La Biometria

Ci sono paesi che spingono per l'introduzione della biometria nei documenti di identificazione, ma ci sono alcuni miti da sf atare per evitare che la maggiore sicurezza sia solo una pericolosa e costosa illusione.


Chip identifica impronte digitali

La preoccupazione sta' nel fatto che la biometria ci viene venduta per quello che non è, ossia una bacchetta magica contro il terrorismo e un sostituto perfetto per le password. Non lo è, e credere che lo sia è un'illusione costosissima.

Per capire perché, occorre un passo indietro. E' facile pensare che la biometria sia una tecnologia modernissima, ma in un certo senso ha origini molto antiche. In soldoni, consiste nell'identificare una persona in base a una sua caratteristica fisica. In questo senso, usiamo la biometria quotidianamente da millenni per riconoscere le persone che ci stanno intorno: ci basta guardarle in viso o sentirne la voce per sapere chi sono. La foto sul vostro passaporto è un identificatore biometrico. Anche il mio gatto, a modo suo, usa la biometria: riconosce le tracce degli altri gatti in base al loro odore.

La differenza della biometria moderna rispetto a queste tecniche antiche è che il processo viene meccanizzato e digitalizzato. Si cerca insomma di usare una macchina al posto dell'*hardware* biologico (l'agente che confronta la foto sul documento con la persona che lo esibisce, il gatto che annusa un altro gatto). L'introduzione della tecnologia permette di usare nuovi elementi di identificazione, come le impronte digitali, l'immagine della retina o dell'iride, il DNA, eccetera.

Quasi tutti i documenti d'identità attuali contengono già una forma di biometria "analogica", verificabile manualmente: la foto sul passaporto o sulla patente, o la firma sul retro della carta di credito, per esempio. Ma molti governi dicono che non basta, e stanno spingendo per l'introduzione di dati biometrici digitali nei documenti d'identificazione. Il *mantra* ripetuto ossessivamente per zittire gli scettici della biometria è che la biometria aiuterà contro il terrorismo. Chi è contro la biometria, è con i

terroristi. E qui cominciano i problemi!

Illusione tecnologica

I governanti sembrano innamorati del nuovo giocattolo biometrico, e come tutti gli innamorati sono ciechi rispetto ai suoi difetti e non ne capiscono il funzionamento. Pensano che la biometria risolverà tutti i loro problemi e immaginano un futuro in cui tutti saremo sicuri e felici perché potremo dimostrare facilmente chi siamo, ci basterà guardare dentro lo scanner dell'iride per superare -- letteralmente in un batter d'occhio -- gli estenuanti controlli aeroportuali, e nessun terrorista o immigrato clandestino potrà entrare nel sistema. Purtroppo non è così.

La biometria è un ottimo strumento, ma non consente nessuna di queste cose. Includere un chip biometrico in un passaporto, per esempio, rende un po' più difficile il lavoro dei falsari e aiuta effettivamente a verificare che la persona che esibisce il documento corrisponde alla persona indicate nel documento stesso, ma *non aiuta a verificare chi è davvero quella persona*, che è un problema assolutamente diverso. Di conseguenza, eludere il sistema è molto facile, anche per un terrorista.

La ragione è semplice. Un documento (biometrico o meno) nasce da altri documenti: quando chiedete il passaporto, dovete esibire certificati di nascita, residenza, cittadinanza, eccetera. Nessuno di questi documenti è biometrico: è semplicemente un pezzo di carta, derivante a sua volta da altri pezzi di carta. Finché quei pezzi di carta provengono dall'interno della burocrazia locale, possono essere considerati ragionevolmente affidabili. Ma se provengono dall'estero? In molti paesi, chi genera quei pezzi di carta è corruttibile, oppure l'intero sistema dell'anagrafe è un colabrodo o non esiste del tutto. Quindi il passaporto biometrico, apparentemente inattaccabile, si poggia in realtà su documenti privi di garanzie, generati al di fuori del sistema, e pertanto non aumenta in alcun modo la sicurezza dell'identità. Ne aumenta soltanto i costi.

