lavoce.info

Il corpo come password. Il futuro è biometrico

17.07.15

Rosamaria Alibrandi

Le password sembrano avere i giorni contati: il corpo è la chiave che la tecnologia usa per sostituire i codici alfanumerici. Entro il 2020 l'industria biometrica varrà 33 miliardi di dollari. Verso un metodo di autenticazione universale, sicuro e semplice da utilizzare. I problemi di privacy.

Orecchi, occhi e succhi gastrici per identificarci

Siamo alla rivoluzione biometrica. Il corpo è la chiave multiforme che la tecnologia usa **per sostituire** i codici alfanumerici con l'avveniristico uso del battito del cuore, o d'un tatuaggio, per autenticarsi su computer, smartphone e siti online. Riconoscimento facciale, lettura delle impronte e del tracciato cardiaco, scansione vocale, identificazione dell'occhio e persino dell'orecchio, sostituiranno le password. Niente più codici, parole, combinazioni complesse da ricordare: il futuro è inscritto nell'unicità corporea dell'utente. Il sensore dell'impronta digitale è già usato per sbloccare gli smartphone di ultima generazione, ma si profilano all'orizzonte sistemi ancor più raffinati. 'Windows Hello' sarà integrato in tablet e smartphone, permettendo di accendere il computer, eseguire l'accesso o spengerlo usando il viso, l'iride o l'impronta digitale attraverso una videocamera. Poiché l'orecchio è risultato la parte più adatta a essere riconosciuta per l'identificazione su dispositivi

mobili, Yahoo sta elaborando 'Bodyprint', una tecnologia che trasforma i display degli smartphone in scanner biometrici per autenticare l'utente mediante le caratteristiche anatomiche: se lo smartphone non identifica l'orecchio accostato, si blocca. Apple progetta 'Low Threshold Face Recognition', un sistema di riconoscimento facciale che farà accedere all'iPhone inquadrando il volto con la fotocamera come per fare un selfie, mentre Google userà la biometria vocale. Come alternativa alle password, Motorola, già dal giugno 2013, sta sperimentando tatuaggi e pillole hitech. I tatuaggi elettronici, sviluppati dall'azienda statunitense MC10, sono circuiti flessibili applicabili alla pelle come cerotti adesivi e impermeabilizzati con uno spray, che funzionano per settimane. Le sorprendenti pillole-password, prodotte dalla Proteus, consistono in capsule da inghiottire, contenenti minuscoli chip. Raggiunto lo stomaco, ricavano dai succhi gastrici l'energia per funzionare e trasmettono una password identificativa sotto forma di deboli impulsi elettrici percepibili attraverso la pelle. Pur essendo già stato certificato che non nuocciano alla salute, non sono ancora state commercializzate. Il colosso giapponese dell'elettronica Fujitsu sperimenta con successo il riconoscimento oculare per l'autenticazione sul suo nuovo smartphone, Arrows NX F-04G, che usa una telecamera a infrarossi frontale in combinazione con una luce Led che scannerizza l'iride, garantendo la certezza del riconoscimento con ampio margine di sicurezza. Un passo avanti enorme, in quanto il sistema potrebbe rivelarsi, nel futuro prossimo, la pratica maggiormente diffusa per la sua affidabilità. Difatti, se la biometrica è diventato un tema sensibile dell'industria tecnologica, soprattutto per la crescita dei sistemi di pagamento online, il problema maggiore resta legato alla sicurezza. Informazioni personali e finanziarie, come quelli relative alle carte di credito conservate negli account, sono vulnerabili e lo sono anche i sistemi biometrici usati finora. La ricerca, quindi, corre per superare se stessa al fine di affiancare alla praticità il conseguimento della inviolabilità dei dati.

