la Redazione

Controllo accessi biometrico: prescrizioni da rispettare

PARTE 5

Controllare gli accessi attraverso le tecnologie biometriche si può, ma solo se si rispettano determinate prescrizioni. A dettare legge, oltre al GDPR, è uno specifico provvedimento emesso sei anni or sono dal Garante della privacy. Impronte digitali e topografia della mano sono le caratteristiche fisiche più sfruttate e per questo prese di mira dal legislatore nazionale. Che però ci dice tutto (o quasi) su cosa fare per essere in regola con la legge ed evitare incombenze burocratiche.

L'impiego della biometria nel riconoscimento automatico delle persone è da sempre nel mirino del Garante della privacy. Dei provvedimenti emessi e delle sanzioni comminate in questi anni per un uso non corretto delle tecnologie biometriche si è perso ormai il conto. Per quanto riguarda il controllo elettronico degli accessi fisici, la biometria si può usare ma solo in ambienti riservati, sensibili o ad alto rischio, e rispettando determinate prescrizioni. L'accesso, in questo caso, non è da confondere con l'ingresso all'azienda o a un reparto in corrispondenza del quale viene rilevato l'orario di entrata (e di uscita) del dipendente per il computo delle ore lavorate. L'impiego della biometria nella rilevazione delle presenze, salvo pochissimi casi espressamente autorizzati, è vietato. Ma al riguardo, molte imprese e istituzioni (complici i fornitori) ignorano la legge o la interpretano in modo meno restrittivo, salvo poi incappare in contenziosi infiniti e pagare multe salatissime, quando la violazione viene a galla.

L'occhio sulla mano

L'identificazione biometrica si basa sulla verifica di una delle tante caratteristiche fisiche e comportamentali dell'essere umano. Il garante per la protezione dei dati personali, tuttavia, ha da sempre tenuto d'occhio la

Insieme alle impronte digitali, la topografia della mano è una delle caratteristiche fisiche più usate nel controllo elettronico degli accessi biometrici. Per i sistemi basati su queste tipologie di impronte è disponibile un set di prescrizioni da rispettare per rendere l'impianto sicuro e in regola con la legislazione vigente in materia di trattamento dei dati personali (courtesy Elex).

La biometria nel controllo accessi è subordinata all'osservanza di regole precise

Rispettare le prescrizioni significa legalità e meno lungaggini burocratiche

L'impronta biometrica, dovunque si trovi, deve essere protetta e difesa a ogni costo

Sì all'impronta (cifrata) nella card e nel lettore, no in un archivio centralizzato

L'ultima incombenza, la relazione tecnica

Un'azienda o un'altra organizzazione simile, pubblica o privata, che intende dotarsi di un sistema elettronico di controllo accessi biometrico è tenuta ad accertare che sussistano i presupposti di legittimità e a rispettare rigorosamente le prescrizioni imposte dal legislatore nazionale in materia di trattamento dei dati biometrici. Se sussiste il presupposto di legittimità – che in ambito privato consiste «nell'istituto del bilanciamento di interessi» (art. 24 c. 1 lett. g del Codice) e in quello pubblico nel «perseguimento delle finalità istituzionali del titolare» – il trattamento può avvenire senza il consenso dell'interessato. Se il titolare del trattamento adotta scrupolosamente le prescrizioni contenute nel provvedimento N. 513/2014 non è più tenuto, come in passato, a presentare al Garante una richiesta di verifica preliminare sul sistema che intende adottare e attendere il benestare (art. 17 del Codice). Si tratta di due incombenze burocratiche di non poco conto. C'è, tuttavia, un ultimo comandamento da osservare: l'immancabile relazione tecnica. Il titolare del trattamento è tenuto a predisporre un documento nel quale deve eseguire una **valutazione sulla necessità e proporzionalità del trattamento biometrico** e descrivere gli aspetti tecnici e organizzativi delle misure di sicurezza messe in atto. La relazione, che va aggiornata almeno una volta l'anno, deve essere tenuta a portata di mano in caso di richiesta del Garante. Non è necessario redigere il documento se l'impresa adotta una certificazione del sistema di gestione della sicurezza delle informazioni (SGSI) secondo la norma ISO/IEC 27001 a condizione che il controllo elettronico degli accessi sia inserito (e documentato) in tale certificazione.

