scorrono in flussi paralleli determinando il noto disegno dell'impronta (Figura 3.2.a). In alcune regioni (dette singolarità) le creste assumono forme particolari: loop (ciclo), delta (triangolo), e whorl (nido), come evidenziato in Figura 3.2.b. A livello locale possiamo poi notare discontinuità nel disegno dell'impronta determinate da terminazioni e/o biforcazioni delle creste (Figura 3.2.c): queste discontinuità, denominate minuzie, sono le caratteristiche dell'impronta più spesso utilizzate per il confronto. La coincidenza spaziale di un certo numero di minuzie (variabile da 10 a 20 a seconda del paese, 17 in Italia) è ritenuta prova valida per l'identificazione di un sospetto.

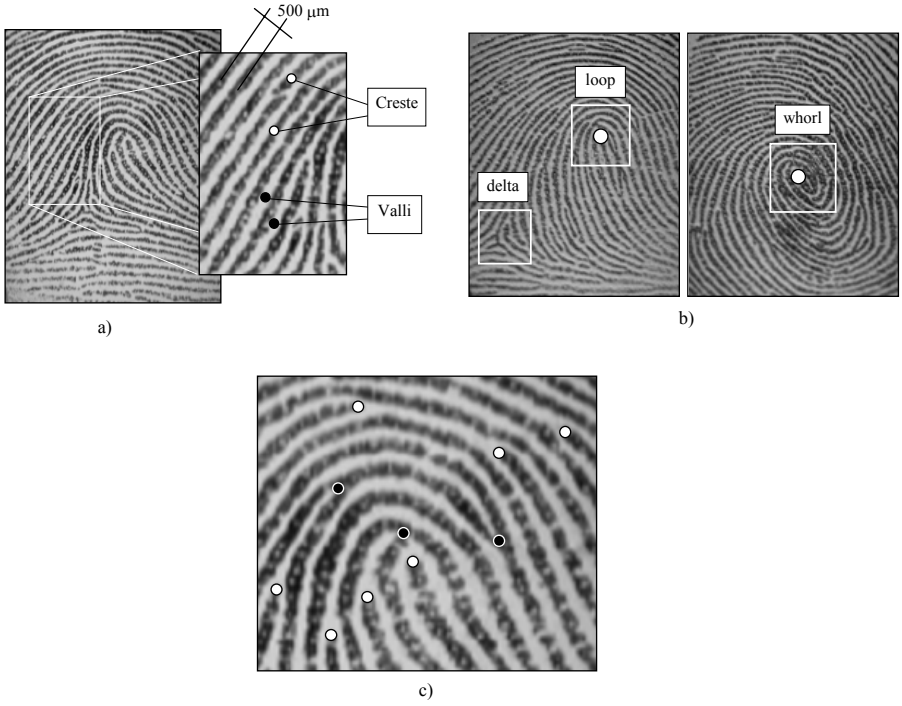


*Figura 3.2: a) creste e valli formano il disegno di un'impronta; b) singolarità di tipo loop, delta e whorl; c) minuzie di tipo terminazione (bianche) e biforcazione (nere).*

### 3.2.2 Acquisizione di impronte digitali

Storicamente, in ambito AFIS, l'acquisizione delle impronte avveniva utilizzando la cosiddetta tecnica dell'inchiostro: il dito dell'interessato veniva spalmato di inchiostro nero e premuto contro un cartoncino; il cartoncino veniva poi digitalizzato con uno scanner a 500 dpi a 256 livelli di grigio producendo un'immagine digitale. Questo tipo di processo, definito acquisizione off-line, è ancora oggi utilizzato in ambito AFIS anche se si assiste a una graduale migrazione verso tecniche di acquisizione denominate "live-scan", dove l'immagine dell'impronta viene direttamente catturata da un sensore, senza nessun tipo di inchiostratura. Per massimizzare la compatibilità tra immagini di impronte digitali il dipartimento CJIS (Criminal Justice Information Services) dell'FBI ha rilasciato nel 1999 una serie di specifiche tecniche per scanner FBI-compatibili. [1].

Il settore AFIS trarrà certamente nel futuro notevoli vantaggi a seguito dell'introduzione di tecniche di acquisizione live-scan, tuttavia questa innovazione è indubbiamente di maggior rilievo sopratutto per applicazioni civili e commerciali. Negli ultimi dieci anni diverse società hanno sviluppato scanner di impronte (live) destinati al mercato non-AFIS; questi sistemi, sebbene non compatibili con le specifiche FBI, hanno un costo nettamente inferiore e sono in genere caratterizzati da un elevato grado di usabilità. Oltre alla tecnologia ottica (Figura 3.3.a), sono emerse tecnologie di acquisizione alternative (Figura 3.3.b e Figura 3.3.c); i sensori allo stato solido (Figura 3.3.b) hanno permesso la riduzione delle dimensioni, e spesso anche il costo, del dispositivo di acquisizione. Purtroppo però in diversi casi, con l'obiettivo di ridurre i costi e le dimensioni, sono stati sacrificati parametri di fondamentale importanza quali l'area di acquisizione e la risoluzione. Se la finestra (o area) di acquisizione di un sensore è piccola, allora la porzione del dito acquisita è altrettanto piccola e contiene un esiguo numero di dettagli (ad esempio di minuzie); quando il dito viene in seguito ripresentato al sensore di acquisizione, a causa delle inevitabili differenze di posizionamento, l'area

catturata è diversa e la parte coincidente è spesso insufficiente per poter procedere al riconoscimento; questa è una delle principali cause di falso rifiuto nei sistemi biometrici basati su impronte digitali.

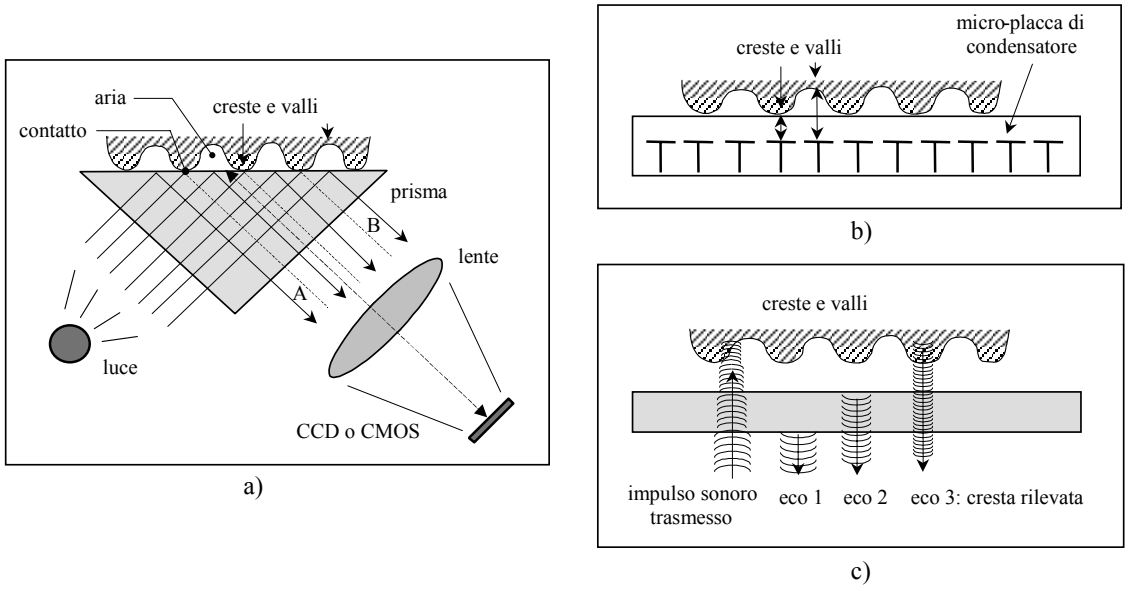


*Figura 3.3: a) acquisizione di impronta tramite sensore ottico FTIR: i raggi di luce vengo riflessi/assorbiti a seconda dei punti di contatto del dito con la superficie di un prisma, e focalizzati attraverso una lente sulla superficie di un CCD o CMOS; b) acquisizione di impronta tramite sensore a stato solido capacitivo: una piastrina di silicio contenente un array di microcondensatori è in grado di rilevare le differenti distanze tra creste e valli e convertirle in segnali elettrici; c) acquisizione di impronta tramite sensore a ultrasuoni che esegue una sorta di ecografia al dito, nella quale il segnale riflesso (eco) varia a seconda della conformazione del derma.*

La Figura 3.4 mostra l'impronta digitale dello stesso dito, acquisita con diversi sistemi commerciali (non AFIS). Le immagini mostrano chiaramente come sensori diversi possano acquisire immagini di diversa qualità e ricchezza di dettagli [2].
Nel caso di sensori ottici i principali fattori che determinano la qualità delle immagini acquisibili tramite uno scanner sono:

1. la dimensione (numero di pixel) e la risoluzione (dpi) del CCD;
2. la qualità dell'ottica e del prisma;
3. l'uniformità della sorgente luminosa;
4. la corretta disposizione geometrica degli elementi che contribuiscono a formare l'immagine sul sensore: piano dell'ottica; piano del CCD; distanze tra i componenti (N.B. un errore anche minimo può generare alterazioni significative dell'immagine in termini di "fuoco" e "geometria");
5. l'accuratezza del software di correzione geometrica dell'immagine (qualora questa operazione non sia eseguita con ottiche speciali);

*Figura 3.4 impronte digitali dello stesso dito acquisite con diversi sensori commerciali, riprodotte in proporzioni reali*

### 3.2.3 Aspetti del processo biometrico nei sistemi basati sul riconoscimento delle impronte digitali

La maggior parte dei sistemi di riconoscimento delle impronte digitali è basato sulla valutazione delle minuzie e per ciascuna minuzia vengono memorizzate le coordinate cartesiane e l'angolo tangente alla cresta nel punto dove la minuzia è presente. Alcuni sistemi estraggono ulteriori caratteristiche di tipo "proprietario". La dimensione del template varia da circa 512 byte ai 2 KB nei sistemi che memorizzano le sole minuzie ad alcune decine di KB in alcuni sistemi che memorizzano altre informazioni estratte dall'impronta; nella maggior parte dei sistemi il template ha una dimensione inferiore ai 4 KB e si presta dunque ad essere memorizzato su carte con capacità di memorizzazione ridotta. La possibilità di ricostruire l'immagine dell'impronta a partire dal solo template dipende dal tipo di informazioni numeriche estratte ma spesso la reversibilità della trasformazione è di fatto impossibile (ad esempio nel caso in cui vengano memorizzate solo le minuzie). Indipendentemente dal modo di operare (verifica o identificazione) la fase di confronto delle caratteristiche con il template non è banale come un semplice confronto di password e può dar origine a errori: falsi rifiuti e false accettazioni (si veda § 7.2.1). Le principali difficoltà insite nel confronto sono dovute alle variazioni delle immagini relative alle impronte. Tali variazioni sono determinate da

fattori come traslazione, rotazione, sovrapposizione parziale delle dita e differente stato dell'epidermide durante acquisizioni diverse. Inoltre sono osservabili distorsioni non lineari causate dalla plasticità della pelle, spesso amplificate da un errato posizionamento del polpastrello sul sensore di acquisizione. I metodi più noti per il confronto di impronte digitali utilizzati sono riconducibili alle seguenti categorie o a combinazioni delle stesse:

- confronto basato sulle minuzie: consiste nel trovare il miglior allineamento tra gli insiemi di minuzie estratte dalle impronte da confrontare. Questa tecnica è la più diffusa;
- confronto basato sulla correlazione (talvolta detto pattern matching): il confronto avviene a livello di immagini di impronte o porzioni di queste opportunamente elaborate;
- confronto basato sulle caratteristiche delle creste: il confronto di basa su caratteristiche numeriche (forma, orientazione, densità, ecc.) estratte dalle creste epidermiche.

### 3.2.4 Punti di forza e debolezza

In Tabella 3.1 vengono identificati alcuni punti di forza e di debolezza dei sistemi biometrici basati su impronte digitali:

| Pro | Contro |
|---|---|
| – Tecnologia consolidata<br>– Elevata accuratezza<br>– Dispositivi di acquisizione di piccole dimensioni<br>– Costi ridotti | – Alcuni soggetti (specialmente anziani e lavoratori manuali) possono incontrare difficoltà a causa dello spessore ridotto delle creste epidermiche.<br>– Non idoneo in alcuni ambienti (troppo umidi o polverosi).<br>– Diffidenza di alcuni soggetti per fattori psicologici |

*Tabella 3.1: punti di forza e debolezza dei sistemi biometrici basati su impronte digitali.*

Le impronte digitali sono la caratteristica biometrica più nota e utilizzata sia in ambito di polizia sia in ambito civile e commerciale. Devono questa loro fama e larga diffusione alle doti di accuratezza, semplicità d'uso dei dispositivi e costo relativamente ridotto.
Le controindicazioni non sono molte, e nella maggior parte delle applicazioni è possibile impiegare un sistema basato su impronte digitali. È necessario però tener conto di alcune problematiche che possono insorgere per alcuni utenti che hanno impronte digitali di scarsa qualità intrinseca. Si tratta di una piccola percentuale della popolazione (3-5%, specialmente anziani e lavoratori manuali) nei quali lo spessore delle creste epidermiche è molto ridotto e gli scanner di acquisizione non sono in grado di acquisire immagini di qualità. In Figura 3.5 sono mostrate 3 impronte digitali di diversa qualità acquisite da tre soggetti diversi: l'impronta c) è di scarsa qualità; un utente con impronte di scarsa qualità è più soggetto a errori di tipo falso rifiuto. Pur non esistendo nessun sistema che possa gestire il 100% di questi casi critici, impiegando scanner di impronte digitali di elevata qualità e algoritmi di confronto efficaci la probabilità di gestire correttamente questi casi difficili aumenta sensibilmente.

a) b) c)

*Figura 3.5 : impronte digitali di a) buona, b) media e c) scarsa qualità*

Le condizioni ambientali d'esercizio possono rappresentare un altro punto di criticità per l'impiego di sistemi basati su impronte digitali. È noto infatti che gli scanner di impronte incontrano maggiori difficoltà a operare con dita troppo secche o troppo umide; pertanto, se l'utente ha utilizzato ad esempio solventi, creme sulle mani oppure opera in ambiente molto umido, le immagini acquisite possono essere di scarsa qualità (Figura 3.6). Si consiglia infine di non installare scanner di impronte digitali in ambienti sporchi o polverosi: il sensore di acquisizione può deteriorarsi/rovinarsi, in questi casi, molto velocemente richiedendo frequenti interventi di manutenzione.

a) b) c)

*Figura 3.6 tre impronte digitali dello stesso dito in condizioni a) normali, b) secche e c) umide.*

### 3.2.5 Campi di applicazione

I sistemi biometrici basati su impronte digitali trovano applicazione in molteplici settori:

- AFIS in ambienti di polizia per l'identificazione dei criminali;
- AFIS in ambito civile (ad esempio in diversi stati americani vengono utilizzati per impedire che un soggetto riceva più volte benefici assistenziali sotto identità diverse);
- documenti elettronici (passaporto, visti, carta identità): per il controllo sicuro dell'identità presso frontiere e aeroporti; per l'identificazione di immigrati clandestini; per gli ordinari controlli eseguiti da organi di polizia;

- accesso a servizi: particolare rilievo riveste l'applicabilità di tale tecnologia per l'erogazione di servizi sulla base di carte contenenti dati biometrici;
- accesso logico a risorse (PC singoli, reti informatiche, singoli applicativi);
- firma digitale con autenticazione dell'utente che appone la firma;
- accesso fisico ad ambienti (locali protetti, laboratori, uffici, ecc.);
- accesso in ambito bancario. In questo caso non viene eseguito il confronto dell'impronta digitale con un template precedentemente acquisito; a ogni transito viene semplicemente catturata un'immagine dell'impronta e salvata in formato cifrato. Le immagini sono consultabili dalla sola autorità giudiziaria e vengono distrutte dopo alcuni giorni;
- controllo delle presenze del personale.

### 3.2.6 Il mercato

Gli introiti sul mercato mondiale per quanto riguarda tecnologie biometriche relative alle impronte digitali (ad esclusione dei sistemi AFIS) nel 2004 sono stimate in circa 370 milioni di dollari USA. Il ritmo di crescita previsto è di circa il 40% anno per i prossimi quattro anni, mentre si stima che la percentuale di mercato ad esso riservata rimarrà pressoché stabile

Escludendo ancora una volta il segmento AFIS, attualmente le principali applicazioni che usufruiscono della tecnologie biometriche e quindi anche di quelle basate su impronte digitali, sono quelle di accesso logico e fisico. È previsto comunque un aumento delle percentuali previste per le applicazioni inerenti a transazioni economiche.

Come già accennato, sul mercato internazionale dei sistemi biometrici basati sulle impronte digitali operano molte società. Alcune di queste sono produttori di hardware (scanner) e/o di software di riconoscimento, altri sono integratori che acquisiscono dai produttori i componenti di base e costruiscono intorno a questi applicazioni generiche e/o verticali. Esistono infine alcune società di distribuzione che agiscono come importatori di soluzioni prodotte all'estero (spesso sul mercato asiatico). La maggior parte dei produttori sono piccole e medie società, mentre tra gli integratori e distributori incontriamo numerose società di grandi dimensioni. Il segmento di mercato AFIS è prerogativa di poche società (5 o 6). Sul mercato italiano sono presenti alcuni produttori e diversi integratori e distributori. I prodotti disponibili possono essere ricondotti alle seguenti categorie:

- scanner di acquisizione per settore AFIS;
- software di riconoscimento per settore AFIS: benché basato sugli stessi principi di funzionamento di quello utilizzato in ambito commerciale, è ottimizzato per eseguire ricerche su archivi di grosse dimensioni, è dotato di interfacce utente per il supporto agli esperti di investigazione ed è concepito per essere eseguito su hardware dedicato/parallelo;
- scanner di acquisizione da tavolo (per PC o per computer portatile);
- scanner di acquisizione in formato OEM: per l'integrazione fisica all'interno di macchinari più complessi (ad esempio una bussola bancaria);
- sistemi di sviluppo software (SDK): consentono agli integratori di includere in applicativi le funzionalità di riconoscimento dell'impronta digitale;
- applicativi per l'accesso a computer o rete (Logon);
- sistemi per il controllo degli accessi: da installare presso varchi (spesso non presidiati) che permettono di comandare le serrature elettroniche di sblocco di porte;

- sistemi per il controllo delle presenze: sostituiscono la tradizionale marcatura del cartellino cartaceo, con il riconoscimento biometrico dell'impronta;
- applicativi centralizzati per controlli accessi e/o presenze: consentono di amministrare in modo centralizzato un impianto costituito da più unità per il controllo di accessi / presenze collegati tra loro in rete;
- moduli stand-alone per il riconoscimento dell'impronta: sono orientati agli integratori; consentono di eseguire l'acquisizione, la memorizzazione dei template e il confronto dell'impronta su hardware dedicato senza richiedere un PC.

## 3.3 Riconoscimento biometrico del volto

Il riconoscimento del volto sta divenendo con gli anni una delle più importanti e mature tecnologie di autenticazione biometrica [3]. Pur non potendo offrire, nelle classiche operazioni di accesso fisico e logico, le prestazioni di accuratezza nel riconoscimento offerte da altre tecniche, essa rappresentata un metodologia per molti versi unica per ciò che attiene ai settori di impiego. Proprio la vasta gamma di applicazioni possibili è alla base di un forte interesse commerciale e scientifico per la tecnologia che si traduce nello sviluppo di nuovi algoritmi e tecniche, come ad esempio quella basata sull'analisi tridimensionale del volto (detta anche "3D") di cui una descrizione è riportata in § 3.3.6.1.
Una delle applicazioni di punta della tecnologia, anche se ancora in fase sperimentale, è rappresentata dal tentativo di controllo dei luoghi o del territorio in una modalità che viene definita "sorveglianza" ("surveillance"). Anche se con limiti imposti dalle comprensibili e non ancora completamente risolte difficoltà tecniche, il riconoscimento biometrico del volto potrebbe essere impiegato per riconoscere, nella folla di un aeroporto o di uno stadio, i volti di soggetti contenuti in un archivio fotografico.
Va infatti messo in evidenza che, a differenza di quasi tutte le altre tecniche biometriche, il riconoscimento del volto può avvenire ad una certa distanza dal soggetto, con o senza la volontarietà di esso, il che, ovviamente, rende questa tecnica particolarmente adatta alle applicazioni di tipo investigativo.

### 3.3.1 Descrizione

Il riconoscimento biometrico del volto si basa sull'acquisizione delle caratteristiche del volto di un soggetto attraverso un dispositivo di ingresso che è generalmente costituito da una telecamera.
Il riconoscimento biometrico può avvenire attraverso la comparazione con una immagine fissa o con sequenze di immagini in movimento e, a seconda del tipo di immagine, si opera generalmente una distinzione fra "riconoscimento statico" e "riconoscimento dinamico".
Il riconoscimento statico è, impiegato, in linea di massima, nelle applicazioni inerenti l'accesso fisico o logico e per l'emergente settore della cosiddetta "ricerca dei duplicati", che verrà descritto più approfonditamente in seguito. La modalità "statica" è caratterizzata,

generalmente, da una buona qualità dell'immagine di riferimento memorizzata[10]. Nelle applicazioni per la ricerca dei duplicati, le fotografie di riferimento sono quelle usate nei documenti o foto segnaletiche. Queste immagini sono generalmente caratterizzate da una buona posa del soggetto, spesso disposto frontalmente e su sfondo controllato e ciò può semplificare notevolmente le operazioni matematiche alla base del metodo biometrico.
Il riconoscimento dinamico, caratteristico della modalità "surveillance" può invece avvenire attraverso l'analisi di immagini con sfondi e pose irregolari, ciò comportando notevoli problemi di tipo computazionale aggravati dalla necessità di dovere operare in tempo reale.
Indipendentemente dalla modalità statica o dinamica del processo, il riconoscimento biometrico del volto si articola in varie fasi:

- individuazione del volto (face detection)
- segmentazione (segmentation)
- estrazione delle caratteristiche (feature extraction)
- riconoscimento (recognition).

### 3.3.2 Punti di forza e debolezza

Mettendo sempre ben in evidenza i differenti aspetti del riconoscimento biometrico del volto ed i differenti contesti applicativi (civile e investigativo), per quanto riguarda il primo, tra i punti di forza, andrebbe sottolineato il buon grado di accettazione della tecnologia da parte degli utenti che apprezzano la natura non invasiva di acquisizione della caratteristica biometrica che avviene senza contatto con il sensore e senza un particolare addestramento. Andando invece ad esaminare il campo investigativo, un punto di assoluta forza è la capacità da parte della tecnica di essere impiegata per scopi quali la sorveglianza o la ricerca dei duplicati non raggiungibili attraverso l'uso di altre tecniche biometriche. Tra gli svantaggi andrebbe annoverato il problema della bassa invarianza temporale della caratteristica biometrica dal momento che le caratteristiche del viso, oltre che per accadimenti accidentali, variano ineluttabilmente con l'età. Un secondo problema consistente può essere inoltre individuato nella forte dipendenza da parte della tecnologia dalle condizioni di illuminazione ambientale, le cui variazioni possono influenzare sensibilmente le prestazioni. A questo proposito andrebbe messo in evidenza che i sistemi basati su acquisizione tridimensionale del volto presentano generalmente una risposta migliore a tale variazioni. Una tabella riassuntiva dei punti di forza e debolezza della tecnologia è riportata di sotto.

| Pro | Contro |
|---|---|
| – Bassa invasività (mancanza di contatto fisico) | – Bassa stabilità della caratteristica biometrica nel |

[10] Un elemento in grado di influire significativamente sulle prestazioni di un riconoscimento di tipo "statico" è l'uso dello stesso dispositivo di acquisizione per l'autenticazione biometrica e per l'enrollment (come accade generalmente nelle applicazioni di accesso logico a personal computer).

| | |
|---|---|
| – Possibilità di acquisizione a distanza | tempo<br>– Prestazioni inferiori a quelle di altre tecniche biometriche<br>– Sensibilità alle variazioni di illuminazione<br>– Dimensioni del template maggiori di quelli prodotti con altre tecnologie (da 1Kbyte a 5 Kbyte per 2D, fino a 10 Kbyte per 3D) |

*Tabella 3.2 punti di forza e debolezza dei sistemi biometrici basati sul riconoscimento biometrico del volto*

### 3.3.3 Campi di applicazione

Il riconoscimento biometrico del volto può essere utilizzato per varie applicazioni di cui alcune comuni ad altre tecniche come il controllo dell'accesso fisico e logico, altre specifiche come:

- sorveglianza (surveillance);
- controllo di documenti;
- ricerca dei duplicati.

#### 3.3.3.1 Sorveglianza (surveillance)

Come già precedentemente messo in evidenza, per "sorveglianza" si intende il tentativo di identificare un soggetto (generalmente in luoghi sensibili come aeroporti) attraverso il confronto tra le immagini acquisite da una telecamera e quelle contenute in un archivio.
Avendo già messo in evidenza il massiccio sforzo computazionale richiesto per una funzionamento in tempo reale, un problema concreto consiste nella corretta determinazione della "soglia di somiglianza" fra soggetto inquadrato e le immagini archiviate, superata la quale il sistema manda una allerta. Una soglia troppo alta rischia di far perdere al sistema qualche "candidato" mentre una soglia troppo bassa può causare una sensibile serie di falsi allarmi, quasi sempre di difficile gestione per mancanza di personale o di tempo.
Il problema dei "falsi allarmi" ha ridimensionato in qualche modo il ruolo del riconoscimento biometrico del volto per ciò che attiene alle attività investigative negli aeroporti. Rimane comunque intatta invece la considerazione generale sulle potenzialità delle tecniche biometriche per il controllo del territorio. Gli esperimenti di videosorveglianza biometrica di Newham, [4] e controllo di manifestazioni sportive di Tampa in Florida (Superbowl del 2001) [5], rafforzano la convinzione di avere a disposizione uno strumento di controllo formidabile dalle piene potenzialità ancora da scoprire.

#### 3.3.3.2 Controllo dei documenti

Il termine "controllo dei documenti" (document control), intende una verifica della autenticità attraverso la validazione della fotografia all'interno del documento che viene comparata biometricamente con l'immagine del soggetto catturata attraverso una telecamera.
Anche se è evidente che la sola validazione della fotografia non è una condizione sufficiente per affermare la validità complessiva del documento, questa applicazione potrebbe risultare importante alla luce delle nuove procedure di immigrazione basate fortemente sul riconoscimento biometrico del volto.

#### 3.3.3.3 Ricerca dei duplicati

La ricerca dei duplicati è invece un interessante applicazione che prevede la comparazione su base biometrica delle immagini all'interno di un archivio alla ricerca di potenziali soggetti le cui fotografie, pur appartenendo allo stesso soggetto, sono dichiarate sotto più identità. In occasione di elezioni politiche in un paese del centro America il metodo sembra abbia permesso di scoprire numerosi duplicati e quindi potenziali brogli elettorali [6].

### 3.3.4 Il mercato

Il mercato del riconoscimento biometrico del volto è in potenziale incremento. Al di là delle applicazioni per l'accesso fisico e logico, settori nei quali la metodologia soffre di una forte concorrenza da parte di altre tecnologie, è nel settore governativo che si attende la maggiore diffusione.

In ambito governativo, le due aree di punta della biometria del volto sono quelle dei nuovi documenti personali e della sorveglianza.

I nuovi documenti di espatrio, in particolare, riporteranno al loro interno una fotografia digitalizzata secondo uno standard definito nel 2003 dall'ICAO ed è ragionevole ipotizzare che sarà installato un certo numero di impianti per il controllo biometrico del volto che, come è stato già messo in evidenza, compareranno nell'ambito delle procedure di frontiera, l'immagine dei soggetti con la fotografia riportata nel proprio documento.

Il delicato contesto internazionale inoltre spingerà, anche se con tutte le riserve espresse al paragrafo precedente, verso l'installazione di sistemi di sorveglianza in ambienti sensibili come aeroporti o stazioni. Al di là di tutte la valutazioni, già espresse, sulla reale efficienza di tali sistemi, la cautela è d'obbligo per ciò che attiene alle delicate intersezioni con la privacy.

### 3.3.5 Dimensioni del template ed elementi di costo [11]

| | |
|---|---|
| **Dimensioni del template** | Da circa 1 Kbyte dei sistemi bi-dimensionali a circa 10 Kbyte per i sistemi tridimensionali |
| **Costo del sensore** | Dalle centinaia di Euro, costo di una normale telecamera da connettere ad un personal computer per accesso logico alle migliaia di Euro per telecamere per "sorveglianza" |

*Tabella 3.3*

[11] Nel caso del riconoscimento biometrico del volto il vero elemento di costo è il software di riconoscimento che parte dalle centinaia di Euro per un sistema per l'accesso logico fino a cifre ingenti nel caso di sistemi per la sorveglianza

## 3.3.6 Approfondimenti

### 3.3.6.1 Il riconoscimento biometrico 3D del volto

A differenza di quelli per applicazioni bidimensionali (2D), i sensori dei sistemi di riconoscimento tridimensionale (3D) del volto non sono apparecchi standard anche se in realtà sono costruiti con parti quasi totalmente acquistabili sul mercato.
Rispetto alle 2D, le tecniche 3D introducono un ciclo in più che consiste nella ricostruzione della superficie del viso che rappresenta quindi il dato di base di partenza per le successive elaborazioni.
Esistono varie tecniche per ricostruire una superficie per punti in tre dimensioni. Tra le altre andrebbero citate :

- stereografia
- laser Scanner
- luce Strutturata

La stereografia fa uso di due video/foto camere la cui posizione relativa tra esse è fissa e nota e che focalizzano nello stesso punto. Gli algoritmi tendono ad individuare punti omologhi del viso estratti dalle due immagini acquisite del viso e con tecniche di triangolazione tentano di ricostruire la posizione nello spazio (3D) di tutti i punti della superficie visibile.
Questa tecnica consente ricostruzioni molto accurate ma ha bisogno di una grande potenza di calcolo e di conseguenza i tempi di elaborazione possono essere molto lunghi.
La cosiddetta tecnica "Laser Scanner" si basa invece sulla misura dei ritardi nella riflessione di un fascio di luce laser proiettato sul viso. L'entità del ritardo consente di acquisire l'informazione relativa alla "profondità" di ogni punto della superficie interessato dal fascio di luce. Anche in questo caso la ricostruzione è molto accurata ma, dal momento che il fascio di luce deve percorrere linearmente l'intera superficie del viso, i tempi di ricostruzioni 3D sono considerevoli considerando inoltre che, a valle del processo di acquisizione, per l'elaborazione sono richieste ingenti risorse computazionali.
Il metodo detto della "luce strutturata" utilizza un proiettore ed una videocamera la cui posizione relativa tra essi è fissa e focalizzati sul viso. Il proiettore proietta sul volto un pattern (una griglia) dalla forma nota. La griglia, deformata dalla superficie del viso, viene acquisita dalla telecamera ed analizzata con tecniche di triangolazioni geometriche in modo da ricostruire per punti la superficie del viso nello spazio. In questo caso la ricostruzione è meno accurata di quella relativa agli altri metodi citati ma, la velocità del processo, è sensibilmente più alta.
Dopo aver ricostruito la superficie 3D, come nel processo bidimensionale, inizia una fase di elaborazione (face detection) tesa a determinare se le immagini acquisite sono o meno quelle di un viso. A valle di tale processo sono estratte le caratteristiche biometriche (feature extraction).
A questo scopo il viso viene diviso in zone meno variabili con l'invecchiamento, le cui superfici sono più legate alla struttura ossea e in zone più variabili nel tempo che, nell'ambito del riconoscimento "pesano" ovviamente meno delle prime. In linea di massima si può affermare che più sofisticata è la tecnica usata e più dettagliata è la suddivisione del viso.
Su queste zone si effettuano misure lineari, di superfici e di volumi e si costruisce un vettore numerico che rappresenta la "firma biometrica" del volto.
Va infine citato che alcuni gruppi di ricercatori hanno provato ad "arricchire" le tecniche 2D con informazioni tridimensionali dando vita alle cosiddette immagini "pseudo-3D". Due metodi che portano ad apprezzabili benefici incrementali in termini di numero di informazioni sfruttabili consistono in:

- acquisizione, nella fase di enrollment, di sequenze multiple di foto prese in posizioni diverse del viso e tentando una ricostruzione tridimensionale con tecniche miste di stereografia off-line e reti neurali.
- uso della foto bidimensionale dell'enrollment, "spalmatura" della stessa su un modello tridimensionale generico pre-costruito e utilizzo della potenzialità della rotazione del modello per effettuare una migliore estrapolazione di dati.

Un semplice modo per distinguere le tecnologie 3D da quelle pseudo-3D consiste nel controllare gli apparecchi di acquisizione che, se normali videocamere, non possono che fare operare in un regime pseudo-3D .

#### 3.3.6.2 Le fasi del riconoscimento biometrico del volto

Il processo di riconoscimento biometrico del volto si articola in varie fasi:

- individuazione del volto (face detection) e segmentazione (segmentation)
- estrazione delle caratteristiche (feature extraction)
- riconoscimento (recognition)

La fase di individuazione è un prerequisito cruciale per un corretto riconoscimento del volto e rappresenta un compito ragionevolmente difficile nel caso di applicazioni all'esterno in condizioni di forte variabilità della luce e questa è una delle ragioni principali per cui il riconoscimento del volto è generalmente limitato alle applicazioni che si svolgono all'interno .
L'idea alla base dell'individuazione del volto è escludere tutte le informazioni non utili, cioè tutto quello che nell'immagine non è un volto. Ciò non è facile come può sembrare perché la differenza fra le regioni del volto e le altre regioni di una scena non sono sempre evidente. La cosa che realmente fa la differenza è che le regioni del volto presentano caratteristiche peculiari come due occhi uno affianco all'altro, due narici appena sotto e, ancora più in basso la bocca. Attraverso una complessa procedura di individuazione e raggruppamento di queste caratteristiche fondamentali è possibile individuare il volto (o i visi) all'interno di una scena che verranno isolati dal contesto attraverso un processo detto di "segmentazione".
L'estrazione delle caratteristiche del volto è la chiave per la fase di "riconoscimento" che avviene attraverso le classiche operazioni di calcolo della "distanza" matematica fra l'immagine digitalizzata e l'archivio delle immagini contenute in un archivio.

## 3.4 Geometria della mano

La geometria della mano si identifica praticamente con un solo prodotto commerciale ed è stata una delle prime tecniche biometriche ad essere sviluppata. Di conseguenza in tutto il mondo c'è un considerevole numero di lettori della geometria della mano che hanno dato prova delle proprie capacità in una vasta gamma di applicazioni [7].
A differenza delle impronte digitali o dell'iride, le caratteristiche della mano di un individuo non sono descrittive al punto da risultare uniche, quindi non possono essere utilizzate per l'identificazione di una persona, ma, allo stesso tempo, sono sufficientemente descrittive per essere impiegate ai fini della verifica di identità (1: 1).
Attualmente il metodo è implementato da un solo costruttore mentre un'altra ditta propone una "geometria delle due dita", descritta nella sezione approfondimenti alla fine del presente paragrafo.

### 3.4.1 Descrizione

Il principio di funzionamento della geometria della mano si basa sulla rilevazione delle caratteristiche geometriche di questa acquisite attraverso un apposito dispositivo di ripresa ad alta risoluzione. L'utente pone la mano su una base, aiutato da alcuni pioli che guidano ad un corretto posizionamento e da una serie di led che confermano il posizionamento corretto. I dispositivi di lettura, composti da una fotocamera, specchi e riflettori, acquisiscono e processano le immagini in bianco e nero mettendo in evidenza circa 90 diverse misure in termini di lunghezza, larghezza o spessore delle singole dita. Il metodo è in grado di tenere conto della presenza di anelli che modificano il profilo della mano ed aggiorna dinamicamente il template in funzione degli inevitabili cambiamenti della conformazione della mano dovuti al tempo o a fenomeni degenerativi osteoarticolari.

### 3.4.2 Punti di forza e debolezza

Il metodo biometrico della geometria della mano offre un buon compromesso tra prestazioni e facilità d'uso. Non può vantare le prestazioni nominali di altre tecnologie biometriche in termini di FAR e FRR ma, a differenza di tecniche più accurate, richiede meno cooperazione da parte dell'utente dando quindi luogo ad una certa omogeneità di prestazioni anche con categorie di utenti differenti. Essendo inoltre imperniato sull'uso di un sensore particolarmente robusto, il metodo risulta adatto alle applicazioni caratterizzate da un uso intensivo, come ad esempio quelle inerenti il controllo dell'accesso fisico e la rilevazione delle presenze nei luoghi di lavoro. Passando ai punti di debolezza andrebbe messo in evidenza che la biometria della mano non è applicabile nel caso di menomazioni o malformazioni significative della mano e che fattori ambientali, ad esempio basse temperature, possono condizionare il riconoscimento [12]. Il riconoscimento inoltre può essere alterato da una esposizione ad un forte luce diurna. Tra i maggiori svantaggi vanno ancora menzionati il costo dell'unità di acquisizione (intorno ai 1000 Euro), il suo ingombro e peso. Sarebbe quindi non appropriato proporre l'uso della geometria della mano nei casi in cui le dimensioni rappresentano un parametro importante come ad esempio l'uso su una scrivania, in prossimità di un personal computer. Una tabella riassuntiva dei punti di forza e debolezza è riportata di sotto.

| Pro | Contro |
|---|---|
| – Tecnologia consolidata<br>– Sensore robusto<br>– Dimensioni del template molto ridotte | – Costo<br>– Dimensione e peso notevoli<br>– Sensibilità a forte luce diurna |

*Tabella 3.4*

[12] Per ovviare a ciò si può ricorrere ad una resistenza che riscalda la superficie del sensore.

### 3.4.3 Campi di applicazione

I sensori per la geometria della mano vengono attualmente utilizzati in vari contesti e si sono rivelati particolarmente efficaci per applicazioni del tipo "time and attendance" cioè per il controllo delle presenze sui luoghi di lavoro.
Dal 1991, un sistema biometrico basato sulla geometria della mano è in funzione all'aeroporto di San Francisco [8] mentre in Canada e negli Stati Uniti, il riconoscimento della geometria della mano è usato in numerosi impianti nucleari
Andrebbe inoltre ricordato che per anni i lettori per la geometria della mano sono stati usati per espletare rapidamente le procedure di immigrazione negli Stati Uniti in conseguenza del programma "InsPass" [9]
Nel 1996, durante i giochi olimpici di Atlanta, il riconoscimento della geometria della mano è stato usato per identificare 150.000 tra atleti, staff e partecipanti. Il sistema è inoltre in funzione all'aeroporto di Tel Aviv [8] per i cosiddetti "frequent travellers".

### 3.4.4 Il mercato

Il mercato è praticamente monopolizzato da un unico fornitore che produce lettori dotati di tastiera per la digitazione di un PIN associato alla persona o di un lettore di smart card. Tale tecnica biometrica detiene circa l'11% del mercato (dato relativo al 2004, fonte IBG) e ben si presta ad essere impiegata in applicazioni biometriche multimodali relative a varchi fisici in combinazione con altre tecniche non invasive (es. riconoscimento del volto) raggiungendo alti livelli di accuratezza e, accoppiata con l'altra caratteristica, divenendo uno strumento valido anche per l'identificazione.

### 3.4.5 Dimensioni del template ed elementi di costo

| | |
|---|---|
| **Dimensioni del template** | Dai 9 byte del dispositivo più diffuso sul mercato alle poche decine di byte |
| **Costo del sensore** | Circa 1500 Euro cui, va aggiunto il costo di altri dispositivi (ad esempio, eventuale lettore di smart card) |

*Tabella 3.5*

### 3.4.6 Approfondimenti

#### 3.4.6.1 La geometria delle due dita

La geometria delle due dita si presenta come una variante della geometria della mano e, a differenza di quest'ultima, richiede il posizionamento di sole due dita nel lettore. Questa particolarità presenta alcuni vantaggi perché possono essere usate indifferentemente le dita della mano destra e sinistra e, in seconda analisi, la superficie di contatto con il sensore è minore ciò comportando, per gli utenti particolarmente sensibili al problema, una minore preoccupazione per problemi di igiene. Per una disamina dell'argomento, si veda l'approfondimento al punto successivo. Gli svantaggi più evidenti consistono in una bassa referenziabilità del prodotto, che ha oggettivamente una diffusione limitata rispetto alla geometria della mano e, soprattutto minori dati sulle applicazioni su larga scala, come quelle del tipo accesso fisico/controllo delle presenze che prevedono il controllo di migliaia di utenti.

#### 3.4.6.2 Alcune riflessioni sulla biometria "con contatto fisico"

Alcuni utenti manifestano motivi di preoccupazione per una potenziale possibilità di contrarre infezioni usando alcuni sensori il cui uso prevede un contatto con essi . Il discorso vale soprattutto per la geometria della mano che, fra i vari dispositivi biometrici, è quello che presenta la maggiore superficie di contatto. Come già messo in evidenza nell'ambito di progetti di ricerca comunitari, non si può ovviamente escludere che il contatto con la superficie del sensore non possa essere un veicolo di infezione ma, tale preoccupazione dovrebbe estendersi a tutti gli oggetti comunemente toccati quali maniglie o telefoni. Per tenere comunque conto di questi aspetti si possono comunque decidere cicli di pulizia della superficie del sensore in grado di minimizzare la possibilità (o meglio la percezione della possibilità) di contrarre una infezione. Nel caso di persistenza di forti perplessità, almeno per la geometria della mano, è possibile usare guanti aderenti di lattice che non inficiano il riconoscimento in attesa di una eventuale futura installazione, all'interno del sensore, di una sorgente UV in grado di abbattere in maniera quasi totale la possibilità di contaminazione.

## 3.5 Riconoscimento dell'iride

Il riconoscimento dell'iride può considerarsi una tecnologia biometrica emergente che, per le sue caratteristiche di sicurezza, si propone quale valida soluzione per gestire in modo sicuro l'identificazione di individui e la verifica di identità, in situazioni che necessitano di un grado di sicurezza molto elevato.

