Pillole di Sicurezza

Dati biometrici e tutela della privacy

Dati biometrici e tutela della privacy.

Il nuovo provvedimento del Garante.

Sono molti e diversi fra loro i dati biometrici che, per caratteristiche di univocità e di persistenza nel tempo, possono essere utilmente elaborati con tecnologie digitali a scopo di identificazione e autenticazione: dalla impronta digitale al riconoscimento facciale o vocale, dall'analisi della retina alla firma grafometrica.

Il loro utilizzo si sta espandendo, anche grazie all'evoluzione delle tecnologie che ne abilitano l'uso, parallelamente al crescere dell'importanza dell'identità nel nuovo ecosistema digitale in cui ormai viviamo.

Si tratta però di dati personali che la normativa vigente classifica in quella categoria di dati che *"presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato*" di cui all'articolo 17 del d.lgs. 196/03.

Per tali dati il trattamento è lecito ma solo previa verifica preliminare da parte del Garante e secondo le prescrizioni da questi decise, in relazione alle caratteristiche specifiche del trattamento in questione: in pratica, chi intende porre in essere un trattamento che preveda l'utilizzo di dati biometrici deve sottoporre al Garante una richiesta di esame preventivo del trattamento e attenersi alle indicazioni che ne derivano, con un appesantimento burocratico non marginale.

Oggi, per alcune tipologie di dati biometrici, questa necessità è superata grazie al Provvedimento del Garante del 12 novembre 2014 (Doc. Web. n. 3556992) che include, come Allegato A, le LINEE-GUIDA IN MATERIA DIRICONOSCIMENTO BIOMETRICO E FIRMAGRAFOMETRICA.

Il provvedimento introduce una significativa semplificazione, rispetto alla normativa precedentemente vigente, dettagliando i casi e le modalità in cui questa si applica. Le linee guida, che sono parte integrante del provvedimento, definiscono la terminologia rilevante nel trattamento di dati biometrici ed il significato dei termini in modo esauriente e sufficientemente chiaro: chi non è familiare con termini come "*campione biometrico*", "*caratteristica biometrica*", "*verifica biometrica*" e molti altri può certamente fare riferimento all'allegato A che costituisce anche uno strumento informativo utile a supporto della decisione di adottare tecnologie biometriche e di quale in particolare.

Ogni tecnologia biometrica, infatti, presenta caratteristiche particolari che la rendono più o meno adeguata alle finalità dello specifico trattamento che si intende porre in essere: dalla necessità o meno della collaborazione dell'interessato (ad un estremo l'analisi dell'iride, all'altro il riconoscimento facciale) alla permanenza nel tempo contrapposta alla volatilità del campione biometrico (si pensi all'impronta digitale, contrapposta al riconoscimento vocale).

Tali specificità delle diverse tipologie di tecnologie biometriche hanno anche implicazioni per la corretta gestione delle esigenze di compliance: l'intrusività di alcune tecnologie richiede un maggiore coinvolgimento dell'interessato mentre l'assoluta trasparenza di altre riduce certamente l'impatto sull'interessato ma apre la strada alla possibilità della totale inconsapevolezza dell'interessato che nel primo caso è impossibile.

La logica di fondo del provvedimento è di individuare alcuni casi d'uso di dati biometrici ben identificati che non presentano elevati livelli di rischio e di definire le misure tecniche ed organizzative che, se correttamente applicate dal Titolare, rendono l'uso del dato biometrico lecito senza la necessità di esame preventivo da parte del Garante. Rimane, invece, l'obbligo di comunicare al Garante l'inizio del trattamento.