topografia della mano e le impronte digitali. Tanta attenzione è giustificata dal fatto che entrambe sono oggi le più sfruttate nel controllo elettronico degli accessi (fisici e logici). Negli ultimi tempi, tuttavia, stanno conquistando terreno altre tecniche d'identificazione e, fra tutte, quella basata sull'analisi del volto. Sebbene le disposizioni impartite e da osservare facciano riferimento alle proprietà della mano, esse possono essere considerate valide anche per altri metodi meno diffusi.

Dove si nascondono le regole

Oltre che nel GDPR (regolamento UE 679/2016) e nel Codice della privacy (d. lgs. 196/2003, modificato dal d. lgs. 101/2008), il documento (piuttosto corposo) riguardante il trattamento dei dati biometrici e nel quale sono elencate nel dettaglio le prescrizioni da rispettare porta il numero 513 e risale al 12 novembre 2014. Tali disposizioni, per quanto concerne il controllo elettronico degli accessi fisici, sono contenute nei capitoli 4.2 (accesso ad aree sensibili o ad alto rischio oppure a macchinari pericolosi) e 4.3 (uso della biometria a scopi facilitativi in ambito pubblico e privato quali biblioteche, aeroporti, centri sportivi ecc.). L'osservanza di queste prescrizioni, è bene ricordarlo, mette l'azienda in regola con la legge ed evita la richiesta di verifica preliminare al Garante (art. 17 del Codice).

"Comandamenti" da rispettare

Quali sono, in sintesi, le prescrizioni principali da rispettare? Se si sfruttano le impronte digitali, il lettore biometrico deve rilevare la "vivezza" del dito. Il trattamento deve essere applicato solo al personale selezionato e autorizzato. I dati biometrici grezzi e i campioni devono essere cancellati subito dopo essere stati trasformati in modelli matematici. I lettori, siano essi dedicati alla registrazione (*enrolment*) che alla lettura in fase di controllo accessi, devono essere integrati nelle rispettive apparecchiature, oppure collegati ad esse direttamente, mentre l'interscambio di dati deve essere reso sicuro attraverso l'adozione di tecniche crittografiche efficaci.

Se nell'adottare un sistema elettronico di controllo accessi biometrico sussiste il diritto di legittimità e se il titolare del trattamento dei dati personali rispetta le prescrizioni tecniche e procedurali previste dal Garante della privacy, non è necessario ottenere l'autorizzazione da parte degli interessati, né presentare la richiesta di verifica preliminare ai sensi dell'art. 17 del Codice.

No alla banca delle impronte

Quando il riferimento biometrico di un utente è conservato in una card, è necessario che sia cifrato e reso inaccessibile mentre il supporto deve essere neutro, rilasciato in un unico esemplare e nell'esclusiva disponibilità dell'interessato. In caso di cessazione dei diritti di accesso, la card deve essere restituita all'ente emittente e distrutta con procedura formalizzata. Quando il riferimento biometrico, invece, è conservato nel lettore installato sulla porta o nel relativo Controller, oltre a essere cifrato e mantenuto per il tempo strettamente necessario (separato dai dati identificativi del soggetto), è obbligatorio adottare una serie di misure di sicurezza e accorgimenti tecnici atti a proteggere i dati, impedire l'accesso da parte di utenti non autorizzati (anche al software), tenere un log degli accessi e altro ancora.
È da escludere la costituzione di una banca dati biometrica centralizzata. Alcune prescrizioni sono chiare, altre meno. E questo, si sa, per noi italiani è una manna dal cielo poiché ci consente spesso di dar sfogo a libere (e a volte azzardate) interpretazioni.