### 3.5.1 Descrizione

Il riconoscimento dell'iride consiste nell'analisi delle caratteristiche dell'anello colorato che circonda la pupilla e che rappresenta un identificatore biometrico particolarmente efficace. Le caratteristiche strutturali dell'iride umano sono molto complesse e comprendono uno strato epiteliale, non trasparente alla luce, alcuni muscoli che controllano l'apertura della pupilla, vasi sanguigni e uno strato di cellule pigmentali dette cromatofori, disposte in modo discontinuo secondo schemi diversi da individuo ad individuo, e diversi tra un occhio e l'altro anche per lo stesso individuo.

La struttura dell'iride è estremamente stabile nel tempo e rimane pressoché invariata, dai 10 mesi di età, per tutta la vita [10]. Dal punto di vista del funzionamento, la scansione dell'iride avviene mediante una video camera che riprende l'occhio da una distanza che va dai 10 ai 60 centimetri in funzione del tipo di sensore usato. Nonostante le dimensioni dell'iride varino in funzione dell'illuminazione ambientale (una forte luce fa restringere la pupilla e di conseguenza aumentare il raggio della corona dell'iride), un apposito algoritmo tiene conto di queste modifiche oltre che della copertura superiore ed inferiore dell'iride dovuta a palpebre parzialmente chiuse. L'uso di occhiali da vista può rendere la fase di registrazione più complessa ma questi stessi possono essere usati per l'autenticazione biometrica senza causare difficoltà [11].

### 3.5.2 Punti di forza e debolezza

La stabilità temporale della caratteristica biometrica è uno dei punti di forza del riconoscimento dell'iride che, grazie anche al numero di singolarità maggiore di quello di altre tecniche, presenta ottime prestazioni in termini di false accettazioni e rigetti.

L'accettazione da parte degli utenti è generalmente alta, grazie soprattutto alla mancanza di contatto con il sensore.
Tra i punti di debolezza, andrebbe citato che il riconoscimento dell'iride può essere, anche se in minima parte, inficiato da problemi dell'occhio (si veda § 3.5.6.1).
Alcuni utenti inoltre manifestano una certa preoccupazione per potenziali danni procurabili all'occhio (si veda il capitolo 6 sugli aspetti medici della biometria). In merito alla poca fondatezza tecnica la maggiore casa costruttrice della tecnologia fornisce una abbondante documentazione accettata a livello internazionali da molti Paesi (Olanda, USA, UK) che hanno in corso progetti stabili o sperimentazioni basate sul riconoscimento dell'iride.
Un elemento negativo che può restringere il campo di utilizzabilità di questa tecnologia è costituito dalla necessità di coinvolgere in modo significativo, anche se in modo non invasivo, l'utente nel processo di acquisizione. L'esperienza di applicazioni su larga scala ha comunque dimostrato che, con una assistenza iniziale mirata, l'utente apprende velocemente le modalità d'uso della tecnologia.
Per ciò che attiene ai costi del sensore, un tempo ragionevolmente elevati, essi sono in diminuzione e si attestano in una fascia di prezzo equiparata ad altri dispositivi di acquisizione biometrica di qualità
Una tabella riassuntiva dei punti di forza e debolezza è riportata di sotto

| Pro | Contro |
|---|---|
| – Tecnologia senza contatto fisico<br>– Alta accuratezza<br>– Velocità di ricerca in un archivio | – Necessità di una fase di apprendimento<br>– Costo medio-alto<br>– Non può funzionare in presenza di una forte illuminazione solare |

*Tabella 3.6*

## 3.5.3 Campi di applicazione

I campi di applicazione del riconoscimento dell'iride sono specializzati verso l'alta sicurezza e si vanno orientando verso il controllo dell' accesso ad aree ristrette e ai controlli di frontiera. Per ciò che attiene alle frontiere, numerosi scali aeroportuali hanno in esercizio applicazioni per l'espletamento automatizzato delle procedure come ad esempio il programma CANPASS-air in Canada [12] e l'Automated Border Crossing di Schipol (Olanda) [13]. Altre applicazioni riguardano l'accesso ad aree ristrette come sale server, o ambienti ospedaliere [14]. Altre applicazioni concernono l'accesso logico a dati medici sensibili [15].

## 3.5.4 Il mercato

Il mercato del riconoscimento dell'iride, valutato attorno al 9% di tutte le tecniche biometriche, è in questo momento praticamente monopolizzato da un unico costruttore e detentore di numerosi brevetti nel settore. Il riconoscimento dell'iride è fra l'altro, insieme con le impronte digitali, una delle tecniche biometriche ritenuta potenzialmente adatta per l'uso in alcuni documenti britannici [16].

### 3.5.5 Dimensioni del template ed elementi di costo

| | |
|---|---|
| **Dimensioni del template** | 512 byte, circa 300 nella nuova versione compressa |
| **Costo del sensore** | Dalle poche centinaia di Euro per un dispositivo per l'accesso logico, a circa una migliaia di euro per il sensore per accesso fisico. |

*Tabella 3.7*

### 3.5.6 Approfondimenti

#### 3.5.6.1 Riconoscimento dell'iride e fisiologia dell'occhio

Ogni tecnica biometrica è associata al problema della difficile gestione in caso di danneggiamento o mancanza della parte fisica utilizzata per l'autenticazione. Con particolare riferimento all'iride, il riconoscimento dell'iride può essere inficiato da alcune patologie dell'occhio come glaucoma o anche da operazioni chirurgiche. Con riferimento alla cataratta, un interessante studio mette in evidenza la correlazione fra mutamenti all'interno dell'occhio dovuti ad una operazione di cateratta e riconoscimento biometrico arrivando alla conclusione che, anche in presenza di alterazioni della struttura dell'iride dovuti all'operazione chirurgica, solo una piccola frazione di pazienti (circa 10%) è stata costretta a registrarsi di nuovo nel sistema (del resto, senza problemi). Una fonte infine riferisce di possibili alterazioni della struttura dell'iride in una piccola percentuale di pazienti, in seguito all'assunzione di particolari farmaci (prostaglandine e prostamidi) per il trattamento del glaucoma.

## 3.6 Riconoscimento biometrico della voce

Il riconoscimento biometrico della voce è considerato tecnicamente un ibrido tra biometria fisiologica e comportamentale, dal momento che l'emissione è determinata non solo dalla conformazione della gola e della laringe, ma anche da aspetti comportamentali dell'utente, quali ad esempio il proprio tono umorale. Come nel caso del riconoscimento biometrico del volto, anche nel caso della voce, alle applicazioni di tipo civile, orientate verso l'accesso fisico e logico, si affiancano quelle investigative. Il riconoscimento della voce infatti può essere effettuato senza la cooperazione da parte del soggetto interessato e, anche se la materia è di estrema complessità tecnica, la determinazione certa dell'identità di una voce è uno dei capisaldi su cui si basa la moderna attività investigativa.

### 3.6.1 Descrizione

Il riconoscimento biometrico della voce avviene attraverso l'uso di un microfono o dell'apparecchio telefonico stesso. Va evidenziato che l'uso del telefono, se da una parte aumenta la fruibilità della tecnologia, dall'altra rende il processo biometrico molto più complesso a causa della drastica riduzione di informazioni dovuta alla limitata banda destinata alla voce su linea telefonica. Nel caso di applicazioni di tipo cooperativo, la fase di enrollment consiste generalmente nella registrazione da parte dell'utente di una frase predefinita (ad esempio una sequenza di numeri) per un certo numero di volte. Il tempo per

l'enrollment è quindi normalmente più lungo di quello necessario per altre tecniche biometriche.

### 3.6.2 Punti di forza e di debolezza

Il vantaggio di non dovere approntare hardware specifici e di potere rendere più sicure le transazioni che si basano sull'uso del telefono, rappresentano i punti di forza di una tecnologia il cui livello medio di sicurezza offerto ne sconsiglia l'uso in applicazioni critiche. Tra gli svantaggi andrebbe citato che una qualità bassa del dispositivo di ingresso vocale e un rumore di fondo possono influenzare sensibilmente le prestazioni del sistema biometrico e, in aggiunta, come si è detto, la procedura di enrollment è spesso più complicata di quella da eseguire per altre tecniche biometriche. La eterogeneità dei microfoni usati per l'enrollment e l'autenticazione biometrica può rappresentare un'ulteriore causa di errore nel riconoscimento. Una tabella riassuntiva dei punti di forza e debolezza è riportata di sotto.

| Pro | Contro |
|---|---|
| – Tecnologia basata su un hardware di larga diffusione<br>– Possibilità | – Lunghi tempi di enrollment<br>– Dimensioni del template<br>– Sensibilità a rumori di fondo e |

*Tabella 3.8*

### 3.6.3 Le applicazioni

Al di là delle applicazioni investigative, l'uso più indicato per i sistemi di riconoscimento vocale è l'autenticazione degli utenti in applicazioni di medio/bassa sicurezza. Sono in fase prototipale applicazioni nelle quali il riconoscimento della voce è accoppiato ad altre tecniche biometriche (ad esempio volto e movimento delle labbra)

### 3.6.4 Il mercato

Sebbene l'attuale giro d'affari del riconoscimento della voce sia relativamente modesto, gli esperti ritengono che esso abbia un forte potenziale di crescita, incrementato dalla caratteristica di non necessitare di alcun sensore particolare (la maggioranza dei personal computer dispone già di un microfono). I settori nei quali si prevede un maggiore utilizzo sono il riconoscimento "forte" attraverso il telefono, per accedere a servizi finanziari o per ordini di acquisti a distanza.

### 3.6.5 Dimensioni del template ed elementi di costo[13]

| | |
|---|---|
| **Dimensioni del template** | Alcune migliaia di Kbyte |
| **Costo del sensore** | - |

*Tabella 3.9*

## 3.7 Riconoscimento biometrico della firma

La propria firma è ragionevolmente unica non solo dal punto di vista ma anche per una serie di caratteristiche, quali ad esempio la velocità di scrittura o i punti nei quali si esercita più pressione che appartengono alla sfera comportamentale e sono pressoché inimitabili. Se la firma non è apposta su un foglio di carta ma con una tavoletta elettronica oppure viene usata una particolare penna, è possibile trasformare in dati gli aspetti comportamentali. Il riconoscimento biometrico della firma gode di una certa popolarità negli ambienti bancari e finanziari in cui l'apposizione della firma è una prassi frequente e, senza richiedere un cambio delle abitudini da parte dell'utente o un particolare addestramento permette un considerevole incremento di sicurezza.

### 3.7.1 Descrizione

Il riconoscimento biometrico della firma valuta un considerevole numero di parametri tra cui:

- la velocità di scrittura;
- la pressione esercitata;
- l'angolo d'inclinazione della penna,
- l'accelerazione del movimento;
- il numero di volte che la penna viene sollevata dalla carta.

Dal punto di vista operativo, l'utente appone la propria firma con una penna speciale o su una tavoletta elettronica in grado di rivelare i parametri descritti che portano alla creazione di un template le cui dimensioni sono intorno ai 1500 byte.

### 3.7.2 Punti di forza e debolezza

Tra i vantaggi va annoverata la alta accettazione da parte degli utenti causata dal fatto che gli utenti sono abituati a ad apporre la propria firma e quindi non trovano una differenza significativa fra il metodo tradizionale di apposizione della firma e quello biometrico.

[13] Nel caso del riconoscimento biometrico del voce il vero elemento di costo è il software di riconoscimento che parte dalle centinaia di Euro.

La vulnerabilità del sistema è considerata relativamente bassa ed i dispositivi per l'acquisizione sono ragionevolmente poco costosi (da 100 a 1000 euro).
Gli svantaggi principali consistono soprattutto nella instabilità nel tempo del campione biometrico in quanto la maniera di apporre la propria firma può variare nel tempo. Una tabella riassuntiva dei punti di forza e debolezza è riportata di sotto.

| Pro | Contro |
|---|---|
| – Hardware poco costoso<br>– Buona accettabilità da parte degli utenti | – Instabilità temporale del campione<br>– Dimensioni del template<br>– Numero limitato di applicazioni |

*Tabella 3.10*

### 3.7.3 Applicazioni

Come già evidenziato l'applicazione più popolare del riconoscimento biometrico della firma è l'accertamento dell'identità nelle transazioni finanziarie.

### 3.7.4 Il mercato

Il mercato del riconoscimento della firma è strettamente connesso al mondo bancario e delle transazioni finanziarie.

### 3.7.5 Dimensioni del template ed elementi di costo

| | |
|---|---|
| **Dimensioni del template** | Circa 1500 Byte |
| **Costo del sensore** | Il costo di una tavoletta grafica si aggira intorno alle poche centinaia di euro. |

*Tabella 3.11*

## 3.8 Bibliografia/Riferimenti in rete

[1]. http://www.fbi.gov/hq/cjisd/iafis/efts70/section1.htm
[2]. D. Maltoni, D. Maio, A.K. Jain e S. Prabhakar, "Handbook of Fingerprint Recognition", Springer, 2003.
[3]. J.Ng and H.Cheung, "Dynamic Local Feature Analysis for Face Recognition", http://www.titanium-tech.com/download/DLFA.pdf, 2004
[4]. http://www.parliament.uk/post/pn165.pdf
[5]. http://www.theregister.co.uk/2001/02/07/feds_use_biometrics_against_super/

[6]. http://www.bioprivacy.org/Mexico.htm
[7]. http://homepage.ntlworld.com/avanti/handgeometry.html
[8]. http://www.securityworldhotel.com/webportal/swh/news/shownews.asp?type=6&id=22860
[9]. http://www.customs.gov/xp/cgov/travel/leavingarrivinginUS/immigrationRequirements/inspass.xml
[10]. http://www.lgiris.com/iris/irt.html
[11]. T. Mansfield, K. Gavin, D. Chandler, and J. Kane. CESG Contract X92A/4009309 Biometric Product Testing Final Report. Draft 0.6. Middlesex: National Physical Laboratory, 2001.
[12]. http://www.ccra-adrc.gc.ca/newsroom/factsheets/2002/sep/canpass-e.html
[13]. http://www.airport-technology.com/projects/schiphol/
[14]. http://www.healthdatamanagement.com/html/PortalStory.cfm?type=newprod&DID=9366
[15]. http://www.findbiometrics.com/Pages/HIPAA_articles/hipaa_3.html
[16]. http://www.homeoffice.gov.uk/docs2/feasibility_study031111_v2.pdf

*Capitolo 4*

# Scenari applicativi delle tecnologie biometriche

## 4.1 Premessa

Il presente capitolo descrive in maniera approfondita i più significativi campi di applicazione delle tecnologie biometriche con particolare riferimento alla Pubblica Amministrazione. Vengono quindi descritti i vari scenari relativi all'accesso fisico e logico e alla gestione dei nuovi documenti personali contenenti identificatori biometrici. Vengono infine descritte le applicazioni basate su soluzioni ibride che combinano tecnologie biometriche con tecnologie orientate alla identificazione sicura, con particolare riferimento all'utilizzo della firma digitale.

## 4.2 Applicazioni nella P.A. inerenti l'accesso fisico

La biometria può essere utilizzata per i sistemi di controllo degli accessi e la rilevazione di presenza in aree riservate, che necessitino di elevati livelli di sicurezza. E' possibile, infatti, abilitare o disabilitare l'accesso a determinate aree, su base sia individuale che temporale, subordinando l'accesso al risultato del confronto biometrico. Tale impiego, ovviamente, trova ampia applicabilità nel settore della PA, reso ancora più sensibile a tali tematiche dall'aumentata esigenza di sicurezza dovuta ai recenti tragici avvenimenti internazionali[14].
Rientrano nella sfera di interesse della PA i controlli dell'accesso fisico in:

- aeroporti, stazioni ferroviarie, porti, luoghi ad alta frequentazione
- sedi governative
- aree riservate all'interno di sedi governative

Le esigenze fondamentali sono quelle della semplificazione e del miglioramento della gestione degli accessi aumentando, al contempo, il livello della sicurezza. Una soluzione in grado di soddisfare entrambe le esigenze è quella dell'introduzione di sistemi di controllo (semi) automatico, o comunque presidiato.
L'utilizzo dei sistemi di controllo degli accessi porta ad un alto grado di sicurezza negli ambienti, consentendo di risalire in ogni momento all'informazione sulle presenze fisiche (chi sia presente, da quanto tempo e dove), permettendo sia di razionalizzare l'utilizzo del personale di sorveglianza, sia di ricostruire cronologicamente il "passaggio" degli utenti.

[14] Si veda la "*Declaration on combating terrorism*", del Consiglio Europeo, Bruxelles 25 marzo 2004, in seguito al tragico attentato di Madrid del 11 marzo 2004.

Il Consiglio Europeo, nella sezione dedicata al rafforzamento dei controlli alle frontiere e della sicurezza dei documenti, ha esplicitamente incoraggiato l'adozione della proposte della Commissione per l'inserimento di identificativi biometrici nei passaporti, nei Visti e nei Permessi di Soggiorno dell'UE.

È evidente come l'inserimento di elementi di riconoscimento univoci, quale gli identificativi biometrici, aggiunge valore e sicurezza a tali sistemi, consentendo un legame più stretto tra la singola sessione di accesso e l'individuo che ne è il protagonista.

### 4.2.1 Sedi governative

L'associazione delle tecniche biometriche con supporti di memoria trasportabili in grado di ospitare i dati biometrici e integrati in *card* o documenti elettronici affidate all'utente è riconosciuta come una valida soluzione per l'accesso fisico alle sedi governative.
La card può essere usata come un unico documento di identificazione aziendale per svariate funzioni (da cui la denominazione di carte multifunzionali o multiservizi) tra le quali la rilevazione presenze e l'accesso logico alla rete, al computer e alle applicazioni del sistema informativo.
Ad una generica sede governativa accedono generalmente impiegati dell'Amministrazione (appartenenti alla stessa sede e non), personale di altre pubbliche amministrazioni e visitatori esterni, provenienti da soggetti non governativi. Al fine di innalzare il livello di sicurezza degli accessi, ridurre le code ai varchi di accesso e concentrare la propria attenzione sulle categorie che presentano maggior criticità, una possibile razionalizzazione delle procedure di ingresso potrebbe essere del tipo:

- impiegati della sede: autenticazione attraverso la Carta di identificazione della Amministrazione (card multifunzionale);
- impiegati di altre sedi della stessa Amministrazione: simile al punto precedente;
- impiegati di altre Amministrazioni: autenticazione attraverso la Carta di identificazione della propria Amministrazione, nel caso di interoperabilità per le card ed i lettori preposti allo scopo. In caso contrario la categoria viene assimilata a quella dei visitatori esterni;
- visitatori esterni frequenti (società esterne cui sono stati affidati dei servizi e che prestano la loro opera nella sede per un periodo continuativo): rilascio di una apposita Carta di identificazione sottoposta a vincoli di validità nell'orario giornaliero;
- visitatori esterni temporanei: identificazione attraverso i documenti di identità e rilascio di una Carta di identificazione temporanea.

All'interno delle sedi governative esistono aree riservate cui debba accedere solo un ristretto gruppo di tutti gli individui autorizzati all'accesso. L'accesso a tali aree sensibili della sede è trattato nel prossimo paragrafo

#### 4.2.1.1 Aree riservate all'interno di sedi governative

All'interno delle sedi pubbliche esistono aree libere cui tutti i visitatori autorizzati all'ingresso possono accedere, ed aree riservate solo ad alcune persone abilitate. Per la gestione di tali aree occorre prevedere dei meccanismi di assegnazione (e controllo) di diversi livelli di autorizzazione e privilegi.
Tali aree consistono tipicamente in:

- uffici di gabinetto di un ministero o di un organo di governo locale;
- sale server, contenenti apparati con applicazioni critiche e/o informazioni riservate;
- aree o archivi che contengono le copie fisiche di documenti o dati riservati o valori;

- sale operative strategiche per il controllo, la gestione e la comunicazione con i diversi livelli di comando ed il personale "in campo", il supporto alle decisioni (es sale operative delle Questure);
- sale con apparati critici di fornitura servizi (telecomunicazioni, generatori di energia o centrali elettriche).

Tali aree dovrebbero essere protette con livelli di sicurezza più elevati che nel caso del generale controllo dell'accesso fisico dei dipendenti. E' opportuno quindi ricorrere a sistemi biometrici di alta sicurezza (si veda il capitolo 3) o ricorrere a soluzioni multibiometriche o tecnologie ibride illustrate nel prosieguo del presente capitolo.

## 4.3 Applicazioni nella P.A. relative all'accesso logico

Un sistema di autenticazione basato su identificativi biometrici trova particolare applicabilità in tutte quelle transazioni per le quali sia possibile accedere alle informazioni e ai servizi forniti da un sistema informativo. In tali contesti può essere opportuna una verifica certa dell'identità dell'operatore e del livello dei suoi privilegi.
Tutte le transazioni nel senso specificato sono legate all'identità del soggetto che tenta di effettuarle e alla legittimità dei diritti posseduti da tale identità alla "fruizione" del servizio o della informazione.
Quanto descritto riguarda il cosiddetto accesso logico ai sistemi informativi.
Un particolare contesto è sicuramente quello dalla P.A., ove l'utilizzo di applicativi del tipo specificato riguarda sia i dipendenti della stessa P.A., sia i cittadini per le applicazioni relative ai servizi di E-Government. In tale ambito può essere opportuno un riconoscimento certo e univoco dell'individuo, con procedure "semplici" e al contempo sicure, da effettuarsi prima di consentirgli l'accesso ad informazioni, o ad applicativi e servizi che rivestono un particolare livello di criticità.
Alla luce di quanto descritto nelle sezioni precedenti, appare naturale la valutazione dell'opportunità di applicare le tecnologie biometriche ai sistemi di controllo degli accessi logici della P.A., svincolando l'utente dalla necessità di utilizzare e conservare appropriatamente "PIN" o oggetti in suo possesso e scongiurando la possibilità di smarrimento o furto.
Il riconoscimento biometrico per la concessione di autorizzazioni all'accesso logico può essere utilizzato, ad esempio, per il "single sign on" o per l'apposizione della firma digitale.
Particolare rilievo riveste l'applicabilità di tale tecnologia per l'erogazione di servizi sulla base di carte o documenti di identificazione contenenti dati biometrici come la Carta d'Identità Elettronica (C.I.E.), il Permesso di Soggiorno Elettronico (P.S.E.), la Carta Multiservizi della Difesa (C.M.D).

### 4.3.1 Accesso ai sistemi informatici

I controlli per l'accesso logico devono verificare l'accesso alle risorse di sistema ed ai dati, al fine di garantire il controllo delle informazioni che gli utenti possono utilizzare, dei programmi che possono eseguire e delle modifiche che possono apportare.

Il controllo degli accessi logici è strettamente legato all'autenticazione, che è il processo attraverso cui un utente dimostra l'autenticità dell'identificativo dichiarato nel tentativo di accesso.
La necessità di rendere più sicuro l'accesso logico ai sistemi informativi, unita alla disponibilità di nuove e più affidabili tecnologie di riconoscimento ed autenticazione degli utenti, impone ai referenti informatici ed agli amministratori di sistema di ripensare il modo in cui oggi, all'interno della propria amministrazione, viene effettuata l'autenticazione degli utenti (Logon), al sistema operativo ed alle applicazioni. Appare ormai indifferibile, in special modo per le Pubbliche Amministrazioni, l'uso di strumenti in grado di contrastare efficacemente i tentativi di accesso fraudolento alle risorse informatiche.

Il primo gennaio 2004 e' entrato in vigore il Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", che abroga e sostituisce la precedente legge 675/1996 sulla Privacy e i decreti successivi, ed introduce novità rilevanti in termini di misure di sicurezza "minime" da adottare in ogni azienda ed amministrazione che tratta dati.
Riguardo alle misure di sicurezza a protezione dei dati (art. 31), in caso di trattamento elettronico, prevede l'*autenticazione*, cioè l'*insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità* e l'*autorizzazione*, fase ulteriore e distinta, che concede o no accesso a definite categorie di dati (art. 34, all. B, cosiddetto "disciplinare tecnico"). È credenziale d'autenticazione anche una caratteristica biometrica dell'incaricato, eventualmente associata ad un identificativo tradizionale (codice o *password*). È quindi da considerarsi autenticazione ex D.Lgs. 196/2003 la verifica d'identità basata su identificativi biometrici.

### 4.3.2 Autenticazione biometrica

La trasformazione dei servizi della pubblica amministrazione in servizi *on-line*, che è l'obiettivo principale dei progetti di *E-government* avviati, richiede modalità di accesso sicure, facili e utilizzabili per i servizi di tutte le amministrazioni.
Il tradizionale processo di autenticazione basato su *Username* e *Password* può essere agevolmente integrato, se non del tutto sostituito, con sistemi di autenticazione robusta basati su tecniche che offrono un elevato livello di affidabilità e sicurezza. Inoltre, l'impiego di questi meccanismi di autenticazione risulta maggiormente semplice ed intuitivo per l'utente finale, che non è più costretto a ricordare complicate *Password* (magari aggiornate frequentemente) per accedere alla postazione di lavoro ed alle applicazioni.
L'autenticazione con dispositivi biometrici presenta alcune differenze con i sistemi di autenticazione classici:

- mentre i sistemi tradizionali consentono di verificare l'identità in modo indiretto, l'autenticazione biometrica consente di stabilire direttamente, dunque con maggiori garanzie, l'identità del soggetto che richiede un determinato servizio informatico;
- i sistemi di autenticazione tradizionali si basano cu credenziali che possono essere modificate dinamicamente, mentre quelli biometrici utilizzano informazioni stabilmente legate all'individuo, dunque non modificabili.

Quest'ultima considerazione evidenzia come nei sistemi di autenticazione biometrici sia particolarmente importante curare la segretezza dei dati di riferimento.

Le maggiori garanzie si hanno quando l'identificatore biometrico di riferimento è registrato su un supporto di memoria sicuro e trasportabile, quindi rilasciato all'utente e da questi custodito.
Un ulteriore elemento di garanzia è la possibilità di evitare la memorizzazione del campione biometrico grezzo, registrando solo il template estratto da esso, che costituisce un formato da cui non è possibile risalire al dato di partenza, così come già sottolineato in precedenza..
Si osserva comunque che soluzioni di autenticazione basate solo sull'identificatore biometrico, difficilmente conseguono un effettivo innalzamento del livello di sicurezza logica se l'architettura prevede che l'informazione biometrica sia trasferita in rete per consentire la verifica delle credenziali presso i diversi punti di accesso ai sistemi.
E' pertanto necessario prevedere l'integrazione dei sistemi di riconoscimento biometrico con l'infrastruttura di sicurezza dei sistemi informativi ed, eventualmente, con un sistema integrato di gestione delle utenze (*Identity Management*).

### 4.3.3 Gestione delle utenze e dispositivi biometrici

L'obiettivo della generica Pubblica Amministrazione è fornire servizi sia ai propri impiegati (es. via Intranet) sia ai cittadini (es. via Internet) o anche particolari categorie di professionisti. In ogni caso il sistema informativo dovrà fornire servizi ad un numero elevato di utenti eterogenei per caratteristiche e privilegi di accesso.
Per gestire efficacemente un'utenza così disomogenea e numerosa, il sistema informativo dovrebbe essere dotato di un sistema integrato di gestione delle utenze.
Gli elementi tipici di un sistema di gestione delle utenze sono:

- un servizio di *directory* basato su protocolli standard, nel quale sono censiti tutti gli utenti ed i gruppi, le rispettive credenziali e le caratteristiche significative ai fini della sicurezza logica.
- un servizio di autenticazione centralizzato (cosiddetto *Single Sign On*) che consenta agli utenti di autenticarsi una singola volta verso il sistema, che poi avrà il compito di "propagare" le credenziali dell'utente verso tutte le applicazioni alle quali abbia accesso.

Un sistema integrato di gestione delle utenze può sfruttare al meglio le potenzialità dei dispositivi biometrici in quanto permette di realizzare i necessari controlli di sicurezza senza propagare le credenziali di tipo biometrico.
In soluzioni di questo tipo i dati biometrici sono infatti utilizzati esclusivamente per l'operazione di *Single Sign On* e dunque possono risiedere su dispositivi protetti. A seguito dell'autenticazione locale, il sistema di *Single Sign On* genererà delle nuove credenziali (chiavi segrete o certificati digitali) che saranno trasmesse in modo sicuro tra i diversi nodi elaborativi per la verifica dei privilegi dell'utente.
La corretta integrazione delle tecnologie di riconoscimento biometrico con un sistema di autenticazione avente le caratteristiche descritte, possibilmente, con una PKI (*Public Key Infrastructure*) consente:

- agli amministratori di sistema di gestire centralmente le risorse e le relative politiche di accesso, garantendo maggior sicurezza e riservatezza dei dati;
- agli utenti finali di effettuare, in modo più rapido e intuitivo, un Logon unico al sistema ed alle applicazioni, e fruire di nuovi servizi.

Occorre sottolineare l'importanza di realizzare sistemi di autenticazione con le caratteristiche menzionate, che siano ottenuti dall'integrazione di infrastrutture standard di Identity Management e di PKI, con sistemi biometrici aventi caratteristiche di interoperabilità.

### 4.3.4 Biometria ed identità federata

Lo sviluppo e la diffusione di Internet e delle sue diverse connotazioni come le Intranet e le Extranet, ha portato ad una crescita delle applicazioni basate su logica web e ad un'evoluzione delle applicazioni esistenti dai modelli tradizionali ai modelli web. In questo contesto la Pubblica Amministrazione è protagonista con numerose applicazioni che sfruttano il modello web per offrire servizi ai cittadini, alle imprese, alle diverse Amministrazioni.
L'esigenza di poter disporre sempre delle credenziali di autenticazione, unita a quelle che obbligano l'utente ad essere fisicamente presente durante la fase di autenticazione, o in quelle in cui occorra verificare la sua reale identità, danno rilievo all'integrazione dei sistemi di riconoscimento biometrico come strumento di autenticazione. La biometria, inoltre, può essere l'elemento da integrare nei sistemi di tipo *Single Sign On*, perché capace di rendere maggiormente sicura la unica fase di autenticazione prevista da un tale sistema.
L'opportunità di assicurare adeguata sicurezza ai sistemi di autenticazione di tipo *Single Sign On* sul Web, e la necessità per le Amministrazioni di estendere l'utilizzo delle applicazioni ad altri soggetti (amministrazioni centrali e/o locali, aziende private), introduce il cosiddetto modello dell'Identità Federata.
In tale scenario, le diverse Amministrazioni, o le Aziende ad esse collegate, sono in grado di offrire servizi personalizzati per l'utente, delegando ad una delle altre entità coinvolte la fase di autenticazione. Attraverso questo modello, una delle entità/Amministrazioni si occupa della fase di autenticazione. L'utente, una volta autenticato, viene diretto su un'altra entità/Amministrazione, senza che questa debba nuovamente autenticare l'utente, fidandosi della fase di autenticazione avvenuta in precedenza.
In un tale contesto, gli elevati requisiti di sicurezza per la prima fase di autenticazione, possono rendere opportuno l'impiego della biometria congiunto a quello dei sistemi basati su password o certificati (sistemi ibridi).
Le istituzioni coinvolte, in tal modo, possono offrire all'utente servizi caratterizzati da criteri di sicurezza elevati proprio perché la fase Logon unico di un sistema di autenticazione di tipo *Single Sign On* avviene con caratteristiche di elevata sicurezza.
È quindi evidente la necessità di un percorso di autenticazione che identifichi in maniera certa l'utente finale e la possibilità offerta in tal senso dall'integrazione di sistemi biometrici. È proprio tale possibilità a rendere la biometria un elemento strategico negli scenari di identità federata.

## 4.4 Documenti di identificazione

La possibilità di associare in modo certo una persona fisica ad un supporto elettronico contenente dati anagrafici e biometrici, conduce direttamente alla possibilità di produrre i cosiddetti documenti di identificazione elettronici contenenti il supporto di memorizzazione elettronico nella parte cartacea o nel supporto plastico di un tradizionale documento di identità.
L'identificatore biometrico, memorizzato all'interno di un supporto elettronico integrato in qualche modo nel supporto cartaceo utilizzato nell'ambito dei documenti di identificazione viene confrontato con quello esibito dal soggetto.
La procedura di acquisizione dell'identificatore biometrico del titolare avviene nell'ambito delle procedure propedeutiche alla emissione del documento elettronico. Dopo aver acquisito il dato biometrico rilasciato all'atto della richiesta del documento, il personale preposto, in osservanza al quadro legislativo corrente, esegue tutti i controlli necessari sia alla attestazione

della identità del richiedente il documento, sia all'accertamento dei requisiti necessari al suo rilascio (es. diritto all'espatrio nel caso di passaporto). All'esito positivo degli accertamenti, il documento può essere personalizzato, legando in modo indissolubile il dato anagrafico del richiedente, cioè la sua identità, al dato biometrico.
Dopo il rilascio, tutte le operazioni relative ai controlli che l'autorità deve effettuare durante l'utilizzo del documento possono essere operazioni di verifica dell'identità (confronti uno-a-uno) tra il dato biometrico registrato nel supporto elettronico del documento e il campione biometrico acquisito direttamente dal portatore del documento stesso.
Occorre tuttavia rilevare come l'inserimento degli identificativi biometrici in un supporto elettronico integrato di un documento, non garantisce da solo che esso sia un regolare documento legittimamente emesso dall'autorità competente, né che il soggetto abbia i necessari requisiti.
Per accrescere la sicurezza dell'intero ciclo di vita del documento, dalla produzione, al controllo dei requisiti del richiedente, alla personalizzazione, fino alla emissione e all'utilizzo da parte del titolare, l'inserimento di identificativi biometrici non può assolutamente prescindere dalla previsione di una infrastruttura che garantisca un efficace meccanismo di gestione di firme digitali (e delle chiavi ad essa relative).
L'applicazione al contenuto del documento della firma digitale da parte dell'autorità che lo emette, è intrinsecamente legata agli stessi dati. Ciò significa che a dati diversi, e quindi a documenti diversi, corrispondono firme digitali diverse. Nonostante il meccanismo di generazione della firma digitale, quindi, sia ovviamente applicabile a tutti i documenti emessi dalla stessa autorità, non è possibile trasferire una firma da un documento ad un altro. Nemmeno disponendo di un documento elettronico valido è possibile realizzarne uno falso e, anche potendo falsificare sia il supporto cartaceo tradizionale (cosa oggi ancora ipoteticamente possibile), sia il supporto elettronico, sia il contenuto, non è possibile certificare lo stesso con la firma digitale.
L'autorità di controllo dei documenti, grazie alla firma digitale del contenuto del documento con la chiave privata dell'autorità emittente, è in grado con estrema certezza, di operare la verifica della provenienza del documento e dell'integrità dei dati in esso contenuti, attraverso la chiave pubblica dell'autorità emittente.
È solo grazie a tale certezza che ha senso effettuare confronti biometrici tra i dati forniti dal portatore e quelli contenuti nel documento. Altrimenti si potrebbero avere confronti positivi di dati aventi però provenienza illecita.
È quindi evidente come i documenti di identità contenenti supporti elettronici per la memorizzazione di dati anagrafici e biometrici, contengano elementi aggiuntivi di protezione da falsificazioni e contraffazioni, in grado di elevare enormemente il livello di sicurezza.
Per ciò che concerne il contesto normativo, nazionale e comunitario, che interessa l'inserimento di identificativi biometrici nei documenti di identità, nei DPR 445/2000, TU in materia di documentazione amministrativa, modificato dal D.Lgs. 10/2002, attuativo della Dir. 1999/93/CE sulle firme elettroniche, e DPR 137/2003, si trovano le definizioni di: firma

digitale e documento informatico (L. 59/97 e provvedimenti attuativi della delega), e dei documenti d'identità, quali la c.d. Carta d'Identità Elettronica, C.I.E., istituita con L. 127/97[15]. Conforme alla C.I.E., agli standard comunitari[16], e alla L. 128/2002 c.d. Fini-Bossi, il Permesso di Soggiorno Elettronico, documento contenente anche dati biometrici (impronta digitale).
I documenti di identità elettronici, quindi, consentono una maggiore sicurezza sia per gli accessi fisici sia per gli accessi logici ai sistemi informativi di E-Government.

**La situazione nazionale**

I documenti elettronici di identificazione vigenti, emessi e circolanti sul territorio, che contengono uno o più elementi biometrici sono:

- Carta d'Identità Elettronica (CIE)
- Carta Multiservizi della Difesa (CMD)

In via di definizione e realizzazione:

- Permesso di Soggiorno Elettronico (PSE)
- Passaporto Elettronico (E-Passport)

Dal punto di vista dell'uso della biometria questo insieme di documenti si presenta in forma omogenea, in quanto l'identificatore biometrico comune utilizzato per tutti è costituito dall'impronta digitale, alla quale deve essere aggiunta, nel caso della CIE e del Passaporto Elettronico, anche la fotografia del volto del titolare in formato digitale.
Il formato di memorizzazione sui vari documenti elettronici dell'elemento biometrico è, nella fase attuale, in corso di standardizzazione. La tendenza consolidata a livello internazionale consiste nell'adozione delle indicazioni e degli standard di riferimento che pervengono dall'ICAO (*International Civil Aviation Organization*), organizzazione particolarmente accreditata su questo tema,
Come rilevato in precedenza, l'acquisizione dell'impronta digitale e della fotografia, per tutti i quattro documenti elettronici CIE, PSE, CMD, E-Passport, avviene alla presenza di un funzionario accreditato appartenente all'Amministrazione Pubblica competente al rilascio (dell'anagrafe del comune emettitore nel caso della CIE, del Ministero della Difesa nel caso della CMD, della Polizia di Stato o del Ministero degli Affari Esteri per il passaporto elettronico, dell'UTG nel caso del PSE), ed è regolata (o dovrà esserlo prima dell'entrata in vigore).
Il Servizio Polizia Scientifica della Polizia di Stato ha storicamente maturato una significativa esperienza nel trattamento delle impronte digitali anche attraverso la gestione del sistema di riconoscimento AFIS (*Automated Fingerprint Identification System*) e la competenza tecnica acquisita è alla base della realizzazione e gestione dei documenti di identificazione biometrici a livello nazionale.

[15] Decreto Ministeriale 19 luglio 2000, come modificato con DM 14.5.2003 e DM 6.11.2003, "Regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici"

[16] "Proposte di Reg. a modifica Regg. (CE) 1683/95 e 1030/2002, istitutivi di modelli uniformi per visti e permessi di soggiorno", Bruxelles, 24 Sett. 2003.

Il Ministero dell'Interno, soprattutto grazie alla competenza istituzionale in materia, ha definito, e sta definendo, le specifiche di realizzazione della CIE, del PSE e, di concerto con il Ministero degli Affari Esteri, del passaporto elettronico dello Stato Italiano, contribuendo all'allineamento del quadro normativo di riferimento e alla precisazione dei contesti organizzativo e tecnologico (come nel caso della CIE dove il Ministero dell'Interno detiene anche il controllo della fase di realizzazione del progetto). Elemento fondamentale nella realizzazione e nella gestione dei diversi tipi di documenti elettronici è costituito dalla loro compatibilità in termini di trattamento dell'identificativo biometrico e delle infrastrutture necessarie alla gestione del ciclo di vita di ciascun documento.

## 4.5 Firma digitale e biometria

### 4.5.1 Biometria e dispositivi sicuri

Intendiamo qui per dispositivi sicuri, componenti elettronici hardware e software, che consentono di garantire l'accesso controllato a informazioni riservate, sotto il controllo del titolare del dispositivo. Tra i dispositivi sicuri più noti possiamo annoverare le smart card, i token crittografici USB, le card a memoria ottica e gli iButton.
La combinazione di dispositivo sicuro e componenti biometriche, comporta in generale un sensibile innalzamento del livello di sicurezza dell'applicazione dal momento che l'identificatore biometrico viene registrato nel dispositivo stesso e quindi è nella sola disponibilità dell'utente.
Un ulteriore vantaggio della soluzione ibrida riguarda la privacy dell'utente; anche se, (come sarà evidenziato nel capitolo 5, dedicato agli aspetti legali), di solito nelle applicazioni non viene quasi mai registrata l'immagine grezza della caratteristica biometrica ma il template di essa, assai meno significativo dal punto di vista della privacy, la memorizzazione di esso nel dispositivo, in possesso dell'individuo tranquillizza l'utente.
Per contro, a fronte della maggior sicurezza, la soluzione ibrida comporta un incremento di costi, sia diretti che non.
Vanno intesi per costi diretti quelli relativi al costo del dispositivo stesso e dell'eventuale componente di lettura (lettore di smart card per esempio). I costi indiretti sono invece i costi gestionali, legati alla gestione del dispositivo:

- gestione dei PIN e PUK;
- supporto agli utenti in caso di:
    - non disponibilità temporanea del dispositivo;
    - dimenticanza del PIN o suo blocco;
    - sostituzione del token in caso di smarrimento;

sono tutti questi i costi, spesso non evidenti, che crescono esponenzialmente al crescere degli utenti e che la soluzione biometrica pura non contempla.

### 4.5.2 Biometria e PKI

Per PKI (Public Key Infrastructure) si intende il complesso di programmi, procedure e servizi necessari per attivare un sistema di cifratura asimmetrica, firma digitale, certificati digitali, in applicazioni di rete. L'attore principale in tale sistema è l'Autorità di Certificazione

(Certification Authority) che emette i certificati digitali che risiedono in un dispositivo sicuro che anche genera al suo interno la coppia di chiavi e ne mantiene protetta quella privata.
Esempi di applicazioni in ambiente PKI sono la firma digitale, le VPN (Virtual Private Network) e la posta elettronica "sicura". Un sistema PKI, pur altamente sicuro, ha un evidente punto debole: la necessità di digitare un PIN per attivare l'uso del dispositivo con la possibilità che la sottrazione o l'individuazione di questo PIN renda il dispositivo utilizzabile da altri. La sostituzione (o l'aggiunta) del PIN con l'autenticazione biometrica risolve egregiamente questa criticità insita nel token che, in tal caso, potrà essere utilizzato solo dal suo proprietario. Inoltre, se l'autenticazione viene effettuata all'interno del token stesso (vedi nel seguito il concetto di match-on-card), viene meno anche il rischio di intercettazione del PIN.
Il numero di applicazioni in via di diffusione presso la pubblica amministrazione che utilizzano questi meccanismi sta crescendo.
Nel medio periodo miglioreranno i livelli di standardizzazione degli algoritmi di verifica e quindi il livello di interoperabilità tra produttori diversi.