I casi specifici a cui il provvedimento si riferisce sono:

1. Utilizzo dell'impronta digitale o dell'emissione vocale per l'autenticazione informatica "*laddove è richiesta maggior certezza nell'identificazione degli utenti per particolari profili di rischio relativi alle informazioni trattate e alla tipologia di risorse informatiche impiegate*".
   La valutazione sulla *maggior certezza* è in capo al Titolare che deve ragionevolmente valutare la proporzionalità dell'uso di tecnologie biometriche. I criteri utilizzati dall'azienda per l'individuazione di un sottoinsieme di impiegati e collaboratori e/o di applicazioni e/o di dispositivi sono, in linea di massima, una buona base di riferimento.
2. Utilizzo dell'impronta digitale o della topografia della mano per il controllo di accesso fisico ad aree "sensibili" e per l'utilizzo di apparati e macchinari pericolosi.
3. Utilizzo dell'impronta digitale o della topografia della mano a scopi facilitativi, come nel caso di accesso a biblioteche, palestre etc.
4. Utilizzo di dati biometrici costituiti da informazioni dinamiche associate all'apposizione a mano libera di una firma autografa avvalendosi di specifici dispositivi hardware per la sottoscrizione di documenti informatici

Il presupposto di legittimità del trattamento è valutato caso per caso e può risiedere nella normativa stessa, come nel caso dell'autenticazione informatica, può derivare da una valutazione relativa al bilanciamento degli interessi del titolare e dell'interessato o dal consenso informato dell'interessato.

Nel caso della firma grafometrica è obbligatorio prevedere una modalità alternativa di sottoscrizione in modo che l'interessato non sia obbligato ad utilizzare quella specifica tecnologia.

In qualsiasi caso di uso di dati biometrici è comunque obbligatorio comunicare al Garante i casi di data breach o gli eventi di sicurezza che possono portare alla compromissione dei dati biometrici.

La comunicazione deve essere effettuata entro ventiquattro ore dalla scoperta dell'incidente o della violazione ogni volta che sia anche solo la possibilità di una conseguenza per la sicurezza dei dati.

Questo è il secondo caso in cui la normativa italiana prevede l'obbligo alla pubblicazione degli incidenti di sicurezza e della violazione dei dati personali che il futuro regolamento europeo sulla Privacy renderà obbligatoria per tutti.

Per quanto riguarda gli obblighi che rimangono in capo al Titolare, il quadro risultante è sintetizzato nella Tabella 1 che segue.

Utilizzo dati biometrici. Mappa riassuntiva degli obblighi. Provvedimento del Garante del 12/11/2014	Consenso degli interessati	Verifica preliminare	Comunicazione del trattamento	Comunicazione data breach
Autenticazione informatica	No	No	Si	Si
Controllo di accesso fisico ad aree "sensibili" dei soggetti addetti e utilizzo di apparati e macchinari	No	No	Si	Si
Uso dell'impronta digitale o della topografia della mano a scopi facilitativi	Si	No	Si	Si
Sottoscrizione di documenti informatici	Si	No	Si	Si

Tabella 1 - Obblighi

Per ciascuno dei quattro casi indicati sono previste specifiche misure di sicurezza il cui rispetto è obbligatorio. Naturalmente variano caso per caso, all'interno delle seguenti categorie in cui possono essere suddivise:

