

Non solo privacy, i nodi dietro la facciata della biometria

8 Ottobre 2019



Dalla suggestiva scansione dell'iride vista in tanti film alla più realistica impronta digitale diventata ormai la regola su smartphone e notebook, per arrivare al riconoscimento facciale, **la biometria è ormai parte integrante nella quotidianità di molto utenti**. Praticità e affidabilità, almeno apparente, ne favoriscono la diffusione, distogliendo però l'attenzione da altri aspetti, la privacy su tutti. Se trascurata, alla fine **con il rischio di rivelarsi più dannosa di una password banale** scritta su un pezzo di carta.

Da una panoramica sull'argomento affrontato da diversi aspetti emerge però **una situazione al momento sotto controllo**, a condizione di affrontarla con la dovuta preparazione e i necessari strumenti, legislativi e tecnici.

La ricerca inoltre, guarda sempre più all'anatomia unica della persona per scovare nuovi sistemi di identificazione, tra i più recenti il battito cardiaco, chiamando così in causa anche il delicato contesto sanitario e **spingendo di conseguenza ancora oltre i necessari requisiti di tutela**.



Avvocato Giulio Graziani, socio dello studio Elexia

Ancorati al GDPR

«Attualmente, **la biometria rappresenta il fondamento della cosiddetta m-health** – spiega l'avvocato Giulio Graziani, socio dello [Studio Elexia](#) – avvocati & commercialisti ed esperto di diritto delle nuove tecnologie -. Vale a dire l'insieme delle tecnologie mobili wireless utilizzate in ambito medico-sanitario o in settori correlati alla salute, oggi sempre più avanzate e semplici da utilizzare non solo dallo specialista, ma da qualsiasi utente in maniera del tutto autonoma».

A differenza di una sequenza di caratteri, la biometria chiama in causa infatti fattori estremamente personali. «È evidente la necessità di individuare la normativa applicabile ai relativi dati – precisa Graziani -. Se da un lato i sistemi di riconoscimento biometrico contribuiscono a incrementare il livello di sicurezza nell'utilizzo dei dispositivi elettronici, dall'altro **potrebbero presentarsi gravi rischi per il titolare di tali dati**, a fronte di un indebito utilizzo degli stessi».

Il riferimento è alle recenti disposizioni in materia di protezione dei dati personali introdotte dal Regolamento dell'UE n. 679/2016 (molto più noto come GDPR) dove i dati biometrici vengono definiti "dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici".

In particolare, l'art. 9 paragrafo 1 del GDPR pone in linea generale **il divieto di trattare i "dati biometrici intesi a identificare in modo univoco una persona"**, a meno che non ricorrano una o più condizioni di liceità espressamente previste al successivo paragrafo 2.

«Tra queste, **la più importante è sicuramente la volontà del titolare** –riprende Graziani -. Il trattamento dei dati biometrici è infatti consentito qualora l'interessato presti il proprio consenso esplicito per uno o più specifici utilizzi. In tal caso devono, sempre e comunque, essere rispettati i diritti dell'interessato previsti dal GDPR, quali rettifica, cancellazione, oblio, portabilità nonché opposizione al trattamento.

Non mancano tuttavia altre eccezioni, pensate **per consentire l'utilizzo dei dati biometrici solo se necessario in ambito lavorativo o nell'ambito della sicurezza sociale e collettiva**, qualora sia necessario per la protezione di un interesse vitale dell'interessato o di altra persona, in un procedimento giudiziario, in presenza di particolari motivi di interesse pubblico o motivi di sicurezza sanitaria, controllo e prevenzione di malattie trasmissibili e per la tutela di gravi minacce per la salute delle persone fisiche.

Tutto questo si trasforma in **una serie di incombenze in più per i responsabili IT**, sia nel momento di progettare e distribuire dispositivi e app sia nella gestione di sistemi aziendali. «Il produttore dei dispositivi e delle app devono prestare particolare attenzione a principi come privacy by design e privacy by default, cercando di (pre)selezionare la scelta meno invasiva per la privacy dell'utente e mettendo in atto tutte le misure tecniche e organizzative adeguate alla peculiarità di tale tipologia di dati».

Dal punto di vista dell'esperto legale, **una prima soluzione potrebbe essere l'utilizzo di strumenti tecnici di rilevamento dei dati biometrici tali da richiedere espressamente la cooperazione consapevole dell'interessato** ("biometrici interattivi"), ipotizzando anche una richiesta di consenso "dinamico" da rinnovare in base alle future finalità di utilizzo del dispositivo e indirizzata di pari passo con il successivo sviluppo tecnologico non prevedibile all'origine.