### 4.5.3 L'identificazione del sottoscrittore

La normativa italiana sulla firma digitale prevede, nel caso specifico, che "il dispositivo sicuro di firma deve poter essere attivato esclusivamente dal titolare prima di procedere alla generazione della firma".
Per il rispetto di questa norma sono possibili due modalità funzionali:
- verifica di una cosa che il sottoscrittore conosce;
- verifica di una caratteristica biometrica del sottoscrittore.

Il primo metodo è quello classico della digitazione di un PIN; il secondo richiede la presentazione di dati inerenti alla fisiologia del sottoscrittore stesso.
Relativamente a questa seconda possibilità verrà illustrato nel seguito il possibile utilizzo di una smart card con controllo di accesso biometrico.

#### 4.5.3.1 L'identificatore biometrico come PIN

L'uso dell'identificatore biometrico come PIN prevede:

- la procedura di memorizzazione dei dati, avendo preventivamente definito quali dati devono essere salvati e le modalità di memorizzazione all'interno della smart card;

- la disponibilità del sensore di rilevamento dei dati biometrici che rilevi questi in fase di sottoscrizione e li invii alla smart card per il confronto.

In quanto alla procedura al punto 1 è indispensabile definire alcuni standard al fine di garantire l'interoperabilità tra i vari ambienti.
Tali standard sono definiti nella serie ISO 7816 e in particolare nel documento numero 4 "Interindustry commands for interchange" e nel documento numero 8 "Security related interindustry commands". Nel documento ISO 7816-11 "Personal verification through biometric methods" sono state inserite delle estensioni che consentono di supportare la verifica delle chiavi biometriche e una serie di funzioni indispensabili per l'interazione con l'utente.

Le strutture da utilizzare sono definite in ISO 7816-11 in conformità al Common Biometric Exchange File Format.
Per le esigenze di interoperabilità, bisogna anche standardizzare l'interfacciamento dei dati biometrici di verifica. In particolare devono essere standardizzati la codifica e la struttura di tali dati. Sia il NIST che l'ANSI hanno emesso documenti in tal senso.
Trattandosi di dispositivi sicuri per la creazione della firma, ovviamente saranno necessarie anche valutazioni e certificazioni di sicurezza conformi all'ITSEC o ai Common Criteria. Per quest'ultima operazione dovranno essere definiti uno o più "Protection Profile".
Applicate tutte queste regole è possibile, procedere alla acquisizione dell'identificatore biometrico da inviare per la verifica alla smart card. Questa tecnica viene definita "match-on-card" e garantisce un elevato grado di sicurezza e di protezione dei dati personali in quanto non esistono memorizzazioni dell'identificatore biometrico al di fuori della smart card o, in generale, del dispositivo sicuro.
Se la verifica è positiva sono possibili tutte le operazioni successive allo sblocco della carta, come l'autenticazione forte tramite TLS/SSL o la firma digitale.
I processi per standardizzare le funzionalità al fine di garantire l'interoperabilità non sono brevi, né semplici. In Italia la biometria dell'impronta viene utilizzata per l'abilitazione all'utilizzo della smart card per la firma digitale e per il voto elettronico (Progetto e-poll).
Ciò significa che esistono apparati funzionanti e affidabili e, ogni volta che il problema dell'interoperabilità non è critico, come non lo è stato per il voto elettronico, si può procedere utilizzando l'offerta di mercato. Nel caso del "match-on-card" vengono utilizzati ancora dei template e algoritmi proprietari, ma si auspica che in tempi ragionevoli si potrà disporre di algoritmi conformi a quanto stabilito in ISO/IEC 7816-11.
In conclusione, deve essere considerato il fatto che il "match-on-card" è ancora in fase di assestamento tecnologico e può risentire della scarsa potenza di calcolo di alcune tipologie di dispositivi.
Sarà quindi in base alle esigenze di sicurezza scaturite dall'analisi del rischio che si dovranno valutare quali siano le soluzioni più opportune tra quelle ibride disponibili sul marcato. Il paragrafo seguente delinea uno scenario generale sull'argomento.

### 4.5.4 Scenario delle soluzioni ibride

La soluzione ibrida, biometria e dispositivo sicuro, può essere attuata con diverse modalità, derivanti dalle diverse possibilità di registrazione del template e dal conseguente confronto dello stesso. Ovviamente le diverse soluzioni comportano livelli di sicurezza e di privacy differenti. Per quest'ultimo aspetto si rimanda al cap.5.
Il template può essere registrato:

- nel PC locale
- nel server
- nel dispositivo di autenticazione
- nel dispositivo sicuro

Analogamente il processo di confronto tra template registrato e template rilevato può essere eseguito dagli stessi dispositivi, in diverse combinazioni.
Senza soffermarci ad analizzare tutte le possibili combinazioni, possiamo fare le seguenti valutazioni:
PC locale: l'utente ha un diretto controllo del template registrato nel suo PC; ma il PC è spesso non sicuro e soggetto ad attacchi che possono permettere l'accesso ai dati in esso

contenuti. Inoltre la mobilità diventa un problema: l'utente può solo autenticarsi nei PC dove si sia precedentemente registrato.
Server: la sicurezza della soluzione è fortemente dipendente dalla sicurezza del server stesso che comunque, è generalmente molto più alta di un singolo PC; l'amministratore controlla eventuali attacchi al data base degli utenti e al sistema nel suo complesso. Peraltro gli utenti possono non gradire che i loro template vengano registrati fuori dal loro controllo diretto. Inoltre la trasmissione del dato biometrico dal lettore (collegato al PC locale) al server richiede una connessione sicura (cifrata); ciò vale certamente quando il server è in Internet, ma anche in rete locale.
Dispositivo di autenticazione: rientrano in questa tipologia, ad esempio, i dischi esterni o le memorie flash dotate di rilevatore biometrico e dispositivi per il controllo dell'accesso fisico (apertura porte, varchi, ecc..). Nel caso l'identificatore biometrico e il processore per il confronto risiedano nello stesso dispositivo la sicurezza è massima ed il dispositivo (e quindi l'identificatore biometrico) è sotto il controllo dell'utente stesso. Diverso il caso in cui il confronto venga effettuato dal dispositivo ma l'identificatore biometrico sta in una card, anche di prossimità, come avviene in alcuni sistemi di controllo di accesso fisico. In tal caso va protetto il trasferimento dell'identificatore biometrico dal token al dispositivo, specie quando avvenga in modalità *contactless*.
Token: la registrazione dell'identificatore biometrico nel token riduce i problemi legati alla privacy ed alla mobilità dell'utente che porta con sè il suo token di autenticazione biometrica. Se però l'autenticazione avviene nel PC o nel server, la necessità di una infrastruttura protetta risulta maggiore, in quanto viene trasmesso oltre all'immagine anche il template registrato. La soluzione ideale è allora quella di eseguire nel token stesso l'autenticazione (match-on-card) perchè in questo caso il template rimane sempre all'interno del token e non vengono digitati PIN. La soluzione è attivabile in ambiente PKI senza la necessità di particolari infrastrutture di sicurezza; il token diventa uno strumento personale, vincolato alla presenza fisica del suo proprietario.
Esistono ancora una serie di problemi di interoperabilità, ma l'industria sta lavorando alacremente in questo settore e sono già disponibili numerose apparecchiature dotate di adeguata affidabilità.
Sono inoltre disponibili come prototipi, smart card con integrati sia i sensori di lettura delle impronte digitali che i moduli di verifica delle stesse.

## 4.6 Bibliografia

Scheuermann, Schwiderski-Grosche, Struif: Usability of Biometrics in Relation to Electronic Signatures. Studio UE 502533/8, 12 settembre 2000

ISO/IEC 7816-4: 1995 - Interindustry commands for interchange

ISO/IEC 7816-8: 1999 - Security related interindustry commands

ISO/IEC 7816-11: 2004 - Personal verification through biometric methods

*Capitolo 5*

# L'impiego delle tecnologie biometriche e il quadro giuridico di riferimento

## 5.1 Premessa

In presenza di una rapida evoluzione nel settore delle tecnologie, per una compiuta valutazione di opportunità e possibilità di implementazione di un sistema biometrico è opportuno tener conto, oltre che dell'ordinamento giuridico nazionale, anche di pareri e orientamenti di organismi sovranazionali con valenza normativa, regolamentare o di orientamento, a secondo della loro rispettiva natura e funzione.
L'ordinamento giuridico nazionale è infatti condizionato dalla produzione normativa europea, mentre diversi organismi internazionali sono intervenuti sulla materia con atti di indirizzo che hanno comunque una non indifferente valenza e una portata che si estende oltre i confini dell'Unione Europea. In questo senso si devono considerare gli interventi sul tema dell'impiego delle tecnologie biometriche da parte dell'Unione Europea, del Consiglio d'Europa, dell'OECD, dell'ICAO.

Con riferimento al contesto normativo nazionale, vedremo poi come l'utilizzo dell'elemento biometrico, inteso quale elemento identificativo della soggettività fisica, non sia normato nell'ordinamento italiano, ad eccezione di alcuni riferimenti specifici proprio nel settore della protezione dei dati personali e di principi giuridici applicabili ad alcuni aspetti del problema.
Il primo corpo di disposizioni sarà oggetto di approfondita illustrazione al paragrafo n. 5.2; gli aspetti normativi di riferimento generale e le ulteriori problematiche sul tema saranno esposte di seguito, insieme a un quadro sintetico degli adempimenti relativi alla protezione dei dati personali in tema di biometria.

### 5.1.1 La biometria nelle norme.

L'elemento biometrico, inteso quale carattere fisico o comportamentale identificativo di un soggetto, non trova oggi una puntuale definizione nella legislazione vigente, dovendosi piuttosto fare riferimento alla sfera scientifica per descriverlo.
A livello generale, l'elemento biometrico, inteso quale aspetto della identità fisica dell'uomo, non trova esplicita tutela, se non con riferimento ai parametri costituzionali della salute ed integrità fisica e del divieto di trattamenti sanitari obbligatori che, peraltro, non sono ammessi se lesivi del rispetto per la persona umana (art. 32 Cost.).

In tale prospettiva, è altresì meritevole di menzione quanto disposto dall'art. 13 della Carta costituzionale, che garantisce l'inviolabilità della libertà personale ed il cui dettato deve essere inteso "con riferimento anche alla libertà di salvaguardia della propria salute e della propria integrità fisica" (Corte di Cassazione, Sez. III, sent. n. 10014 del 25 novembre 1994).

La legge 23 dicembre 1978, n. 833, recante "Istituzione del servizio sanitario nazionale", sanziona il richiamato principio costituzionale con l'art. 33 che esclude la possibilità di accertamenti e di trattamenti sanitari contro la volontà del paziente se questo è in grado di prestarlo e non ricorrono i presupposti dello stato di necessità (Cfr. Cass. cit.).

Sotto il medesimo angolo visuale si inserisce la disposizione di cui all'art. 5 c.c. che impedisce gli atti dispositivi del proprio corpo che incidano sulla integrità fisica.
Dal punto di vista normativo l'elemento biometrico, come pure il dato biometrico che coincide nella oggettivizzazione del primo, pur non definito, è varie volte citato in corpi normativi emanati a partire dal 2000; in particolare una prima significativa citazione si rinviene nell'art. 36, d.P.R. n. 443/2000 in tema di carta di identità elettronica con un rinvio ad emanando Decreto del Presidente del Consiglio dei Ministri; due specifiche citazioni si rinvengono nel d.l.vo n. 196/2003, in tema di protezione dei dati personali e del quale si parlerà al paragrafo n. 5.2.5; una ulteriore citazione si rinviene all'art. 9, d.l.vo n. 117/2004 in tema di carta nazionale dei servizi.
In mancanza di una legale definizione si ritiene di adottare il concetto espresso dal Gruppo dei Garanti Europei (istituito sulla base dell'art. 29 della direttiva 95/46/CE sulla protezione dei dati personali, e pertanto noto come "Working Party Art. 29") nel documento adottato il 1° agosto 2003, laddove si dice che "i dati biometrici possono sempre essere considerati come informazioni concernenti una persona fisica in quanto sono dati che, per la loro stessa natura, forniscono indicazioni su una determinata persona" [17].

Come non è definito il dato biometrico, così, a livello normativo, non è definita e regolata la tecnologia che di tali dati fa uso.
In mancanza di specifiche indicazioni deve farsi ricorso ai consueti principi in merito alle attività umane che sono generalmente ammesse, nel rispetto dei diritti e delle libertà fondamentali, della salute, della dignità, con particolare riferimento alla riservatezza e all'identità personale, e della integrità fisica.

### 5.1.2 Le responsabilità

L'utilizzo di tecnologie che interferiscono con la soggettività dell'uomo può determinare il sorgere di responsabilità non solo per l'illiceità dell'uso, ma anche per il colposo o doloso utilizzo di esse.
Si apre, cioè il campo alla problematica della responsabilità civile e penale per lesione di diritti od interessi individuali derivante dall'impiego di tecnologie biometriche.
Schematicamente la problematica concerne la fase del prelievo od acquisizione del dato biometrico, quella della sua conservazione, quella dell'uso.
Dal punto di vista della acquisizione o prelievo del dato mette conto di segnalare che, al pari di ogni altra attività umana, una azione colposamente o dolosamente lesiva dei diritti o

[17] **Documento di lavoro sulla biometria adottato il 1°agosto 2003 (12168/02/IT) WP 80** "It appears that biometric data can always be considered as "information relating to a natural person" as it concerns data, which provides, by its very nature, information about a given person".

dell'integrità fisica del soggetto determina il sorgere della corrispondente responsabilità civile sia essa di origine contrattuale (accordo per il prelievo del dato con danni in detta fase) o extracontrattuale. Trattandosi, in ipotesi, di attività rischiosa l'agente è responsabile se non da prova di avere adottato tutte le misure idonee ad evitare il danno (art. 2050 c.c.).
Dal punto di vista della responsabilità penale, senza ipotizzare i più gravi delitti a tutela dell'incolumità fisica, la colposa azione che danneggi l'integrità fisica dell'uomo ingenera la fattispecie di cui all'art. 590 c.p.

Le tematiche di responsabilità per la fase di raccolta, conservazione ed uso del dato biometrico sono adeguatamente normate dal d.l.vo n. 196/2003, il cui art. 15[18] richiama la disposizione dell'art. 2050 c.c. in punto di responsabilità civile, estendendo la responsabilità ai danni non patrimoniali derivanti dalla violazione delle modalità di trattamento di cui all'art.11, stesso decreto[19].
Le disposizioni di cui agli artt. 167[20] e 169[21], d.l.vo n. 196/2003 stabiliscono fattispecie di rilevanza penale per colui che tratti in maniera illecita i dati personali ovvero contravvenga alle misure minime di sicurezza di cui all'art. 33, stesso decreto[22].

[18] "1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. 2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11".

[19] "1. I dati personali oggetto di trattamento sono: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. 2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati".

[20] "1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi. 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni".

[21] "1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro. 2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare unasomma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili."

[22] "1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali."

### 5.1.3 Limitazioni all'utilizzo delle biometrie

Si è detto in esordio del capitolo che la caratteristica biometrica, attenendo all'identificazione più pregnante ed univoca della persona, pur non essendo espressamente tutelata dalla carta, ha assunto una rilevanza costituzionale, confermata di recente anche dagli artt. 7 e 8 della Carta dei diritti proclamata a Nizza nel 2000; in questa ottica si inseriscono le disposizioni del d.l.vo n. 196/2003.
Inoltre le tecnologie biometriche trovano oggi applicazioni sempre più diffuse e a costi contenuti: per tale ragione devono essere individuati i limiti al loro utilizzo e le garanzie adeguate.
Prima di analizzare le disposizioni del d.l.vo n. 196/2003 per quello che concerne l'uso delle caratteristiche e dei dati biometrici, mette conto di accennare alla problematica dell'acquisizione del dato in questione, comunque non sottratta, perché in realtà parte integrante del trattamento, alle previsioni del Codice.
La possibilità, dunque, di acquisire, coattivamente e contro la volontà del soggetto cui appartiene, un dato biometrico incontra precisi limiti imposti dalla carta costituzionale che, come si è detto, osteggia le condotte invasive della soggettività giuridica se non in correlazione a poteri o doveri specificamente individuati.

Le norme a tutela dell'ordine e della sicurezza pubblica ed il sistema processuale penale, in taluni casi, prevedono la facoltà per l'autorità di acquisire dati biometrici dei cittadini, pur nel rispetto della dignità umana e per gli scopi propri definiti dalle disposizioni che introducono tali poteri (ad esempio art. 347, 349 c.p.p., art. 3, R.D. n. 773/1931, art. 23, d.P.R.. n. 230/2000). Va sottolineato che, fatte salve le indicate disposizioni, non sono consentiti, ad esempio, atti di acquisizione coattiva di impronte digitali; inoltre, per costante giurisprudenza, non è consentito procedere a prelievo coattivo di sangue, se non per necessità di cura e nei casi previsti dalle norme a tutela della salute, per effettuare accertamenti sullo stesso volto alla individuazione del gruppo sanguigno, del fattore Rh o del DNA (diverso è il caso in cui l'autorità venga in possesso di elementi biologici da cui ricavare i dati biometrici suddetti).
Fermo il divieto suddetto, la problematica della acquisizione coattiva delle caratteristiche biometriche di un soggetto si pone soltanto per quelle caratteristiche che non sono evidenti e che, in quanto tali, possono essere captate anche senza invadere la sfera personale del soggetto in questione; l'acquisizione della immagine del viso di un individuo identificabile non è generalmente invasiva e dunque, anche tenuto conto che la stessa è, per definizione, strumento di individuazione, sembra essere lecita (l'immagine del volto fornisce comunque dati personali, quindi si devono rispettare tutti i limiti e le garanzie previste dalle norme per il trattamento di dati personali: inclusi i principi di necessità, proporzionalità e finalità).
Diverso è il caso dell'acquisizione coattiva di caratteristiche biometriche che sono più strettamente connesse all'ambito personale dell'individuo e che, generalmente, coincidono con quelle caratteristiche per acquisire le quali è richiesta una certa collaborazione del soggetto; si pensi, ad esempio, alla acquisizione di impronte papillari delle dita della mano, alla geometria della mano, alla scansione della retina, all'analisi dell'iride ed altre.
In tali casi è richiesto che il soggetto presti la propria, seppur minima in alcuni casi, collaborazione; ci si chiede, cioè, se sia possibile imporre una tale condotta attiva. La questione, prima che con riferimento alle norme per la protezione dei dati personali, impinge con le problematiche di carattere generale che riguardano la possibilità di costringere l'individuo a compiere atti che coinvolgono la sua sfera fisica privata. Si vuole cioè rimarcare che le problematiche di tutela del dato personale in questione presuppongono che il dato sia stato legittimamente acquisito; si tratta, finalmente, di individuare gli eventuali strumenti

giuridici che consentano alla pubblica amministrazione di imporre ai propri dipendenti od utenti di prestare la propria collaborazione per la acquisizione di caratteristiche biometriche.
Il legislatore ha consentito, allo scopo di dare attuazione alle disposizioni in tema di misure minime di sicurezza di cui agli artt. 31 e segg. D.l.vo n. 196/2003, di implementare sistemi di autenticazione informatica incentrati sull'uso di caratteristiche biometriche per i trattamenti di dati effettuati con strumenti elettronici; l'allegato B al codice della privacy prevede espressamente che "*Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave*".
Dalla disposizione in questione si desume che, per assicurare adeguate misure di sicurezza del sistema informatico entro cui sono contenuti dati personali, può essere imposto agli utenti di tale sistema l'utilizzo di caratteristiche biometriche a fini di autenticazione informatica. Mette conto di precisare che la disposizione in questione, pur riferita alle credenziali di autenticazione per accedere ad un sistema informatico, stabilisce un principio applicabile anche alle credenziali di autenticazione necessarie per l'accesso fisico a locali dove siano collocati i sistemi informatici in questione o dove si trattino, senza strumenti informatici, i dati medesimi, qualora si tratta di dati sensibili o giudiziari: "*L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate*".

Al paragrafo 5.2.3. saranno analizzate in dettaglio le problematiche di necessità e proporzionalità del trattamento.

Resta al di fuori della problematica di acquisizione coattiva di dati biometrici, in quanto regolata da specifiche disposizioni, la potestà dell'ente pubblico di acquisirli in vista del rilascio di documenti di identità (qualunque acquisizione di dati personali da parte di enti pubblici deve comunque essere regolata da disposizioni normative).

Esorbita, infine, dalle problematiche descritte nel presente paragrafo la tematica delle modalità di trattamento dei dati acquisiti; in particolare, la possibilità di procedere coattivamente all'acquisizione del dato biometrico non esonera colui che procede al trattamento dal rispetto delle disposizioni in materia di protezione dei dati personali che, in alcuni casi, potrebbero avere anche natura sensibile.

## 5.2 Biometria e privacy

Benché la pertinenza della normativa sulla protezione dei dati rispetto alla complessa questione dell'utilizzo, in vari ambiti della vita sociale, di "caratteristiche biometriche" degli individui sia da considerare un fatto conclamato, se non ovvio, non è qui superfluo evidenziare come questo tipo di dati rivestano per loro natura il carattere di dati personali, in misura peraltro, per certi versi, qualitativamente più rilevante rispetto ad altri dati comunque correlati alla persona, ma non a essa così strettamente legati come le grandezze e i

comportamenti dell'essere umano sul cui rilevamento e rappresentazione si basano i sistemi biometrici.

Quest'ultima considerazione dà ragione della particolare sensibilità con cui vengono percepite le diverse iniziative volte all'utilizzo delle caratteristiche biometriche per scopi, di volta in volta, di autenticazione informatica, di identificazione, di controllo degli accessi ad aree riservate: esse, infatti, sono connaturate all'individuo, essendo una rappresentazione di una grandezza fisica corporea o di un comportamento della persona.

Spesso poi, l'associazione di una caratteristica biometrica a una persona è pressoché permanente , come nel caso delle impronte digitali, e ciò induce a particolari cautele, a differenza di quanto avviene con le credenziali di autenticazione informatica, che possono essere in qualunque momento revocate, quindi scollegate dall'individuo, e sono pur tuttavia oggetto di estrema cautela nel loro uso e nella loro protezione.

La rilevanza della protezione dei dati nei trattamenti biometrici è poi tale che nel corso degli anni sono intervenuti sulla materia diversi organismi che con indagini conoscitive o atti normativi e regolamentari di varia natura hanno affrontato i rapporto tra le elaborazioni biometriche e la privacy degli individui.

L'utilizzo di caratteristiche biometriche va quindi accuratamente disciplinato e ricondotto anche alle previsioni del nuovo Codice in materia di protezione dei dati personali, oltre che di eventuali specifiche normative che potrebbero trovare applicazione in certi settori relativamente ai medesimi trattamenti.

### 5.2.1 Evoluzioni tecnologiche e loro impatto sul trattamento dei dati personali

Lo sviluppo tecnologico tuttavia rende lo scenario delle applicazioni biometriche molto variabile, poiché i progressi nelle tecnologie dell'informazione, l'abbassamento dei costi, con la produzione su larga scala di dispositivi e di software specializzati in questo tipo di elaborazioni, consentiranno nel futuro a costi molto bassi la realizzazione di procedure biometriche estremamente efficienti e con un grado di protezione dei dati dell'interessato molto elevato.

Ci si riferisce in particolare all'evoluzione delle tecnologie RFID, basate sull'uso di processori "passivi" attivati da un campo elettromagnetico, e a quelle delle smart card, la cui capacità di memorizzazione e di elaborazione locale consentirà in futuro la realizzazione di procedure in cui non solo il trattamento dei dati personali avverrà sul dispositivo in possesso dell'interessato (*matching on card*) ma perfino la fase di acquisizione (per esempio, la lettura di un'impronta digitale a un varco di accesso con successiva generazione del template e il suo confronto con quello dell'interessato) potrà essere pilotata da procedure in esecuzione sulla tessera dell'utente.

E' da evidenziare comunque che un'elaborazione di questo tipo, pur consentendo, in certe condizioni, di riportare il trattamento dei dati personali biometrici nella sfera di controllo dell'interessato escludendo dalla conoscibilità del dato il titolare che abbia predisposto, per esempio, un sistema di controllo degli accessi basato su questo tipo di tecnologia, non sottrae

comunque il titolare alle sue peculiari responsabilità quale soggetto che pone in essere un'operazione di trattamento ed è quindi tenuto al rispetto di tutti gli obblighi in materia di protezione dei dati.

### 5.2.2 Fonti normative, regolamentari e di indirizzo su biometria e privacy

Le implicazioni e i problemi derivanti dall'utilizzo delle tecniche biometriche sono state dibattute in diverse sedi con valenza normativa, regolamentare o di indirizzo in ambito internazionale. A questo proposito, i documenti prodotti da comitati od organizzazioni di indirizzo rivestono pure una notevole importanza, in quanto costituiscono delle indicazioni di carattere più generale che si applicano a una pluralità di soggetti al di là dell'ambito nazionale o comunitario e che pur tuttavia, per il prestigio e il riconoscimento internazionale degli organismi coinvolti, sono suscettibili di influenzare gli atteggiamenti di stati e governi, interessando anche i rispettivi ordinamenti giuridici nazionali.

Tra le sedi internazionali di maggior rilievo si citano l'Unione Europea, con i suoi organismi che a vario titolo si sono interessati dei rapporti tra biometria e privacy, e il Working Party Art. 29 in primo luogo; il Consiglio d'Europa; l'OCSE/OECD (Organisation for Economic Co-operation and Development); l'ICAO (International Civil Aviation Organization).

#### 5.2.2.1 Working Party Art. 29

Il Gruppo di lavoro dei Garanti europei ha in proposito adottato il 1° agosto 2003 il "Documento di lavoro sulla biometria" (doc. n. 12168/02/IT WP80) in cui, tenuto conto della rapida espansione dell'impiego di tecnologie biometriche e delle preoccupazioni in merito al loro possibile incontrollato utilizzo, venivano formulate delle raccomandazioni in forma di linee-guida per l'industria e gli utenti, con lo scopo di contribuire a un'omogenea ed efficace applicazione delle norme nazionali rispetto alla direttiva 46/95/CE in materia di sistemi biometrici. Specifica attenzione veniva dedicata al possibile effetto di insensibilità del pubblico come conseguenza dell'uso generalizzato dei dati biometrici, esemplificato dall'uso di sistemi biometrici per l'accesso a delle biblioteche scolastiche. Il documento rimarca il carattere di dato personale dei dati biometrici, richiamando i principi di finalità e proporzionalità che costituiscono le basi di legittimazione del trattamento secondo l'articolo 7 della direttiva 95/46/CE, nonché l'adozione di misure di sicurezza conformemente all'articolo 17 della stessa direttiva.
Una notazione a parte merita nel documento la possibilità che alcuni dati biometrici possano essere considerati di natura delicata a termini dell'articolo 8 della direttiva 95/46/CE, perché suscettibili di rivelare l'origine razziale o etnica o lo stato di salute. In questi casi devono trovare applicazione le speciali garanzie di cui all'articolo 8 della direttiva oltre ai principi generali di protezione in essa previsti.
In precedenza il Gruppo di lavoro aveva affrontato, con un documento di lavoro approvato il 25 novembre 2002, il tema dell'elaborazione dei dati personali conseguente alla messa in opera di sistemi di videosorveglianza ("Working Documento on the Processing of Personal data by means of Video Surveillance", 11750/02 EN WP 67). Le indicazioni di quel documento rivestono un notevole interesse anche per quanto attiene ai trattamenti biometrici,

tra i quali è compreso il riconoscimento facciale che, come si vedrà in seguito, è una delle tecniche suscettibili di ampia diffusione su scala internazionale per identificazione e riconoscimento personale con finalità di sicurezza. Peraltro, i Garanti europei richiamano esplicitamente l'applicabilità dei principi esposti anche all'elaborazione di suoni e di caratteristiche biometriche rilevate nell'attività di videosorveglianza. Tra le misure ritenute necessarie per assicurare un'adeguata sicurezza ai trattamenti derivanti dalla videosorveglianza si richiama l'esigenza di sottoporre le implementazioni di sistemi biometrici a controllo preventivo (*prior* checking) da parte delle Data Protection Authorithies nazionali almeno nei casi in cui i trattamenti prevedano o possano dar luogo a:
a) interconnessione permanente di sistemi di video sorveglianza gestiti da diversi titolari;
b) possibile associazione di immagini e dati biometrici come el impronte digitali (per esempio, all'ingresso di una banca);
c) uso di sistemi di identificazione vocale;
d) realizzazione, in linea con i principi di proporzionalità e basata su specifiche previsioni, di sistemi di indicizzazione applicati alle immagini registrate o sistemi per il loro simultaneo e automatico trattamento, con specifico riferimento a dati identificativi;
e) uso di sistemi di risonoscimento facciale non limitati al rilevamento di camuffamenti di persone in transito, come barbe finte e baffi, ma che siano basati sull'identificazione di potenziali sospetti sulla base dell'aspetto esteriore o di schemi comportamentali;

Successivamente, il WP Art. 29 ha adottato l'11 agosto 2004 il documento di lavoro "Opinion 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)" (11224/04/EN WP 96). Questo documento prende in considerazione le proposte di inclusione di elementi biometrici nei permessi di soggiorno e nei visti di ingresso nell'Unione Europea per cittadini di Paesi esterni, quindi affrontando un particolare e delicato contesto applicativo della biometria.

Le considerazione e le preoccupazioni in esso espresso rivestono interesse generale, in particolare sul rischio di trattamenti eccedenti le finalità, sulla possibilità di accesso ai dati da parte di soggetti diversi e addirittura esterni all'Unione Europea, sulla consapevolezza degli utenti interessati relativamente agli utilizzi dei dati memorizzati su supporti sicuri (smart cards o altri dispositivi), sulla sicurezza del processo di enrolment e sui rischi di erronea o fraudolenta associazione di dati anagrafici a dati biometrici, finalizzata ai cosiddetti furti di identità. Ulteriori preoccupazioni vengono espresse in merito alla possibile adozione di database centralizzati di dati biometrici, che potrebbero più facilmente consentire il perseguimento di fini eccedenti e nello stesso tempo sottraendo all'interessato le possibilità di controllo sull'utilizzo dei propri dati.

#### 5.2.2.2 Consiglio d'Europa

Nel documento sui principi di protezione dei dati personali trattati tramite *smart cards* ("Draft guiding principles for the protection of personal data with regard to smart cards", 2003) il Consiglio d'Europa ha richiamato l'attenzione su taluni aspetti dei trattamenti che possono determinare pregiudizio per i diritti dei cittadini interessati. Non vi è nel documento un esplicito riferimento alla biometria, tuttavia le considerazioni in esso espresse, rivolte ai trattamenti su *smart cards,* risultano in più punti pertinenti ai trattamenti biometrici, che peraltro spesso coinvolgono quel tipo di supporto tecnologico.

Vengono richiamati, infatti, quali linee di indirizzo, i seguenti principi:
liceità e trasparenza dei trattamenti.
finalità e non eccedenza.
specificità dei fini.
responsabilità dei rispettivi titolari del trattamento anche per quanto riguarda le cosiddetta *carte multiservizi* (contitolarità).
consenso esplicito per la registrazione di dati sensibili, il cui trattamento dovrebbe avvenire soltanto sulla base di previsioni di legge che garantiscano le appropriate tutele, e dell'esercizio dei diritti di modifica o revoca del consenso senza conseguenze negative per l'interessato.
sicurezza dei dati memorizzati da garantire con mezzi tecnici adeguati alla delicatezza dei dati trattati e ai possibili rischi, e della informativa sui possibili soggetti che potranno avere accesso ai dati memorizzati sulla carta e delle condizioni in base alle quali potrà avvenire l'accesso per i diversi scopi previsti.
Informazione agli interessati sull'uso della smart card e sui comportamenti da mettere in atto in caso di frodi o divulgazione dei dati.
consapevolezza da parte dell'interessato dei singoli trattamenti dei dati memorizzati, che non potranno essere elaborati a sua insaputa (per esempio, con un lettore di prossimità nascosto) o senza una preventiva informativa.
conservazione dei dati per un definito limite temporale legato agli specifici scopi per cui la carta è usata.

Il Consiglio d'Europa ha inoltre espresso riserve sull'utilizzo delle *smart cards* come mezzo di pagamento se in esse sono registrati dati sensibili, a causa del maggiori rischio di abusi.
A tal proposito ha ricordato come, oltre alla Convenzione del Consiglio n. 108, che ha costituito fonte d'ispirazione anche per i lavori che hanno portato all'adozione della Direttiva 95/46/CE sulla protezione dei dati personali, numerosi altri riferimenti siano contenuti nelle Raccomandazioni che il Consiglio ha successivamente formulato, nel corso degli anni, per quanto riguarda, ad esempio, la protezione dei dati sanitari e della previdenza sociale.

#### 5.2.2.3 OECD

Sugli stessi temi è intervenuta l'O.E.C.D. (Organisation for Economic Co-operation and Development), che ha recentemente pubblicato, a cura del Working Party on Information Security and Privacy, il documento "Biometric-based technologies" (9 marzo 2004) in cui si analizzano le caratteristiche dei sistemi biometrici e le loro relazioni rispetto alla sicurezza e alla privacy.

#### 5.2.2.4 ICAO

Già nel maggio del 2003 l'Internation Civil Aviation Organization ha proposto l'utilizzo di caratteristiche biometriche nei passaporti e in altri documenti di viaggio leggibili automaticamente (MRTDs), al fine di velocizzare il transito dei passeggeri attraverso i controlli nelle aree aeroportuali a fini di sicurezza. La caratteristica biometrica consente, secondo l'ICAO, di accrescere la sicurezza e di aggiungere protezione contro i furti di identità.
Come tecnica biometrica d'elezione per l'inclusione nei passaporti e nei documenti di viaggio l'ICAO ha proposto il riconoscimento facciale, in virtù della maggiore interoperabilità dei

sistemi su di esso basati, anche rispetto alle impronte dattiloscopiche e alle immagini retiniche o dell'iride. Nello stesso tempo, il riconoscimento facciale risulta il corrispondente tecnologico del riconoscimento effettuato *de visu* tramite il confronto della fotografia nel documento di viaggio o nel passaporto con le fattezze del suo possessore. In questo senso, il riconoscimento facciale viene accreditato di una maggiore "accettabilità" sociale. ICAO raccomanda inoltre l'utilizzo di carte ad alta capacità e senza contatti per memorizzare le informazioni identificative negli MRTDs. La tecnologia a banda magnetica o dei codici a barre non consentirebbe infatti di memorizzare le rappresentazioni di una o più caratteristiche biometriche o comportamentali.

### 5.2.3 I principi sanciti dal codice della privacy

Prima di analizzare in dettaglio gli aspetti normativi legati alla privacy dei dati biometrici è opportuno introdurre le principali definizioni del codice della privacy che sono pertinenti alle tecnologie biometriche.

L'articolo 4, lettera b) del D.Lgs. n. 196/2003 definisce il dato personale come "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".

In funzione di tale definizione, è evidente come il trattamento di dati biometrici sia un trattamento di dati personali; come rilevato dal Gruppo dei Garanti Europei, solo nel caso in cui i dati biometrici, quali ad esempio un modello, vengono registrati in modo tale che non esistano mezzi ragionevolmente utilizzabili dal Titolare del trattamento o da altri per identificare la persona interessata, tali dati possono non essere considerati come dati personali. Nella maggior parte dei casi il dato biometrico è invece un dato personale, anche in forma di "template", in quanto è sempre possibile considerarlo come un'informazione relativa ad una persona fisica "identificata o identificabile" anche attraverso "uno o più elementi specifici caratteristici della sua identità fisica". Ai dati biometrici dunque si applicano integralmente i principi del D. Lgs. n. 196/2003 in materia di protezione dei dati personali, fin dalla fase di "iscrizione" (*enrolment*). Il trattamento dei dati biometrici può dunque essere considerato lecito solo se tutte le procedure utilizzate, a partire dall'iscrizione, vengono effettuate conformemente alle disposizioni di legge.

La legge definisce inoltre, all'art. 4 lettera d), i dati sensibili come "i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale".

Alcuni dati biometrici possono essere considerati dati sensibili, precisamente i dati che rivelano l'origine razziale o etnica o i dati relativi alla salute. Nei sistemi biometrici basati sul riconoscimento del volto, ad esempio, possono essere trattati dati che rivelano l'origine razziale o etnica. La valutazione se un trattamento comprende dati di natura sensibile è dunque legata alle specificità delle caratteristiche biometriche utilizzate nonché

all'applicazione biometrica stessa. Il trattamento di dati sensibili è maggiormente probabile nel caso in cui vengono trattati dati biometrici sotto forma di immagini, dato che in linea di massima i dati grezzi non possono essere ricostruiti a partire dal modello.

Di seguito vengono esposti i principi che regolano il trattamento dei dati biometrici, così come sono stati recepiti nel nostro ordinamento e compiutamente esposti a livello normativo nel decreto legislativo n. 196/2003.

#### 5.2.3.1 Principio di liceità del trattamento

Il trattamento dei dati biometrici è possibile solo se è fondato su uno dei presupposti di liceità che il Codice prevede espressamente per i soggetti pubblici da un lato (svolgimento di funzioni istituzionali: artt. 18-22) e, dall'altro, per soggetti privati ed enti pubblici economici (consenso espresso, adempimento ad un obbligo di legge, provvedimento del Garante di c.d. "bilanciamento di interessi"etc.: artt. 23-27). Si tratta di presupposti operanti in settori diversi e che sono pertanto richiamati separatamente in relazione ai trattamenti in ambito pubblico e privato[23].

Il trattamento di dati biometrici deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati, anche di quanto prescritto da altre disposizioni di legge rivolte a specifici trattamenti, come quelli che possono aver luogo nell'ambito lavorativo e per i quali vanno tenute presenti le norme riguardanti la tutela dei lavoratori, con particolare riferimento alla legge n. 300/1970 (Statuto dei lavoratori).

#### 5.2.3.2 Principio di necessità

Il trattamento dei dati biometrici non può prescindere dal principio di necessità. Ciascun sistema informativo e il relativo programma informatico vanno quindi conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi o codici identificativi. Qualora il sistema preveda l'acquisizione e l'elaborazione del dato biometrico e la sua organizzazione in una banca dati sotto il controllo di un titolare, il software va configurato in

[23] È dunque necessaria una valutazione accurata della finalità e della necessità e proporzionalità dei dati biometrici trattati. In Italia l'Autorità Garante per il trattamento dei dati personali ha ribadito il principio che gli strumenti utilizzati ai fini di sicurezza non devono essere sproporzionati rispetto agli scopi che intendono perseguire. L'occasione è stata offerta da due accertamenti in corso da parte dell'Autorità stessa nei confronti di pubbliche amministrazioni, un comune ed un ente regionale per il diritto allo studio universitario, che hanno deciso di adottare sistemi di rilevazione biometrici, rispettivamente per il controllo dei dipendenti in una biblioteca comunale e per il controllo degli accessi degli studenti in una mensa universitaria . Il Garante ha voluto, innanzitutto, accertare se l'uso di un sistema così intrusivo come quello di rilevazione delle impronte digitali non eccedesse la finalità che si voleva perseguire, ossia di consentire l'accesso al servizio di mensa universitaria, di controllare l'orario di servizio dei dipendenti o l'accesso alla biblioteca comunale da parte degli aventi diritto; inoltre, ha voluto verificare se non fossero più idonei altri sistemi o procedure atti a creare minori rischi per i diritti e le libertà fondamentali di chi deve rilasciare le impronte. A tal proposito, si veda la newsletter del Garante n. 197 del 18-24 gennaio 2004: il comune avrebbe invitato tutti i dipendenti, ed in particolare quelli in servizio presso la biblioteca comunale, a depositare le proprie impronte digitali per costituire "una banca dati da utilizzare per la rilevazione delle presenze". Mentre nel caso dell'ente regionale, il Garante ha avviato accertamenti sul progetto di installare lettori di impronte digitali presso ristoranti convenzionati per controllare che l'accesso al servizio di ristorazione avvenga esclusivamente da parte degli aventi diritto, per porre fine così all'utilizzo dei ticket da parte di chi non ne ha diritto.

modo da cancellare periodicamente e automaticamente i dati eventualmente registrati che non siano più necessari agli scopi per i quali sono stati acquisiti.
Se non è osservato il principio di necessità riguardante le installazioni di sistemi biometrici le attività conseguenti non sono lecite (artt. 3 e 11, comma 1, lett. a), del Codice).

#### 5.2.3.3 Principio di proporzionalità

Nel commisurare la necessità di un sistema al grado di sicurezza richiesto e, in origine, al rischio presente in concreto, va evitata la rilevazione di dati biometrici in contesti o attività che non sono soggetti a concreti pericoli, o per le quali non ricorre un'effettiva esigenza di identificazione certa. Un sistema di riconoscimento biometrico previsto per l'accesso di un abbonato a uno spettacolo teatrale, per mero esempio, sarebbe del tutto sproporzionato in assenza di specifiche esigenze e in presenza di procedure alternative per verificare il possesso del titolo di accesso.

I sistemi biometrici possono, quindi, essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi.

Le applicazioni biometriche per l'identificazione e il riconoscimento sono quindi lecite solo se è rispettato il c.d. principio di proporzionalità, sia nella scelta progettuale sul tipo di sistema da adottare, sia nelle varie fasi del trattamento (art. 11, comma 1, lett. d) del Codice).

Il principio di proporzionalità consente, ovviamente, margini di libertà nella valutazione da parte del titolare del trattamento, ma non comporta scelte del tutto discrezionali e insindacabili.

Il titolare del trattamento, prima di installare un impianto di riconoscimento biometrico, deve valutare, obiettivamente e con un approccio selettivo, se l'utilizzazione ipotizzata sia in concreto realmente proporzionata agli scopi prefissi e legittimamente perseguibili, evitando un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli altri interessati.
Come si è detto, la proporzionalità va valutata in ogni fase o modalità del trattamento, per esempio quando si deve stabilire quali dati rilevare, se registrarli o meno, se avvalersi di una rete di comunicazione o creare una banca di dati, indicizzarla, abbinare altre informazioni o interconnettere il sistema con altri gestiti dallo stesso titolare o da terzi, la durata dell'eventuale conservazione (che, comunque, deve essere sempre temporanea).