Per esempio, supponiamo che **Osama bin Laden** voglia procurarsi una (per ora ipotetica) carta d'identità biometrica italiana. Si presenterà alle autorità italiane esibendo documenti d'identità falsi, in cui risulta chiamarsi Marco Brambilla, cittadino yemenita (senza offesa per lo Yemen o per chi si chiama Brambilla; è soltanto un esempio). Come potranno essere verificati quei documenti, ovviamente privi di dati biometrici? All'anagrafe yemenita? Andando nello Yemen a chiedere in giro se c'è qualcuno che riconosce una foto di bin Laden e dice che si chiama Marco Brambilla? Certo che no: a un certo punto il controllo dovrà fermarsi, e l'autorità nazionale dovrà fidarsi di un'autorità estera di dubbia affidabilità e dovrà prendere per buoni documenti non verificati e non verificabili.

Così il funzionario prenderà le impronte digitali e l'immagine dell'iride di bin Laden e le memorizzerà nel chip della carta d'identità, che consegnerà al ricercatissimo saudita salutandolo con un bell'*"Ecco a lei, signor Brambilla"*, magari con un'ombra di perplessità per quella somiglianza straordinaria con qualcuno visto in televisione. Bin Laden avrà il suo bel superdocumento biometrico *autentico*, che però dirà che lui si chiama Marco Brambilla. I dati biometrici sul documento e quelli della persona coincideranno perfettamente, ma l'identità sarà falsa. Supererà in un lampo i controlli alle frontiere, perché alla vista del documento biometrico nessuno si porrà dubbi sulla sua identità. Ecco come si entra nel sistema.

Non sono certo il primo a notare che i terroristi dell'11 settembre 2001 e quelli di Madrid avevano

documenti autentici, regolarmente rilasciati sulla base di documenti provenienti da paesi terzi. Avere la biometria non avrebbe fatto alcuna differenza.

Catene infrante

La prima lezione da tenere presente, insomma, è che la biometria può garantire l'identità delle persone soltanto se la catena biometrica non viene mai interrotta. Se a un certo punto, andando a ritroso nella verifica delle origini dell'identità di una persona non ci sono più dati biometrici, se occorre appoggiarsi a dati provenienti dall'esterno del sistema, quell'identità non è verificata più di quanto lo fosse nell'era pre-biometrica e la biometria diventa semplicemente un inutile travaso di soldi dalle casse dello Stato a quelle dei produttori di tecnologie biometriche.

Sarebbe teoricamente possibile garantire questa catena raccogliendo dati biometrici sin dalla nascita (per esempio col DNA o le impronte digitali): cosa forse fattibile nei paesi tecnologicamente sviluppati, ma impensabile nel resto del mondo. L'implementazione richiederebbe comunque decine di anni, perché l'identità di tutti i cittadini nazionali nati prima dell'avvio della raccolta biometrica e di tutti coloro che provengono da paesi non biometrizzati continuerebbe ad essere garantita soltanto con metodi "tradizionali". Altro che soluzione rapida al terrorismo.

E' per questo che l'attuale foga biometrica è pericolosa: non tanto per le presunte invasioni della privacy in stile orwelliano, peraltro non trascurabili, ma semplicemente perché i governanti trattano la biometria come una garanzia assoluta. Se le autorità prendono l'abitudine di considerare infallibile un passaporto biometrico, allenteranno i controlli su chi lo possiede. Abbasseranno la guardia, pensando di essere protette da un sistema impenetrabile, e questo potrebbe essere fatale.

L'unico vantaggio di un documento d'identità digitale è che la presenza del chip lo rende più difficile da falsificare. Ma attenzione: è la presenza del chip, non il suo contenuto di dati biometrici, a renderlo meno falsificabile. I dati biometrici, per definizione, non sono segreti: chiunque li può raccogliere (basta una foto o un'impronta su un bicchiere), e anzi l'intero sistema poggia sulla facilità di acquisizione automatica di questi dati al momento della verifica. In realtà, se il chip contenesse una firma digitale generata dall'amministrazione pubblica con PGP o programmi analoghi, invece di dati biometrici, il beneficio in termini di contrasto alla falsificazione e snellimento della verifica sarebbe più alto.