Pierluigi Torriani, Check Point

Biometria, l'importante è conoscere limiti e regole

Dal punto di vista dell'IT invece, l'aspetto principale è **governare una situazione in rapido sviluppo**. «Negli ultimi anni, la biometria ha registrato crescita importanti – conferma Pierluigi Torriani, security engineering manager Italy di Check Point -. Parliamo di tassi oltre il 50% all'anno negli ultimi tre. Possiamo tutto sommato considerarla una soluzione sicura, favorita dalla semplicità d'utilizzo».

La combinazione di mobility e l'avvento dei sistemi di riconoscimento facciale offrono inoltre **un terreno particolarmente fertile, per superare le situazioni dove gestire sequenze di caratteri risulta poco pratico e più rischioso dal punto di vista della riservatezza**. «Quando si tratta di servizi basati sul Web, attualmente si tende a utilizzare ancora le password tradizionali – precisa David Jacoby, security evangelist, european research center di

Kaspersky – Credo però che con l'integrazione di password manager e Single Sign-On/OAuth ci stiamo muovendo verso un uso maggiore della biometria».

In particolare, **il riconoscimento facciale viene visto con maggior favore nelle situazioni più delicate**, a partire dalle transazioni bancarie online o l'accesso a dati aziendali sensibili. Altro aspetto importante, la biometria presenta tutte le carte in regola per risolvere definitivamente l'annosa questione legata al single sign on, mandando definitivamente in pensione la necessità, almeno teoria, di pensare a una password per ogni accesso, ricordarla e all'occorrenza cambiarla.



David Jacoby, Kaspersky

Questioni pronte a trasformarsi in problemi sul fronte della privacy e relativa regolamentazione. «Le password oggi rappresentano un grosso problema – ammette Jacoby -. Leggiamo della violazione di database quasi ogni giorno. È difficile far comprendere alle persone cosa significhi che le sue credenziali online vengano attivamente vendute e riutilizzate dai criminali informatici».

Certamente, l'uso della biometria risolve molti di questi problemi. D'altra parte, **apre anche la strada ad altre implicazioni, come la falsificazione dell'impronta biometrica**. Non solo delle dita, ma di tutto ciò usato per identificare un utente. «La biometria presenta un margine di errore più grande, legato alla creazione dei template per l'identificazione – avverte Torriani. Per intenderci, è come se a fronte di una password 55555 venisse riconosciuta come valida anche 55554».

A oggi, si tratta di un margine di errore fisiologico, indispensabile per superare anche i problemi di lettura dei dati in diverse circostanze ambientali. O, nel caso del riconoscimento facciale, per non incorrere in falsi positivi. **«Nei casi dei sistemi consumer, l'affidabilità può addirittura scendere al 50% - ribadisce Torriani -**. Per spingersi oltre, servono anche strumenti di livello superiore, per esempio quelli usati negli aeroporti».

Lo scenario risultante sembra scritto apposta per rendere ancora più complicata la vita ai responsabili IT. Al riguardo però, gli esperti si mostrano molto tranquilli. **«I problemi di privacy sono quelli legati all'immagine biometrica stessa** – riflette Torriani -. Prima di tutto, come viene costruita l'immagine e in questo caso si tratta di un dato sensibile, al pari degli altri. In caso di danni o intrusioni, restano validi i criteri già noti».

In sostanza, con standard normativi considerati già molto esigenti, la privacy resta comunque tutelata, al punto da non dover neppure prevedere accorgimenti particolari. «Quando si tratta di biometria, **la memorizzazione di informazioni personali non comporta reali problemi legati alla privacy** – assicura Jacoby -. Si tratti di una password, di impronta digitale o di riconoscimento facciale, **non vengono memorizzate realmente queste informazioni**. Viene invece memorizzato l'algoritmo matematico dell'impronta digitale o del volto. Proprio per questo, non vedo alcun reale problema di privacy, a meno di non trovarsi in presenza di un malware che sfrutti la fotocamera o il sensore, ma questo comporterebbe altri problemi che vanno oltre».

In circostanze analoghe infatti, **una solida cifratura resta la soluzione al momento più affidabile e la più accessibile**. Riflettendo però più a fondo su alcuni aspetti, alla fine emergono particolari non trascurabili.

«Perdita accidentale o furti restano comunque sempre aspetti da considerare – rilancia Torriani -. Mentre cambiare una password è relativamente facile, **dovesse essere trafugato un database di dati biometrici l'unica soluzione sarebbe eliminare la matrice**. Per questo, non si può prescindere da una cifratura ai massimi livelli».

Nel malaugurato caso, al momento l'unica via è agire in linea con le indicazioni del GDPR. «Certamente, la diffusione dei dati biometrici riguarda la privacy – conclude Torriani -. **In caso di incidente, bisogna mettere in atto procedure di analisi forense a posteriori**. Capire la ragione dell'uscita di dati e quali siano effettivamente i dati personali trafugati».