In applicazione del predetto principio va altresì delimitata rigorosamente:

- l'utilizzazione di specifiche soluzioni quali il collegamento ad appositi "centri" cui inviare segnali di allarme sonoro o visivo, oppure l'adozione di interventi automatici per effetto di meccanismi o sistemi automatizzati d'allarme (chiusura accessi, afflusso di personale di vigilanza, ecc.), tenendo anche conto che in caso di trattamenti volti a definire profili o personalità degli interessati il Codice prevede ulteriori garanzie (art. 14, comma 1, del Codice);
- l'eventuale duplicazione dei dati biometrici registrati;
- la creazione di una banca di dati quando, per le finalità perseguite, è sufficiente un trattamento senza registrazione (per esempio, per il controllo di un varco di

accesso con l'uso di un dispositivo sicuro in possesso dell'interessato quando l'emissione e l'uso del dispositivo avvengano da parte del titolare con specifiche procedure per garantire la sicurezza e l'integrità dei dati in essa registrati).

#### 5.2.3.4 Principio di finalità

Gli scopi perseguiti devono essere determinati, espliciti e legittimi (art. 11, comma 1, lett. b), del Codice). Ciò comporta che il titolare possa perseguire solo finalità di sua pertinenza (nel caso di soggetti pubblici le finalità devono essere connesse allo "svolgimento delle funzioni istituzionali").

In ogni caso, possono essere perseguite solo finalità determinate e rese trasparenti, ossia direttamente conoscibili attraverso adeguate comunicazioni (fatta salva l'eventuale attività di acquisizione di dati disposta da organi giudiziari o di polizia giudiziaria), e non finalità generiche o indeterminate, tanto più quando esse siano incompatibili con gli scopi che vanno esplicitamente dichiarati e legittimamente perseguiti (art. 11, comma 1, lett. b), del Codice). Le finalità così individuate devono essere correttamente riportate in un'informativa sul trattamento dei dati personali che faccia esplicito riferimento ai trattamenti biometrici.

### 5.2.4 Le disposizioni specifiche sulla biometria nell'ordinamento nazionale

Il Codice in materia di protezione dei dati personali (d.l.vo n. 196/2003) disciplina il trattamento di dati biometrici assoggettandolo, in generale, a un regime di maggiore severità rispetto ai trattamenti di meri dati personali.
I trattamenti di dati biometrici devono quindi rispettare, oltre che i principi generali di liceità dei trattamenti precedentemente introdotti (e per far ciò il titolare, tra l'altro, deve valutare la necessità, la proporzionalità e le finalità del trattamento prima del suo inizio), anche delle disposizioni specifiche.

#### 5.2.4.1 Adempimenti preventivi all'inizio del trattamento

Nel caso in cui il dato biometrico che si intende trattare non abbia carattere di dato sensibile, trova infatti applicazione l'Art. 17 del Codice relativo ai trattamenti che presentano rischi specifici per i diritti e le libertà fondamentali e per la dignità dell'interessato. In questi casi occorre rispettare le misure e gli accorgimenti prescritti dal Garante nell'ambito di una verifica preliminare all'inizio del trattamento, che può svolgersi a seguito di interpello del titolare.
Nel caso poi di trattamenti biometrici da parte di forze di polizia trova applicazione l'Art. 55 del Codice relativo ai trattamenti mediante particolari tecnologie, che prevede il rispetto delle misure e degli accorgimenti prescritte ai sensi dell'Art. 17 sopra citato e che il trattamento avvenga sulla base di una preventiva comunicazione ai sensi dell'Art. 39 (obblighi di comunicazione).
Il trattamento di dati biometrici rientra poi nei casi in cui è richiesta la notificazione al Garante: il primo comma lettera a) dell'art. 37 prevede un obbligo di notifica al Garante qualora il trattamento che si intende iniziare abbia per oggetto, tra gli altri, dei dati biometrici, senza riferimento alcuno a specifiche modalità o finalità di trattamento. Da ciò si deduce un obbligo generale di notificazione per chiunque intenda iniziare un trattamento di dati biometrici in qualità di titolare.

La notifica è una dichiarazione con la quale un soggetto pubblico o privato rende noto al Garante per la protezione dei dati personali, l'esistenza di un'attività di raccolta e di utilizzazione di dati personali, svolta quale autonomo Titolare del trattamento.
La notifica deve essere trasmessa per via telematica all'Autorità Garante, tramite il sito www.garanteprivacy.it, utilizzando la procedura indicata nelle istruzioni presenti sul sito stesso. Tutte le notifiche sono inserite in un registro pubblico consultabile gratuitamente da tutti on-line. Gli interessati dunque possono così acquisire notizie ed utilizzarle per le finalità di applicazione della disciplina in materia di protezione dei dati personali (ad es., per esercitare il diritto di accesso ai dati o altri diritti riconosciuti dal Codice in materia di protezione dei dati personali). Per le attività di trattamento di dati biometrici che non esistevano prima del 1° gennaio 2004, la notifica va effettuata antecedentemente all'inizio del trattamento medesimo; per le attività già in essere al 1° gennaio 2004, la notifica andava effettuata entro il 30 aprile 2004. La notifica va resa *una tantum*, indipendentemente dalla durata, dal tipo e dal numero delle operazioni di trattamento. Una nuova notifica è richiesta solo prima che cessi definitivamente l'attività di trattamento dei dati biometrici oppure prima che si apportino al trattamento alcune modifiche agli elementi da indicare nella notifica.

#### 5.2.4.2 Adempimenti richiesti nella fase di trattamento

**Informativa**

In ossequio al requisito della liceità del trattamento, il titolare deve rilasciare sempre un'informativa agli interessati, deve cioè informare, oralmente o per iscritto, gli interessati conformemente all'articolo 13 del Codice. I requisiti dell'informativa da fornire agli interessati comprendono, tra l'altro, l'indicazione delle finalità e delle modalità del trattamento cui sono destinati i dati biometrici, nonché dei soggetti o delle categorie di soggetti ai quali i dati biometrici possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati.
Anche i soggetti pubblici, che possono trattare i dati soltanto per lo svolgimento delle funzioni istituzionali, sono tenuti a fornire un'informativa agli interessati ai sensi dell'art. 13 del Codice.
I dati biometrici poi devono essere trattati e soprattutto rilevati in modo leale: devono essere evitati, dunque, i sistemi che raccolgono dati biometrici all'insaputa dei soggetti interessati, come può avvenire per le tecnologie di riconoscimento facciale e comportamentale, che consentono l'acquisizione di immagini a distanza senza l'esplicita collaborazione dell'interessato.

**Consenso**

Per i soggetti privati, la legittimità del trattamento, oltre che sull'informativa, si basa sul principio del consenso del singolo interessato, che deve essere "specifico" e "libero". Il consenso infatti, ai sensi dell'art. 23, è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato tutte le informazioni previste all'articolo 13 del Codice.

Casi in cui il consenso non è necessario sono elencati nell'articolo 24 del Codice, e riguardano, tra l'altro, i trattamenti necessari per adempiere a un obbligo previsto da leggi, da regolamenti o dalla normativa comunitaria, quelli la cui necessità scaturisca da obblighi derivanti da un contratto di cui è parte l'interessato o da specifiche richieste dell'interessato, i trattamenti necessari per la salvaguardia della vita o dell'incolumità fisica di un terzo.

**Misure minime e documento programmatico di sicurezza**

Tutti i trattamenti di dati personali comportano l'adozione obbligatoria delle misure minime di sicurezza previste dall'articolo 34 del Codice, più dettagliatamente descritte nell'allegato "B" ("Disciplinare tecnico"). Nel caso dei dati biometrici queste misure di sicurezza trovano applicazione sia alla gestione del processo biometrico, fin dalla fase di prima acquisizione e di *enrolment*, che alla fase di esercizio.
Nel caso di dati biometrici che abbiano qualità di dati sensibili o giudiziari si incorre inoltre negli obblighi di adozione di misure ulteriori di protezione, che prevedono anche l'uso di tecniche crittografiche qualora si trattino dati genetici. Il trattamento di dati sensibili o giudiziari implica comunque la redazione entro il 31 marzo di ogni anno, e la aggiornata tenuta, di un *Documento programmatico sulla sicurezza*.

E' da notare poi come delle caratteristiche biometriche siano previste nello stesso Disciplinare tecnico sulla sicurezza quali componenti ammissibili delle credenziali di autenticazione informatica, in sostituzione o in aggiunta rispetto ai convenzionali identificativi d'utente e parole d'ordine (username, password). Mentre ciò costituisce indubbiamente, in una certa misura, un riconoscimento esplicito da parte del Legislatore dell'adeguatezza delle tecnologie biometriche per certi fini, i trattamenti determinati da esigenze di autenticazione informatica devono comunque sottostare alle stesse regole previste per la generalità dei trattamenti biometrici, rispettando gli stessi adempimenti.

*Capitolo 6*

# Aspetti non tecnici della biometria

## 6.1 Premessa

Come è accaduto in passato per altre innovazioni tecnologiche, anche la biometria sta vivendo un momento in cui, parallelamente ad un forte interesse, può suscitare sospetti e preoccupazioni in una parte della opinione pubblica. Al di là di una certa "cattiva reputazione" nata all'ombra di varie "fiction" cinematografiche, è opinione di alcuni che, sulla base di motivazioni sociali ed etiche, diversi aspetti della biometria possano essere definiti poco attinenti all'essere umano o addirittura inaccettabili.
In linea di massima, tali opinioni sono causate essenzialmente dalla poca familiarità che caratterizza l'approccio di alcuni utenti con il mondo della biometria e da alcuni timori di tipo "orwelliano" su controlli troppo intrusivi nella vita quotidiana.
Tradotte in elementi concreti, le preoccupazioni maggiori nascono dal timore di una centralizzazione dei dati biometrici ed un potenziale uso improprio di essi.
Altre forme di preoccupazione possono nascere dal carattere percepito come invasivo di alcune tecnologie. In generale, ad esempio, alcuni denunciano uno certo timore di danni alla vista potenzialmente derivanti dalla biometria dell'occhio. Altri invece si dicono preoccupati della possibile contrazione di infezioni attraverso il contatto con una superfici di sensori toccati da altri utenti. Tutte queste preoccupazioni sono probabilmente destinate a scomparire con il tempo, man mano che la biometria diverrà uno strumento di uso comune, ma, almeno per il momento rappresentano una rilevante ipoteca sulla diffusione della biometria e vanno ad intaccare quella cosiddetta "percezione dell'utente (user's perception)" che è la sommatoria dei dubbi razionali ed irrazionali dell'utente e che può trasformarsi in una più o meno radicata ostilità nei confronti della biometria.
Lo scopo del presente capitolo è quindi mettere in evidenza come anche altri aspetti non tecnici della biometria, oltre alla privacy, possano considerarsi fattori di influenza determinanti sulle prestazioni di un processo biometrico arrivando, al limite, a decretare una vera e propria inapplicabilità sul campo di esso.

## 6.2 Fattori di influenza sulla percezione dell'utente

Parecchi studi nel settore hanno tentato di determinare le cause di diffidenza nei confronti della biometria che vanno ad influire sulla percezione dell'utente. Alcune voci, raggruppate per aree potrebbero essere costituite da:

- tutela de i dati personali:
  - function creep;
  - uso improprio dei dati;
  - tracciamento;
- aspetti medici:
  - danni fisici derivanti dall'uso della biometria;
  - problemi di igiene;

  - rilevazione di informazioni mediche;
- aspetti sociali:
  - accessibilità ai sistemi biometrici;
  - discriminazione razziale.

### 6.2.1 Tutela dei dati personali

L'utente mostra spesso una certa perplessità quando i dati vengono raccolti in maniera massiccia. Le preoccupazioni riguardano ad esempio la cosiddetta *"function creep"* che indica lo "scivolamento" dell'obiettivo della raccolta dei dati verso un'altra finalità che potrebbe portare, se non ad un *uso improprio* di essi, almeno ad un trattamento senza il consenso degli interessati. Con riferimento ad avvenimenti recenti, tipico è il caso di alcune compagnie aeree che hanno rivelato i dati dei passeggeri ad altri soggetti [24], suscitando molta preoccupazione nell'opinione pubblica.
Il discorso si lega fortemente a quella del tracciamento. L'uso, sia nel settore pubblico che in quello privato, di massicci database contenenti informazioni personali dettagliate, hanno fatto nascere delle serie preoccupazioni sulla possibilità per un soggetto di mantenere il proprio anonimato. Il tracciamento, che può considerarsi una sorta di "function creep", fa riferimento all'abilità di monitorare in tempo reale le azioni di un individuo o fare una ricerca in archivi che contengono informazioni su queste azioni.

### 6.2.2 Aspetti medici della biometria

Un fattore da non sottovalutare nell'implementazione di un sistema biometrico è la percezione da parte degli utenti di un potenziale rischio medico associato all'uso del dispositivo di acquisizione. Si può operare una distinzione di massima fra "Implicazioni mediche dirette – Direct Medical Implication (DMI)" e cioè connesse alla percezione di un rischio fisico associato all'uso di un dispositivo biometrico e "Implicazioni Mediche Indirette – Indirect Medical Implication (IMI) che fanno riferimento alla preoccupazione che il processo biometrico possa rivelare informazioni sullo stato di salute dell'utente.

Implicazioni mediche dirette
Le implicazioni mediche dirette possono essere potenzialmente causate da (i) contatto con superfici potenzialmente infette e (ii) esposizione ad irraggiamento all'infrarosso. Se è infatti abbastanza evidente che l'apposizione di un dito su un lettore di impronte digitali non possa essere ragionevolmente percepita come pericolosa dal punto di visto dell'igiene, quando la superficie di contatto aumenta, come nel caso della geometria della mano o delle due dita, è possibile che taluni abbiano una certa riluttanza ad apporre la propria caratteristica biometrica. Le argomentazione a supporto della scarsa rilevanza di questa preoccupazioni e le contromisure sono parecchie.

[24] http://www.epic.org/privacy/airtravel/profiling.html

Un contesto dove la valutazione del rischio fisico diventa più delicata concerne la biometria basata sull'analisi di parti dell'occhio, organo per il quale tutti gli esseri umani sono particolarmente protettivi e che può coinvolgere l'emissione di luce nello spettro dell'infrarosso vicino.
Anche se l'esperienza maturata sul campo ha, fortunatamente, dimostrato la generalizzata e trasversale innocuità fisica delle tecniche biometriche, i particolari e le informazioni non sono generalmente note a tutti e, comunque, non sono sufficienti a garantire che tutti gli utenti affrontino con serenità e senza preoccupazioni la procedura biometrica. Occorre quindi che, alla base dell'implementazione ci sia il tentativo di descrivere quanto più compiutamente le fasi ed i dispositivi del processo mettendo bene in luce le motivazioni alla base della presunzione di innocuità del procedimento biometrico.

Implicazioni mediche indirette
Un'altra forma di preoccupazione per l'utente è che il processo biometrico possa rivelare informazioni sul proprio stato di salute. Ciò è stato alimentato in parte dal diffondersi di alcune pionieristiche implementazioni biometriche basate sul riconoscimento della retina.
E' infatti noto che dall'analisi della vascolarizzazione del fondo oculare possono essere diagnosticate alcune condizioni mediche quali ad esempio ipertensione o diabete. In realtà anche il cosiddetto metodo del riconoscimento della retina (propriamente definito dall'unico produttore di tale tecnologia "retinal scanning" e non "retinal analysis)) non si basava sull'analisi del completo fondo oculare, come si intende nel senso di una fluoroangiografia, ma prendeva in considerazione informazioni tratte da una sezione circolare di esso, ragionevolmente insignificante dal punto di vista medico. Ciò nonostante il riconoscimento della retina è spesso riportato come potenzialmente lesivo della privacy e tale informazione, anche se non esatta, è ormai radicata in molti utenti.
Sempre a proposito dell'occhio, preoccupazioni sono state espresse per possibili sovrapposizioni fra analisi biometrica dell'iride ed iridologia. Gran parte delle osservazioni sono state innescate dal fatto che, per aiutare l'utente a trovare la posizione ottimale di ripresa, durante il processo di enrollment o riconoscimento biometrico, sullo schermo della postazioni, appare una immagine magnificata e definita dell'iride.
Ci sono molte motivazioni alla base del rigetto della possibilità di analisi iridologica da questa immagine. La più significativa è che l'iridologia si basa anche su una immagine cromatica che il processo biometrico, proposto dall'unico costruttore attuale della tecnologia, si basa su una immagine in scala di grigio. Anche però in questo caso la convinzione che qualche iridologo possa arrivare ad una diagnosi attraverso il riconoscimento biometrico dell'iride è dura da sradicare.

### 6.2.3 Aspetti sociali

Tra gli aspetti sociali, grande importanza assume il concetto di *"accessibilità"* che intende, fra l'altro, la valutazione delle eventuali discriminazioni che potrebbero verificarsi a causa di una mancata fruibilità di una tecnologia biometria per handicap fisici. La tendenza è quella quindi di studiare metodi alternativi in grado di potere garantire l'accessibilità a tutti.

## 6.3 Conclusioni

Uno dei presupposti su cui si basa la biometria è che alla base delle applicazioni ci sia una profonda considerazione per l'utente. E' quindi evidente che, con l'eccezione delle applicazioni biometriche di tipo non cooperativo, l'utente con le sue preoccupazioni, razionali od irrazionali, vada sempre posto al centro dell'attenzione in quanto è dalla sua accettazione del processo biometrico che può dipendere il successo dell'implementazione.
Mettere l'utente in una posizione preminente significa dunque andare a valutare gli aspetti descritti nel presente capitolo e tenere, ancora una volta conto che il buon processo biometrico, se cooperativo, nasce attraverso una profonda fase concertazione fra le varie parti interessate. Non è un caso che la mancata osservazione degli aspetti non tecnici, e quindi del fattore umano sia annoverato da molti esperti fra le cause determinanti delle scarse prestazioni o addirittura di alcuni sonori insuccessi che hanno sinora caratterizzato il settore delle tecniche biometriche.

*Capitolo 7*

# Elementi per la progettazione e la realizzazione di una soluzione biometrica

## 7.1 Premessa

Il presente capitolo ha l'obiettivo di fornire elementi di carattere generale a supporto della progettazione e della realizzazione di una soluzione biometrica indipendentemente dalle motivazioni che portano a valutare l'opportunità di adottare tali tecnologie.
Nel seguito vengono fornite indicazioni per la valutazione e la scelta di sistemi biometrici in relazione alle particolari applicazioni; vengono forniti elementi per la valutazione degli impatti tecnico-organizzativi e per l'analisi costi-benefici; vengono infine affrontati alcuni aspetti di legati alla sicurezza del dato biometrico. La parte finale del capitolo è dedicata a problematiche che caratterizzano il caso più frequente in cui la biometria voglia rappresentare la risposta a problematiche di sicurezza. L'adozione di una soluzione biometrica di per sé non comporta un incremento del livello di sicurezza ma può rappresentare una notevole opportunità in tale direzione. L'opportunità di ricorrere alla biometria e la scelta di un meccanismo di sicurezza di tipo biometrico deve rappresentare l'ultimo passo di un attento processo di analisi del rischio e di individuazione delle contromisure.

## 7.2 Valutare e scegliere una tecnica biometrica

Questa sezione introduce alcuni criteri per la valutazione e la scelta di sistemi biometrici con il duplice obiettivo di fornire elementi oggettivi per stabilire se una tecnologia è idonea per una specifica applicazione e di confrontare le diverse soluzioni disponibili sul mercato. Di seguito è riportata una classificazione gerarchica dei principali parametri di valutazione di un sistema biometrico: sicurezza, robustezza, usabilità, accettabilità e miscellanea sono le cinque classi adottate per il primo livello di classificazione.
L'accuratezza del riconoscimento è uno degli aspetti principali per la descrizione di un sistema biometrico. In appendice vengono approfonditi aspetti inerenti gli errori che caratterizzano i sistemi biometrici (FAR, FRR, EER, …), le tecniche per la loro valutazione, la teoria degli errori e viene fornita una visione pragmatica sulla valutazione dei sistemi biometrici al di fuori degli ambienti di laboratorio.

### 7.2.1 I principali parametri di valutazione

Di seguito viene riportato uno schema di classificazione dei principali paramenti di valutazione.

A. Sicurezza.
  A.1. Accuratezza.
    A.1.1. FAR (False Acceptance Rate).
    A.1.2. FRR (False Rejection Rate).
    A.1.3. ROC e DET.
    A.1.4. EER (Equal Error Rate)
    A.1.5. ZeroFAR.
    A.1.6. ZeroFRR.
  A.2. Resistenza ai tentativi di inganno con false caratteristiche biometriche.
    A.2.1. Vivezza.
    A.2.2. Mimica.
  A.3. Resistenza ai tentativi di manomissione.

B. Robustezza.
  B.1. Rispetto all'accuratezza dell'acquisizione.
  B.2. Rispetto alla stabilità della caratteristica biometrica.
  B.3. Rispetto ad alcuni soggetti, popolazioni, lavoratori.
  B.4. Rispetto all'ambiente.

C. Usabilità.
  C.1. Interazione con l'utente.
    C.1.1. Semplicità d'uso.
    C.1.2. Praticità d'uso.
    C.1.3. Necessità di addestramento dell'utente o supervisione iniziale.
    C.1.4. Criticità della fase di enrollment.
  C.2. Interazione con l'amministratore del sistema.
    C.2.1. Praticità d'uso.
    C.2.2. Strumenti di controllo e di monitoraggio.
    C.2.3. Necessità di supervisione.
    C.2.4. Necessità di manutenzione.
  C.2. Efficienza.
    C.3.1. Tempo di enrollment.
    C.3.2. Tempo di verifica/identificazione.

D. Accettabilità.
  D.1. della caratteristica biometrica.
  D.2. delle operazioni di enrollment e di verifica/identificazione.

E. Miscellanea.
  E.1. Costo.
  E.2. Ingombro.
  E.3. Dimensione dell'identificativo biometrico.
  E.4. Aderenza a standard.
  E.5. Integrabilità con altri sistemi.
  E.6. Adattabilità rispetto a specifiche applicazioni o ambienti operativi.

*Figura 7.1: i principali parametri di valutazione*

**A. Sicurezza**: caratterizza il grado di affidabilità di un sistema, ovvero la capacità di distinguere efficacemente caratteristiche biometriche di diversi individui e di resistere ai tentativi di accesso fraudolento.

**A.1. Accuratezza**: riveste un ruolo primario nella definizione della sicurezza di un sistema biometrico; comprende le percentuali di false accettazioni e falsi rifiuti e una serie di parametri da queste derivati. Si richiama l'attenzione sulla possibilità che anche qualora si dovesse operare una verifica d'identità degli utenti, potrebbe apparire preferibile il ricorso ad

un sistema che operi in modalità identificazione in quanto, evitando la fase di dichiarazione di identità, potrebbe rendere più semplice ed efficiente l'interazione con il sistema. D'altro canto operare in modalità identificazione è molto rischioso dal punto di vista dell'accuratezza, infatti, come approfondito in appendice, la probabilità di false accettazioni in un modalità identificazione, aumenta linearmente con il numero di soggetti oltre a comportare un evidente appesantimento dei tempi di calcolo è pertanto necessario ricorrere a sistemi con elevata accuratezza per minimizzare gli effetti legati alla perdita di accuratezza all'aumentare del numero di individui, quindi, nel caso del riconoscimento positivo, si consiglia di evitare l'impiego di un sistema biometrico in modalità identificazione (1:N) se non per N molto ridotto (es. minore di 100).
Nel seguito si riporta una breve descrizione dei 6 parametri principali comunemente utilizzati; maggiori approfondimenti possono essere trovati in appendice.
**A.1.1. FAR (False Acceptance Rate)**: percentuale di false accettazioni (o falsi positivi), ovvero percentuale di tentativi di accesso riusciti eseguiti da soggetti non abilitati.
**A.1.2. FRR (False Rejection Rate)**: percentuale di false reiezioni (o falsi rifiuti o falsi negativi), ovvero percentuale di tentativi di accesso non riusciti eseguiti da utenti abilitati.
**A.1.3. ROC e DET**: grafici che descrivono l'accuratezza del sistema al variare del punto di lavoro (ovvero della soglia di decisione).
**A.1.4. EER (Equal Error Rate)**: specifica la percentuale di errore in corrispondenza del valore di soglia per cui FAR e FRR coincidono.
**A.1.5. ZeroFAR**: percentuale di false reiezioni con la soglia di decisione regolata in modo da non causare mai false accettazioni (almeno sui database impiegati per la valutazione). Per avere un valore univocamente individuato, si può definire come ZeroFAR: "Il FRR ottenuto per il valore della soglia minimo tale che il FAR sia nullo."
**A.1.6. ZeroFRR**: percentuale di false accettazioni con la soglia di decisione regolata in modo da non causare mai false reiezioni (almeno sui database impiegati per la valutazione). Per avere un valore univocamente individuato, si può definire come ZeroFRR: "Il FAR ottenuto per il valore della soglia massimo tale che il FRR sia nullo"
**A.2. Resistenza ai tentativi di inganno con false caratteristiche biometriche**: alcuni sistemi biometrici di elevata sicurezza incorporano meccanismi per rilevare i tentativi di accesso fraudolento, ad esempio attraverso false caratteristiche biometriche.
**A.2.1. Vivezza**: resistenza rispetto a repliche sintetiche o copie di caratteristiche biometriche che potrebbero essere utilizzate per accedere fraudolentemente a un sistema (si veda § 7.5).
**A.2.2. Mimica**: resistenza rispetto a imitazioni di alcune caratteristiche comportamentali che possono essere sfruttate da individui dotati di particolari abilità mimiche (per i sistemi basati sul riconoscimento vocale) o di riproduzione calligrafica (per il riconoscimento della firma o della calligrafia in genere).
**A.3. Resistenza ai tentativi di manomissione:** indica la protezione garantita dal sistema a fronte di attacchi hardware o software.

**B. Robustezza**: capacità di funzionare in modo corretto, o comunque di garantire prestazioni minime, anche in condizioni non ottimali.
**B.1. Rispetto all'accuratezza dell'acquisizione**: la maggior parte dei sistemi biometrici sono in grado di elaborare correttamente campioni acquisiti in modo ottimale. D'altro canto al fine di rendere semplici e pratici i dispositivi di acquisizione non è possibile imporre vincoli stringenti e/o costringere l'utente a improbabili modalità di interazione con il dispositivo. Nella pratica dunque, specialmente quando l'uso del dispositivo biometrico è saltuario, l'acquisizione delle caratteristiche biometriche non è ottimale, e possono verificarsi anche

falsi rifiuti di utenti abilitati. Nel caso di impronte digitali, per esempio, se il dito non viene allineato correttamente con il sensore di acquisizione possono verificarsi errori. A tal fine è stata dimostrata l'importanza di utilizzare sensori con ampia area di acquisizione e risoluzione elevata; purtroppo ciò contrasta con la tendenza attuale dove per ridurre i costi e miniaturizzare i dispositivi vengono introdotti sul mercato sensori dall'area molto limitata a forte discapito della robustezza.

**B.2. Rispetto alla stabilità della caratteristica biometrica**: un'importante proprietà delle caratteristiche biometriche è rappresentata dalla loro "immutabilità" nel tempo dalla quale discende la garanzia che acquisizioni diverse determinino istanze molto simili tra loro. Purtroppo, anche se in misura diversa, alcune alterazioni possono causare instabilità: tagli ed escoriazioni nel caso di impronte digitali, trucco, espressioni e pettinatura nel caso del volto, raffreddamenti e umore nel caso della voce, ecc. Queste alterazioni producono normalmente un degrado nell'accuratezza del sistema (incremento di falsi rifiuti). Strategie che prevedono l'adattamento dinamico dei modelli memorizzati, l'impiego di modelli multipli o la richiesta di nuovo enrollment, sono generalmente adottate dai sistemi biometrici a fronte di variazioni significative della caratteristica considerata. Particolare cautela è necessaria in questo caso per evitare il cosiddetto "effetto deriva" che consiste nell'adattamento del modello di un individuo alla caratteristica biometrica di un altro individuo (anche non abilitato). Per questo motivo le operazioni di adattamento sono eseguite normalmente sotto la supervisione del responsabile della sicurezza.

**B.3. Rispetto ad alcuni soggetti, popolazioni, lavoratori**: in alcuni soggetti, popolazioni o classi di lavoratori manuali sono stati riscontrati problemi nell'impiego di specifiche tecnologie biometriche; ad esempio: menomazioni o handicap fisici limitano la capacità di interazioni con alcuni dispositivi; l'esiguo spessore delle creste epidermiche rende difficile l'acquisizione delle impronte digitali di persone anziane o di lavoratori manuali che sottopongono l'epidermide dei polpastrelli ad abrasione meccanica. L'impiego di sensori di elevata qualità (elevata risoluzione, ampia area di acquisizione, elevato contrasto, ecc.), anche se non risolve completamente il problema, consente di limitarne gli effetti negativi. Per gli aspetti legati a problematiche di accessibilità si rimanda al Capitolo 6.

**B.4. Rispetto all'ambiente**: in ambienti particolari alcuni sensori di acquisizione o sistemi di riconoscimento possono avere un comportamento non ottimale e causare un degrado di prestazioni. Ad esempio i sistemi di riconoscimento del parlato incontrano difficoltà in ambienti rumorosi, alcuni sensori per l'acquisizione di impronte digitali esibiscono un cattivo comportamento in ambienti particolarmente umidi, i sistemi per il riconoscimento del volto possono essere disturbati da variazioni di illuminazione. Per questi motivi le caratteristiche dell'ambiente che deve ospitare un'applicazione biometrica devono essere attentamente analizzate a priori.

**C. Usabilità**: specifica la semplicità e la praticità d'uso del sistema da parte sia dell'utente sia dell'amministratore responsabile della sua gestione, e indica l'adeguatezza dei tempi di risposta.

**C.1. Interazione con l'utente**: all'utente di un sistema biometrico può essere richiesto di eseguire un'operazione di verifica/identificazione anche molto frequentemente (più volte nell'arco di una giornata); è importante quindi che questa operazione avvenga nel modo più semplice e naturale possibile. Inoltre non sempre gli utenti sono esperti di sistemi informatici e quindi possono incontrare difficoltà con interfacce poco "user-friendly".

**C.1.1. Semplicità d'uso**: con particolare riferimento all'interfaccia uomo-macchina e alla sequenza temporale delle operazioni che devono essere eseguite a ogni accesso. Gli

applicativi software dovrebbero ad esempio esporre un'interfaccia utente con messaggi sempre espressi nel linguaggio della nazione in cui il sistema deve essere utilizzato; analogo discorso vale per i manuali utente e/o la documentazione informativa.

**C.1.2. Praticità d'uso**: indica la comodità d'uso del dispositivo, ovvero se sono richiesti scomodi, prolungati, o innaturali posizionamenti del corpo o di alcuni arti rispetto al sensore di acquisizione. Alcuni sistemi "economici" basati sul riconoscimento dell'iride richiedono un accurato allineamento (guidato dall'utente) dell'occhio con il dispositivo, a scapito della praticità d'uso; il problema non sussiste nei sistemi di fascia professionale dove la localizzazione/zoom del volto e degli occhi è eseguita automaticamente.

**C.1.3. Necessità di addestramento dell'utente o supervisione iniziale**: in genere al primo utilizzo di un nuovo sistema è necessaria una breve sessione di addestramento supervisionato dall'amministratore del sistema oppure guidato da un programma interattivo. È bene che il software applicativo sia dotato di funzionalità di auto-apprendimento che permettano agli utenti di verificare se operano nel modo corretto.

**C.1.4. Criticità della fase di enrollment**: a prescindere dall'addestramento iniziale, in alcuni sistemi la fase di enrollment è un'operazione piuttosto critica e talvolta può essere necessario ripeterla più volte. Nel caso di impronte digitali, risulta molto utile, specialmente in fase di prima registrazione degli utenti poter visualizzare "live" l'immagine dell'impronta digitale (si noti che non tutti i sistemi consentono di operare in questa modalità). Questo accorgimento permette agli utenti di rendersi conto del modo ottimale di posizionamento del dito (e ciò rende più veloce l'apprendimento) e della qualità intrinseca delle diverse dita.

**C.2 Interazione con l'amministratore del sistema**: la maggior parte dei sistemi biometrici richiede un'amministrazione centralizzata da parte di una persona responsabile al quale sono delegati compiti quali: definizione degli utenti, assegnazione dei codici di identificazione perdonale (PIN), addestramento iniziale degli utenti, monitoraggio degli accessi, intervento in caso di anomalie, regolazione delle soglia di sicurezza.. L'amministratore è tipicamente un esperto di strumenti informatici e quindi il requisito di semplicità delle procedure di amministrazione non è critico come quello nei confronti degli utenti. Ciononostante la presenza di un'esaustiva documentazione rispondente a criteri di qualità, , costituisce un importante elemento.

**C.2.1. Praticità d'uso**: valuta l'adeguatezza delle procedure di amministrazione e il tempo necessario per la loro esecuzione.

**C.2.2. Strumenti di controllo e di monitoraggio**: controllo delle mancate identificazioni; statistiche sull'utilizzo e sulle prestazioni del sistema possono essere svolti efficacemente dall'amministratore solo se il sistema mette a disposizione gli strumenti opportuni. Un costante monitoraggio è molto importante per la corretta gestione di un sistema biometrico con numerosi utenti.

**C.2.3. Necessità di supervisione**: alcune operazioni critiche quali l'enrollment e l'adattamento di un modello a fronte di salienti variazioni possono richiedere la supervisione dell'amministratore del sistema.

**C.2.4. Necessità di manutenzione**: alcuni dispositivi di acquisizione richiedono interventi di manutenzione (ordinaria e straordinaria), ad esempio per la pulizia/sostituzione di componenti ottiche e/o meccaniche. Con riferimento ai sensori di acquisizione di impronte digitali è bene prevedere una pulizia periodica, specialmente nel caso di sensori allo stato solido (capacitivi, campo elettrico, ecc.) che tendono ad accumulare velocemente sporco e grasso compromettendo la qualità delle immagini acquisite.

**C.3. Efficienza**: indica il tempo necessario per l'esecuzione delle due operazioni più comuni: l'enrollment e la verifica/identificazione. Ovviamente tempi di risposta elevati, specialmente

per l'operazione di verifica/identificazione, infastidiscono l'utente e rendono il sistema inutilizzabile in determinate applicazioni.
**C.3.1. Tempo di enrollment**: tempo necessario per completare un'intera operazione di enrollment (comprende i tempi di calcolo del sistema e i tempi impiegati dall'utente per l'interazione): varia tra alcuni secondi e qualche decina di minuti nei sistemi esistenti; è solitamente piuttosto elevato nei sistemi basati su caratteristiche comportamentali.
**C.3.2. Tempo di verifica/identificazione**: tempo necessario per completare un'intera operazione di verifica/identificazione (comprende i tempi di calcolo del sistema e i tempi impiegati dall'utente per l'interazione): varia tra alcuni secondi e qualche minuto nei sistemi per la verifica di identità, può essere notevolmente maggiore per sistemi di identificazione che operano su grandi database.

**D. Accettabilità**: alcuni fattori psicologici o emozionali possono contribuire a far sì che una particolare caratteristica biometrica o le procedure di accesso di un sistema biometrico risultino poco accettabili per specifici utenti o classi di utenti.
**D.1. Accettabilità della caratteristica biometrica**: è stato dimostrato che alcuni utenti provano diffidenza nell'utilizzo di alcune caratteristiche biometriche. Le impronte digitali vengono normalmente associate all'identificazione di criminali da parte della polizia e quindi, talvolta, gli utenti accettano di malgrado un'operazione di enrollment che è vista come una schedatura. D'altro canto, e per lo stesso motivo, la tradizione e la lunga storia delle impronte digitali contribuiscono a creare una grande fiducia nei sistemi di sicurezza basati su di esse. I sistemi che fanno ricorso a caratteristiche oculari creano invece negli utenti una preoccupazione, anche se ingiustificata, di arrecare danni ai propri organi visivi.
**D.2. Accettabilità delle operazioni di enrollment e di verifica/identificazione**: alcune procedure di enrollment e/o verifica/identificazione possono richiedere di fornire generalità o informazioni private (ad esempio l'altezza, il peso o l'età) che l'utente vorrebbe mantenere personali.

**E. Miscellanea**: non essendo correlati tra loro, i parametri riportati nel seguito sono stati raggruppati nella generica classe miscellanea, ma non per questo motivo deve essere attribuita loro minore importanza.
**E.1. Costo**: risulta determinante per una diffusione su larga scala dei sistemi biometrici e negli ultimi anni si sta verificando, di pari passo con la crescita del volume di affari, un calo marcato dei prezzi. Il costo dei sistemi commerciali esistenti varia da qualche centinaia di euro a qualche decina di migliaia di euro per postazione a seconda delle diverse caratteristiche biometriche utilizzate e delle finalità del sistema.
**E.2. Ingombro**: alcune tecnologie richiedono sensori di acquisizione non facilmente miniaturizzabili (ad esempio i sistemi basati sulla geometria della mano) e pertanto non possono essere impiegate dove sono richieste dimensioni ridotte. Nuove tecnologie sono state recentemente proposte per la miniaturizzazione dei sensori: nel campo delle impronte digitali, speciali sensori allo stato solido consentono di integrare l'hardware di acquisizione in una chip-card; anche se al momento le prestazioni di questi sensori risultano inferiori rispetto a quelli tradizionali si possono prevedere per il futuro evoluzioni interessanti.
**E.3. Dimensione dell'identificatore biometrico**: alcune applicazioni richiedono di memorizzare l'identificatore biometrico su un dispositivo (ad esempio: smart card, optical memory card o carta magnetica), che l'utente deve portare con sé e presentare al sistema in fase di autenticazione. Questo permette una memorizzazione distribuita delle informazioni personali e consente l'accesso a diversi sistemi anche non collegati in rete tra loro. Per questo

motivo sono particolarmente apprezzati i sistemi in grado di produrre identificatori di dimensioni molto contenute. Le dimensioni degli identificatori nei sistemi commerciali attualmente disponibili variano da pochi byte a qualche decina di Kbyte.

**E.4. Aderenza a standard**: come discusso in appendice sforzi significativi sono tuttora in corso nei diversi gruppi di lavoro ISO per la definizione di standard nel settore della biometria. In particolare a livello di interfaccia applicativa di un sistema biometrico, il comitato ISO sta adottando l'interfaccia BIOAPI che consente ad una applicazione di colloquiare con i dispositivi biometrici dei diversi fornitori in modo uniforme, semplificando il progetto, l'evoluzione e la manutenzione dei sistemi sviluppati. Benché pochi sistemi commerciali siano oggigiorno compatibili all'interfaccia BIOAPI (anche in ragione del fatto che non si è ancora giunti ad uno stadio finale), nel futuro l'aderenza a standard affermati assumerà senz'altro un ruolo sempre più importante. Spingendosi un passo oltre rispetto alla compatibilità a livello applicativo, si può pensare alla compatibilità dei modelli prodotti dai diversi sistemi che operano con la stessa caratteristica biometrica; in questo caso i modelli prodotti dal sistema del fornitore X sarebbero compatibili con il sistema del fornitore Y, con grossi benefici per la manutenzione, evoluzione, sostituzione ed espansione di sistemi, nonché per l'interoperabilità di diverse applicazioni. I gruppi di lavoro ISO stanno elaborando standard di riferimento per i modelli relativamente alle diverse tecnologie biometriche (come descritto in appendice).

**E.5. Integrabilità con altri sistemi**: l'integrazione di più tecnologie biometriche (sistemi multimodali) è stata sperimentata con successo in applicazioni che richiedono un elevato grado di robustezza. La possibilità di collegamento con altri sistemi, eventualmente già esistenti, è quindi un aspetto importante che non deve essere trascurato in fase di acquisizione di nuovi dispositivi hardware/software. Qualora un'organizzazione intenda dotarsi di sistemi biometrici sia per la sicurezza fisica (es. controllo d'accesso a locali) sia per la sicurezza logica (es. logon a PC e altre risorse) è fortemente consigliabile scegliere sistemi che prevedano una stretta integrazione delle due tipologie di sistemi, fornendo strumenti per l'amministrazione centralizzata ed evitando agli utenti di sottoporsi a sessioni di enrollment disgiunte.

**E.6. Adattabilità rispetto a specifiche applicazioni o ambienti operativi**: la scelta di una specifica tecnologia biometrica è talvolta dettata dal grado di adattabilità di una tecnologia rispetto a un'applicazione. A volte, infatti, procedure preesistenti richiedono già di interagire con dispositivi in grado di acquisire caratteristiche biometriche (ad esempio un apparecchio telefonico acquisisce normalmente il segnale vocale) e in questo caso l'aggiunta di un sistema biometrico che utilizza come caratteristica la voce può avvenire in modo trasparente e assolutamente non invasivo. è inoltre necessario verificare la compatibilità di dispositivi e soluzioni che si intende acquisire con i sistemi operativi utilizzati.

Prima di affrontare il problema della scelta della tecnica biometrica è opportuno sottolineare che non esiste una tecnologia biometrica migliore ma esistono applicazioni per le quali è più indicata una certa tecnologia piuttosto che un'altra. Con riferimento alle tecnologie biometriche descritte nel capitolo 3 di seguito viene riportata una tabella comparativa relativa ad alcuni dei parametri di valutazione sopra esposti.

| | impronte | geometria della mano | iride | viso | voce | firma |
|---|---|---|---|---|---|---|
| accuratezza | alta | medio/alta | molto alta | media | medio/bassa | medio/bassa |
| accettabilità | medio/alta | medio/alta | media | alta | alta | alta |
| usabilità | medio/alta | alta | medio/alta | alta | alta | alta |
| stabilità nel tempo della caratteristica fisico/comp. | alta | media | alta | medio/bassa | media | medio/bassa |
| costo del sensore [25] | basso [26] | medio | basso/alto [27] | medio/alto | basso | medio |
| dimensioni del template [28] | 800 – 1500 byte | 10 byte | 512 byte | 1000 – 2000 byte | 2000 – 10000 byte | 1500 byte |
| maggiori cause di errore | aria troppo secca<br><br>scarsa accettazione<br><br>polpastrello sporco e/o rovinato | lesioni traumatiche della mano | condizioni di illuminazione<br><br>danneggiamento dell'occhio | rumori di fondo<br><br>scarsa accettazione<br><br>polpastrello sporco e/o rovinato | media | media |

*Tabella 7.1: : comparazione relativa ad alcuni dei parametri di valutazione esposti*

Nella tabella seguente è riportata una sintesi dei principali campi di applicazione per le diverse tecnologie biometriche in esame.