Problemi di sicurezza e di privacy

Entro il 2020 l'industria biometrica varrà 33 miliardi di dollari. Nessuna azienda tralascerà di integrare i propri dispositivi con tale tecnologia. Controindicazioni? Se una normale password viene compromessa, è ovvio che possa essere facilmente cambiata. Di contro, con riguardo alla conservazione dei dati biometrici, i rischi per l'utente sono potenzialmente più gravi rispetto allo smarrimento, o al furto, di una password alfanumerica. Guardare in una telecamera, o sfiorare un sensore con la punta dell'indice, per autorizzare un pagamento costituiscono comportamenti innovativi che tuttavia rilanciano l'antica sfida della sicurezza: così come le riserve di dati sensibili accrescono l'interesse degli hacker, la violabilità dei sistemi biometrici fa sì che l'autenticazione sicura sia la vera scommessa del futuro, ma senza al momento risolverne l'aspetto negativo. Se la password viene dimenticata, rubata o estorta, la si può cambiare e presto, possibilità esclusa nel caso dei dati biometrici. La biometrica non sarà (forse mai) di per sé, garanzia assoluta di sicurezza. Si può inoltre presentare, anche se appare un evento raro, più che improbabile, il problema della coercizione, che, più che una soluzione tecnologica, richiederebbe un sistema di protezione 'fisica', specie qualora si consideri che le tecnologie biometriche per l'identificazione della pupilla o dei vasi sanguigni che la circondano sono utilizzate per evitare intrusioni in centri di ricerche, basi militari e aree sensibili di grandi industrie. Sul piano giuridico, i tratti somatici che distinguono un soggetto da tutti gli altri esseri umani costituiscono il patrimonio di dati biometrici impiegati per stabilire l'identità di un individuo (identificazione) o che sia chi dichiara di essere (autenticazione). Memorizzandoli, si crea un connotato biometrico

di riferimento, che viene poi confrontato con la caratteristica fisica esibita al fine di verificarne la corrispondenza. Quando i due elementi coincidono si ha la conferma che una persona è, ad esempio, titolare di un conto bancario o è autorizzata a entrare in un certo edificio. La tecnica si fonda sulla registrazione delle caratteristiche biometriche, acquisite tramite uno scanner e trasformate in un codice binario, cifrato e depositato in un'apposita banca dati, che spesso non vengono più cancellate. L'incrocio di tali dati consente di risalire a informazioni di ogni genere, quali ad esempio la razza o lo stato di salute del soggetto cui si riferiscono, permette di ricostruirne i movimenti e si presta a controlli non autorizzati dalla legge. Occorre verificare se e in che misura l'uso di sistemi biometrici in ambito privato sia ammissibile sotto il profilo della protezione della privacy e, caso per caso, valutare se l'obiettivo perseguito non possa essere raggiunto con misure meno lesive dei diritti della personalità. Infine, i dati biometrici non andrebbero memorizzati in una banca dati centrale, ma su un supporto di sicurezza (smart card o chiave usb), conservato dal titolare dei dati. Giganti come **Google**, **Samsung** e **Microsoft** cooperano per realizzare un metodo di autenticazione universale, sicuro e semplice da utilizzare, e hanno dato vita alla ***Fast Identity Online Alliance***, un consorzio industriale che il 9 dicembre 2014 ha pubblicato le specifiche tecniche dei protocolli necessari per uniformare a livello internazionale i metodi di autenticazione; su base nazionale, la garanzia della privacy resta demandata agli organi di controllo preposti in ciascun paese.

:A Commenta

Stampa

In questo articolo si parla di: autenticazione, biometrica, dati biometrici, industria biometrica, password, privacy

BIO DELL'AUTORE

ROSAMARIA ALIBRANDI

Rosamaria Alibrandi, PH.D. in Storia delle Istituzioni Giuridiche dell'Età Medievale e Moderna presso l'Università di Messina, ha conseguito un ulteriore dottorato internazionale in Storia e Comparazione degli Ordinamenti Politici e Giuridici Europei. Si occupa di storia del diritto e delle istituzioni e di legislazione sanitaria. E' autrice di monografie e di saggi apparsi su riviste nazionali e internazionali; collabora con vari periodici. Tra le sue pubblicazioni, In salute e in malattia. Le leggi sanitarie borboniche fra Settecento e Ottocento (Franco Angeli); Germs of Revolutions, Germes de Liberté (La Città del Sole).

Altri articoli di Rosamaria Alibrandi