1. Misure per evitare l'utilizzo truffaldino del dato biometrico. Rientrano in questa categoria, ad esempio, le seguenti
    a. La capacità di verificare la cosiddetta "vivezza" da parte del rilevatore delle impronte digitali;
    b. L'utilizzo del riconoscimento vocale in accoppiata con altre tecniche di autenticazione e con accorgimenti che impediscano l'utilizzo di frasi registrate;
    c. L'utilizzo della firma grafometrica solo previa identificazione del firmatario.
2. Misure volte a regolare la conservazione dei dati biometrici nelle diverse fasi del processo di utilizzo, dall'enrollment all'uso operativo. Rientrano in questa categoria:
    a. La cancellazione dei dati grezzi una volta utilizzati;
    b. L'uso di tecniche crittografiche adeguate, rispetto al ciclo di vita del dato biometrico, anche in tutti i trasferimenti di dati biometrici su rete;
    c. La limitazione e la regolamentazioni di archiviazioni temporanee in transit;
    d. La distruzione tramite procedura formalizzata e documentata delle smart card o dei dispositivi equivalenti in possesso dell'interessato quando questi perde il diritto all'utilizzo della stessa;
    e. La protezione delle porzioni di memoria in cui sono conservate le credenziali biometriche in caso di utilizzo di dispositivi mobili;
    f. Cancellazione automatica dei dati biometrici alla cessazione degli scopi per cui sono stati impiegati;
    g. La conservazione dei dati biometrici in archivi separati dai dati identificativi degli interessati;
    h. Divieto di costituzione di archivi centralizzati di dati biometrici.
3. Misure volte a proteggere l'infrastruttura che rende possibile il trattamento con dati biometrici:
    a. Registrazione dei log degli accessi degli amministratori di sistema;
    b. Controllo delle configurazioni per evitare l'installazione di software non previsto;
    c. Protezione nei confronti del malware;
    d. Protezione dell'accesso alle risorse utilizzate.
4. Misure organizzative. Rientrano in questa categoria
    a. La redazione di una relazione che descriva le misure tecniche ed organizzative poste in essere a tutela dei dati biometrici con verifica annuale. E' da notare che le organizzazioni certificate ISO 27001 possono collocare le informazioni relative alla protezione dei dati biometrici all'interno della documentazione relativa a tale certificazione, senza produrre ulteriori documenti.

Non è obiettivo di questo documento realizzare una disamina analitica del Provvedimento, a cui si rimanda anche per la corretta applicazione della normativa, quanto dare informazioni utili per affrontare la materia.

Cosa deve, dunque, fare un titolare che voglia utilizzare dati biometrici nella propria organizzazione? Può seguire la seguente scaletta:

1. Qualificare le proprie necessità, individuare la tipologia di dato biometrico utile, precisare le finalità e gli ambiti del suo utilizzo e le motivazioni che la rendono preferibile ad altre soluzioni meno critiche dal punto di vista della privacy. Il dato biometrico, anche nei casi in cui il suo utilizzo è stato reso più semplice, rimane comunque un dato a cui prestare particolare attenzione ed alla base del suo utilizzo ci deve essere una valutazione del titolare di proporzionalità e di ragionevolezza.

2. Verificare se il caso d'uso di suo interesse rientra tra le quattro tipologie "liberalizzate" dal provvedimento del novembre 2014. Se non lo è dovrà presentare istanza di verifica preliminare al Garante delle Privacy.
3. Se il caso d'uso è tra quelli previsti dal Provvedimento, applicare le misure indicate analiticamente nel provvedimento e verificare che la tecnologia utilizzata sia compatibile.
4. Comunicare al Garante l'inizio del trattamento.

Per i casi considerati, il provvedimento garantisce una semplicità ed una efficienza prima impossibili sia nella valutazione dell'opportunità sia nella selezione delle tecnologie. La scelta di questi casi d'uso deriva dall'analisi delle richieste di verifica ricevute dall'Ufficio del Garante e dovrebbe pertanto riguardare i casi più frequenti.

Il Garante ha espressamente previsto, all'interno del provvedimento, la possibilità di estendere, in futuro, questo approccio ad altre tipologie di dati biometrici e ad altri casi d'uso, in funzione delle richieste e dell'evoluzione della tecnologia.

Sergio Fumagalli

sergio.fumagalli@zeropiu.it

Vice President di Zeropiu Spa, società di system integration e consulenza specializzata sui temi della sicurezza delle identità digitali e dei dati, attiva in Italia e nei Paesi Scandinavi.

Dopo un'esperienza parlamentare nella XIII legislatura, dal 2001 inizia a occuparsi professionalmente di Privacy, collaborando con il Garante della Privacy e pubblicando, come co-autore, il testo "Privacy guida agli adempimenti", IPSOA, 2004, 2005.

Partecipa, fin dal 2008 alla Oracle Community for Security: è stato co-autore dei documenti prodotti dalla Community e attualmente coordina il gruppo di lavoro sul nuovo Regolamento europeo sulla privacy.

E' membro del direttivo di Clusit.

Dal 2004 al 2012 è stato membro del Cda di Webank, la banca online del gruppo BPM.