[25] Per basso si può intendere, microscopicamente, un prezzo inferiore ai 500 Euro, medio dai 500 ai 2000 Euro, alto oltre i 2000 Euro

[26] Alcuni sensori, basati su tecniche di acquisizione più sofisticate, come ad esempio, gli ultrasuoni, si collocano in fascie più alte

[27] I sensori per accesso logico si collocano nella fascia di prezzo bassa, quelli per l'accesso fisico nella fascia alta

[28] Le dimensioni del template possono influire sui tempi di accesso ad un archivio (soprattutto di grandi dimensioni) e sulla possibilità di essere inglobati su smartcard. La scala dei valori premia dunque i template di dimensioni minori.

| | impronte digitali | geometria della mano | iride | viso | voce | firma |
|---|---|---|---|---|---|---|
| accesso fisico di massa | buono | ottimo | buono | buono / medio | - | - |
| accesso fisico a zone sensibili | buono | buono/medio | ottimo | buono / medio | - | - |
| accesso logico | ottimo | - | medio | buono/ medio | medio | - |
| documenti | ottimo | - | buono | ottimo | - | - |
| transazioni economiche/ e-government | buono | - | medio/buono | medio/buono | buono | buono |
| sorveglianza | - | - | - | buono | - | - |

*Figura 7.2*

Deve essere infine valutata la possibilità di ricorrere per specifiche applicazioni (specie quando si deve/vuole operare in modalità identificazione) a sistemi multimodali dove più tecniche biometriche vengono utilizzate in congiunzione o in alternativa. Ricorrere all'uso congiunto di più tecnologie biometriche ha tipicamente l'obiettivo di accrescere i livello di sicurezza. In questo caso l'utente viene riconosciuto dal sistema soltanto se i controlli basati su tutte le chiavi biometriche prescelte danno esito positivo. Ricorrere a più tecnologie biometriche in modo alternativo ha generalmente l'obiettivo di limitare le "eccezioni". In questo secondo caso affinché l'utente venga riconosciuto dal sistema è sufficiente che il controllo dia esito positivo su almeno una delle chiavi biometriche prescelte. Più in dettaglio:

- l'uso congiunto (AND) di tecniche biometriche può portare a un forte incremento delle prestazioni in termini di accuratezza. Un sistema basato su impronte digitali che richiede l'acquisizione di due dita, a fronte di un incremento solo lineare delle false reiezioni (FRR), garantisce una riduzione esponenziale delle false accettazioni (FAR), consentendo nella pratica di operare anche in modalità identificazione su archivi di grosse dimensioni. Un sistema ibrido volto e impronta potrebbe "scremare" l'elenco dei candidati ricorrendo alla similarità tra volti e raffinare la ricerca sulla base dell'impronta digitale. L'impiego di più caratteristiche biometriche minimizza inoltre la probabilità di successo in caso di attacchi al sistema, ad esempio con false caratteristiche biometriche;
- l'uso in alternativa di tecniche biometriche (OR) consente in genere di gestire meglio casi critici. Nessuna caratteristiche è veramente universale e non è infrequente la presenza di individui che, temporaneamente o permanentemente, si trovino nella impossibilità di utilizzare in modo efficiente una particolare caratteristica biometrica. Tali problematiche possono essere gestite da sistemi multimodali che prevedano appunto l'uso in alternativa di tecniche biometriche. In questo caso possiamo affermare che, a fronte di un livello di sicurezza circa pari a quello garantito dalla tecnologia biometrica più "debole" fra quelle individuate, si ha una notevole riduzione dei falsi rigetti.

## 7.3 Aspetti tecnico-organizzativi

### 7.3.1 Localizzazione dell'identificatore biometrico

Elemento molto importante nella individuazione dei requisiti di una soluzione biometrica è rappresentato dalle modalità di localizzazione dell'identificatore biometrico sul supporto di memoria. Esistono due possibili approcci, il primo consiste nell'affidare al titolare del dato la custodia dell'identificatore biometrico; il secondo consiste nel memorizzare tale identificatore in una banca dati centralizzata.

DATO BIOMETRICO CUSTODITO DALL'INDIVIDUO

In questo approccio viene effettuato il confronto tra l'identificatore biometrico rilevato "dal vivo" dal soggetto e le informazioni recuperate dal supporto di memoria da egli stesso custodito. Il risultato del confronto consente la conclusione del processo di autenticazione che, nel caso in cui il sistema preveda la trasmissione in rete di tale informazione, vista la quantità (minima) e la qualità dei dati trasmessi (esito) può usufruire della rete già esistente.
Con questo approccio a rigore non è strettamente necessario prevedere l'esistenza di una base dati per la raccolta centralizzata degli identificatori biometrici. Tale aspetto consente, talaltro, di rispettare in modo assoluto gli eventuali vincoli all'uso di identificativi biometrici, imposti dall'autorità Garante per la protezione dei dati.
Occorre comunque sottolineare che nel caso della mancanza di una base dati e della relativa infrastruttura di comunicazione non sia possibile la gestione di situazioni eccezionali nelle quali tali informazioni non siano recuperabili dal supporto di memoria trasportabile (es. malfunzionamento o usura del supporto) pertanto in tal caso occorre prevedere delle adeguate procedure alternative.
Nelle applicazioni ove la gestione delle eccezioni non possa essere effettuata diminuendo i livelli di sicurezza occorre valutare l'opportunità di avere una banca dati, e della relativa infrastruttura di rete, adeguatamente protette, da utilizzarsi non per l'identificazione 1:N dell'individuo che effettua il tentativo di accesso, ma solo"ad evento", per recuperare l'identificatore dell'utente a seguito di situazioni "eccezionali", effettuando la usuale verifica attraverso l'identificatore acquisito dal vivo, durante la sessione corrente.

Di seguito vengono riportati alcuni dei principali vantaggi e svantaggi di tale approccio.
Vantaggi:

- favorisce il rispetto della riservatezza del dato biometrico. L'identificatore biometrico è recuperabile dal supporto di memoria trasportabile e non è strettamente necessario, a tal proposito, garantire la consultabilità di una base dati centralizzata ad ogni confronto;
- è integrabile con i sistemi per il controllo degli accessi eventualmente esistenti;
- nel caso di un sistema di controllo accessi eventualmente già esistente, e le procedure di gestione ad esso relative, possono essere aggiornate con impatti minimi per l'integrazione del sistema biometrico;
- l'autorizzazione all'accesso prevede un processo di confronto del tipo uno-a-uno (verifica) tra il template recuperato dal supporto e quello calcolato dal dato acquisito dal vivo durante la sessione di accesso corrente. L'effettuazione di controlli uno-a-uno consente l'utilizzo di un maggior numero di tecnologie

biometriche (la scelta è allargabile a quelle nelle quali l'efficacia in caso di confronti uno-a-molti non è ancora garantita).

Svantaggi:

- ipotetica realizzazione fraudolenta di supporti di memoria contenenti un template diverso da quello cui si riferisce l'identificativo. Misura di controllo: il livello di sicurezza può essere alzato inserendo nella fase di registrazione dei dati (biometrici e non) nel supporto la loro firma digitale con la chiave privata del soggetto avente l'autorità necessaria ad emettere la carta o il documento di accesso;
- la necessità di sostituzione dei sistemi di lettura di token tradizionali con sistemi di lettura di supporti di memoria contenenti il dato biometrico;

DATI BIOMETRICI CUSTODITI IN UNA BANCA DATI CENTRALIZZATA

L'identificatore del soggetto che effettua il tentativo di accesso è contenuto dalla banca dati che custodisce in modo centralizzato tutti i dati relativi agli individui iscritti al sistema. In tal caso il tipo di confronto effettuato può ancora essere "uno-a-uno". Occorre, pertanto, prevedere una infrastruttura di rete di trasmissione. Sia la banca dati, sia la relativa infrastruttura di rete, devono essere tali da garantire la operatività con requisiti di affidabilità molto stringenti, giacché in tale approccio il loro utilizzo è per ogni sessione di accesso e non "ad evento", per la sola gestione delle eccezioni.

L'architettura con banca dati centralizzata consente di effettuare sia un confronto "uno-a-uno" per la verifica dell'identità, recuperando l'identificatore biometrico relativo al soggetto che dichiara di essere l'utente che effettua il tentativo di accesso, sia un confronto "uno-a-molti" per l'identificazione verso tutti i membri iscritti nell'archivio.

Di seguito vengono riportati alcuni dei principali vantaggi e svantaggi di tale approccio.

Vantaggi:

- è possibile effettuare sia la "verifica" (confronti "uno-a-uno"), sia l'"identificazione" (confronti "uno-a-molti");
- minor vulnerabilità legata al furto o alla falsificazione del dato biometrico, che è custodito in una banca dati e non dall'utente.

Svantaggi:

- necessità della rete per la trasmissione degli identificatori biometrici opportunamente protetta;
- possibili problemi legati al rispetto della riservatezza dei dati biometrici memorizzati nella base dati centralizzata, soprattutto nel caso di identificazione (confronti "uno-a-molti");
- i dati biometrici rimangono in esclusivo possesso dell'amministratore della banca dati;
- nel caso di identificazione (confronto "uno-a-molti") le prestazioni diminuiscono all'aumentare della popolazione della base dati (tempi di ricerca e frequenza di errori).

### 7.3.2 Componenti tecniche e organizzative di un sistema biometrico

Un sistema biometrico può essere scomposto in quattro sottosistemi che verranno illustrati nel seguito. Inoltre in funzione delle dimensioni del sistema biometrico può essere prevista o meno la creazione di apposite strutture organizzative o l'attribuzione delle funzioni previste ad unità organizzative esistenti.

**Sottosistema di registrazione (enrollment) degli utenti**

Il sottosistema di registrazione deve accertare l'identità dell'utente che viene inserito nel sistema e svolgere le azioni necessarie all'acquisizione delle caratteristiche biometriche previste. La maggior parte di queste attività sono similari a quelle svolte attualmente per rilasciare un badge di riconoscimento ad un dipendente (anche in quel caso si acquisisce in genere una caratteristica biometrica: l'immagine del viso) anche dal punto di vista della sicurezza con cui trattare i dati acquisiti. Nel caso di un'applicazione biometrica interna alla amministrazione tale funzione è generalmente gestita dall'unità organizzativa che sovrintende la gestione del personale. Tra i compiti affidati al responsabile della registrazione:

- *Istruire gli utenti sull'impiego di hardware e software*. I manuali utente a corredo dei sistemi biometrici sono spesso difficilmente comprensibili *dall'utente non esperto e ancor più raramente essenziali.*
- *Gestire e/o supervisionare la fase di enrollment degli utenti*. La fase di prima registrazione delle caratteristiche biometriche assume un ruolo molto importante per il funzionamento a regime del sistema. In questa fase il responsabile deve: 1) verificare che l'utente abbia compreso come utilizzare il sistema procedendo ad alcuni test pratici; 2) quando possibile scegliere tra le diverse caratteristiche biometriche quella ottimale (ad esempio il dito di miglior qualità); 3) assicurarsi di aver acquisito campioni di elevata qualità; 4) far eseguire all'utente alcuni tentativi di accesso verificando che tutto funzioni correttamente; 5) se previsto e necessario, personalizzare i parametri di sicurezza dell'utente.
- *Gestire modalità di accesso non-biometriche*. Qualora, pur avendo adottato tutti gli accorgimenti del caso, un utente continui ad incontrare difficoltà nell'utilizzo del sistema o si incorra in frequenti falsi rifiuti è opportuno meccanismi di accesso alternativi.

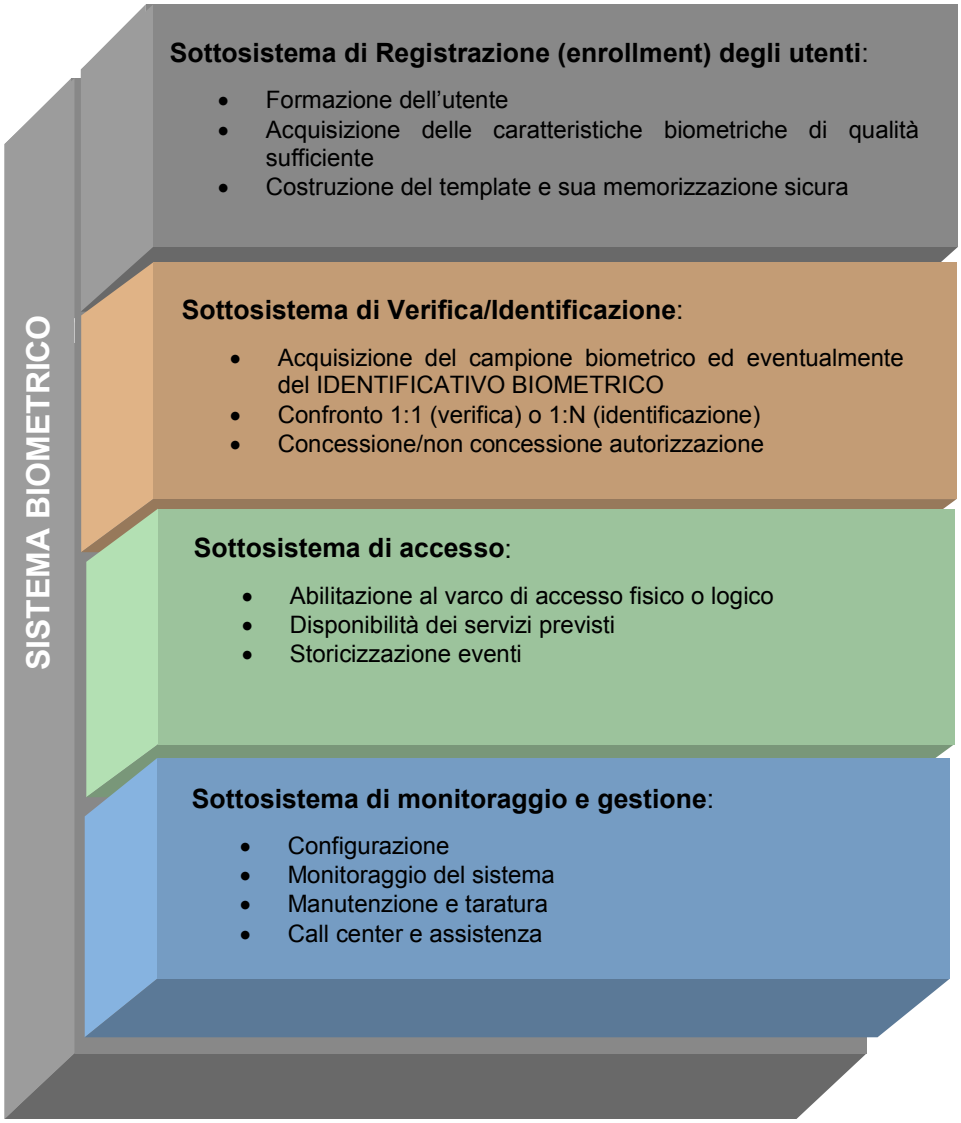


*Figura 7.3:i sottosistemi che costituiscono l'implementazione e la messa in esercizio di un sistema biometrico.*

Casi particolarmente complessi sono costituiti dalle applicazioni che richiedono una registrazione di massa (es. documenti di identificazione, autorizzazioni per accedere ad aree a rischio, ecc…). In queste situazioni occorre opportunamente progettare il sistema tecnico ed organizzativo necessario ponendo particolare attenzione alla riduzione degli "errori di registrazione" impliciti in alcune tecniche biometriche prevedendo una procedura di "test reale" del dato acquisito; infatti, una percentuale di errore del 2,8% (documentata in alcuni esperienze precedenti) rapportata a un universo di 10.000.000 di individui significa 280.000 errori; il costo del recupero di tali errori non è solo rappresentato dal dover ripetere l'operazione con i costi associati (es. un costo di € 10,00 per ogni recupero equivale su 280.000 casi da recuperare con un costo aggiuntivo di € 2.800.000,00) ma soprattutto di immagine nell'opinione pubblica circa l'affidabilità del sistema complessivo e la conseguente accettazione dei nuovi strumenti.

**Sottosistema di Verifica / Identificazione**

Il sottosistema di verifica/identificazione consiste nella stazione operativa biometrica che può realizzarsi con un semplice sensore di lettura o con un sofisticato sistema multimodale, nel

caso di una applicazione per il controllo di un'area a elevato rischio. In una tale situazione può essere necessario garantire l'interoperabilità con altri sistemi per procedure di identificazione negativa. Tale sottosistema è del tutto similare a quello già oggi presente per i sistemi di rilevazione delle presenze, di controllo degli accessi fisici e logici mediante un badge identificativo.

**Sottosistema di accesso**

Il sottosistema di accesso consiste nel varco fisico o logico che consente il transito della persona autorizzata, o non autorizzata, nella fase di verifica /identificazione. Nelle aziende, anche in questo caso, l'organizzazione è del tutto similare a quella già in essere per gli accessi fisici, porte automatiche e barriere di ogni genere, o per gli accessi logici, single sign-on e profiling degli utenti. Un caso particolare è rappresentato dai varchi fisici: la progettazione di un sistema di controllo degli accessi richiede l'integrazione di dispositivi di diversa natura: meccanici (tornelli, bussole, barriere motorizzate), dispositivi elettronici per l'acquisizione ed elaborazione del dato biometrico, con altri sistemi di sicurezza (sistemi video e anti-intrusione).

Nella realizzazione di applicazioni inerenti l'accesso fisico, la valutazione e l'accurata scelta dei dispositivi meccanici di ingresso e la disposizione di questi ultimi giocano un ruolo fondamentale sulle prestazioni del sistema. Nel caso di un elevato volume di transiti da gestire nell'unità di tempo, o di un elevato livello di sicurezza richiesto dallo specifico varco, occorre prevedere la presenza di due uscite: una per le situazioni di normale verifica ed l'altra presidiata per gestire le eccezioni (occorre, ad esempio, prevedere la possibilità di accedere rapidamente ad un servizio di assistenza all'uso dell'unità biometrica), o alla necessità di pulizia dei sensori di rilevazione dell'unità biometrica (nel caso di lettori di impronte digitali, dopo un certo numero di letture, in funzione del tipo e qualità del lettore e dalle modalità di impiego).

Per quanto riguarda l'accesso logico si rimanda alla § 4.2 sottolineando nuovamente che il sottosistema di accesso rappresenta l'integrazione del sottosistema di verifica/identificazione con l'infrastruttura di gestione dell'autenticazione/autorizzazione.

**Sottosistema di monitoraggio e gestione**

Il sottosistema monitoraggio e gestione consiste nell'unità organizzativa e nell'infrastruttura tecnologica che sovrintende al funzionamento dell'intero sistema biometrico. Le attribuzioni sono simili a quelle del centro di gestione dei sistemi informatici o, più in generale, dei sistemi tecnici. Nel caso di sistemi biometrici complessi è necessaria la creazione di un'apposita struttura che garantisca il funzionamento dello stesso, con l'ausilio di opportuni strumenti automatici, che provvedano a monitorare costantemente gli eventi "critici" intercettati. Tale funzione può avere modalità di erogazione stringenti quali la presenza continua di operatori sulle 24h per 7 giorni alla settimana. Il raggiungimento dei requisiti e dei benefici che hanno determinato l'introduzione del sistema biometrico è fortemente correlata dal tale struttura operativa. In particolare è necessario:

*verificare che gli utenti riescano ad accedere regolarmente al sistema*. In caso negativo cercare di comprenderne le cause. Una variazione sopravvenuta a seguito della registrazione (ad esempio taglio o seria escoriazione di un dito) può creare problemi a un sistema per il riconoscimento di impronte digitali. In alcuni casi è consigliabile procedere a una nuova registrazione o a un aggiornamento della stessa;

supervisionare i tempi di accesso, per evitare che alcuni utenti interagendo in modo errato con i dispositivi siano costretti a più tentativi. Alcuni utenti, interagendo con il dispositivo di

acquisizione in modo sbagliato, sono spesso costretti a ripetere diverse volte la procedura. Attraverso i log di sistema, l'amministratore può rendersi conto del verificarsi di queste situazioni, e addestrare nuovamente l'utente all'impiego ottimale del dispositivo;
*personalizzare i parametri di sicurezza per utenti diversi*. La possibilità di variare la soglia di sicurezza utente per utente, è molto importante in quanto permette di gestire al meglio utenti "difficili" senza diminuire significativamente il livello di sicurezza generale del sistema. Non tutti i sistemi permettono di modificare la soglia a livello di utente ma, quando questa opzione è disponibile, è buona norma farvi ricorso. Si supponga che un utente sia l'unico in un gruppo di cento utenti che incontra difficoltà ad avere accesso tramite impronte digitali e che debba, a ogni tentativo di accesso, ripetere la procedura di verifica di identità diverse volte. L'amministratore di sistema può intervenire riducendo ragionevolmente la soglia di tale utente senza alterare quella dei rimanenti 99. Un impostore che volesse sfruttare questa riduzione di soglia dovrebbe, innanzitutto sapere che la soglia del particolare utente è stata diminuita e in secondo luogo impersonare obbligatoriamente nei tentativi di accesso fraudolento l'utente riducendo significativamente le sue probabilità di successo;
*rilevare accessi "strani" sintomatici di attacchi al sistema*. I log di sistema possono aiutare l'amministratore a capire se sono stati eseguiti tentativi di accesso non autorizzato al sistema. Infatti qualora la frequenza di tentativi di accesso subisca picchi anomali e/o vengano registrati molti falsi rifiuti, l'amministratore può, anche con l'aiuto degli utenti, capire se si tratta di tentativi di accesso fraudolento;
*verificare il funzionamento del sistema e ottimizzarne i parametri*. Alcuni sistemi prevedono procedure di "calibrazione" dell'hardware e l'esecuzione periodica di programmi di consolidamento e/o ottimizzazione delle prestazioni. Rientrano in questa categoria anche le operazioni di pulizia periodica dei sistemi di acquisizione;
*gestire i rapporti con il fornitore della tecnologia, e caricare aggiornamenti*. L'amministratore matura con il tempo una buona conoscenza del sistema e del suo comportamento. Questi è quindi la figura più indicata a gestire i rapporti con il fornitore per quanto riguarda la segnalazione delle anomalie, l'assistenza e l'aggiornamento del sistema.

## 7.4 Elementi per l'analisi costi benefici

Gli elementi da considerare durante l'analisi costi-benefici per l'adozione di un sistema biometrico variano naturalmente da applicazione ad applicazione (accesso logico, accesso fisico, documenti di identità, ecc.). In Tabella 2 vengono identificati alcuni fattori per l'analisi costi-benefici che vanno integrati con gli elementi peculiari della applicazione.

| Costi | Benefici |
|---|---|
| Hardware biometrico<br>Licenze software biometrico<br>Contratti di servizio e/o manutenzione<br>Installazione e integrazione con i sistemi esistenti<br>Manutenzione periodica<br>Amministratore di sistema<br>Supporti di memorizzazione (acquisto e gestione) | Maggiore affidabilità del processo di autenticazione<br>Gestione password sicure<br>Maggiore comodità per l'utente<br>Effetto deterrente rispetto a comportamenti indesiderati |

*Tabella 7.2: elementi per l'analisi costi-benefici*

Il costo di un sistema biometrico varia in funzione del numero di utenti anche a parità di hardware e software. Pertanto il costo di acquisizione del sistema è composto da una parte fissa e da una variabile in funzione del numero di utilizzatori. Benché esistano studi di settore piuttosto analitici, risulta spesso difficoltoso quantificare economicamente il risparmio indotto dalla non necessità di gestione di password sicure e la riduzione del rischio derivanti da intrusioni illecite.

Oltre alle problematiche di natura economica si vuole qui sottolineare un altro aspetto, spesso sottovalutato, ovvero quello della comodità d'uso: l'implementazione di un sistema biometrico può comportare per gli utenti/amministratori reali vantaggi in termini di operatività quotidiana. Si sottolinea infatti che dover ricordare molte password è spesso complesso e molti studi di settore indicano che la maggior parte degli utenti ha dimenticato almeno una volta la propria password per l'accesso al telefonino, al bancomat, alla carta di credito, al conto corrente, al PC, ecc.. Se le password sono sicure (lunghe, difficili e cambiate frequentemente) spesso si commettono errori nella digitazione, specialmente quando si è costretti a inserirle in presenza di altre persone.

## 7.5 La sicurezza dei dati e dei sistemi biometrici

### 7.5.1 Criticità

Il dato biometrico ideale rappresenta una caratteristica di un individuo unica e inscindibile dal proprietario. Tale aspetto rappresenta il punto di forza a sostegno dell'impiego di sistemi biometrici per il riconoscimento certo degli individui. Le stesse peculiarità di unicità e inscindibilità del dato biometrico dall'individuo, rappresentano al contempo un elemento di debolezza dei sistemi biometrici. Mentre una password non più sicura o violata può essere sostituita, anche in base ad un piano di aggiornamento periodico programmato, lo stesso non può dirsi di una caratteristica biometrica (non è pensabile la sostituzione dell'iride di un individuo o dell'impronta digitale, al massimo è possibile rilevare un nuovo dato biometrico dello stesso tipo per un numero limitato di volte: l'impronta di una latro dito, l'iride dell'altro occhio, ecc.).
Da tale considerazione emerge l'importanza della sicurezza, e della necessità di protezione, del dato biometrico.
La sicurezza del dato biometrico riguarda l'insieme delle misure adottate durante le fasi di trattazione dei campioni biometrici caratteristiche di un sistema biometrico, segnatamente della registrazione e conservazione del campione (o del suo template) in un supporto di memoria, nelle modalità di trasporto e nell'integrazione del dato all'interno del sistema.
Le vulnerabilità dei sistemi biometrici sono evidenziate in questa sezione, mentre gli aspetti di gli aspetti di riservatezza del dato biometrico, legati al livello di sicurezza dello stesso, sono stati affrontati nel capitolo 5.
Per ciò che riguarda le modalità di trasporto del dato, e quelle di conservazione dello stesso, tra loro non indipendenti, si può utilmente consultare nella sezione precedente sulla localizzazione del dato biometrico, dove sono state descritte sia le soluzioni di memorizzazione dei dati biometrici di ciascun utente (su banca dati centralizzata, e su supporto trasportabile), sia le relative eventuali necessità di rete di trasmissione.

Nella sezione corrente è comunque utile ribadire alcune raccomandazioni auspicabili.
Utilizzare per la conservazione del dato biometrico di riferimento acquisito durante la fase di iscrizione, il template da esso calcolato. La giustificazione di tale raccomandazione risiede nella considerazione che estraendo dal campione le sole caratteristiche utili al confronto, con compressione e perdita dell'informazione globalmente contenuta nel campione biometrico, si evita di trattenere dati che:

- non migliorano le prestazioni del sistema,
- possono contenere elementi in grado di ricondurre al proprietario del dato,
- si prestano meglio alla falsificazione e alla realizzazione di campioni biometrici fittizi e al loro impiego.

L'utilizzo del template va dunque considerato ogni volta che sia possibile, con ciò intendendo ogni volta che con tale scelta vengano soddisfatti gli eventuali requisiti di interoperabilità dell'applicazione.
E' poi fortemente raccomandabile che, nell'eventualità della trasmissione di dati biometrici, siano previsti meccanismi di protezione della comunicazione (es. crittografia, protocolli di rete sicuri). Tale esigenza è particolarmente rilevante nel caso di utilizzo di banche dati centralizzate per la conservazione dei dati biometrici. In tale soluzione i dati biometrici (o i template) devono essere trasferiti ogni volta per l'effettuazione del confronto biometrico con il campione acquisito dal vivo.

### 7.5.2 Vulnerabilità

Un sistema biometrico, come qualsiasi altro tipo di sistema, non è inattaccabile in termini assoluti, ma presenta specifiche vulnerabilità che possono essere sfruttate per attacchi da parte di soggetti che ne conoscono i principi di funzionamento.
Le due principali tipologie di attacco sono l'attacco attraverso false caratteristiche biometriche e l'attacco all'hardware/software del sistema.

**Attacco attraverso false caratteristiche biometriche**

La letteratura e la cinematografia ci hanno abituato da tempo a casi di amputazioni di dita e replicazioni dei bulbi oculari. Anche senza considerare situazioni estreme di questo genere, è stata recentemente dimostrata la possibilità di riprodurre in laboratorio alcune caratteristiche biometriche. Occorre inoltre osservare, a tal proposito, come un dato biometrico di qualsiasi tipo non sia da considerarsi intrinsecamente protetto o segreto. L'iride può essere osservata, quindi rilevata, praticamente ovunque, se dotati delle giuste apparecchiature fotografiche. Le dita vengono quotidianamente utilizzate senza particolari precauzioni; anche le impronte digitali sono rilevabili da persone con le giuste competenze tecniche e attrezzature. Lo stesso dicasi per il volto, la voce, e molte altra caratteristiche biometriche.
Ne consegue che la sicurezza di un sistema con componenti che effettuano riconoscimento d'identità basata su identificativi biometrici, non debba essere unicamente basata sulla "conoscenza" del dato biometrico, da intendersi precisamente come possesso della caratteristica fisiologica, alla stregua di una password per l'accesso fisico, logico o per il controllo dell'identità del portatore di un documento, come descritto in 4.2. Tale sicurezza potrebbe essere ottenuta, scagionando il pericolo dell'uso fraudolento di tecniche di "mimica", plagio o furto della caratteristica fisiologica misurata, solo accertando la provenienza del dato biometrico da una persona fisica "viva" all'atto della cattura appena precedente il confronto.

Per smascherare tentativi di accesso effettuati tramite caratteristiche biometriche posticce, alcuni sistemi basati su impronte digitali incorporano dispositivi che cercano di rilevare la "vivezza" del soggetto attraverso misure di parametri quali temperatura, flusso sanguigno, capacità dielettrica e movimento. Nel caso del riconoscimento volto umano può essere rilevato ad esempio il periodico movimento di chiusura delle palpebre per evitare che una fotografia possa essere presentata alla telecamera. Si raccomanda la massima prudenza nell'analisi di informazioni relative a questo aspetto. Da una parte, infatti, fin troppe speculazioni sono state fatte circa la relativa semplicità con cui sarebbe possibile ingannare sistemi con false caratteristiche biometriche (operazione nella pratica non semplice quando l'utente di cui si vogliano clonare le caratteristiche non è consenziente); dall'altra i fornitori di sistemi biometrici hanno contribuito a creare un clima di diffidenza vantando soluzioni in grado di risolvere il problema che poi si sono rilevate inadeguate e/o immature nei test sul campo. La ricerca scientifica è molto attiva in questo settore, ed è lecito attendersi che negli anni a venire i dispositivi di acquisizione incorporeranno meccanismi efficaci per la soluzione del problema.
Oltre alla effettiva verifica di vivezza della caratteristica, i progettisti di sistemi possono impiegare tecniche di tipo challenge/response, ove al soggetto viene richiesto un campione biometrico specifico della sessione di confronto corrente scelto ogni volta in modo pseudocasuale (es. un particolare atteggiamento nel caso di riconoscimento del volto o dell'andatura, ovvero una delle dita, per il riconoscimento basato sulle impronte digitali).
Infine, l'utilizzo congiunto della caratteristica biometrica e di un token può significativamente incrementare la sicurezza rispetto a "furti" delle caratteristica biometrica.

**Attacco all'hardware e/o al software del sistema**

I principali attacchi al sistema sono riconducibili alle seguenti categorie:

- furti e/o intercettazioni dei dati biometrici: l'aggressore potrebbe ricorrere ai cosiddetti attacchi-replay nei quali, forzando l'accesso al sistema informatico, ruba una copia dell'immagine digitale e/o del template del dato biometrico, per servirsene in altre occasioni. In caso di furto le caratteristiche di immutabilità e di quasi insostituibilità di una caratteristica biometrica divengono aspetti sfavorevoli che ne precludono per sempre l'uso. Appare pertanto di fondamentale importanza nella progettazione di sistemi biometrici l'impiego di tecniche di firma digitale e crittografia, nonché di protocolli challenge/response che impediscono la ri-trasmissione iterata delle stesse informazioni;
- inganno nella fase del confronto: anche se il campione biometrico in input è corretto, il risultato generato dal sistema viene alterato, con trasformazione, in particolare:
    - del dato biometrico fornito al sistema nella sessione corrente di confronto (l'aggressore, ad es., potrebbe veicolare nel sistema informatico un virus del tipo "cavallo di Troia", che alteri il funzionamento del software applicativo di effettuazione del confronto, somministrando dati erronei al modulo di estrazione dei parametri biometrici del campione acquisito);
    - del valore dello score prodotto dal singolo confronto (con il metodo del "cavallo di Troia" sopra descritto, sarebbe anche possibile alterare il risultato del confronto della procedura biometrica);
    - del valore della soglia utilizzata nella fase di decisione (l'aggressore potrebbe alterare la soglia di decisione, aumentandola per causare

l'accettazione da parte del sistema, ovvero diminuirla per aumentare i falsi rifiuti e mettere in crisi il sistema di gestione delle eccezioni).

Vengono in genere considerati separatamente gli "attacchi puliti", ovvero quelli che non lasciano traccia dell'azione perpetrata, e i sabotaggi, che, al contrario, alterano il normale stato o funzionamento del sistema. Per una quantificazione oggettiva del livello di protezione di uno specifico sistema non esistono ancora criteri e metodologie consolidate, ma nell'ambito dei Common Criteria (CC) si sta da tempo lavorando per definire criteri di valutazione specifici per i sistemi biometrici; è stata ad esempio introdotta una Biometric Evaluation Methodology (BEM) e sia dagli Stati Uniti sia dal Regno Unito sono stati proposti Protection Profile (PP) per diversi livelli di sicurezza (EAL). Pochissimi prodotti sono stati però sottoposti a certificazione e l'unica finora rilasciata è stata ottenuta prima della formalizzazione di BEM e PP. In futuro questo tipo di certificazione assumerà un ruolo crescente specialmente in applicazioni di massima sicurezza. In assenza di criteri precisi, in questa sede sono fornite solamente alcune semplici indicazioni sulla resistenza alla manomissione:

- in genere i sistemi che eseguono estrazione delle caratteristiche e matching su hardware protetto (dispositivo sicuro) sono più resistenti rispetto ai sistemi di sola acquisizione che prevedono successive elaborazioni su PC. D'altro canto essi sono in genere dotati di una minore potenza computazionale (imponendo di fatto una perdita significativa sull'accuratezza) e sono caratterizzati da un maggior costo; ciò li rende meno appetibili per applicazioni di massa. Grazie alle loro doti di resistenza agli attacchi e di massima tutela della privacy (in quanto le informazioni biometriche non abbandonano mai l'hardware protetto) si può prevedere che i cosiddetti sistemi "match on token" guadagneranno in futuro un ruolo significativo;
- tutti i dispositivi che richiedono elaborazione esterna dovrebbero implementare funzionalità crittografiche per la trasmissione di informazioni cifrate (al PC, sulla rete, ecc.) ed essere resistenti ad attacchi di tipo "replay" (ad esempio attraverso meccanismi challenge-response);
- nei sistemi per la sicurezza fisica, la circuiteria per lo sblocco degli attuatori (ad esempio le elettroserrature) dovrebbe sempre essere installata sul lato protetto, e la comunicazione tra questa e l'unità di controllo (spesso esterna) dovrebbe essere protetto da crittografia.

## 7.6 La biometria nella strategia generale di sicurezza

### 7.6.1 La pianificazione della sicurezza

La scelta di un meccanismo di sicurezza di tipo biometrico è l'ultimo passo di un processo che deve partire dalla definizione delle strategie generali di sicurezza [29]. Si tratta di un'attività prioritaria che ha lo scopo di definire le azioni necessarie per la sicurezza in funzione dello scenario di rischio, degli obiettivi strategici aziendali o istituzionali e del contesto tecnico ed organizzativo in cui si opera. Tale attività è prevista dal Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196) attraverso la stesura del documento programmatico per la sicurezza[30], nonché da documenti di indirizzo e da norme internazionali[31].

Senza entrare nel merito dei metodi, fortemente dipendenti dal contesto, con cui è possibile pianificare la sicurezza informatica, si può asserire che in generale occorre almeno identificare:

- i rischi cui si è soggetti,
- i rischi da fronteggiare ed individuare;
- le soluzioni più idonee per ridurre il livello di tali rischi.

### 7.6.2 La valutazione dei rischi

Secondo la letteratura, la sicurezza informatica consiste nell'assicurare la **riservatezza, integrità** e **disponibilità** delle informazioni anche in condizioni operative non ordinarie, causate da eventi accidentali o fraudolenti. Il compito di stabilire le condizioni in cui devono essere salvaguardate le tre proprietà dell'informazione, spetta all'attività di **valutazione dei rischi** (o *risk assessment*)[32]. L'obiettivo della valutazione dei rischi è quello di consentire la scelta ottimale delle contromisure, definendo e modulando le protezioni in funzione del valore dei beni con il criterio della massima omogeneità, evitando cioè che rischi residui vanifichino

[29] Secondo la norma ISO/IEC 7498-2 che definisce un modello per la sicurezza delle comunicazioni, le funzioni di sicurezza possono essere realizzate attraverso opportuni meccanismi, ossia prodotti hardware e software che abilitano tali funzioni. La stessa norma inserisce le tecniche biometriche tra quelle idonee a realizzare il meccanismo di autenticazione tra le parti.

[30] Il documento programmatico della sicurezza è previsto dall'articolo 34 lettera g) del D. Lgs. 196/03 ed è descritto dall'articolo 19 dell'allegato B.

[31] Linee guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati nella Pubblica Amministrazione – Gruppo di Lavoro AIPA-ANASIN-ASSINFORM-ASSINTEL, Direttiva del Presidente del Consiglio dei Ministri 16 gennaio 2002, Dipartimento per l'Innovazione e le Tecnologie – Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali, Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione – Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni – marzo 2004, ISO/IEC IS 17799-1 - Information security management - Part 1: Code of practice for information security management

[32] La terminologia utilizzata per le attività di gestione della sicurezza è spesso disomogenea è contraddittoria. In questo capitolo sono state adottate le definizioni proposte dalla guida ISO/IEC 73:2002 - Risk management - Vocabulary - Guidelines for use in standards

l'intero impianto di sicurezza consentendo di aggirare le protezioni messe in campo. Un altro obiettivo di questa attività è tenere traccia del processo decisionale che ha portato all'attuazione delle contromisure, per verificare il raggiungimento degli obiettivi prefissati e correggere ciclicamente l'analisi in funzione di quanto rilevato in fase attuativa[33].
Si osserva che per raggiungere il citato criterio di omogeneità delle protezioni, dovrebbero essere presi in considerazione tutti i processi che direttamente o indirettamente trattano le informazioni che si vuole rendere sicure, siano essi processi informatici, cartacei o di altra natura.
L'analisi del rischio può essere condotta sulla base dell'esperienza maturata, per analogia con situazioni simili, attraverso ragionamenti e considerazioni soggettive oppure seguendo una metodologia[34]. Queste diverse prassi non sono tra loro esclusive, anzi di solito il ricorso all'esperienza personale e a giudizi soggettivi è utilizzato nelle fasi iniziali delle metodologie di analisi del rischio.
I metodi di valutazione dei rischi si basano per lo più sulla stima di **beni** (o *assets*), **vulnerabilità** e **minacce**. Il bene è ciò che bisogna salvaguardare: persone, oggetti, software, informazioni, ecc. Le vulnerabilità sono caratteristiche dei sistemi e dei processi che, in particolari situazioni, possono portare alla perdita di riservatezza, integrità o disponibilità delle informazioni (ad esempio un errore del software). Le minacce consistono nella possibilità che avvenga un evento non desiderato che porti alla perdita di riservatezza, integrità o disponibilità delle informazioni (ad esempio un attacco di un *hacker*) e dipendono dal valore del bene e dal contesto in cui il bene si trova.
Il rischio è la probabilità che si concretizzi una minaccia nei confronti di un bene, sfruttando una vulnerabilità del sistema. La valutazione dei rischi comprende l'individuazione delle possibili cause di rischio attraverso il censimento dei beni e delle relative vulnerabilità e minacce (*risk analysis*) nonché la stima del loro impatto (*risk evaluation*) in termini di potenziali perdite economiche, di immagine, ecc.
I metodi con cui tale analisi può essere condotta sono diversi, ma di solito sono necessarie alcune semplificazioni per ridurre il gran numero di variabili in gioco e fare in modo che i risultati della valutazione possano essere efficacemente utilizzati.

### 7.6.3 La predisposizione delle contromisure

A seguito della valutazione dei rischi, occorre determinare le eventuali contromisure e renderle attive[35].
Per ogni rischio individuato bisogna decidere se:

a) rifiutarlo, evitando il coinvolgimento nella situazione a rischio (ad esempio rinunciando ad un progetto);
b) mitigarlo con opportune contromisure;

[33] Secondo la norma BS7799-2 la gestione della sicurezza (ISMS) deve consistere in un processo ciclico di tipo PDCA (Plan Do Check Act).

[34] Si citano, a titolo di esempio, i metodi CRAMM, RiskWatch, COBRA e Defender Manager

[35] La citata guida ISO/IEC 73:2002 definisce questa attività come trattamento del rischio (*risk treatment*)

c) trasferirlo completamente od in parte a terzi (ad esempio con contratti assicurativi);
d) accettarlo.

La decisione deve essere presa considerando nell'ordine: le norme cogenti che possono imporre il contenimento di determinati rischi, specifiche richieste di soggetti interessati oppure la convenienza a ridurre o trasferire il rischio attraverso la stima del rapporto tra costi e benefici.
Nei casi in cui si decide di ridurre il rischio, occorre scegliere la contromisura più opportuna che può essere di tipo organizzativo o tecnologico, in quest'ultimo caso è necessario individuare il meccanismo (ossia il prodotto) idoneo. In generale i migliori risultati si ottengono con l'accoppiamento di misure organizzative e tecnologiche.
La scelta della contromisura deve essere fatta considerando:

- la sua robustezza, ossia la sua capacità di ridurre il rischio;
- la sua invasività e l'impatto sull'ambiente in cui viene introdotta;
- il costo.

