GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Privacy: nuove regole per impronte digitali e firma grafometrica
Niente più verifica preliminare per alcuni usi, ma introdotto l'obbligo di comunicare al Garante le violazioni ai sistemi biometrici

Il Garante per la privacy ha approvato un quadro unitario di misure e accorgimenti di carattere tecnico, organizzativo e procedurale per mantenere alti livelli di sicurezza nell'utilizzo di particolari tipi di dati biometrici, semplificando tuttavia alcuni adempimenti. L'intervento dell'Autorità si è reso necessario alla luce della crescente diffusione di dispositivi biometrici, anche incorporati in prodotti di largo consumo.

Sempre più spesso infatti aziende e pubbliche amministrazioni si servono di dati biometrici, come le impronte digitali, la topografia della mano o le caratteristiche della firma autografa, per il controllo degli accessi, per l'autenticazione degli utenti (anche su pc e tablet) o per la sottoscrizione di documenti informatici.

Nel provvedimento generale [doc. web n. 3556992] - adottato a seguito di una consultazione pubblica e in corso di pubblicazione sulla G.U. con le allegate Linee guida [doc. web n. 3563006] e un modulo [doc. web n. 3563019] per la comunicazione all'Autorità di violazioni dei sistemi biometrici - il Garante ha individuato alcune tipologie di trattamento che, per le specifiche finalità perseguite, presentano un livello ridotto di rischio e non necessitano più della verifica preliminare da parte dell'Autorità**.**

La semplificazione riguarderà solo le specifiche tipologie di trattamento che dovranno in ogni caso essere effettuate nel rispetto delle rigorose misure di sicurezza individuate dal Garante, e comunque rispettando i presupposti di legittimità previsti dal Codice privacy, in particolare informando sempre gli interessati sui loro diritti, sugli scopi e le modalità del trattamento:

- **Autenticazione informatica**

  Le caratteristiche biometriche dell'impronta digitale o dell'emissione vocale di una persona possono essere utilizzate come credenziali di autenticazione per l'accesso a banche dati e sistemi informatici. Tale trattamento può essere effettuato **anche senza il consenso dell'utente**.

- **Controllo di accesso fisico ad aree "sensibili" e utilizzo di apparati e macchinari pericolosi**

  Le caratteristiche dell'impronta digitale o della topografia della mano potranno essere trattate per consentire l'accesso ad aree e locali ritenuti "sensibili" oppure per consentire l'utilizzo di apparati e macchinari pericolosi ai soli soggetti qualificati. Tale trattamento può essere realizzato **anche senza il consenso dell'utente**.

- **Sottoscrizione di documenti informatici**

  L'analisi dei dati biometrici associati all'apposizione a mano libera di una firma autografa potrà essere utilizzata per la firma elettronica avanzata. Questa modalità è però consentita solo con il consenso degli interessati, consenso non necessario invece in ambito pubblico, se devono essere perseguite specifiche finalità istituzionali. Dovranno comunque essere resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione, che non comportino l'utilizzo di dati biometrici.

- **Scopi facilitativi**

  L'impronta digitale e la topografia della mano potranno essere utilizzate anche per consentire l'accesso fisico di utenti ad aree fisiche in ambito pubblico (es. biblioteche) o privato (es. aree aeroportuali riservate). Anche in questo caso l'utilizzo è consentito **solo con il consenso degli interessati**. Dovranno comunque essere previste **modalità alternative** per l'erogazione del servizio per chi rifiuta di far utilizzare i propri dati biometrici.

Ogni sistema di rilevazione dovrà essere configurato in modo tale da raccogliere un numero limitato di informazioni (principio di minimizzazione), escludendo l'acquisizione di dati ulteriori rispetto a quelli necessari per il conseguimento della finalità perseguita. Ad esempio, in caso di autenticazione informatica, i dati biometrici non dovranno essere trattati in modo da poter desumere anche informazioni di natura sensibile dell'interessato.

Tra le numerose misure di sicurezza individuate dal Garante vi è quella che obbliga a cifrare il riferimento biometrico con tecniche crittografiche, con una lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati. Particolare attenzione è inoltre rivolta alla messa in sicurezza dei dispositivi mobili (come tablet o pc) che potrebbero più facilmente essere compromessi o smarriti.

Anche al fine di prevenire eventuali furti di identità biometrica, **tutte le violazioni dei dati o gli incidenti informatici** ("data breaches") che possano avere un impatto significativo sui sistemi biometrici o sui dati personali custoditi, **dovranno essere comunicati** da chi detiene i dati al Garante **entro 24 ore** dalla scoperta, così da consentire di adottare opportuni interventi a tutela delle persone interessate. A tal fine è stato predisposto un modulo che consente di semplificare il predetto adempimento.

Sono esclusi dalle modalità semplificate individuate nel provvedimento del Garante i trattamenti che prevedono la realizzazione di archivi

biometrici centralizzati, per i quali continuerà ad essere obbligatorio richiedere una verifica preliminare. Rimane in vigore anche l'obbligo di notificazione al Garante per i trattamenti non esplicitamente esclusi dal provvedimento, come quelli effettuati da esercenti le professioni sanitarie e da avvocati.

Per le verifiche preliminari in corso sono state previste specifiche disposizioni transitorie.

Roma, 26 novembre 2014