Problemi "digitali"

La seconda illusione pericolosa che circonda la biometria è il suo uso come sostituto delle password, dei PIN e di tutti gli altri codici segreti che usiamo quotidianamente. Come dicevo, i dati biometrici non sono segreti: sono letteralmente in bella vista. Di conseguenza, è semplicemente assurdo usarli come sostituti di un codice che funziona proprio perché è segreto.

Toglietevi quindi dalla testa tutti i cliché hollywoodiani su case e auto con serrature comandate a voce o con la pressione del pollice, e lasciate perdere le banche che vi chiedono di verificare chi siete

ponendo un dito su un sensore d'impronte digitali e i PC che si attivano soltanto con l'impronta digitale del padrone. Sono trovate di marketing, illusioni di sicurezza che fruttano miliardi a chi le propina ad aziende e governi, e sono pericolosissime.

Per esempio, i sensori di impronte digitali si possono burlare con estrema facilità: non occorre neppure ricorrere all'altro truculento cliché hollywoodiano del dito mozzato. Il professor Tsutomu Matsumoto, dell'Università di Yokohama, ha realizzato una **dimostrazione www.itu.int/itudoc/itu-t/workshop/security/present/s5p4_pdf.zip** spettacolare, creando "dita false" con Photoshop e gelatina, ottenendo un tasso di successo dell'80% contro varie marche di sensori. Con questa tecnica è facilissimo rubare un'impronta digitale a un'altra persona, senza ricorrere a sgradevoli amputazioni estemporanee, e poi usarla come "chiave" per entrare armati in una banca oppure aprire la porta blindata di una casa o una cassaforte o un laptop. E una volta commesso il crimine, si possono far scomparire le prove inghiottendo il finto polpastrello di gelatina.

Rubare dati biometrici è insomma di una semplicità impressionante, perché li lasciamo in giro spontaneamente. Quindi non vanno assolutamente usati come sistema di sicurezza al posto di PIN e password: sarebbe come scrivere i nostri codici segreti su tutto ciò che tocchiamo e tatuarceli in fronte. E c'è un altro problema fondamentale di questo uso scorretto della biometria. Una password compromessa si può cambiare: un dato biometrico no.

Col sistema attuale, se divulghiamo il nostro PIN per furto o distrazione, chiediamo semplicemente alla banca di darcene un altro. Ma se il "PIN" è costituito dalla nostra impronta digitale, o dalla nostra voce, non possiamo farcene dare un'altra. Non possiamo farci dare due pollici nuovi. La nostra sicurezza è compromessa per sempre; la nostra "password" biometrica è in mano a chissà chi, e non è neppure revocabile.

Come se non bastasse, c'è un ulteriore problema nell'uso dei dati biometrici come chiavi d'accesso: uno dei comandamenti fondamentali della sicurezza informatica è che non si usa mai la stessa password per più di un tipo di accesso, in modo da contenere il danno in caso di intercettazione della password. Il PIN del Bancomat deve essere diverso da quello del telefonino e da quello dell'antifurto di casa; altrimenti, se uno di questi codici cade in mano a un aggressore, può non solo vuotarci il conto in banca, ma anche razziarci la casa (e telefonare a scrocco). Con la biometria saremmo costretti ad avere una sola "password" per tutti i servizi che usiamo. Se viene compromessa quella singola password, tutto ciò che possediamo è a portata di mano dell'aggressore.

Ben venga la tecnologia, dunque, ma solo se funziona e se la si usa nei limiti delle sue vere capacità. Ora come ora, mi sembra che si stia facendo una pericolosa fuga in avanti senza capire i veri termini del problema e senza pensare alle conseguenze e soprattutto al rapporto costi/benefici. Stando a **Privacy International www.privacyinternational.org/issues/idcard/uk/, l'**introduzione della carta d'identità biometrica in Inghilterra, paese paragonabile per popolazione all'Italia, costerà circa 9 miliardi di euro, ossia quanto gli stipendi di diecimila poliziotti in più per dieci anni. Secondo voi, quale delle due misure sarebbe più efficace contro il terrorismo....

Bibliografia:

www.itu.int/

www.privacyinternational.org