Si noti che l'attuazione delle contromisure modifica l'ambito dell'analisi ed introduce nuove vulnerabilità che sono peculiari delle protezioni stesse (ad esempio una protezione basata su crittografia può essere soggetta ad attacchi che mirano a decifrarne gli algoritmi). Comunque, nella pratica, si assume che le protezioni introdotte abbiano un grado di vulnerabilità sensibilmente inferiore a quello dell'ambiente protetto e dunque non modifichino i risultati della fase di valutazione dei rischi.

*La scelta dei meccanismi basati su tecniche biometriche*

Nella matrice che correla i rischi con le contromisure, quasi sempre è presente un sistema di autenticazione in quanto l'adozione di questa contromisura consente di ridurre significativamente il rischio di accesso indebito alle informazioni.
Di regola i meccanismi di autenticazione vengono divisi in due categorie: deboli e robusti.
I primi corrispondono essenzialmente all'impiego della password mentre fanno invece parte dei secondi i sistemi basati su token[36] o su certificati.
Le tecniche di riconoscimento biometrico possono essere impiegate per l'autenticazione degli utenti con due diverse modalità:

a) come sistema di autenticazione robusto basato sul controllo delle informazioni biometriche dell'utente che dichiara il proprio identificativo,
b) come tecnica per migliorare l'efficienza di altri sistemi di autenticazione robusta, basati ad esempio su certificati elettronici.

La prima soluzione ha costi ed efficacia paragonabili a quelli degli altri sistemi di autenticazione robusta, presentando però una minore complessità operativa.
Di converso essa può avere impatti nei confronti della tutela della privacy e può introdurre nuovi problemi di sicurezza, legati alla memorizzazione delle informazioni biometriche. Le

[36] Inserire la definizione di token

informazioni necessarie per l'autenticazione devono infatti essere opportunamente protette per evitare che possano essere lette ed usate per scopi non leciti, o modificate per accedere dolosamente al sistema informativo[37]. Inoltre vi possono essere attacchi, non considerati nella fase di valutazione dei rischi, che sfruttano i margini fisiologici di errore dei sistemi biometrici (false accettazioni).
La scelta della protezione biometrica di tipo a) introduce dunque ulteriori rischi che devono essere opportunamente valutati per evitare che nuove vulnerabilità vanifichino la robustezza del sistema di autenticazione.

La soluzione di tipo b) prevede tipicamente un utilizzo congiunto con sistemi di autenticazione basati su card e delega all'elemento biometrico la verifica della la liceità dell'utilizzo della carta da parte dell'utente. In altri termini l'identificatore biometrico viene utilizzato per accertare che chi utilizza la carta sia effettivamente il legittimo proprietario. In questo contesto, che rappresenta uno dei possibili scenari di utilizzo, la verifica biometrica può sostituire l'introduzione manuale di una credenziale (ad esempio un PIN) per lo sblocco della carta. Questa soluzione, sebbene più costosa di quella basata sulla digitazione della credenziale non biometrica, riduce sensibilmente i rischi di utilizzo della carta in caso di perdita o furto. In questa soluzione, di regola, gli identificatori biometrici sono memorizzati all'interno della card e non possono essere letti da parti non autorizzate ed in alcuni casi l'operazione di verifica può essere effettuata all'interno della carta (smart card), per cui si riducono fortemente i problemi di protezione dei dati tipici della soluzione a).

[37] Di norma il rischio di uso illecito dei dati biometrici viene ridotto memorizzando solo un estratto di tali dati (template) che il sistema di verifica confronta con l'estratto ricavato dalle informazioni acquisite dall'utente, questa soluzione non riduce comunque il rischio che qualcuno possa sostituire il template del legittimo utente con quello di una persona che intende accedere dolosamente al sistema.

*Capitolo 8*

# Esempi di implementazioni biometriche

## 8.1 Premessa

Il presente capitolo intende fornire una breve rassegna, divisa per tipo di applicazione, di alcune implementazioni delle tecniche biometriche a livello internazionale e nazionale, attinenti alla Pubblica Amministrazione o a settori di grande interesse come quelli della sicurezza aeroportuale nei quali la Pubblica Amministrazione ha specifiche competenze (ad esempio quella del controllo dei titoli di espatrio). Nella scelta dei casi da proporre, a livello internazionale, è prevalso il principio di riportare alcuni casi significativi dal punto di vista biometrico, per numero di utenti, per importanza sociale o per caratteristiche tecniche. A livello nazionale, oltre che descrivere in dettaglio i documenti elettronici con caratteristica biometrica, introdotti al paragrafo 4.3, è riportato un classico approccio per il controllo dell'accesso logico ed uno per l'accesso fisico. Per ciò che attiene ai sistemi AFIS (Automated Fingerprint Idenfication System), anche se tali sistemi rappresentano una fetta cospicua del mercato, non verrà fatto specifico riferimento a singoli esperienze ma saranno descritte le caratteristiche generali con particolare riferimento all'adeguamento a nuove tecnologie.

## 8.2 Esperienze italiane

### Accesso logico - Società Generale d'Informatica

La Sogei S.p.A. ha avviato nel 2003 un progetto interno per innalzare i livelli di sicurezza, nell'accesso alle postazioni di lavoro del proprio personale, attraverso strumenti di riconoscimento biometrico associato all'utilizzo di smart card.
A tal fine è stata condotta una sperimentazione per mettere a punto le soluzioni tecnico/organizzative nell'ambito di alcune unità produttive e si prevede l'estensione a tutto il personale entro il corrente anno.
Gli obiettivi del progetto riguardano:

- certezza dell'identità dell'utente che opera sui sistemi informatici;
- protezione delle postazioni di lavoro da accessi di persone non autorizzate;
- centralizzazione delle politiche di sicurezza delle postazioni di lavoro;
- tutela delle informazioni critiche scambiate attraverso l'utilizzo della crittografia;
- utilizzo della firma digitale.

La soluzione individuata e sperimentata è caratterizzata da:

- smart card con capacità crittografiche;

- lettore di smart card che preveda, sullo stesso dispositivo, anche il lettore di impronta digitale;
- funzionamento in ambiente Microsoft/Windows nelle versioni 2000, XP e 2003;
- controllo accesso alla postazione attraverso il riconoscimento dell'impronta digitale;
- registrazione del "template" dell'impronta, di almeno due dita, e software di confronto nell' "area privata" della smart card;
- confronto, tra il "template" dell'impronta letta e quello di una delle due impronte registrate, effettuato a bordo della smart card stessa ("match on card");
- accesso al dominio attraverso il certificato di autenticazione (Smart Logon) attivato dal riconoscimento biometrico;
- definizione del file system e funzionamento della smart card compatibili con le specifiche fissate per le firme digitali rilasciate dalla Certification Authority della Sogei;
- compatibilità con la 'Carta Nazionale dei Servizi'.

Le caratteristiche illustrate consentono di migliorare la sicurezza complessiva attraverso:

- **Controllo accesso alla postazione attraverso il riconoscimento biometrico**: l'utilizzo di tecniche di controllo biometrico permette infatti di effettuare il confronto attraverso il riconoscimento dell'impronta digitale che è qualcosa che una persona ha sempre con sé, non si può scordare e non può essere carpita, migliorando il riconoscimento attuale effettuato attraverso userid/password.
- **Certificati digitali di autenticazione/crittografia con chiave privata registrata nell' "area privata" del dispositivo sicuro**: l'utilizzo dei certificati per l'autenticazione elimina i problemi relativi sia all'intercettazione delle password sia alla possibile dimenticanza. La registrazione nell'area privata ne impedisce la lettura dall'esterno.
- **Calcolo del template dell'impronta letta direttamente sul lettore**: viene garantita la riservatezza sul template generato e dell'immagine dell'impronta letta.
- **Registrazione del "template" dell'impronta e software di confronto nell' "area privata" del dispositivo sicuro**: la registrazione dell'impronta nell'area privata ed il confronto con l'impronta letta a bordo del dispositivo sicuro stesso consentono di evitare ogni accesso in lettura dall'esterno del template registrato.
- Tale soluzione risponde in maniera piena alle esigenze di tutela della privacy in quanto non prevede la costituzione di alcuna banca dati delle impronte dei dipendenti.
- **Politiche di protezione delle postazione di lavoro**: è stato scelto di non consentire l'operatività delle postazioni se l'utente non sia stato autenticato ed autorizzato e di disabilitare la postazione nel momento in cui il dispositivo sicuro viene tolto dal lettore.
- **Accesso attraverso smart logon al dominio**: lo smart logon impone di collegarsi al dominio esclusivamente all'atto del logon. In tal modo vengono centralizzate le politiche ed uniformate le misure di sicurezza in relazione a classi di utenti, nonché si rendono possibili azioni in tempo reale per contrastare eventuali attacchi sulla rete.

- **Firma digitale**: la stessa smart card può contenere il certificato di firma digitale emesso dalla Certification Authority di Sogei. Ogni volta che si utilizzerà la chiave di firma verrà richiesto uno specifico PIN.

#### 8.2.1.1 Problematiche organizzative

L'utilizzo dei dispositivi sicuri con riconoscimento biometrico e certificato per il controllo degli accessi al sistema informativo comporta l'implementazione di specifiche procedure organizzative.
Infatti, oltre alle procedure tipiche per la gestione dei dispositivi (rilascio, revoca e sostituzione in caso di smarrimento o di malfunzionamento), occorre disporre di soluzioni di recovery per consentire al dipendente di poter operare anche in caso di indisponibilità momentanea del dispositivo. La soluzione adottata prevede la disponibilità di un ulteriore dispositivo di backup, custodito con apposite misure di sicurezza, privo ovviamente del certificato di firma.

### 8.2.2 Accesso fisico- Aeroporto di Fiumicino

| | |
|---|---|
| Obiettivo | Controllo dell'accesso fisico per i dipendenti aeroportuali |
| Tecnologia | Riconoscimento biometrico del volto |
| Anno | 2003 |
| Status | Progetto pilota terminato |

Il progetto pilota coordinato dalla società Aeroporti di Roma, ha visto l'installazione di un sistema per il controllo degli accessi presso il varco staff a quota 6 del Terminal A e per quattro mesi è stato utilizzato da circa 3.300 operatori aeroportuali per accedere all'interno delle cosiddette aree sterili dell'aerostazione "Voli Domestici" dell'Aeroporto di Fiumicino "Leonardo da Vinci".
La soluzione per il controllo accessi, sviluppata con tecnologie di riconoscimento biometrico del volto, il cui template è stato memorizzato su una smart card, è stato impostato nelle due consuete fasi di enrollment e verifica.
Durante il processo di registrazione l'utente ha espresso preventivamente il consenso per il trattamento dei dati personali secondo il dlgs. 196/2003 (testo unico sulla privacy) e successivamente l'operatore ha acquisito i dati anagrafici dell'utente e l'immagine digitale del volto che, trasformata in template, insieme ai primi, è stata immagazzinata nel chip della smart card in modalità sicura attraverso firma digitale.
Per sopperire ai problemi derivanti dalla differente altezza degli utenti, nel corso del progetto è stata sperimentata l'originale possibilità di inserire il dato di inclinazione del sensore di ripresa all'interno della smart card.
Gli obiettivi principali della sperimentazione sono stati:
- verifica della maturità della specifica soluzione tecnologica proposta ed il grado di confidenza degli utenti coinvolti con sistemi di identificazione alternativi a quelli tradizionali;
- acquisizione di expertise su dispositivi e procedure di riconoscimento biometrico, che presto saranno obbligatorie in alcune procedure aeroportuali di immigrazione;
- Minimizzazione dell'impatto del metodo biometrico sui flussi in ingresso degli operatori aeroportuali.
Il progetto ha rappresentato il primo test su larga scala compiuto in un aeroporto italiano.

### 8.2.3 Documenti Elettronici - Carta d'Identità Elettronica

La CIE, nell'ambito degli aspetti biometrici, contiene il template e l'immagine dell'impronta digitale del legittimo titolare, compressa secondo l'algoritmo WSQ (*Wavelet Scalar Quantization*), che è un algoritmo ottimizzato per la compressione delle immagini delle impronte digitali, e garantisce un elevato livello di sicurezza in fase di identificazione del portatore che la esibisce.
Il cosiddetto il Sistema di Sicurezza del Circuito di Emissione, S.S.C.E., provvede a controllare ogni operazione prevista nell'intero processo del ciclo di vita del documento: rilascio dei certificati digitali agli Enti coinvolti, controlli in fase di inizializzazione dei supporti fisici, autenticazione del Comune emettitore, verifica dei dati anagrafici del cittadino, rilascio del documento.
Il template viene utilizzato ai fini di riconoscimento dell'impronta originale pur non consentendone una sua qualsivoglia ricostruzione, consentendo quindi la salvaguardia del diritto alla privacy. Si sottolinea come tale riconoscimento non presupponga la presenza di nessuna banca dati, avvenendo il confronto direttamente tra il template memorizzato sulla C.I.E. e quello generato durante la fase di lettura da parte del dispositivo di acquisizione utilizzato dalla postazione *client* che richiede il servizio. Nessuna operazione di tracciamento è effettuata né dal *client*, nè dal server. Un simile confronto garantisce, per i servizi che lo richiedano, la presenza fisica del titolare della CIE.
Durante la fase di inizializzazione, l'impronta assunta tramite i lettori certificati dal sistema SSCE, Sistema di Sicurezza del Circuito di Emissione, è trasformata in template, secondo l'algoritmo fornito dal Ministero dell'Interno, e memorizzata nell'area dedicata assieme ad un progressivo (da zero a nove) per l'individuazione del dito utilizzato per l'assunzione dell'impronta (ciò consente di rilasciare la CIE anche a persone mancanti di alcune delle dita)..
Allo scopo di aumentare la sicurezza dei dati contenuti nel documento, lo spazio dedicato alla memorizzazione del template, dopo la sua installazione, viene reso non riscrivibile: Anche fase di installazione dell'impronta non richiede la memorizzazione di dati sulle postazioni del comune (o centro servizi) emettitore.
La C.I.E., è una smart card ibrida, in grado di integrare nel supporto fisico sia una banda a memoria ottica che un microprocessore.
La banda ottica a lettura laser è utilizzata per la memorizzazione dei "dati" identificativi[38] ai fini della salvaguardia delle esigenze di pubblica sicurezza, ivi inclusa la fotografia, la firma ed una impronta digitale del titolare. L'elevata capacità di memoria disponibile (circa 1 MB), utilizzata per la memorizzazione di immagini o di informazioni di grosso volume, associata alla capacità di elaborazione del microchip, può consentirne un utilizzo anche per la fruizione di servizi locali o nazionali.
Il microprocessore è utilizzato per assolvere le funzioni di "carta servizi"[39], per consentire l'identificazione in rete e, quindi, l'erogazione di servizi telematici di *E-government*.
I rischi di utilizzo fraudolento e falsificazione delle carte d'identità, dovuti anche ai furti di carte "in bianco", con l'adozione del documento elettronico, sono notevolmente ridotti,

[38] D.M. 19 luglio 2000, come modificato con DM 14.5.2003 e DM 6.11.2003, Art. 1, comma 1, lettera f)

[39] D.M. 19 luglio 2000, come modificato con DM 14.5.2003 e DM 6.11.2003, Art. 1, comma 1, lettera g)

principalmente grazie alla natura del supporto e alle garanzie di inalterabilità delle informazioni riportate, tanto sul chip che sulla banda ottica.
La banda ottica rappresenta l'elemento centrale della sicurezza: la caratteristica di base della scrittura WORM (*Write Once Read Many)* non permette alterazioni, realizzate mediante la cancellazione di dati e la loro sostituzione con altri. Infatti, le informazioni memorizzate non sono cancellabili e riscrivibili. Eventuali aggiornamenti possono unicamente consistere in aggiunte.
Come per gli altri documenti elettronici, tutte le attività di trasmissione dati avvengono in modalità cifrata al fine di garantire l'integrità dei dati e certificare che le informazioni pervenute a destinazione siano identiche a quelle originariamente inviate.

#### 8.2.3.1 Obiettivi della nuova carta di identità elettronica

- Aumento della sicurezza del documento di identità che consentirà, alle forze dell'ordine, una identificazione certa del possessore;
- Riconoscimento certo del titolare per consentire l'esercizio del diritto di voto elettronico;
- Possibilità di verifica dei dati biometrici per garantire la presenza fisica del titolare della CIE durante l'accesso ai servizi in rete.
- Integrazione tra i sistemi informativi e la cooperazione applicativa tra amministrazioni sono oggi un obiettivo fondamentale perseguito da questo Ministero.
- Funzioni di documento di viaggio equipollente al passaporto e, grazie al rispetto delle caratteristiche previste dalla vigente normative ICAO e ISO, abilitazione all'espatrio in 32 Paesi esteri.

Gli enti governativi responsabili del nuovo documento d'Identità sono

- Ministero dell'Interno:
  - Dipartimento per gli Affari Interni e Territoriali
  - Direzione Centrale per i Servizi Demografici (compito di verifica dello stato anagrafico dei cittadini italiani)
  - Dipartimento della Pubblica Sicurezza – Direzione Centrale della Polizia Criminale – Servizio Polizia Scientifica (tramite il Sistema di Sicurezza del Circuito di Emissione, SSCE, controllo di tutte le operazioni previste nell'intero processo dal rilascio dei certificati digitali agli Enti coinvolti, ai controlli durante l'inizializzazione dei supporti fisici alla autenticazione del Comune emettitore, verifica dei dati anagrafici del cittadino e rilascio del documento).
- Ministero dell'Economia e delle Finanze (vigilanza sulla produzione dei supporti e distribuzione presso gli Uffici Territoriali di Governo)

La prima fase di sperimentazione, con il coinvolgimento di 83 Comuni distribuiti sull'intero territorio nazionale, è stata completata ed è in attuazione la fase di consolidamento e razionalizzazione della sperimentazione che prevede l'emissione delle nuove carte d'identità elettroniche per l'intera popolazione, con età superiore ai 15 anni, nei 56 Comuni individuati dalla Direzione Centrale per i Servizi Demografici, con oltre un milione di C.I.E. distribuite ai sopra citati Comuni (giugno 2004).

### 8.2.4 Documenti Elettronici - Carta Multiservizi della Difesa

Il Ministro per l'Innovazione e le Tecnologie, nel delineare la politica dell'e-government per il triennio 2003-2005, allo scopo di dare un notevole impulso alla digitalizzazione della PA, aveva posto come obiettivo strategico l'erogazione on-line dei servizi al cittadino prevedendo l'introduzione della Carta d'Identità Elettronica (CIE), della Carta Nazionale dei Servizi (CNS) e la diffusione della firma digitale stabilendo gli standard e i criteri organizzativi da seguire.

Peraltro, la necessità di una carta elettronica era stata avvertita quale esigenza operativa da parte dell'Esercito allorquando ebbe l'urgente necessità di fornire alla Commissione Governativa "Mandelli" i dati anagrafici e sanitari del personale impiegato in operazione nei Balcani. Furono pertanto avviate le azioni necessarie per realizzare il software per la gestione delle informazioni di carattere personale e sanitario attraverso l'utilizzo di una smart card.

La Difesa, quindi, allo scopo di dare una corretta e sinergica collocazione alle diverse attività in atto, ha elaborato un progetto unitario per la realizzazione della Carta Multiservizi della Difesa (CMD).

Per dare validità legale alla CMD quale documento di riconoscimento e valenza internazionale quale carta sanitaria, la Difesa ha richiesto ed ottenuto:

- il riconoscimento della CMD come "carta valori" e l'inserimento di essa tra le "carte valori" da parte del Dipartimento del Tesoro del Ministero dell'Economia e delle Finanze, secondo le attuali disposizioni legislative;
- la registrazione della carta stessa presso l'Ente Nazionale di Unificazione per le tecniche informatiche (UNINFO) e Registration Authority per l'Italia, con il conseguente rilascio del previsto Issuer Identification Number (IIN).

Il progetto della CMD è stato molto apprezzato in ambito governativo, tanto che il Comitato dei Ministri per la Società dell'Informazione, nel corso della riunione del 29 luglio 2003, ne ha riconosciuto la validità e ne ha approvato i contenuti, mentre il Dipartimento del Tesoro del Ministero dell'Economia e delle Finanze, come già messo in evidenza, ha inserito la CMD tra le "carte valori".

Infine, la distribuzione a tutti i dipendenti pubblici di tale modello di carta multiservizi è stata inserita dal Ministro per l'Innovazione e le Tecnologie nella direttiva "Linee guida in materia di digitalizzazione dell'amministrazione per l'anno 2004", fra i settori di intervento prioritari.

#### 8.2.4.1 Requisiti di base

Nell'elaborazione del progetto della Carta Multiservizi Difesa è stato deciso che essa dovesse avere una valenza giuridica sia "Esterna" all'amministrazione Difesa sia "Interna" ad essa. Quindi, utilizzabile a "vista" ed in forma elettronica in modo da:

- Contenere i certificati di "Firma Digitale" e "Strong Authentication" pienamente rispondenti alle attuali normative di legge;
- fungere da "Documento di Riconoscimento" (identità personale);
- contenere i dati sanitari relativi al dipendente e necessari ad assicurare le funzionalità di "emergency card";
- contenere i "template" delle impronte di 2 (due) dita delle due mani;
- Realizzare la piena e completa interoperabilità a livello:
    - nazionale, con la carta d'Identità Elettronica (CIE);
    - internazionale, con la struttura dati sanitari "NetLink";
    - interforze ed in ambito Ministero della Difesa;

- essere dotata di banda magnetica, idonea a salvaguardare gli investimenti pregressi.

Inoltre fu parimenti considerato requisito irrinunciabile, ai fini della sicurezza INFOSEC e DATASEC, la certificazione a livello ITSEC "e4-High", relativa al "Chip" ed al Sistema Operativo, che rappresenta la massima protezione attualmente in Europa.

#### 8.2.4.2 Funzionalità della carta

Con i sopraccitati requisiti di base, la Carta Multiservizi Difesa garantisce le seguenti funzionalità essenziali:

**Identificazione.**

Le caratteristiche di identificazione sono soddisfatte secondo le seguenti modalità:

- a "vista" tramite i dati riportati sul fronte e sul retro della carta senza l'ausilio di mezzi informatici;
- elettronica conforme allo standard previsto per la CIE, attraverso il controllo dei dati anagrafici;
- in rete, grazie al certificato digitale di autenticazione presente sulla carta, abilitando l'utente all'accesso ed ai servizi su canale sicuro "Secure Socket Layer" (SSL) attraverso un software specifico ("browser").

**Firma Digitale.**

La Carta contiene una struttura di Firma Digitale, la cui esecuzione è possibile tramite un "Personal Identification Number" (PIN) aggiuntivo, esclusivamente dedicato a tale funzione.. Il certificato digitale e la coppia di chiavi di firma digitale sono distinti e indipendenti da quelli usati per l'autenticazione.

**Dati Sanitari.**

La Carta contiene una struttura dei dati sanitari rispondente alle necessità operative della Difesa. Detta struttura è compatibile con il protocollo di standardizzazione dei dati sanitari adottato a livello internazionale (NetLink).

Il suddetto modello NetLink (HC4016) prevede la seguente suddivisione:

(1) Dati ad accesso limitato, questi dati possono essere letti in condizioni di emergenza sia dal personale autorizzato dal Servizio Sanitario Nazionale (SSN) sia dal personale autorizzato dal Servizio Sanitario Militare (SSM); essi sono riferiti a dati amministrativi (cognome, data di nascita, codice fiscale, indirizzo, ecc.) e a dati sanitari da trattare in caso di emergenza (gruppo sanguigno e trasfusioni, immunizzazioni, terapie correnti, organi mancanti, ecc.);

(2) Dati ad accesso protetto, questi dati devono poter essere letti e scritti solo da personale autorizzato in possesso di chiavi di lettura/scrittura rilasciate dal SSM e poter essere consultati dal titolare della carta attraverso la digitazione del proprio PIN. Le informazioni proprie di questa area sono quelle di carattere medico-sanitario necessari alle F.A. (vedasi Teatri Operativi).

**Dati di Vestiario.**

Nella Carta sono inserite le informazioni relative all'attagliamento, alle misure antropometriche ed alla Tabella Vestiario del titolare.

**Dati Matricolari.**

I dati matricolari inseriti sono quelli standard previsti dal Sistema Informativo del Personale dell'Amministrazione Difesa (SIPAD) (grado, anzianità di servizio, anzianità di grado, incarico ricoperto, ecc.).

#### 8.2.4.3 Il punto della situazione sulla implemenntazione della carta

La produzione della carta è prevista secondo l'organizzazione funzionale del Ministero della Difesa, che è caratterizzata da cinque grandi aree – Organi Centrali (Stato Maggiore della Difesa / Segretariato Generale della Difesa), le 3 Forze Armate (EI, MM, AM) ed il Comando Generale Arma Carabinieri – dotate di un'autonomia programmatica.
Al momento l'Esercito ha iniziato la produzione e la distribuzione delle carte al proprio personale.
Anche il Comando Generale della Guardia di Finanza ha aderito al progetto CMD. Al momento sta implementando una propria struttura di PKI riconoscendo quale Autorità di Certificazione la CA-Difesa.

#### 8.2.4.4 Sviluppi attuali e futuri

La Carta Multiservizi Difesa vuole essere usata in particolare per le seguenti applicazioni:

- Gestione dati sanitari: le informazioni sanitarie sono inserite automaticamente, sotto la responsabilità di un medico militare, tramite le procedure informatiche sviluppate in ambito infermerie/ospedali militari;
- Posta sicura: scambio di e-mail firmate e/o cifrate con garanzia di autenticità del mittente integrità e sicurezza;
- Postazione di lavoro sicura: accesso in totale sicurezza alla postazione di lavoro (eventualmente congiunta all'uso dell'impronta digitale);
- Ingresso ad aree riservate: autenticazione forte tramite utilizzazione congiunta della CMD e delle impronte digitali in essa contenute;
- Accesso a servizi: rifornimento carburanti, prelievo materiale/vestiario, "passi" per ingresso in infrastrutture, acquisto beni presso strutture della Difesa (borsellino elettronico).

### 8.2.5 Documenti elettronici - Passaporto biometrico

Il progetto del nuovo Passaporto Elettronico italiano, sotto la responsabilità del Ministero degli Affari Esteri e del Ministero dell'Interno, prevede l'introduzione di identificativi biometrici (immagine digitale del volto e impronte digitali di due dita, una per ciascuna mano) nel documento di viaggio, provvisto di un dispositivo elettronico microchip a Radio Frequenza, c.d. *contactless* (la comunicazione avviene per mezzo di onde a radiofrequenza, quindi, senza contatto) per la memorizzazione e la protezione dei dati del portatore.
Al fine di ampliare i requisiti di sicurezza dei documenti di viaggio, fino ad oggi costituiti essenzialmente da elementi di sicurezza fisica, come per i documenti di identità tradizionali, in ambito ICAO (International Civil Aviation Organization) sono in corso di elaborazione documenti tecnici per estendere le funzionalità dei documenti di viaggio leggibili in maniera automatica, i cosiddetti MRTD (Machine Readable Travel Document).
Le novità rispetto al modello ad oggi in uso sono sia tecnologiche che organizzative.

#### *8.2.5.1* Innovazioni tecnologiche

- Microprocessore di prossimità – integrato anche all'interno di supporti cartacei, leggibile senza contatto elettrico diretto. Il chip "contactless" amplia le possibilità fino ad ora offerte dalla zona MRZ a lettura ottica, Machine Readable Zone, che contiene informazioni utili per verificare la genuinità del documento stesso. Nel documento di nuova concezione la MRZ non viene soppressa, ma diviene il collegamento essenziale tra le informazioni stampate graficamente, e quelle in

formato digitale contenute nel microprocessore. La struttura interna del microchip *contactless* dovrà essere predisposta secondo le indicazioni dell'ICAO[40];

- Identificativi biometrici - La risoluzione di New Orleans, elaborata dall'ICAO/*New Technology Working Group*, ha indicato nella fotografia digitale l'elemento di interoperabilità globale per la conferma dell'identità assistita da strumenti informatici. La stessa risoluzione e le successive indicazioni dell'ICAO hanno indicato nelle impronte digitali e nell'iride ulteriori due elementi biometrici da affiancare, in modo opzionale, al viso. Recenti indicazioni della Commissione Europea indicano le impronte digitali quale ulteriore identificativo biometrico, obbligatorio, per consentire anche identificazioni personali automatiche.
- Infrastruttura a Chiave Pubblica (PKI)[41]– al fine di evitare possibili alterazioni dei dati memorizzati all'interno del microchip *contactless*, questi dovranno essere firmate con la chiave privata dell'Autorità di Certificazione del Paese che ha emesso il documento. La relativa chiave pubblica dovrà essere inviata a tutti i Paesi aderenti all'ICAO, al fine di consentire la lettura del passaporto elettronico e offrire le necessarie garanzie sull'autenticità del documento.

#### *8.2.5.2* Innovazioni Organizzative

- Controllo sulla identità personale – l'introduzione di un microchip contactless e di due identificativi biometrici consente di modificare sensibilmente i controlli prima dell'emissione del documento e nel corso del suo utilizzo. Prima dell'emissione, al momento dell'assunzione degli elementi biometrici, è possibile verificare, anche su basi dati biometriche, se il richiedente possiede i requisiti necessari a ricevere un passaporto. I controlli successivi possono limitarsi alle verifiche, per accertare che l'identità del legittimo titolare del documento sia la stessa del portatore che lo esibisce. La presenza di due identificativi biometrici, viso e impronte digitali, migliora notevolmente la capacità di verifica eliminando completamente i rischi di false accettazioni o di falsi rigetti;
- Verifiche automatiche – grazie alla presenza di identificativi biometrici ed alla presenza di sistemi di cifratura asimmetrica, gran parte delle attività di controllo presso le frontiere possono essere rese automatiche, lasciando agli specialisti le eccezioni (falsi rifiuti, documento non funzionante, etc.);
- Metodologie di controllo uniformi – con il nuovo passaporto elettronico le attività precedenti l'emissione ed il rilascio dovranno subire dei processi di trasformazione che ne aumentino gli automatismi. All'atto della richiesta sarà necessaria la presenza fisica del richiedente per assumerne gli elementi biometrici (almeno per quanto riguarda le impronte digitali).

[40]"Development of a logical data structure - LDS for optional capacity expansion technologies", ICAO Technical Report

[41]"PKI Digital Signatures For Machine Readable Travel Documents", ICAO Technical Report

#### 8.2.5.3 Obiettivi del nuovo passaporto italiano

- aumentare la sicurezza del documento di viaggio, in particolare della legittimità della titolarità del portatore, della certezza del suo legame con il documento, della resistenza alla falsificazione e alla contraffazione del documento stesso;
- semplificare e rendere più sicuri gli spostamenti internazionali, migliorando la qualità dei controlli alle frontiere e negli accessi ai mezzi di trasporto (es. aeroporti) , rendendo disponibili agli specialisti strumenti ulteriori e in grado di assicurare un maggiore automatismo nelle attività;
- integrazione delle raccomandazioni e degli standard individuati nei gruppi di lavoro dell'ICAO nel passaporto, in modo da garantire una interoperabilità globale tra i documenti di viaggio;
- garantire l'interoperabilità con gli altri documenti di identificazione rilasciati in Italia.

### 8.2.6 Documenti elettronici - Permesso di soggiorno

Il progetto del nuovo permesso di soggiorno apporta modifiche sostanziali alla struttura del documento e prevede che tutte le informazioni in esso presenti vengano memorizzate in una banca dati.
Tre sono stati i principali motivi ispiratori che hanno guidato la definizione dell'architettura del nuovo permesso di soggiorno:

- rispondere alla esigenza di produrre uno strumento sicuro sotto i diversi aspetti della produzione, rilascio e utilizzo da parte del titolare. La sicurezza non solo deve accompagnare tutti i flussi informatici, ma deve anche essere presente sul supporto fisico, al fine di scoraggiare facili contraffazioni, nonché di consentire una identificazione certa da parte delle istituzioni competenti;
- fornire un supporto standard, perfettamente in linea con le indicazioni dell'Unione Europea;
- consentire un migliore monitoraggio dei confini del Paese, grazie all'utilizzo del sistema informativo a cui sono delegati i controlli dattiloscopici degli immigrati illegali e dei chiedenti asilo politico in ambito UE.

Il controllo dell'intero ciclo di vita del nuovo documento fino alla sua naturale scadenza e la possibilità di verificare per via telematica la copia elettronica del permesso di soggiorno, consente di rilevare con immediatezza eventuali tentativi di falsificazione o contraffazione e di procedere all'identificazione a vista del titolare con margini di sicurezza maggiori.

Il raggiungimento degli obiettivi di sicurezza presuppone l'utilizzo di materiali e tecnologie standard, affidabili e nello stesso tempo in grado di garantire alti livelli di sicurezza. Il solo utilizzo di un supporto plastico, per quanto sofisticato, non sarebbe sufficiente a soddisfare tutte le esigenze sopra esposte. Per questo la scelta e' stata quella di una carta in grado di ospitare anche un duplice supporto elettronico, costituito da un microprocessore e da una banda a memoria ottica, al pari della C.I.E., al fine ulteriore della più completa interoperabilità tra i due documenti elettronici.
Il supporto elettronico consente di memorizzare sia i dati presenti sul documento in forma grafica, ottenendo una duplicazione di sicurezza, sia ulteriori informazioni che altrimenti non potrebbero essere riportate sul documento stesso.

La capacità di elaborazione propria del microcircuito chip permette di annoverare il P.S.E. tra le smart card.
All'interno del supporto sarà pertanto inserito sia il template che l'immagine di una impronta digitale, utile per confermare l'identità del titolare nei controlli successivi, ed i dati (Nome, data di nascita, etc.) relativi ai figli.
Come per gli altri documenti elettronici,

- tutte le attività di trasmissione dati avvengono in modalità cifrata al fine di garantire l'integrità dei dati e certificare che le informazioni pervenute a destinazione sono identiche a quelle originariamente inviate;
- la presenza di una memoria non riscrivibile e non volatile, rende possibile una maggior protezione dei dati memorizzati.

La caratteristica, propria del microcircuito, di poter nascondere informazioni al suo esterno, al contempo, di poter eseguire istruzioni programmate al suo interno, rende possibile il riconoscimento sicuro della carta per via telematica e la conseguente ed immediata erogabilità dei servizi.
La caratteristica propria della banda di memoria ottica è l'assoluta inalterabilità accidentale o fraudolenta dei dati identificativi e biometrica in essa contenuti, ai fini di garantire l'identità del titolare, per l'accesso a servizi e per eventuali controlli operati dalle forze di P.S, al pari della C.I.E.

## 8.3 Esperienze internazionali

### 8.3.1 Border Crossing Card (U.S.A) – 1998: Visto Biometrico per I lavoratori pendolari Messicani

| | |
|---|---|
| **Obiettivo** | Disbrigo agevolato delle procedure di immigrazione negli Stati Uniti |
| **Tecnologia** | Impronte digitali |
| **Anno** | 1998 |
| **Status** | In esercizio |

Iniziato nel 1998, ma obbligatorio dal 2001, il documento, noto come "Laser VISA", con la medesima tecnologia a banda ottica da 2.8 MB della "Green Card" (descritta di seguito),, consente il passaggio della frontiera ed il riconoscimento biometrico del portatore ai confini meridionali degli U.S.A.con il Messico e nei principali aeroporti con destinazioni provenienti dal questo Paese, ove vi sono perfino "corsie preferenziali" per i possessori di Laser VISA. Il programma governativo prevede la sorveglianza di oltre 100 punti di ingresso dotati di oltre mille sistemi integrati di verifica biometrica "BVS" (Biometric Verification System) in grado di autenticare e verificare tutti i documenti dotati di banda ottica.
Come per la Green Card", nella banda a memoria ottica sono digitalizzate in maniera indelebile, oltre ai dati anagrafici, la fotografia e la firma due impronte digitali, sia in forma di template proprietario, che come immagine in formato WSQ compatibile con i sistemi AFIS internazionali..
I sistemi di verifica biometrica funzionano esclusivamente in modalità "uno a uno", con conseguente beneficio economico deivante ad un uso limitato delle infrastrutture.

Ad oggi sono in circolazione oltre 7 milioni di Laser VISA-BCC, possedute quindi da circa il 66% dei cittadini messicani che si recano negli Stati uniti per lavoro o per studio.
La Border Crossing Card è prodotta e personalizzata centralmente sotto il controllo dell'INS (Immigration and Naturalization Service) usando gli stessi sistemi (ICPS - Integrated Card Production System), adoperati per le emissione delle Green Card con ovvio conseguente vantaggio economico.

### 8.3.2 Green Card (U.S.A.) – 1998: Permesso di Soggiorno Permanente con impronta digitale, fotografia e firma

| | |
|---|---|
| **Obiettivo** | Disbrigo delle procedure di immigrazione negli Stati Uniti |
| **Tecnologia** | Impronte digitali |
| **Anno** | 1998 |
| **Status** | In esercizio |

Per proteggersi dalle frodi e dalle contraffazioni, il Dipartimento di Giustizia degli Stati Uniti – Servizio per l'Immigrazione e Naturalizzazione (INS) ha sostituito il vecchio documento cartaceo noto come "Green Card" con uno dei più sofisticati documenti anti-contraffazione mai prodotti dal Governo.
Il documento incorpora un notevole numero di elementi di sicurezza, tra cui l'immagine digitalizzata della fotografia, firma ed impronta digitale, microscritture, ologrammi sulla superficie, il tutto incorporato in un supporto dati di capacità di 2,8 Megabyte a banda ottica non riscrivibile, né alterabile.
L'impronta digitale, ai fini di maggiore interoperabilità, è memorizzata come immagine, in formato JPEG. (Fonte: U.S. Dept. Of Justice)
Ad oggi sono in circolazione oltre 8 milioni di card emesse, la cui validità è di dieci anni, grazie alla particolare robustezza del supporto in policarbonato.
La "Green Card" è compatibile con gli standard ICAO e quindi ha validità di documento di viaggio (9303, parte 3a) ed è predisposta all'impiego di tecnologie biometriche multiple.

### 8.3.3 Immigrazione ed emigrazione - Programma INSPASS, U.S.

| | |
|---|---|
| **Obiettivo** | Nuovo permesso di soggiorno negli Stati Uniti |
| **Tecnologia** | Geometria della mano |
| **Anno** | 1993 |
| **Status** | Formalmente non dimesso, ma in pratica non più manutenuto da alcuni anni |

La soluzione, introdotta nel 1993 e mai ufficialmente dimessa, anche se non più supportata, nelle more della introduzione di nuove procedure (US VISIT), per molti anni ha permesso ad un cospicuo numero di passeggeri (circa 15.000) in arrivo nei più importanti aeroporti degli Stati Uniti, di evitare i meticolosi controlli di immigrazione. Per utilizzare il programma INSPASS, il viaggiatore doveva "iscriversi" che prevedeva il rilascio di una carta con i dati personali e il template della geometria della mano Una volta iscritto nel programma,

l'autorizzazione all'immigrazione avveniva attraverso un chiosco elettronico che acquisiva l'identità del passeggero tramite la smart card oltre al template della geometria della mano.

### 8.3.4 Immigrazione ed emigrazione - Permanent Resident Card (Canada) – Permesso di Soggiorno Elettronico - 2002

| | |
|---|---|
| **Obiettivo** | Nuovo permesso di soggiorno in Canada |
| **Tecnologia** | Impronte digitali |
| **Anno** | 2002 |
| **Status** | In esercizio |

Allineandosi al trattato NAFTA (North America Free Trade Agreement), dal 28 giugno 2002 il Governo Canadese ha introdotto il nuovo Permesso di Soggiorno elettronico per i residenti permanenti, con la stessa tecnologia di card con banda ottica utilizzata dal 1998 negli Stati Uniti (Green Card) e Messico (Border Crossing Card).
A differenza delle due card sopra citate, la PRC Canadese utilizza un supporto con banda ottica da un Megabyte, ed è totalmente compatibile con gli attuali standard ICAO e predisposto per l'impiego di tecnologie biometriche multiple.
Sono in circolazione oltre un milione di PRC, ed il vecchio documento cartaceo è fuori produzione dal dicembre 2003.
(fonte: Citizenship and Immigration Canada, http://www.cic.gc.ca/english/pr-card/index.html).

### 8.3.5 Immigrazione ed emigrazione - Programma BASEL, Israele

| | |
|---|---|
| **Obiettivo** | Controllo dei frontiera tra Israele e Gaza |
| **Tecnologia** | Geometria della mano, caratteristiche biometriche del volto, impronte |
| **Anno** | 2003 |
| **Status** | In esercizio |

Il programma BASEL, attualmente in esercizio, utilizza un approccio biometrico multimodale per rendere più spediti e sicuri i controlli di frontiera per i circa 50.000 lavoratori che ogni giorno entrano in Israele da Gaza.
I partecipanti al programma, una volta registrati i dati anagrafici e quelli biometrici (geometria della mano, volto e impronta di un dito), ricevono smart card con PKI e di tipo "contactless" contenente i dati biometrici dalla mano e del volto.
Tra i requisiti richiesti per la soluzione spiccano il "throughput" del sistema che riesce a gestire un transito di 15.000 persone ogni ora attraverso i 42 varchi fisici di frontiera. Il processo biometrico dura non più di 9-10 secondi, con una percentuale di falsi rifiuti pari allo 0,01% e consiste di varie fasi:

- acquisizione dalla smart card degli estremi anagrafici, della chiave digitale e del template dei dati biometrici;

- acquisizione, attraverso i sensori presenti nei varchi di transito dei dati relativi alla geometria della mano e dei tratti somatici;
- fusione dei dati biometrici
- Controllo delle credenziali attraverso l'anagrafico dell'individuo e verifica biometrica della titolarità al possesso della carta.

I sensori biometrici utilizzati sono prodotti di mercato e sono connessi ad un sistema centralizzato di gestione che garantisce la costante funzionalità dei varchi.

### 8.3.6 Immigrazione ed emigrazione - Aeroporto Ben Gurion, Israele

| | |
|---|---|
| **Obiettivo** | Espletamento facilitato delle procedure di emigrazione ed immigrazione per i frequent flyer |
| **Tecnologia** | Geometria della mano |
| **Anno** | 1998 |
| **Status** | In esercizio |

La soluzione adottata all'aeroporto Ben Gurion di Tel Aviv, è un sistema d'ispezione e riconoscimento automatico in esercizio da 1998 per il frequent flyer. Nella fase di enrollment del passeggero, il sistema archivia i dati biometrici relativi alla geometria della mano ed altre informazioni relative alla sua identità. Successivamente, ad ogni nuovo passaggio, il viaggiatore, servendosi di appositi chioschi automatici, fa riconoscere al sistema la geometria della propria mano e ritira una ricevuta comprovante la sua identità che gli permette di velocizzare gli ulteriori controlli. I vantaggi di questa soluzione sono evidenti in quanto il personale aeroportuale preposto al controllo dei passeggeri può concentrarsi sui viaggiatori considerati "sconosciuti", aumentando quindi il livello di sicurezza complessivo dell'aeroporto. I partecipanti al programma biometrico riducono in modo significativo il tempo di attesa al controllo passaporti, che passa dagli abituali 60/90 minuti a poche decine di secondi. Con la stessa tecnica biometrica sono stati realizzati i sistemi di confine alla frontiere di Israele con la Giordania ed il Libano.

### 8.3.7 Immigrazione ed emigrazione - Programma US VISIT, U.S.

| | |
|---|---|
| **Obiettivo** | Espletamento delle procedure di immigrazione (ed in seguito di emigrazione) per tutti i cittadini ad esclusione di quelli residenti negli U.S., Canada e Messico. |
| **Tecnologia** | Impronte digitali, riconoscimento biometrico del volto |
| **Anno** | 2004 |
| **Status** | In esercizio per |

Il programma US VISIT (United States Visitor and Immigrant Status Indicator Technology), è un programma affidato per legge al Dipartimento della Homeland Security (DHS) che ha l'obiettivo di:

- proteggere la sicurezza dei Cittadini Americani, residenti permanenti e visitatori;
- rendere più spediti viaggi e commerci legittimi;
- assicurare l'integrità del sistema di immigrazione
- salvaguardare (allo stesso tempo) la privacy personale dei visitatori.

Il programma US VISIT consiste nel collezionare e conservare informazioni di tipo biografico, riguardanti viaggi e di tipo biometrico (ad es. fotografie ed impronte digitali) di pertinenza del visitatore.
Le informazioni sono collezionale ed usate per verificare l'identità di individui che entrano od escono dagli Stati Uniti dando la possibilità alle Autorità U.S. preposte di incrementare la sicurezza degli Stati Uniti identificando in maniera più effettiva gli individui che sono:

- noti per essere una minaccia o avere costituito una minaccia per gli Stati Uniti;
- noti per avere violati i termini della loro ammissione agli Stati Uniti;
- ricercati per avere commesso atti criminali all'interno o fuori degli Stati Uniti.

Il primo rilascio del programma è avvenuto a gennaio 2004 negli aeroporti e nei porti (POE - Ports Of Entry) prevede una serie di implementazioni successive fino al 2006 allo scopo di estendere i controlli alla globalità dei POE.
Il programma richiede ai visitatori degli Stati Uniti il rilascio di impronte digitali e di una immagine del volto acquisita all'atto dell'immigrazione. In una fase successiva il controllo biometrico verrà esteso anche ai visitatori che lasciano gli Stati Uniti.

### 8.3.8 Immigrazione ed emigrazione - Programma AUTOMATED BORDER CROSSING, Aeroporto di Schiphol, Olanda

| | |
|---|---|
| **Obiettivo** | Espletamento automatico delle procedure di immigrazione ed emigrazione |
| **Tecnologia** | Riconoscimento dell'iride |
| **Anno** | 2001 |
| **Status** | In esercizio |

L'esecuzione del progetto ABC (Automated Border Crossing) ha permesso la realizzazione di un sistema automatico di espletamento delle formalità di emigrazione ed immigrazione. Gli utenti che, formalmente aderiscono ad un consorzio (Privium), per una quota di circa 100 Euro all'anno, oltre ad altri benefici (agevolazioni all'uso dei parcheggi nella zone aeroportuale) ricevono una smart card che contiene i propri dati anagrafici e la rappresentazione dell'iride.
La fase di enrollment in cui il passeggero viene "accreditato" attraverso una serie di controlli svolti da un funzionario di Polizia e rilascia la propria caratteristica biometrica (iride) dura circa 15 minuti.
Una volta in possesso della smart card, il passeggero che lascia l'Olanda per recarsi verso un Paese esterno alla cosiddetta "area Shengen", invece di recarsi alla fila del controllo dei passaporti, utilizza un apposito spazio delimitato (detto "chiosco"), cui viene abilitato all'ingresso inserendo la propria smart card. Mentre il passeggero si dirige verso il sensore delle caratteristiche dell'iride, i dati anagrafici vengono controllati per verificare l'esistenza di motivazioni che possono ne inibire l'espatrio. Una volta acquisita l'abilitazione a lasciare il Paese, il sensore delle caratteristiche dell'iride, permette al sistema di verificare che il possessore della smart card sia effettivamente il titolare della carta. Una volta superato il secondo controllo, l'apertura di un cancelletto permetterà al passeggero di entrare direttamente nella zona dei gate di imbarco mentre, nel caso della mancanza di una delle due abilitazioni, si aprirà un differente varco che condurrà ad un funzionario che procederà in maniera manuale ai controlli di espatrio di rito. Il sistema, che annovera alcune migliaia di

utenti, è operativo per ora solo nell'aeroporto Schipol ed è in grado di processare circa 4-5 persone al minuto per ogni chiosco.

### 8.3.9 Documenti elettronici - "NAFA" Portafoglio Elettronico per la "Poste du Senegal" – 2004:

| | |
|---|---|
| **Obiettivo** | Sostituzione vecchio libretto di risparmio al portatore |
| **Tecnologia** | Impronte digitali |
| **Anno** | 2004 |
| **Status** | In esercizio |

In sostituzione del vecchio Libretto di Risparmio al Portatore, il progetto NAFA (Portmonnaie Electronique) che prende il nome dal termine "portafoglio" in Wolof, lingua parlata, tra l'altro in Senegal, consente ai lavoratori stagionali delle Associazioni Cotoniere, così come ai Pensionati, di effettuare oltre 1000 versamenti e prelievi impiegando una card a banda ottica da 2,8 MB, contenente le informazioni anagrafiche, fotografia e firma in formato digitale. Le impronte digitali di due dita sono memorizzate in formato di template ed in formato immagine WSQ.
Ulteriore spazio per futuri impieghi di tecnologie biometriche multiple è riservato, fin dall'emissione, sulla card.
Il Sistema di Emissione impiega un database AFIS Civile ove sono memorizzati i due template delle dita, effettuando tutti i controlli preliminari al rilascio e per il controllo accurato di possibili richiedenti duplicati.
Al momento del ritiro della card è necessario provare di esserne l'effettivo richiedente mediante una prima verifica biometrica che "attiva" la card, spedita per posta e comunque priva di valore in quanto precedente al primo versamento. Le operazioni successive, previa verifica biometrica del tipo "uno a uno" con i dati memorizzati sulla banda ottica, avvengono off-line da filiali che aggiornano le operazioni sul database centrale mediante singoli collegamenti quotidiani. Oltre all'ammontare della transazione effettuata, vengono riportati il codice dell'operatore, filiale, luogo e data della transazione stessa.
Gli operatori hanno accesso in lettura e scrittura alla NAFA card dopo essersi autenticati con una apposita card ed una impronta digitale (in modalità "uno a uno"), e possono effettuare transazioni solo se il portatore è stato identificato positivamente. Ogni transazione, così come i dati del titolare, viene trascritta in otto copie allocate in differenti settori della banda ottica, ai fini di ottenere il più elevato livello di anti-contraffazione e robustezza ai danneggiamenti fisici del supporto.
Progetti analoghi sono in via di sperimentazione in Nigeria a Sud Africa.

### 8.3.10 Documenti elettronici - "MyKad" Carta d'identità multiservizi, Malesia

| | |
|---|---|
| **Obiettivo** | Realizzaizione di una carta di identità multiserviuzi |
| **Tecnologia** | Riconoscimento delle impronte digitali e dell'iride |
| **Anno** | 1999 |
| **Status** | Programma esecutivo |

La Malaysia é stato il primo Paese a realizzare un progetto per la creazione di una carta elettronica multiservizi (Government Multi-Purpose Card - GMPC), in grado di abilitare l'utente sia ad applicazioni private, che istituzionali, quali ad esempio quella di documento di riconoscimento.. Il progetto ha avuto inizio nel 1999 e la distribuzione delle carte é iniziato nel maggio dello stesso anno.
Il completamento della fase di distribuzione delle carte a tutti i cittadini con più di 12 anni é previsto per il 2005, con un ammontare stimato di circa 23 milioni di carte in circolazione.
Il progetto ha preso il nome di "MyKad", dalla composizione di "My", che, oltre al termine inglese, é il suffisso degli indirizzi internet malesi, e "Kad" che é l'acronimo di "Kad Akuan Diri" che significa in malese "carta d'identità".
Pur non essendo la prima applicazione della tecnologia biometrica ai documenti di identificazione personale, MyKad é certamente una carta multiservizi molto avanzata possedendo le funzioni di:

- carta di identità
- patente di guida
- passaporto
- carta dei servizi sanitari
- carta di accesso ai servizi della pubblica amministrazione
- carta di pagamento (caselli autostradali, trasporti e parcheggi pubblici)
- carta precaricata per acquisti di modesta entità (sino a $ 500)
- carta ATM

Da un punto di vista tecnologico, la carta, contenente, oltre ai dati biometrici (impronte digitali e iride), le informazioni demografiche del possessore, possiede attualmente un chip della capacità di 64k che può essere utilizzato sia con i dispositivi di lettura tradizionale che in modalità "contactless", .
Per garantire l'integrità delle carte, é stato inserito un certificato di firma digitale (PKI) emesso da un Ente governativo.

### 8.3.11 Documenti Elettronici – Nuovo passaporto elettronico, Australia - 2002

| | |
|---|---|
| **Obiettivo** | Realizzazione di un nuovo tipo di passaporto con identificatori biometrici. |
| **Tecnologia** | Riconoscimento bimetrico del volto |
| **Anno** | 2002 |
| **Status** | In fase di esecuzione |

L'Australia dal 2002 è impegnata nella realizzazione di un nuovo tipo di passaporto contenente le caratteristiche biometriche del volto del possessore. In particolare il progetto ha comportato:

- Il ridisegno del processo di emissione del Passaporto Australiano, aumentandone la sicurezza e l'integrità
- L'adeguamento ai nuovi standard di sicurezza dettati dal governo americano al fine di rispettare gli accordi bilaterali che regolano i mutui ingressi negli U.S. e in Australia
- Il controllo biometrico (in fase di emissione) di tipo "uno a molti", per cui l'immagine del richiedente viene confrontata con tutte le immagini presenti nel database per verificare che non sia già presente
- Per rinnovi e sostituzioni é stato implementato un controllo "uno a uno" per verificare che la nuova immagine coincida con quella del proprietario originario del passaporto.

Una seconda fase del progetto ha riguardato lo sviluppo di uno "unità di memorizzazione" nel passaporto imperniata su un chip di tipo "contactless" in grado di memorizzare i dati anagrafici e biometrici (volto) del proprietario del documento. Ad oggi (1° semestre 2004), sono stati emessi 10 milioni di nuovi passaporti.

### 8.3.12 Documenti elettronici – Nuova carta d'identità, Perù – 2002

| | |
|---|---|
| **Obiettivo** | Realizzazione di un nuovo tipo di passaporto con identificatori biometrici. |
| **Tecnologia** | Riconoscimento biometrico del volto |
| **Anno** | 2002 |
| **Status** | In fase di esecuzione |

Il sistema di identificazione Peruviano è stato sviluppato allo scopo di fornire a tutti cittadini un documento di identità "sicuro" tramite l'inclusione in esso di un elemento biometrico (impronta digitale).

Il "National Registry of Peru", Ente promotore del progetto, ricercava una soluzione che oltre a consentire l'identificazione dell'individuo permettesse anche l'accesso a servizi governativi come il voto o anche l'incasso di assegni. Il tempo di consegna ai cittadini del documento, di cui sono stati rilasciati, al 2002, circa 13 milioni di documenti è dell'ordine dei due giorni con la garanzia che la carta è rilasciata ad un singolo individuo e che questo è univocamente identificato.

### 8.3.13 Applicazioni nel settore sociale – Il programma DSS (Connecticut, U.S.) - 1996

| | |
|---|---|
| **Obiettivo** | Prevenzione delle frodi nell'ambito della fruizione di servizi sociali |
| **Tecnologia** | Riconoscimento delle impronte digitali |
| **Anno** | 1996 |
| **Status** | In esercizio |

Il progetto di identificazione biometrica realizzato nello stato del Connecticut (U.S.) è iniziato nel gennaio del 1996 dopo l'approvazione di una legge nel suddetto Stato che richiedeva una identificazione biometrica per coloro che intendevano usufruire di sussidi. Per gli scopi del Connecticut, l'identificazione biometrica intende l'acquisizione di due impronte digitali dell' indice allo scopo di mettere in evidenza le frodi derivanti da più godimenti dei sussisti fatti dalla stessa persone sotto identità differenti. L'acquisizione dell'immagine è fatta in maniera elettronica ed il processo di enrollment è dura meno di cinque minuti per ogni soggetto che aspira ad assistenza sociale. Le impronte sono immagazzinate in un archivio centralizzato insieme ad una fotografia e la firma dell'interessato. Durante il processo di enrollment gli utenti possono vedere le proprie impronte digitali sullo schermo del calcolatore usato per l'enrollment e mentre viene effettuata la ricerca nell'archivio per controllare eventuali duplicati, l'operatore del sistema acquisisce una fotografia e la firma del candidato e, in qualche minuto l'utente riceve una carta di riconoscimento. contenente la foto, un numero di identificazione di assistenza sociale, un codice a barre 2D rappresentante le minuzie dell'impronta digitale per una verifica veloce di tipo uno a uno dell'identità e una banda magnetica a norma ISO che può riportare altri dati personali. Le informazioni raccolte con il processo digitale di formazione immagine sono conforme alle regole di riservatezza di DSS e non possono essere usate per gli scopi tranne la gestione del programma anche se è prevista la possibilità di uno scambio di dati fra Stato e Stato.

### 8.3.14 Applicazioni nel settore sociale – Programma AFIRM (California, US) - 1991

| | |
|---|---|
| **Obiettivo** | Prevenzione delle frodi nell'ambito della fruizione di servizi sociali |
| **Tecnologia** | Riconoscimento delle impronte digitali |
| **Anno** | 1991 |
| **Status** | In esercizio |

Allo scopo di prevenire i casi di frode e abuso correlati alla distribuzione di "servizi di assistenza sociali" erogati da pubbliche amministrazioni, nella contea di Los Angeles e altre sei contee della California un sistema biometrico basato sul riconoscimento delle impronte digitali tende a evitare che lo stesso cittadino si presenti ad uffici pubblici diversi per richiedere il l'assistenza previsto; nei primi 4 mesi di attivazione del servizio (nella sola Contea di Los Angeles) sono stati intercettati circa 3.100 casi di richieste provenienti da soggetti che avevano già ottenuto il sussidio da un ufficio diverso per un controvalore di circa 5,4 milioni di US$ . Attraverso tale tecnica sono stati distribuiti all'incirca l'80% dei sussidi previsti dai programmi californiani di assistenza pubblica ai cittadini indigenti.. Tale sistema è stato esteso nella Contea di Los Angeles anche al programma di assistenza per le famiglie bisognose con figli a carico e da una stima condotta Ernst & Young valuta in circa 55 milioni di US$ il risparmio generato in 3 anni da tale applicazione.

### 8.3.15 Applicazioni nel settore sociale – Identificazione dei cittadini votanti – Costarica – 2002

| | |
|---|---|
| **Obiettivo** | Sistema elettronico di identificazione per i cittadini votanti |
| **Tecnologia** | Impronte digitali |
| **Anno** | 2002 |
| **Status** | In esercizio |

Progetto per la realizzazione di un sistema elettronico di identificazione biometrica per i cittadini votanti del Costa Rica, a prova di contraffazione per conto del Tribunal Supremo de Elecciones (TSE) .
Al posto della fotografia con la copertura in plastica che può essere facilmente rimossa per eventuali contraffazioni, la carta ora comprende la foto, la firma, l'impronta digitale di due dita, e un codice a barre contenente le minuzie associate alle impronte. La presenza di più informazioni in formato elettronico consente un'adeguata riduzione del rischio di emissione di carte duplicate in quanto, al momento che un cittadino registra la propria impronta digitale (enrollment) per ottenere una nuova carta d'identità, il TSE può confrontare le impronte con quelle presenti nel database
Le nuove carte d'identità non servono solo per votare, ma per una serie di servizi aggiuntivi quali:

- richiesta di duplicati della patente di guida
- richiesta del rinnovo del passaporto
- pagamento delle tasse
- accesso ai servizi sanitari
- accesso a servizi bancari

Finora sono state emesse circa 2.3 milioni di carte.

### 8.3.16 Applicazioni nel settore sociale - Informatizzazione della Pubblica Amministrazione - Andalusia (Spagna) – 1997

| | |
|---|---|
| **Obiettivo** | Identificazione ed accesso ai servizi sociali |
| **Tecnologia** | Impronte digitali |
| **Anno** | 1997 |
| **Status** | In esercizio |

Il Ministero del Lavoro e degli affari sociali in Spagna ha attuato un programma di ammodernamento dei servizi sociali dedicati ai cittadini, basato principalmente sulla creazione e distribuzione di una carta elettronica per l'identificazione e l'accesso ai servizi sociali. Sfruttando le nuove tecnologie informatiche e, in particolare, quella relativa alle smart card, il progetto ha raggiunto l'obiettivo di:

- incrementare l'utilizzo dei servizi online della Pubblica amministrazione, nel rispetto della privacy
- Fornire un accesso sicuro ai dati sensibili registrati nella carta e nei database contenenti informazioni sullo stato di salute dei cittadini

- realizzare un sistema di identificazione basato su tecnologia biometrica, al fine di garantire che le transazioni siano effettuate solo dal possessore della carta
- Ridurre degli usi impropri della carta servizi

La soluzione biometrica adottata si basa sul riconoscimento delle impronte digitali. A tal l'uopo sono state predisposte apposite workstation per la lettura, l'enrollment e la verifica delle impronte digitali. Inoltre, si é effettuata una integrazione tra il meccanismo di riconoscimento biometrico con le applicazioni fruibili attraverso chioschi selfservice disponibili in modo continuato.

### 8.3.17 Applicazioni nel settore sociale - Sistema "HANIS" (Sud Africa) - 2003

| | |
|---|---|
| **Obiettivo** | Identificazione dei cittadini e rilascio di carte di identità |
| **Tecnologia** | Impronte digitali |
| **Anno** | 1997 |
| **Status** | In esercizio |

La soluzione prevista dal Ministero dell'Interno sudafricano si é concretizzata nella creazione di un database denominato HANIS (Home Affairs National Identification System), considerato uno dei principali database di impronte digitali (con più di 43 milioni di cittadini registrati) per combattere le contraffazioni dei documenti d'identità.
Il progetto ha comportato un approccio integrato alle diverse discipline consulenziali, dall'analisi organizzativa e dei processi, alla gestione della comunicazione, alla implementazione tecnologica. La soluzione ha previsto la realizzazione di:

- un sistema di produzione di carte di identità elettroniche
- un sistema di identificazione mediante riconoscimento delle impronte digitali (AFIS),
- un sistema di interfaccia con la banca dati centralizzata del Ministero dell'Interno
- integrazione delle varie banche dati governative contenenti le informazioni demografiche dei cittadini

Lo sviluppo del sistema ha comportato dei vantaggi in termini di snellimento dei processi amministrativi ma anche di agevolazione all'accesso ai servizi privati, fornendo un sistema di autenticazione e di verifica dell'identità personale sia in linea che fuori linea..

# *Capitolo 9* Appendice

## 9.1 Laboratori di ricerca

### 9.1.1 In Italia

| Nome | Laboratorio Impronte Digitali - Polizia Scientifica - Ministero dell'Interno |
|---|---|
| Responsabile | ing. Stefano Petecchia |
| Attività | AFIS per identificazione su banche dati impronte digitali, ricerca impronte latenti (reperite sul luogo del crimine), documenti elettronici con biometria (passaporto, carta di identità, ecc). |
| Note | |
| Web | http://www.poliziadistato.it/pds/chisiamo/territorio/reparti/scientifica/scientifica.htm |

| Nome | Laboratorio di Sistemi Biometrici (BioLab) dell'Università di Bologna |
|---|---|
| Responsabili | prof. Dario Maio, prof. Davide Maltoni |
| Attività | Impronte digitali (riconoscimento, classificazione, generazione sintetica: SFinGe), volto umano, geometria della mano, valutazione delle prestazioni di sistemi biometrici. |
| Note | Organizza bi-annualmente la competizione internazionale FVC per il riconoscimento di impronte digitali ( http://bias.csr.unibo.it/fvc2004 ) |
| Web | http://bias.csr.unibo.it/research/biolab |

| Nome | Istituto di Biostrutture e Bioimmagini (CNR) presso Università Federico II di Napoli |
|---|---|
| Responsabile | ing. Mario Savastano |
| Attività | Definizione di standard a livello internazionale, privacy e usabilità dei sistemi biometrici. |
| Note | Partecipa al sottocomitato SC37 (ISO) sulla Biometria in rappresentanza di UNI (Ente Nazionale Italiano di Unificazione) |
| Web | |

| Nome | Centro di Ricerca presso DIEE (Università di Cagliari) |
|---|---|
| Responsabile | prof. Fabio Roli |
| Attività | Impronte digitali, volto umano, sistemi multimodali (accoppiamento di più sensori o di diverse tecniche biometriche). |
| Note | |
| Web | http://ce.diee.unica.it/it/prag/ |

| Nome | Centro di ricerca presso DIST (Università di Sassari) |
|---|---|
| Responsabile | prof. Massimo Tistarelli |
| Attività | Volto umano |

| | |
|---|---|
| Note | Ha organizzato la scuola estiva internazionale sulla biometria (Alghero, giugno 2003) |
| Web | http://www.dist.unige.it/DIST/MDIST/mtistarelli.html |

| Nome | Centro di ricerca della Fondazione Ugo Bordoni |
|---|---|
| Responsabile | ing. Mauro Falcone |
| Attività | Riconoscimento della voce |
| Note | |
| Web | http://www.fub.it/ |

| Nome | Centro di ricerca presso IIT-CNR di Pisa |
|---|---|
| Responsabile | dr.ssa Anna Maccarelli |
| Attività | Riconoscimento impronte digitali in combinazione con smart card e firma digitale |
| Note | |
| Web | http://www.iat.cnr.it/home.html |

### 9.1.2 All'estero

| Nome | Biometrics - NIST (National Institute of Standard and Technologies) |
|---|---|
| Responsabili | dr. Fernando Podio |
| Attività | Partecipa alla definizione di standard sulla biometria. Organizza periodicamente campagne di valutazione di sistemi biometrici: volto umano (FRVT), impronte digitali (FPVTE), voce. |
| Note | Molto attivo nel processo di standardizzazione (sia in ambito ISO che a livello nazionale attraverso INCITS M1 - Biometrics Technical Committee). |
| Web | http://www.itl.nist.gov/div893/biometrics/<br>http://www.itl.nist.gov/iaui/vip/ |

| Nome | Biometric Consortium (USA) |
|---|---|
| Responsabili | Fernando Podio (NIST), Jeffrey S. Dunn |
| Attività | Gruppo di discussione sulle tecnologie biometriche. Organizza conferenze periodiche. |
| Note | Mantiene la lista di discussione (internet) più nota sulla biometria. |
| Web | http://www.biometrics.org |

| Nome | Centro di ricerca sulla Biometria (Michigan State University - USA) |
|---|---|
| Responsabili | prof. Anil. K. Jain |
| Attività | Impronte digitali, volto umano, geometria della mano, valutazione delle prestazioni di sistemi biometrici. |
| Note | |
| Web | http://biometrics.cse.msu.edu/ |

| Nome | Centro di ricerca su tecniche di identificazione CITeR (West Virginia - USA) |
|---|---|
| Responsabile | |
| Attività | Consorzio finanziato da NSF (US National Science Foundation) e da soggetti privati per la ricerca multi tematica sulla biometria. |
| Note | |
| Web | http://www.citer.wvu.edu |

| Nome | Centro di ricerca su Sistemi Biometrici (San Jose State University - USA) |
|---|---|
| Responsabile | dr. James Wayman |
| Attività | Valutazione delle prestazioni di sistemi biometrici. |
| Note | |
| Web | http://www.sjsu.edu/ |

| Nome | Centro di ricerca Hong Kong (Polytechnic University - Cina) |
|---|---|
| Responsabile | prof. David Zhang |
| Attività | Geometria della mano, dermatoglifi della mano |
| Note | |
| Web | http://www.comp.polyu.edu.hk/research/researchlab/bl.html |

| Nome | UK Biometrics Working Group (BWG) |
|---|---|
| Responsabile | Philip Statham |
| Attività | Policy nazionale sull'uso della biometria nelle applicazioni governative<br>Sviluppo di standard, test di prodotti biometrici, indicazioni generali sui criteri di scelta e approvvigionamento di sistemi biometrici |
| Note | |
| Web | http://www.cesg.gov.uk/site/ast/index.cfm?menuSelected=4&displayPage=4 |

| Nome | National Physical Laboratori – NPL - (UK) |
|---|---|
| Responsabile | dr. Tony Mansfield |
| Attività | Valutazione delle prestazioni di sistemi biometrici. Partecipazione allo sviluppo di standard. |
| Note | Il Dr. Mansfield è autore delle linee guida: "Best Practices in Testing and Reporting Performance of Biometric Devices". |
| Web | www.npl.co.uk |

## 9.2 Importanza della standardizzazione

Il mondo della standardizzazione è caratterizzato da un rigore procedurale e formale che spesso provoca un certo isolamento dai tradizionali contesti tecnologici. D'altra parte, una certa complessità dei processi è comprensibile visto e considerato che la posta in gioco è molto alta e uno standard ben riuscito può spianare la strada ad una tecnologia o prodotto favorendone una crescita armonizzata a livello internazionale con tutte le ovvie e dirette ricadute di tipo commerciale.

Dal punto di vista pratico, un aspetto particolarmente critico per Pubblica Amministrazione, collegato alla standardizzazione, concerne essenzialmente l'interoperabilità. Il discorso naturalmente si semplifica totalmente quando il produttore della tecnologia è unico [42] perché in questo caso si può porre al più un problema di compatibilità tra i vari modelli e le varie release di software anche se, la tendenza, è cercare di garantire in maniera totale la migrazione verso prodotti più evoluti e software più avanzati.
Molto più impegnativi sono invece i problemi di interoperabilità nel caso che i produttori della tecnologia biometrica siano numerosi come accade nel settore delle impronte digitali caratterizzato da un alto numero di produttori che commercializzano dispositivi con diverse particolarità meccaniche ed frequente uso di algoritmi proprietari. Usando sensori di tipo differente per l'acquisizione e la lettura, il problema è particolarmente sentito come bene messo in evidenza in [1]. A questo punto è evidente che alcuni esperti del settore facciano notare come uno dei requisiti per la scelta, da parte di una Amministrazione, di un particolare sensore, dovrebbe consistere nella valutazione della "solidità" della società produttrice della tecnologia biometrica che dovrebbe garantire una certa vita del prodotto (una nuova operazione di registrazione degli utenti potrebbe presentare un costo considerevole).

### 9.2.1 Il sottocomitato 37 (SC 37) dell'ISO/IEC TCI

Nel Giugno del 2002 l'ISO (International Organization for Standardization) ha formato un nuovo sottocomitato sulla biometria (ISO/IEC JTC1 SC37 "Biometrics") il cui obiettivo del sottocomitato (d'ora in poi chiamato, brevemente, "SC37") è il "rapido" (il processo può durare molti anni) sviluppo di standard generici nel settore della biometria e, a tal fine sono stati creati sei gruppi di lavoro (Working Group, detti, sempre "WG"), nell'ordine:

- WG1 sull'armonizzazione della terminologia e delle definizioni (Harmonised Biometric Vocabulary and Definitions).
- WG2 sulle interfacce (Biometric Technical Interfaces)
- WG3 sui formati di scambio dei dati (Biometric Data Interchange Formats)
- WG4 sui profili per le applicazioni (Profiles for Biometric Applications)
- WG5 sulla valutazione delle prestazioni (Biometric Testing and Reporting)
- WG6 sugli aspetti giuridici e sociali (Cross-Jurisdictional and Societal Aspects).

Una esemplificata descrizione della attività dell'SC37 potrebbe mettere in evidenza che WG1 è impegnato nella definizione dei termini giusti, WG2 nel far dialogare tra loro i dispositivi biometrici, WG3 a fare in modo che si "capiscano", WG4 che raggiungano gli scopi prefissi, WG5 che funzionino a dovere e, finalmente, WG6 che siano ben accetti agli utenti.
Escludendo il prezioso lavoro di WG1, dedicato alla armonizzazione terminologica, immancabile ingrediente in qualsiasi contesto normativo, già da una prima analisi, comincia ad essere chiaro che mentre l'attività dei tutti i gruppi di lavoro è quella classica di un Comitato di Standardizzazione, WG6, che tratta gli aspetti giuridici e sociali della biometria, rappresenta un elemento di novità perché, gruppo intrinsecamente "non tecnico" in un consesso strettamente tecnico.

[42] o, per quota di mercato, praticamente unico (vedi geometria della mano o riconoscimento dell'iride). Va comunque evidenziato che entrambi hanno avviato un processo di standardizzazione dei formati.

#### 9.2.1.1 Il ruolo dell'Italia nel WG6 del SC37

Un esperto italiano ha il compito di coordinare le attività di WG6 (gli altri gruppi di lavoro sono guidati da personali canadese, statunitense, coreano, tedesco ed inglese) per cui l'Italia occupa una posizione di primo piano nel quadro internazionale.
Gli aspetti attualmente allo studio nel WG6 sono:

- Intersezioni fra medicina e biometria
- Accessibilità (diritto alla)
- Privacy

Il lavoro sulle delicati intersezioni fra medicina e biometria, già messo in evidenza nel capitolo 6, prevede la valutazione delle cosidette "implicazioni mediche dirette", e cioè degli (assolutamente potenziali) effetti delle tecniche biometriche dal punto di vista fisico e le "implicazioni mediche indirette" e cioè la valutazione della (potenziale) estrazione, nel corso del processo biometrico di (eventuali) informazioni mediche relative all'utente. Va subito chiarito che le possibilità di simili eventualità sono veramente remote ma, sempre allo scopo di rassicurare l'utente, è necessario che l'implicazione medica indiretta sia messa in campo, sia determinato il suo peso e siano suggerite le adeguate contromisure per ridurre questo rischio che, come è evidente, compete alla delicata sfera della tutela della privacy. L'argomento "accessibilità" intende, fra l'altro, la valutazione delle eventuali discriminazioni che potrebbero verificarsi a causa di una mancata fruibilità di una tecnologia biometria per handicap fisici, va detto che, nell'ambito dei temi di lavoro del WG6, quello della privacy è il più complesso per le forti differenze, a livello internazionale, in tema di protezione dei dati personali. Allo spirito più pragmatico di alcuni Stati si contrappone infatti un atteggiamento più conservativo da parte di altri e, per ora, l'unica strada percorribile è quella "piccoli passi", alla ricerca di un minimo denominatore comune in grado di essere accettabile per tutti e, almeno per ora, il rispetto per le implicazioni mediche della biometria sembra il primo, timido, esempio di consenso generalizzato.

### 9.2.2 BioAPI

Il consorzio BioAPI (www.bioapi.org) nasce nell'aprile del 1998 con lo scopo di definire delle Application Programming Interface (API) standard per il mondo biometrico; per intenderci qualcosa come le API pc/sc per le smart card, con la differenza che queste ultime sono state realizzate da un unico produttore (Microsoft) mentre nel consorzio BioAPI partecipano i principali operatori mondiali di prodotti biometrici.
Nel marzo 1999 nel consorzio BioAPI è confluito anche il consorzio Human Authentication API (HA-API), sotto la spinta del National Institute of Standards and Technology (NIST).
Nel marzo 2000 venivano pubblicate le API versione 1.0 ed in settembre le 1.1, tuttora rilasciate.
Soci del consorzio sono più di un centinaio di aziende, tra operatori del settore, utenti (banche, system integrator, organizzazioni militari,..) e organizzazioni istituzionali (standards).
L'obiettivo del consorzio è quello di definire standard applicativi, indipendenti dai sistemi operativi, in grado di supportare diversi dispositivi e diverse tecniche biometriche: quindi un applicazione sviluppata con le BioAPI opera automaticamente con tutti quei dispositivi dichiarati BioAPI compatibili, contemporaneamente nelle diverse tecnologie biometriche (impronta digitale, voce, viso, iride, ecc.). Le BioAPI soddisfano i processi di:

- registrazione (enrollment);

- autenticazione (uno a uno);
- identificazione (uno a molti).

Al momento sono disponibili numerosi prodotti e applicazioni che si dichiarano compatibili con gli standard BioApi.

Per l'utente, l'utilizzo di prodotti compatibili BioAPI presenta numerosi vantaggi:

- in fase di valutazione dei prodotti biometrici, scelta (o sviluppata) l'applicazione è possibile effettuare test di diversi rilevatori biometrici nell'ambito della stessa tecnologia biometrica od anche comparare diverse tecnologie
- è possibile utilizzare contemporaneamente diverse tecnologie biometriche nell'ambito della stessa applicazione
- è possibile svincolarsi dalla dipendenza da un unico fornitore di dispositivi biometrici, anche se ciò richiede accorgimenti nello sviluppo dell'applicazione, in quanto i template restano pur sempre proprietari dei vari produttori e non sono quindi intercambiali
- è possibile utilizzare diverse applicazioni, con gli stessi dispositivi biometrici, od anche cambiare l'applicazione, mantenendo l'investimento fatto nella dotazione di dispositivi biometrici

### 9.2.3 CBEFF (Common Biometric Exchange File Format)

Dal 1999 al 2000 un gruppo di lavoro sponsorizzato dal NIST (National Institute of Standards and Technology – U.S.) e del Biometric Consortium (U.S.), ha sviluppato il CBEFF (Common Biometric Exchange File Format) pubblicato nel 2001 come in forma di NISTIR (NIST Interagency Report).

CBEFF descrive la struttura di dati necessaria per supportare le tecnologie biometriche in una maniera comune, indipendentemente dall'applicazione e dal tipo di uso.

I punti di forza di CBEFF consistono in:

- facilitazione dello scambio di dati biometrici fra differenti componenti del sistema o fra differenti sistemi,
- promozione dell'interoperabilità dei programmi e dei sistemi basati sulle tecniche biometriche,
- supporto alla compatibilità futura in conseguenza dei miglioramenti delle tecnologie biometriche,
- facilitazione dei processi di integrazione hardware/software

Attualmente l'approvazione del CBEFF a livello internazionale è in stato di avanzamento nell'ambito dei lavori del sottocomitato 37 dell'ISO/IEC JTC1.

### 9.2.4 Human Recognition Services (HRS) Module

Lo Human Recognition Services (HRS) Module è una estensione dell'Open Group's Common Data Security Architecture (CDSA). CDSA è un insieme strutturato di servizi di sicurezza e un framework crittografico per generare applicazioni di sicurezza, indipendenti dalla piattaforma ed interoperabili,per ambienti client/server:

L'obiettivo di CDSA di rendere sicuro l'e-commerce ed altre applicazioni commerciali/gestionali con servizi che vanno dalla crittografia, all'amministrazione del certificato, l'amministrazione di politica di fiducia ed il recupero chiave.

Il componente biometrico presente nel CDSA è usato insieme ad altri moduli di sicurezza (crittografico, certificati, librerie…) ed è compatibile con le specifiche BioAPI ed il CBEFF.

### 9.2.5 ANSI X984

Approvato nel 2001 dall'ANSI [43], l' **X9.84-2000** (Biometrics Management and Security for the Financial Services Industry) è un documento del comitato X9F4 orientato alle procedure di sicurezza nell'industria finanziaria in relazione all'adozione di tecnologie biometriche. Andrebbe sottolineato che, con riferimento a tale standard l'IBIA [44] viene identificata come interlocutore ufficiale per la registrazione di sistemi di identificazione, con il compito di coordinamento con i formati BIOAPI e CBEFF.

### 9.2.6 ICAO

Fin dal 1980 l'ICAO (International Civil Aviation Organization) ha pubblicato documenti in merito alla standardizzazione dei passaporti ed il primo passo sono state le specifiche per i passaporti leggibili in maniera automatica (i cosiddetti machine readable passports). Il lavoro è continuato con la definizione di convenzioni sui nomi, traslitterazione di caratteri nazionali nella cosiddetta MRZ, Machine Readable Zone e cioè l'area del passaporto leggibile in maniera automatica ed il calcolo della check digit.
Per ciò che attiene alla emissione del nuovo passaporto elettronico, l'ICAO ha indicato tre tecnologie biometriche per il passaporto di cui una, il riconoscimento biometrico del volto, obbligatoria e due, impronte digitali e riconoscimento dell'iride opzionali.

### 9.2.7 ISO 7816-11

Lo standard ISO/IEC 7816-11, sviluppato da ISO/IEC JTC1/SC177WG4, tratta aspetti quali:

- l'uso dell'ISO/IEC 7816-4 ai fini della verifica di identità su base biometrica;
- individua le informazioni necessarie per il mach-on-card (o off-card) in riferimento ai data object individuati in CBEFF;
- affronta problematiche di sicurezza;
- presenta esempi per l'uso dell'ISO/IEC 7816-4 ai fini della verifica di identità su base biometrica.

### 9.2.8 NIST 2000

Lo standard ANSI/NIST-ITL 1-2000, proviene dalle norme ANSI/NIST-CSL 1-1993 "Formato dei dati per lo scambio delle informazioni inerenti le impronte digitali" che come specifica il nome, definivano un formato di interscambio sia per le impronte digitali che per altri dati in formato immagine. In 1997, un nuovo documento ANSI (ANSI/NIST-ITL 1a-

[43] American National Standard Institute

[44] International Biometric Industries Association

1997) allargava il campo di analisi anche ad altre caratteristiche quali foto segnaletiche o tatuaggi. Nel 2000, a seguito di un lungo processo di revisione dei due standard, e con l'aggiunta di nuovi campi, di nuove strutture record, e della fusione dei primi due standard, si perveniva all' ANSI/NIST-ITL 1-2000. Questo standard definisce il contenuto, il formato, e le unità di misura per lo scambio di impronte digitali, impronte del palmo, foto segnaletiche, descrizione di cicatrici, marchi e tatuaggi (Scar, Mark and Tattoo - SMT) che possono essere usate nel processo dell'identificazione di un soggetto. Le informazioni consistono di una varietà di punti, alcuni obbligatori altri facoltativi tra cui i parametri per la digitalizzazione delle immagini ed i formati delle immagini compresse o non compresse. Queste informazioni sono intese a gestire lo scambio di informazioni fra le Amministrazioni interessate.

## 9.3 Approfondimenti tecnici

### 9.3.1 Teoria degli errori

Nessun sistema biometrico reale, data la sua modalità di funzionamento e la variabilità del dato misurato nelle diverse sessioni, è in grado di fornire risposte assolute (ovvero non affette da errore) sull'identità di un soggetto.
Si consideri, infatti, un sistema biometrico per la verifica d'identità, che è stato impostato dall'amministratore per operare con una determinata *soglia di decisione* (corrispondente a uno specifico "punto di lavoro")[45].
In fase di verifica, dopo aver valutato lo *score* (punteggio) di similarità prodotto dal confronto del campione corrente con un template precedentemente memorizzato, il sistema confronta lo score con il valore della soglia di decisione: se lo score è maggiore della soglia il sistema conclude che si tratta dello stesso soggetto, in caso contrario che si tratta di soggetti diversi.
La decisione del sistema non è esente da errore; infatti si possono presentare due tipi di errore:

- **Falso Rifiuto** (FRE, False Rejection Error, o errore di tipo 1): la vera identità di un regolare utente registrato è rifiutata perché non verificata o non identificata, giacché lo score prodotto è troppo basso (inferiore al valore di soglia scelto);
- **Falsa Accettazione** (FAE, False Acceptance Error, o errore di tipo 2): viene accettata l'identità falsa di un impostore come quella di un regolare utente registrato, poiché lo score prodotto è troppo alto (superiore al valore di soglia scelto).

In corrispondenza a questi eventi d'errore si definiscono (e si calcolano) le relative probabilità di occorrenza, stimabili, e generalmente identificate, in termini di frequenze di occorrenza indicate come FRR e FAR, rispettivamente FRE Ratio e FAE Ratio:

[45] la modalità di impostazione della soglia varia da sistema a sistema; in alcuni sistemi può essere impostata in modo molto semplice agendo su un cursore che viene posizionato tra un minimo e un massimo previsto; altri prevedono un controllo più accurato attraverso l'input di un valore numerico che talvolta può essere anche modificato per utenti diversi.

- **FRR (False Rejection Rate)** è la frequenza (o probabilità di occorrenza) di errori di tipo False Rifiuto.
- **FAR (False Acceptance Rate)** è la frequenza (o probabilità di occorrenza) di errori di tipo False Accettazione.

In un sistema ideale le suddette probabilità (FRR e FAR) sono nulle. In un sistema reale, invece, detti valori sono non nulli, e dipendono dal particolare valore della soglia di decisione. Ad esempio, se per un particolare valore della soglia, si ha FAR = 0.0001 = 0.01% significa che in media il sistema accetta ingiustamente un impostore ogni 10.000 tentativi fraudolenti, e FRR = 0.02 = 2% significa che in media un utente abilitato viene rifiutato 2 volte ogni 100 tentativi di accesso. Attenzione all'uso della notazione percentuale (%) quando si confrontano accuratezze di sistemi diversi: alcuni fornitori riportano il dato %, altri come probabilità assoluta.

Alcune precisazioni sono necessarie a questo punto per maggiore chiarezza:

- innanzitutto il contesto applicativo considerato dalle definizioni precedenti è quello di un sistema biometrico per il riconoscimento positivo (ad esempio il controllo degli accessi o delle risorse); in alcune applicazioni l'identificazione biometrica, ovvero la ricerca della caratteristica dell'individuo all'interno di un database, è utilizzata per prevenire accessi multipli di un soggetto a una o più risorse (riconoscimento negativo): in diversi stati americani sistemi basati su impronte digitali aiutano a prevenire il fatto che lo stesso soggetto riscuota più volte (sotto identità diverse) i benefici assistenziali. In questo caso una falsa accettazione (ovvero un'ingiusta concessione di assistenza) è conseguenza del mancato match (rifiuto) con una delle caratteristiche già presenti nel database di coloro che hanno usufruito dell'assistenza e viceversa un falso rifiuto (ovvero un ingiusta concessione di assistenza) deriva dal match (accettazione) con uno dei modelli memorizzati. In questo caso dunque le definizioni precedenti sono ambigue e FAR ed FRR vengono sostituiti dalle più generiche ma meno comuni denominazioni: FMR (False Match Rate) e FNMR (False Non-Match Rate).
- in secondo luogo nel caso di sistemi di identificazione un terzo tipo di errore può essere causato da scambi di identità (anche se in realtà questi errori sono spesso considerati false accettazioni). In questo caso utenti abilitati all'accesso vengono riconosciuti dal sistema come altri utenti anch'essi abilitati: la percentuale di questi errori è denominata ER1-N (Exchange Rate). Ciò ha generalmente conseguenze meno gravi rispetto alle false accettazioni di soggetti non abilitati, ma può essere altamente indesiderato se le risorse controllate dal sistema in questione devono essere assegnate differentemente in base all'identità degli utenti. Per maggiore chiarezza, nel caso di sistemi biometrici di identificazione, si indicano FAR e FRR rispettivamente con FAR1-N e FRR1-N.
- è poi necessario specificare esattamente che cosa si intenda per tentativo di accesso. Alcuni sistemi, per ridurre al minimo la possibilità che un utente abilitato non riesca a guadagnare accesso al sistema, concedono al soggetto più tentativi, e, in modo molto ambiguo, definiscono tentativo di accesso l'intera sequenza di prove. Un modo più corretto di procedere prevede, in presenza di tentativi multipli di accesso che consentono al massimo m prove, di rinominare FAR con m-trials-FAR e FRR con m-trials-FRR. Nell'ipotesi di concedere

l'accesso se almeno una delle m prove ha dato esisto positivo è piuttosto semplice dimostrare la dipendenza di m-trials-FAR da FAR e di m-trials-FRR da FRR:
m-trials-FAR = 1– (1–FAR)m ≈ m × FAR (approssimazione valida per FAR piccolo)
m-trials-FRR = (FRR)m

- I vantaggi in termini di accuratezza di identificazione derivanti dall'uso di tentativi multipli sono più che evidenti in quanto, come mostrato dalle formule, m-trials-FRR decresce esponenzialmente (essendo FRR<1) mentre m-trials-FAR cresce solo linearmente.
- infine è necessario precisare che sebbene FRR e FAR siano riferiti al caso medio, nella pratica gli errori sono spesso "sbilanciati" a seconda degli utenti del sistema. Frequente è il caso in cui per alcuni utenti (denominati goat in letteratura) la probabilità di essere rifiutati risulti significativamente superiore alla media a causa, ad esempio, della difficoltà di apprendere il corretto modo di interagire con il dispositivo di acquisizione o della minor "qualità intrinseca" della caratteristica biometrica utilizzata; per contro, per altri utenti, la suddetta probabilità risulta spesso molto inferiore alla media. è stato inoltre notato che per certe caratteristiche biometriche, come la voce, alcuni utenti possono essere più semplicemente imitati da altri utenti e ciò si riflette in uno sbilanciamento di FAR rispetto al valore medio.

Per mettere in evidenza la dipendenza di FAR ed FRR dalla soglia di decisione ***t*** del sistema i due valori sono talvolta indicati come FAR(*t*) e FRR(*t*). FAR(*t*) e FRR(*t*) sono strettamente legati tra loro: se la soglia *t* viene aumentata, al fine di decrescere la probabilità di frodi, conseguentemente aumenta la probabilità che il sistema non identifichi utenti autorizzati, e viceversa. Il valore da scegliere per la soglia di decisione dovrebbe essere il risultato di una fase di analisi in grado di effettuare un compromesso opportuno tra FAR e FRR. I criteri non possono non dipendere dalla applicazione cui il sistema è destinato, come descritto nella sezione 9.3.2. Si sottolinea che un sistema biometrico, una volta tarato, è in grado di funzionare in un solo punto di lavoro alla volta, e che, quindi, non è mai realistico pensare di ottenere, o dichiarare, valori allo stesso tempo molto bassi per i due tipi di errore. Il miglior FAR ottenuto, o ottenibile, da un sistema biometrico, quindi, non è mai corrispondente al miglior FRR.

Ogni volta che si richiedono (o si dichiarano) le prestazioni di un sistema, pertanto, occorre specificare a quale punto di lavoro ci si riferisce: se si dichiara un FRR si deve specificare per quale FAR è stato ottenuto e viceversa: non si deve indicare, né accettare, un valore di FAR (o di FRR) in modo assoluto, ma si può solo parlare di FAR vs FRR o FRR vs FAR. Non ha molto significato, pertanto, la modalità con la quale i fornitori di solito indicano le prestazioni dei loro sistemi: allorché si dichiara che un sistema, ad esempio, riesce ad ottenere un FAR<0.001% e un FRR<0.01%, senza che se ne siano indicati i relativi valori di soglia, non si è di fatto fornita una esatta indicazione delle prestazioni operative che il sistema è in grado di garantire. Nulla autorizza a ritenere che i valori dichiarati di FAR e FRR, indicati generalmente come i migliori raggiungibili dal sistema, siano ottenibili insieme, vale a dire per lo stesso punto di lavoro, cioè per lo stesso valore di soglia di decisione.

FAR(*t*) e FRR(*t*) si incontrano nel punto detto **EER** (Equal Error Rate), ove FAR coincide con FRR (si veda Figura 9.1); EER non corrisponde generalmente a un punto di funzionamento di pratica utilità, poiché individua un punto di lavoro non ottimale né per

applicazioni di sicurezza come il controllo degli accessi, né per applicazioni in ambito forense. D'altro canto, EER viene spesso utilizzato per la definizione dell'accuratezza del sistema, in quanto consente di definirla indipendentemente dalla soglia e pertanto rende comparabili le prestazioni di sistemi diversi[46]. ZeroFAR e ZeroFRR, così come definiti in sezione 12.1, sono altresì riportati sul grafico delle funzioni FAR(*t*) e FRR(*t*).

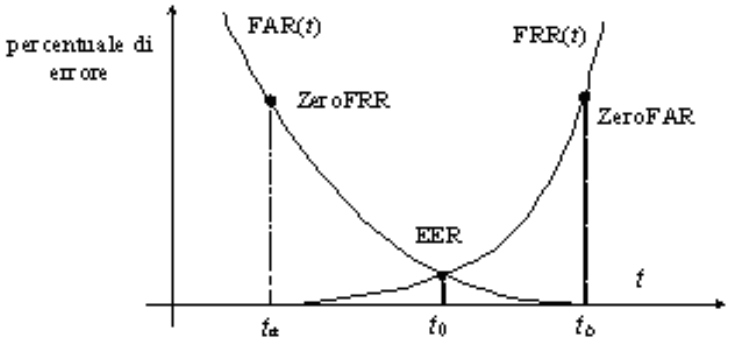


*Figura 9.1: FAR(t) e FRR(t) al variare della soglia t per un sistema biometrico per la verifica di identità.*

Il valore di EER è un utile elemento di valutazione e confronto per le prestazioni di un sistema biometrico, ma, proprio per come è definito, non esplora tutta la scala di possibili modalità di funzionamento di un sistema. Il funzionamento di un sistema biometrico per i diversi punti di lavoro è descritto da due grafici denominati ROC e DET:

**ROC** (Receiver's Operating Curve) riporta la probabilità di corretta accettazione del sistema, espressa come 1-FRR, al variare della probabilità di false accettazioni FAR (si veda Figura 9.2). Il confronto di due sistemi biometrici diversi può essere effettuato disponendo delle relative ROC. Nel caso le due curve non si intersechino, il sistema uniformemente più accurato (per tutta la possibile gamma di modalità operative) è quello la cui curva di prestazioni è più vicina all'angolo in alto a sinistra. Nel caso di curve con punti di intersezione, il sistema con migliore accuratezza è quello che nella zona di interesse dell'applicazione (per specifiche modalità operative) presenta il tratto di ROC più vicino al punto ideale. Nel caso in cui occorra confrontare le prestazioni di sistemi biometrici diversi, tutti caratterizzati da buone prestazioni (non molto dissimili tra loro), le curve ROC tendono ad essere molto sovrapposte e condensate nell'angolo superiore sinistro del grafico[47]; per questo motivo si preferisce ricorrere a grafici di tipo DET (come descritto nel seguito).

[46] si veda ad es. "Extracting forensic evidence from biometric devices", Z.Geradts, A.Ruifrok, Soc. Photo-Optical Instr. Eng., proc. Investigative Image Processing, 2003.

[47] "The DET Curve Assessment of Detection Task Performance", A. Martin et al., Proc. EuroSpeech 97, IEEE CS Press, Los Alamitos, Calif., 1997, pp. 1895-1898.

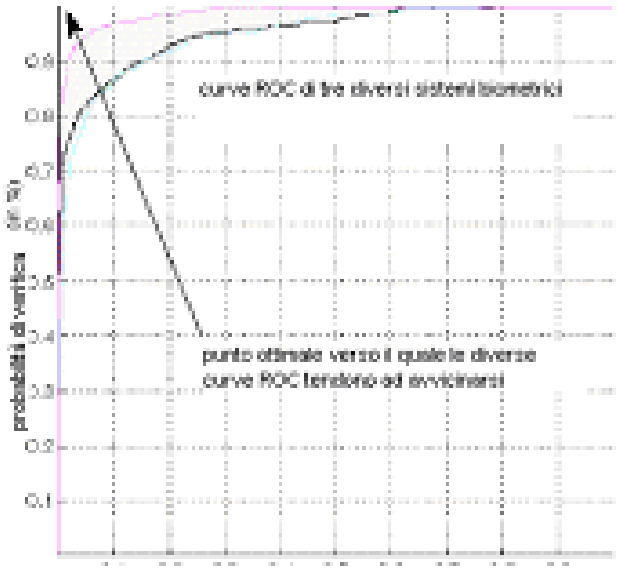


*Figura 9.2: ROC di tre diversi sistemi biometrici per la verifica di identità.*

**DET** (Detection Error rate  Trade-off) riporta la probabilità di false accettazioni del sistema FRR, al variare della probabilità di false accettazioni FAR (si veda Figura 9.3). Generalmente per una migliore rappresentazione delle regioni di interesse DET è disegnato in scala logaritmica. DET consente, in genere, una migliore separazione tra le diverse curve rispetto a ROC e si presta quindi a una migliore analisi comparativa delle prestazioni.

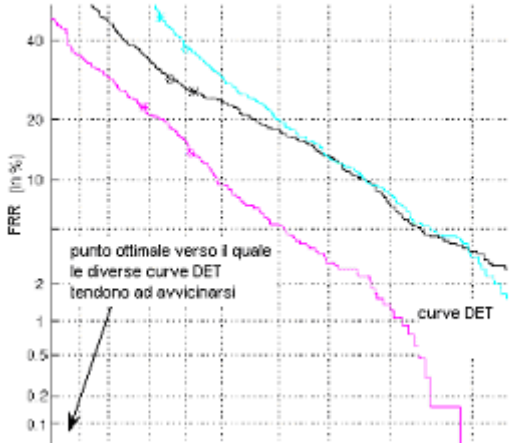


*Figura 9.3DET di tre diversi sistemi biometrici per la verifica di identità.*

### 9.3.2 Gli errori nel contesto di laboratorio e nelle applicazioni reali

Il valore della soglia di decisione del sistema, vale a dire il suo punto di lavoro, e quindi delle probabilità di errore considerate accettabili nell'applicazione del sistema in esame, deve essere scelto mediando tra sicurezza e usabilità. Tale compromesso è fortemente dipendente dalla applicazione cui il sistema è destinato.

Nelle applicazioni di elevata sicurezza, tipiche del controllo degli accessi, considerando generalmente molto importante l'errore di falsa accettazione, si utilizzano valori di soglia elevati per avere delle probabilità di false accettazioni molto basse, FAR→0 (la notazione →0

indica "tendente a zero"), accettando una corrispondente probabilità di falso rifiuto FRR di regola non trascurabile. Ciò è motivato dal fatto che lo scopo delle suddette applicazioni è tenere "fuori" del contesto protetto gli indesiderati e i non autorizzati, quindi, avere un numero di accessi indesiderati che sia pressoché nullo, sopportando un corrispondente numero di rifiuti indebiti che non è, per quanto visto, il migliore ottenibile dal sistema, ma che tuttavia l'applicazione pratica deve essere in grado di gestire, anche se come eccezioni. Occorre sottolineare infatti come, nonostante nelle applicazioni di sicurezza l'errore di falso rifiuto sia generalmente ritenuto meno importante, non sia utile accettarne valori troppo elevati per spingere l'errore di falsa accettazione al minimo: i falsi rifiuti costituiscono comunque delle eccezioni che la struttura di sicurezza nella quale il sistema biometrico è inserito deve gestire, attraverso la previsione di procedure diverse dal flusso ordinario. In un aeroporto il flusso ordinario di controllo è ottenuto attraverso dispositivi automatici, basati, ad esempio, sulla verifica di identità attraverso documenti di viaggio contenenti identificativi biometrici (si veda la sezione 4.2). Le eccezioni a tale flusso ordinario dovrebbero essere costituite dai falsi rifiuti, vale a dire dai casi in cui viene negata ai soggetti legittimati la possibilità di varcare il gate aeroportuale. Questi soggetti verranno indirizzati verso un controllo di tipo tradizionale effettuato da operatori di polizia di frontiera, che consisterà in analisi fatte da esperti di falso documentale tradizionale, e/o da interrogazioni su particolari banche dati per gli accertamenti dei casi sospetti. Tali controlli risultano essere molto onerosi dal punto di vista del tempo e dal personale impiegato per la loro effettuazione. Il personale, in particolare, è costituito da esperti in falso documentale, che devono tenere un livello di concentrazione elevato durante tutta la loro delicata attività. In tali ambiti, quindi, è evidente la necessità di mantenere il livello dei falsi rifiuti accettabile per evitare code di passeggeri troppo lunghe e/o per mantenere elevata la qualità dei controlli di tipo tradizionale (affaticamento degli operatori).
Nella fase di fissazione del punto di lavoro di un sistema biometrico per applicazioni di sicurezza, occorre considerare che il numero dei falsi rifiuti dipende, non solo dall'accuratezza intrinseca del sistema, ma anche dal modo nel quale viene acquisito il dato biometrico. Occorre considerare le eventualità in cui una frequenza elevata di falsi rifiuti sia dovuta a una procedura non ideale di acquisizione del campione biometrico (es. a un dito in cattive condizioni durante un controllo basato su impronte digitali, ovvero dal non corretto allineamento del dispositivo di acquisizione durante la cattura dell'immagine dell'iride).

Nelle applicazioni in ambito forense, considerando generalmente più importante l'errore di falso rifiuto, si utilizzano valori di soglia più bassi per avere probabilità di falso rifiuto molto basse, FRR→0, accettando una corrispondente probabilità di falsa accettazione FAR di regola non trascurabile. Lo scopo di tali applicazioni è avere un numero di (falsi) rifiuti di colpevoli che sia pressoché nullo, sopportando un corrispondente numero di identificazioni erronee che non è, per quanto visto, il migliore ottenibile dal sistema, ma che tuttavia l'applicazione e gli esperti umani di analisi dei candidati, siano in grado di gestire. Occorre sottolineare, infatti, come nonostante nelle applicazioni forensi l'errore di falsa accettazione sia generalmente ritenuto meno importante, non sia utile accettarne valori troppo elevati per spingere l'errore di falso rifiuto al minimo: un sistema di identificazione per applicazioni forensi fornisce come risultato di ciascuna sessione, una lista composta da un numero di candidati, tra i quali possono esistere diverse "versioni" dell'individuo cui il campione biometrico appartiene, iscritto al sistema più di una volta, i cosiddetti alias, ma anche i riferimenti ad altri individui che non corrispondono al dato biometrico da identificare, ma la cui caratteristica biometrica è giudicata "somigliante" a quella del proprietario. La dimensione della lista di candidati, quindi, è in gran parte determinata dall'entità dell'errore FAR ottenuto dal sistema. La lista va

fornita a un esperto umano, nel caso delle impronte digitali all'esperto in dattiloscopia, che è in grado di interpretare la lista fornita dal sistema e di individuare quale sono gli alias o il riferimento corretto al proprietario del dato biometrico, scartando i falsi allarmi. È evidente come l'esperto umano sia in grado di gestire solo liste non troppo numerose di candidati, per ogni elemento dei quali lo score fornito sia comunque ben distribuito (il sistema deve fornire valori di score per gli "alias" che siano significativamente più alti di quelli prodotti dagli altri candidati, in modo che l'esperto umano possa esaminare una lista ordinata di candidati ed indirizzare la sua attenzione solo verso quelli che tra loro il sistema ha classificato come più somiglianti).
Nella Figura 9.4, che mostra il grafico DET per un particolare sistema biometrico, sono indicate le aree di scelta della modalità operativa del sistema in funzione dell'applicazione.


*Figura 9.4La scelta del punto di lavoro sul grafico DET a seconda dell'applicazione.*

Per una corretta valutazione delle prestazioni effettivamente raggiungibili da un sistema biometrico calato in un'applicazione reale, devono essere considerati con molta attenzione i seguenti aspetti in grado di degradare anche pesantemente le prestazioni misurate in condizioni ideali:

- rumore nei dati biometrici acquisiti: ascrivibili alle condizioni di acquisizione, relative allo stato della caratteristica biometrica (es. dita ferite nel caso di impronte digitali), a quello del sensore (sensore sporco), ovvero a quello dell'ambiente di utilizzo (scarsa illuminazione nel caso di riconoscimento del volto);
- variazioni *intra-class*: i dati biometrici, acquisiti da un medesimo individuo durante la verifica/identificazione, possono essere anche molto diverse da quelle che hanno generato il template durante la registrazione, ciò a causa di differenze tra i sensori utilizzati durante le due fasi, o da una diversa interazione dell'utente con il sensore;
- non universalità: alcuni utenti possono avere una caratteristica biometrica scarsamente misurabile (es. creste papillari poco rilevate), ovvero esserne del tutto privi.

### 9.3.3 Valutazioni comparative e benchmarking

La misurazione affidabile dell'accuratezza di un sistema biometrico richiede competenze tecniche e un notevole dispendio di risorse per la necessità di eseguire sessioni molto ampie di test. Si supponga infatti di voler misurare FAR per un sistema di verifica di identità in corrispondenza della soglia di "default", basandosi sull'indicazione del fornitore che indica FAR = 0.0001 (1 errore su 10.000). Per la misurazione statisticamente rilevante di un tasso di errore così ridotto è necessario eseguire diverse decine di migliaia di tentativi fraudolenti

coinvolgendo diverse centinaia di soggetti. Nella maggior parte delle applicazioni pratiche l'utente finale non è quindi in grado di eseguire in proprio la misurazione delle prestazioni.
Purtroppo ad oggi non esistono ancora organismi di certificazione ufficiali per prodotti e applicazioni in ambito biometrico, e l'introduzione di metodologie specifiche (es: BEM in ambito Common Criteria), che siano accessibili in termini di costi da parte dei fornitori (solitamente medie o piccole imprese), sembra ancora lontana. Come comportarsi quindi nella pratica per verificare l'adeguatezza di un certo sistema o tecnologia rispetto a una specifica applicazione? Esistono esperienze precedenti cui fare riferimento? Di chi fidarsi?
La tabella seguente individua quattro possibili fonti di informazione utili per rispondere alle precedenti domande:

| **Brochure e specifiche tecniche dei fornitori** |
|---|
| Indicano spesso correttamente le caratteristiche meccaniche, ottiche ed elettroniche dei dispositivi hardware:<br>Es: risoluzione (dpi), area sensibile (mm2)<br>Tipo di interfaccia, crittografia, tempi di calcolo …<br>Quando includono dati circa l'accuratezza (FAR ed FRR) spesso questi sono inaffidabili. Non è raro leggere sulle brochure proclami del tipo:<br>FAR < 1 su 1.000.000<br>FRR < 1 su 1.000<br>Ammesso che sia possibile con la tecnologia odierna raggiungere tali livelli di accuratezza, misurare un errore su un milione (in modo statisticamente rilevante) richiede di eseguire decine di milioni di confronti su migliaia o decine di migliaia di soggetti. |
| Test comparativi su riviste del settore IT |
| Alcune riviste del settore IT (es. PC Magazine, PC Week, Byte, … ) propongono recensioni comparative. Questo tipo di valutazione, sebbene imparziale, ha grossi limiti. Infatti:<br>Le persone incaricate spesso non hanno una sufficiente conoscenza del settore biometrico.<br>Vengono evidenziate correttamente caratteristiche quali semplicità d'uso e di installazione delle periferiche e del software applicativo (quante volte è necessario eseguire il boot per portare a termine l'installazione…).<br>L'accuratezza di riconoscimento viene misurata eseguendo qualche decina di tentativi "live"! |
| Test eseguiti da organizzazioni accademiche/industriali del settore |
| Si tratta di test indipendenti, spesso comparativi, su sistemi biometrici o parti di essi:<br>FVC2000/FVC2002: competizione internazionale per algoritmi di verifica d'identità di impronte digitali. Organizzate con cadenza biennale da: Biolab (Università di Bologna) + Michigan State University + San-Josè University.<br>Feret ('93..'97), FRVT2000, FRVT2002: test su algoritmi di riconoscimento del volto. Organizzato da CDTDPO + DARPA + NJI e NIST<br>BWG's Biometric Product Testing (marzo 2001): vengono valutati sistemi completi tra cui: volto, impronta, voce, iride. Organizzato da UK Biometric Working Group (http://www.cesg.gov.uk/technology/biometrics/).<br>IBG's Comparative Biometric Testing: vengono periodicamente valutati sistemi completi. Organizzato da International Biometric Group (http://www.biometricgroup.com/), che è |

| |
|---|
| un'associazione profit che si propone come consulente nel campo della biometria. Non molto attendibile a causa dell'esiguo numero di test |
| **Sperimentazione sul campo** |
| Si tratta dell'unico vero metodo per verificare se una certa tecnologia è idonea per una specifica applicazione di massa.<br>Una seria sperimentazione sul campo richiede la messa in opera di numero ridotto di "postazioni" nelle stesse condizioni ambientali e con la stessa tipologia di utenti che successivamente dovranno utilizzare il sistema.<br>Può avere un costo rilevante dal punto di vista organizzativo e richiedere il ricorso a consulenti esterni qualificati.<br>Prima di procedere in tal senso, è bene identificare il successo/fallimento di tecnologie biometriche su applicazioni analoghe.<br>Dovrebbero essere identificati alcuni fornitori sulla base delle valutazione dei loro sistemi fatte da organizzazioni accademiche/industriali. Talvolta i fornitori sono reticenti a farsi "certificare". In ogni caso su richiesta devono essere disponibili a valutazioni comparative da parte del committente.<br>Non sempre precedenti esperienze o il possesso di grosse fette di mercato sono validi indicatori di miglior qualità dei prodotti. |

La tabella seguente riassume alcuni risultati ottenuti nelle recenti valutazioni comparative FVC2002 (Impronte) e FRVT2002 (Volto).

| | |
|---|---|
| Impronte **FVC2002** | Risultati presentati in Agosto 2002 alla 16th ICPR (Conferenza Internazionale di Pattern Recognition) in Canada.<br>4 database di impronte (non troppo facili, non troppo difficili) acquisite con i sensori:<br>Identix TouchViewII (Ottico)<br>Biometrika FX2000 (Ottico)<br>Precise Biometrics 100SC (Capacitivo)<br>SFinGe (Sintetico)<br>31 partecipanti (internazionali):<br>21 dall'industria<br>6 gruppi universitari<br>4 sviluppatori indipendenti<br>Migliore accuratezza (media sui 4 database):<br>EER = 0.19%<br>FRR = 0.28% per FAR = 0.1%<br>Maggiori informazioni: http://bias.csr.unibo.it/fvc2002 |
| Volto FRVT2002 | 10 partecipanti (tutti dall'industria).<br>Due tipi di test:<br>Il primo in ambiente indoor con immagini di elevata qualità, sfondo omogeneo e condizioni di luce controllate. |

| | |
|---|---|
| | Il secondo in ambiente outdoor, sfondi complessi, luce variabile<br>Nel primo test (indoor), l'accuratezza del miglior sistema:<br>FRR = 10% per FAR = 1%<br>Nel secondo test (outdoor) l'accuratezza del miglior sistema:<br>FRR = 50% per FAR = 1%<br>In modalità watch list (ricerca su lista sospetti) in ambiente indoor, l'accuratezza del miglior sistema:<br>77% di corrette intercettazioni con falsi allarmi 1% (lista di 25 persone)<br>69% di corrette intercettazioni con falsi allarmi 1% (lista di 300 persone)<br>55% di corrette intercettazioni con falsi allarmi 1% (lista di 3000 persone)<br>Maggiori informazioni: http://www.frvt.org/FRVT2002/default.htm |

## 9.4 Glossario

A

Algoritmo biometrico
Sequenza finita di istruzioni che guidano un sistema biometrico alla risoluzione di un particolare problema. Un algoritmo biometrico è tipicamente usato per (i) il calcolo del template a partire dai dati biometrici o (ii) per il confronto del campione biometrico corrente con uno o più template di riferimento.

AFIS - Automated Fingerprint Identification Systems
Sistema in uso presso numerosi organi investigativi e giudiziari internazionali per l'identificazione automatica degli individui sulla base delle impronte digitali.

ANSI (American National Standards Institute)
Ente statunitense preposto alla realizzazione di standard nazionali.

API (Application Programming Interface)
Genericamente, un insieme di routine, protocolli e strumenti per costruire applicazioni che definiscono una interfaccia tra i programmi applicativi ed il sistema operativo.

Autenticazione biometrica - Biometric Authentication
Processo attraverso il quale un individuo dimostra la propria identità a un sistema informatico. Può avvenire attraverso verifica di identità o identificazione.

B

Binning

Processo inerente la classificazione dei dati biometrici che permette di partizionare un archivio in sottoinsiemi o "pre-ordinarlo" allo scopo di incrementare la velocità di ricerca all'interno di esso. Il termine viene particolarmente usato in riferimento agli AFIS.

BIOApi (BIOmetric Application Programming Interface)
Standard orientato alla definizione di una interfaccia comune (Standardized Application Programming Interface - API) compatibile con una vasta gamma di programmi applicativi e di tecnologie biometriche in grado di promuovere un alto grado di interoperabilità nell'ambito delle soluzioni biometriche. I produttori di tecnologia biometrica che hanno deciso di adottare BIOApi sono riuniti in un Consorzio (BioAPI Consortium).

BIOApi (Consorzio) - BIOApi Consortium
Consorzio formato da più di 100 organizzazioni che condividono lo scopo di promuovere la crescita del mercato biometrico attraverso l'adozione e lo sviluppo dello standard BIOApi.

Biometria (Biometrics)
Riconoscimento automatizzato degli individui sulla base di caratteristiche biologiche e/o comportamentali.

Biometria comportamentale - Behavioural Biometrics
Biometria basata sugli aspetti comportamentali dell'utente piuttosto che biologici. Esempi di biometria comportamentale sono l'analisi dell'andatura (gait) o della dinamica di apposizione della firma.

Biometria fisica – Phyisical Biometrics
Biometria basata sugli aspetti biologici dell'utente piuttosto che comportamentali. Esempi di biometria fisica sono il riconoscimento delle impronte, iride o viso.

Biometric Consortium
Iniziativa statunitense di riferimento relativamente alla cooperazione e diffusione di informazioni nel settore dei sistemi biometrici . L'iniziativa è patrocinata dal NIST (National Institute of Standards and Technology – Gaithersburg – MD – US).

C

Campione biometrico - Biometric sample
Informazioni estratte da un sensore biometrico. L'immagine di una impronta digitale rappresenta un esempio di campione biometrico. Le informazioni estratte dal campione biometrico (dati biometrici) possono essere impiegate per la costruzione del template.

CBEFF (Common Biometric Exchange File Format)

Standard che descrive un insieme di elementi necessari per supportare le tecnologie biometriche in maniera comune con lo scopo di promuovere l'interoperabilità, le metriche di valutazione e la sicurezza.

CCD (Charge-Coupled Device)
Dispositivo a semiconduttori in grado di registrare elettronicamente le immagini.

CMOS (Complementary Metal Oxide Semiconductor)
Tecnologia costruttiva per semiconduttori che permette di costruire microchip caratterizzati da un basso consumo. usati da alcuni sistemi biometrici grazie al basso consumo. Recentemente, in alcuni sistemi biometrici, dispositivi CMOS sostituiscono i CCD all'interno di sistemi di acquisizione elettronica di immagini, grazie al costo inferiore.

Comparazione - Comparison
Il processo di confrontare un campione biometrico con uno o più campioni di riferimento, o con uno o più template.

Creste papillari
Strato dell'epidermide che riveste le papille dermiche. I depositi delle impronte digitali sono dovute essenzialmente ai prodotti delle secrezioni eccrine, che fuoriescono dai pori di tali creste.

Crossover Error Rate
Vedi EER (Equal Error Rate)

D

Dato biometrico - Biometric Data
Informazione estratta da un campione biometrico ed usata per: 1) costruire il template di riferimento nella fase di registrazione; 2) per essere comparata con il/i template di riferimento durante l'autenticazione.

Dinamica di battitura (analisi della) - Keystroke Dynamic
Tecnologia biometrica che analizza le caratteristiche temporali con cui vengono digitate particolari sequenze alla tastiera di un computer (ad esempio per la digitazione di una password).

DMI – Implicazione medica diretta - Direct Medical Implication
Grado di potenziale implicazione di aspetti medici nell'uso di sistemi biometrici. Una potenziale contaminazione causata dal contatto con un sensore biometrico o l'uso di illuminazione nello spettro dell'infrarosso possono essere annoverate fra le cause di DMI. Si possono definire anche implicazioni mediche indirette (IMI) quelle derivanti dalla (ipotetica) messa in evidenza di aspetti medici di un utente finale da parte di sistemi biometrici.

E

EER (Equal Error Rate)
Indica il tasso di errore nel punto in cui le curve di FRR (False Rejection Ratio – falso rigetto) e FAR (False Accept Ratio – falsa accettazione) si intersecano. Detto anche "Crossover Error Rate", rappresenta il tasso di errore che caratterizza un sistema la cui soglia di decisione viene fissata in modo che la proporzione di falsi rigetti sia approssimativamente uguale a quella delle false accettazioni. Essendo indipendente dalla soglia di utilizzo del sistema, viene utilizzato per la comparazione dell'accuratezza di sistemi diversi.

Enrollment
Vedi "registrazione"

Estrazione – Extraction.
Il processo di conversione di un campione biometrico acquisito in un dato biometrico allo scopo di crearne un template.

EURODAC
Progetto Europeo incentrato sull'uso di un archivio centralizzato, di impronte digitali. Le impronte di coloro che fanno richiesta di accesso ad uno degli Stati dell'Unione vengono inviate all'archivio centralizzato per controllare se il soggetto ha già tentato di accedere in un altro Stato dell'Unione. EURODAC è stato istituito in conseguenza della dichiarazione de Dublino di 1990 orientata a dare un indirizzo alle modalità di richiesta di asilo negli Stati Membri. L'unità centrale di Eurodac è basata a Lussemburgo ma controllata da Bruxelles e soggetta a controllo da un'autorità di sorveglianza unita formata da rappresentanti dagli Stati Membri.

F

Failure to acquire
Vedi "Insuccesso nell'acquisizione"

Failure to acquire rate
Vedi "tasso di insuccesso nell'acquisizione"

Failure to enrol
Vedi "Insuccesso nella registrazione"

Failure to enrol rate
Vedi "tasso di insuccesso nella registrazione"

Falsa accettazione - False acceptance
(o errore di tipo 2) Evento in cui viene accettata l'identità falsa di un impostore come quella di un regolare utente registrato, poiché il grado di somiglianza è superiore al valore di soglia scelto.

Falso rigetto - False reject
(o errore di tipo 1) Evento in cui la vera identità di un regolare utente registrato è rifiutata perché non verificata o non identificata, giacché il grado di somiglianza prodotto è inferiore al valore di soglia scelto.

FAR – Tasso di falsa accettazione - False Accept Rate
Frequenza (o probabilità di occorrenza) di errori di tipo False Accettazione.

FRR – Tasso di falso rigetto - False Reject Rate
è la frequenza (o probabilità di occorrenza) di errori di tipo False Rifiuto.

G

Grado di somiglianza - Biometric matching score
Valore della somiglianza di un immagine o template di un campione biometrico, con una o più immagini o template di riferimento

H

Hit
Successo in un processo di identificazione biometrica

I

IBIA (International Biometric Industry Association)
Associazione statunitense avente l'obiettivo di far progredire, sostenere, difendere e supportare gli interessi collettivi nel settore dell'industria biometrica a livello internazionale.

ICAO (International Civil Aviation Organization)
Agenzia specializzata delle Nazioni Unite il cui mandato è tutelare una sicura, efficiente ed ordinata crescita della aviazione civile internazionale. Alla fine di maggio 2003, l'International Civil Aviation Organization (ICAO) ha adottato uno standard per l'integrazione di informazioni di identificazioni biometriche all'interno dei passaporti e altri documenti di viaggio di tipo elettronico, (Machine Readable Travel Documents -MRTD).

Identificatore biometrico
Termine usato nel testo delle linee guida per indicare indifferentemente il campione biometrico o il template da esso estratto nelle operazioni di verifica o identificazione

Identificazione - Identification
Processo di comparazione di un campione biometrico con i template contenuti in un archivio allo scopo di identificare un individuo (ovvero di trovare uno o template il cui grado di somiglianza (matching score) è superiore alla soglia di decisione (decision thresold)). Altresì definito come confronto one-to-many.

Identificazione negativa
Una delle due funzionalità (identificazione positiva e negativa) di un sistema biometrico. In un processo di identificazione negativa l'utente prova di NON ESSERE chi DICE DI NON ESSERE. In un sistema di identificazione negativa, se il sistema non trova una corrispondenza fra il template corrente e quello di riferimento si ottiene una accettazione, in caso contrario un rigetto. Un esempio di sistema di identificazione negativa potrebbe adoperato per il controllo biometrico della titolarità all'usufrutto di servizi in cui l'utente prova, biometricamente, di non appartenere all'insieme dei soggetti che hanno già beneficiato dei servizi.

Identificazione positiva
Una delle due funzionalità (identificazione positiva e negativa) di un sistema biometrico. In un processo di identificazione negativa l'utente prova di ESSERE chi DICE DI ESSERE. In un sistema di identificazione positiva, se il sistema non trova una corrispondenza fra il template corrente e quello di riferimento si ottiene un rigetto, in caso contrario una accettazione.

IMI – Implicazione medica indiretta - Indirect Medical Implication
Implicazione di aspetti medici messi potenzialmente in evidenza da sistemi biometrici. Un esempio di IMI potrebbe essere costituito da una condizione fisica dell'utente rilevabile attraverso un processo biometrico

International Standards Organization (ISO)
La più importante organizzazione internazionale in tema di standard . Le attività del settore biometrico sono curate da un apposito sottocomitato (SC 37 "Biometrics" dell'ISO/IEC JTC1)

Insuccesso nell'acquisizione - failure to acquire
Fallimento del sistema biometrico nell'acquisire un campione biometrico.

Insuccesso nella registrazione - failure to enrol
Fallimento del sistema biometrico nel portare a termine l'operazione di registrazione. Le cause possono essere l'acquisizione di un campione di qualità non sufficiente o un errore nella creazione del template.

M

Match/Matching
La comparazione di un campione biometrico con uno o più template precedentemente immagazzinati che si conclude con l'attribuzione di un grado di somiglianza. L'accettazione o il rigetto saranno quindi basati su un superamento o meno di una determinata soglia da parte del grado di somiglianza.

Minuzia (plurale "Minuzie") - Minutia – plur. minutiae

Caratteristiche delle creste papillari adoperate per caratterizzare una impronta digitale. Una minuzia corrisponde essenzialmente al punto di terminazione o biforcazione di una cresta papillare.

NIST (National Institute of Standard and Technology)
Fondato nel 1901 il NIST è una agenzia federale statunitense che opera all'interno dell' U.S. Commerce Department's Technology Administration con la missione di sviluppare e promuovere la metrologia, gli standard e la tecnologia. Nel Luglio del 2000, l'ANSI ha approvato lo standard americano ANSI/NIST-ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT). L' ANSI/NIST-ITL 1-2000 specifica, tra l'altro, un formato comune da usare per l'interscambio di impronte digitali tra sistemi realizzati da costruttori differenti.

O

One-to-Many (uno-a-molti)
Vedi "identificazione"

One-to-One (uno-a-uno)
Vedi "verifica di identità"

P

Pin (Personal Identification Number)
Un codice numerico scelto od attribuito ad un utente per potere accedere a vari servizi

Postazione di enrolment - enrollment station
Postazione equipaggiata con sistemi informatici che permette l'acquisizione delle caratteristiche biometriche (ad esempio impronte, voce oppure iride) e (generalmente)delle informazioni personali degli utenti di un sistema biometrico.

PKI (Public Key Infrastructure)
Insieme di tecnologie, politiche, processi e persone utilizzate per gestire (generare, distribuire, archiviare, utilizzare,revocare) chiavi di crittografia e certificati digitali in sistemi di crittografia a chiave pubblica.

PUK
Acronimo di "Personal Unblocking Key". Si riferisce ad un numero utile allo sblocco di un dispositivo (ad esempio un token) nel caso si sia digitato per più volte in modo erroneo il PIN. Non può essere variato e, generalmente, una lunga serie di errori (ad esempio, 10) nella digitazione del PUK rendono completamente inutilizzabile il token.

R

Registrazione - enrollment
La fase di un processo biometrico che, in maniera generalizzata, consiste (i) nell'acquisizione del campione biometrico dall'utente finale, (ii) la eventuale elaborazione del campione (iii) l'eventuale estrazione dei dati biometrici per la creazione del template di riferimento e (iv) la memorizzazione su un apposito supporto.

Riconoscimento biometrico
Termine genericoche può indicare sia una verifica di identità sia un'identificazione.

S

Sistema biometrico
Sistema automatizzato capace, in termini generali, di (i) acquisire un campione biometrico da un utente, (ii) estrarre i dati biometrici dal campione, (iii) comparare i dati biometrici con uno o più template, (iv) stabilire il grado di coincidenza e (v) indicare se il processo di riconoscimento si è concluso con successo o meno.

Sensore biometrico
Dispositivo in grado di acquisire il campione biometrico.

Soglia di decisione - decision thresold
Valore (in genere configurabile) il cui superamento o meno da parte del grado di similarità implica l'accettazione o il rigetto di un dato biometrico. La soglia può essere regolata in base alle caratteristiche dell'applicazione influenzando in tal modo il trade-off tra FARe FRR.

SDK (Software Developer's Kit)
Sistema di sviluppo software che permette ad un programmatore di sviluppare applicazioni per una specifica piattaforma integrando funzionalità di riconoscimento biometrico. Uno SDK include tipicamente una o più API (Application Programming Interface), strumenti di programmazione e documentazione tecnica.

T

Tasso di insuccesso nell'acquisizione (failure to Acquire Rate)
Frequenza di fallimenti nell'acquisizione di campioni biometrici.

Tasso di fallimento nell'enrollment (Failure to Enrol Rate)
Frequenza di fallimenti in operazioni di enrollment.

Template

Insieme di valori numerici estratti da un campione biometrico, che ne descrivono caratteristiche utili al fine del riconoscimento. In genere non è possibile ricostruire il compione biometrico originale a partire dal template.

Template di riferimento
Template ottenuti al momento della registrazione dell'utente nel sistema biometrico

Template (grandezza del) – template size
La quantità di memoria necessaria per la memorizzazione del template

Tentativo (Attempt)
La sottomissione di un campione biometrico ad un sistema biometrico a scopo di identificazione o verifica di identità. Un sistema biometrico può permettere più tentativi di identificazione o verifica.

Tentativo "impostore" (Impostor attempt)
In un sistema di identificazione positiva, il tentativo compiuto in cattiva fede da un soggetto "sconosciuto al sistema" al fine di ottenere una corrispondenza indebita della propria caratteristica biometrica con un template.

Tentativo Genuino (Genuine Attempt):
In un sistema di identificazione positiva, il tentativo compiuto in buona fede da un soggetto "conosciuto dal sistema" al fine di ottenere una corrispondenza debita della propria caratteristica fisica con un template.

Tempo di Enrollment (Enrolment Time)
Il tempo necessario per la registrazione nel sistema di un nuovo utente, includendo il tempo necessario alla generazione del template.

Tempo di risposta di un sistema biometrico (Response Time)
Il tempo richiesto da un sistema biometrico per fornire un responso in termini di identificazione o verifica.

Token
Dispositivo elettronico attraverso il quale si può ottenere l'abilitazione ad accedere a un sistema (generalmente ad una risorsa informatica). Smard Card e "chiavi" USB sono i token più frequentemente utilizzati in ambito informatico.

U

Utente - User
Nella tassonomia biometrica, l'acquirente o il gestore di un sistema biometrico. A differenza dell'utente finale (end user), è il responsabile della gestione e della implementazione del sistema biometrico piuttosto che colui che interagisce direttamente con esso.

Utente finale - End User
Nella tassonomia biometrica, colui che interagisce (spesso fisicamente) con sistema biometrico e fornisce ad esso la propria caratteristica biometrica, allo scopo, ad esempio di registrarsi nel sistema o provare la propria identità.

V

Verifica di identità - Verification
Processo di comparazione del template estratto da un campione biometrico (template corrente) con un unico template (template di riferimento) memorizzato in un supporto in possesso dell'utente o in un archivio e, in tal caso, indicizzato da altri dati (ad esempio un pin).Se il grado di somiglianza (matching score) tra il template corrente e quello di riferimento è superiore alla soglia di decisione (decision thresold) viene ottenuta la verifica dell'identità. Altresì definito come confronto one-to-one.