anno V, n. 1, 2015
data di pubblicazione: 2 aprile 2015

Il provvedimento e le linee guida del Garante privacy in materia di biometria

di Valentina Fiorillo *

Lo scorso novembre il Garante per la protezione dei dati personali ha adottato un provvedimento prescrittivo in tema di biometria (doc. web n. 3556992, 12 novembre 2014, pubblicato sulla *Gazzetta Ufficiale* n. 280 del 2 dicembre 2014) unitamente alle linee guida in materia di riconoscimento biometrico e firma grafometrica (Allegato A al Provvedimento del Garante del 12 novembre 2014,doc. web n. 3563006). I due atti si propongono di individuare, dando attuazione alle disposizioni contenute all'interno del Codice *privacy* (d.lgs. 30 giugno 2003, n. 196), delle misure e degli accorgimenti di carattere organizzativo, procedurale e, non da ultimo, tecnico per assicurare che il trattamento dei dati personali biometrici avvenga nel rispetto della disciplina di protezione dei dati personali.

* Dottore di ricerca in Teoria dello Stato e Istituzioni politiche comparate, Università di Roma «la Sapienza». Le opinioni espresse nel presente lavoro sono del tutto personali e non rappresentano in alcun modo il punto di vista dell'Ufficio presso il quale l'autrice presta attualmente servizio.

Lo schema di delibera, con allegate le linee guida, è stato sottoposto alla consultazione pubblica, come è prassi del Garante nel caso dei provvedimenti più significativi che necessitano di un dialogo con cittadini e imprese. La consultazione pubblica, avviata nel maggio 2014, ha previsto un periodo di 30 giorni entro i quali studiosi e ricercatori, produttori e sviluppatori di sistemi biometrici e di sistemi di firma grafometrica, così come associazioni rappresentative di aziende e consumatori hanno potuto far pervenire al Garante i propri contributi scritti.

Scaduti i termini della consultazione, si è poi proceduto all'adozione definitiva della delibera (provvedimento generale) e delle allegate linee guida nel Collegio del 12 novembre.

Come si evince dalla comunicazione ufficiale (Comunicato stampa del 26 novembre 2014, reperibile su www.gpdp.it) nonché dalla premessa stessa della delibera, il Garante ha ritenuto di intervenire a fronte della sempre crescente diffusione di dispositivi biometrici, da un lato, e dell'elevato numero di notificazioni presentate all'Ufficio ai sensi dell'art. 37 del Codice *privacy*, dall'altro. Proprio quest'ultimo dato è stato decisivo nell'operare una valutazione di opportunità al fine di indicare in maniera organica e sistematica i necessari adempimenti in materia di tutela dei dati personali e della riservatezza.

Il punto di partenza non può che essere quello della definizione di "dato biometrico", definizione che non è esattamente rinvenibile a livello normativo. Nelle linee guida il Garante fa propria la definizione di dato biometrico contenuta nel parere del Gruppo per la tutela dei dati personali *Articolo 29* costituito da rappresentanti delle Autorità di protezione dati dei diversi stati membri (il riferimento è al Parere 3/2012 sugli sviluppi nelle tecnologie biometriche, WP193, adottato il 27 aprile 2012).

In esso i "dati biometrici" vengono convenzionalmente definiti come dati ricavati da «proprietà biologiche, aspetti comportamentali, caratteristiche fisiologiche, tratti biologici o azioni ripetibili laddove tali caratteristiche o azioni sono tanto proprie di un certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità».

Lo sviluppo tecnologico ha molto ampliato le tipologie di tecniche applicabili ma la definizione di dato biometrico come connesso a tratti biologici, comportamentali e fisiologici dell'individuo ha una portata applicativa assolutamente attuale.

Provando, dunque, a sintetizzare il contenuto del provvedimento, si può dire che i perni su cui esso è costruito sono principalmente tre: a) si introduce, mutuandolo dalla disciplina del c.d. *data breach*, l'obbligo di segnalare al Garante le violazioni ai sistemi biometrici; b) si chiarisce che l'obbligo di verifica preliminare ai sensi dell'articolo 17 del Codice *privacy* si applica a tutti i trattamenti di dati biometrici; c) si definiscono, limitandoli (per il momento) a sole quattro tipologie, i casi in cui i titolari del trattamento possono considerarsi esentati dal presentare istanza di verifica preliminare, a patto che rispettino delle rigide prescrizioni di carattere giuridico e tecnico-organizzativo.

In primo luogo il punto 3 del provvedimento stabilisce che i titolari del trattamento comunicano all'Autorità «[t]utte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici o sui dati personali ivi custoditi», questo al fine di consentire l'adozione di opportuni interventi a tutela delle persone interessate, i cui dati personali sono "violati".

La parte più corposa dell'intervento del Garante, tuttavia, è quella relativa all'individuazione dei casi di esonero dalla verifica preliminare. In essa si rinviene traccia della tendenza a voler, contemporaneamente, chiarire gli obblighi, innalzare il livello di tutela dei dati personali e semplificare gli adempimenti per i titolari del trattamento (punto 4).

Prima di individuare i casi di esonero, il Garante ricorda che i titolari sono tenuti a presentare una richiesta di verifica preliminare, ai sensi dell'articolo 17 del Codice *privacy*. Tale disposizione di legge non cita espressamente i dati biometrici e, dunque, l'importanza dell'affermazione del Garante nel novembre scorso è proprio quella di aver chiarito che i dati biometrici ricadono sempre nella categoria dei trattamenti che presentano «rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato» (art. 17). Per tale motivo il loro trattamento deve essere di regola sottoposto a verifica preliminare ai sensi del Codice *privacy*. Questo poiché, a prescindere dalla singola tecnica utilizzata, «i dati biometrici sono, per loro natura, direttamente, univocamente e in modo tendenzialmente stabile nel tempo, collegati all'individuo e denotano la profonda relazione tra corpo, comportamento e identità della persona, richiedendo particolari cautele in caso di loro trattamento. L'adozione di sistemi biometrici, in ragione della tecnica prescelta, del contesto di utilizzazione, del numero e della tipologia di potenziali interessati, delle modalità e delle finalità del trattamento, può comportare quindi rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato» (Punto 4 provvedimento generale).

Come testimoniano i numerosi provvedimenti citati in calce alle linee guida, la prassi del Garante è sempre stata quella di considerare i dati biometrici come fattispecie che necessita della procedura di garanzia

rappresentata dalla verifica preliminare. Tuttavia mai questa affermazione era stata formulata in maniera esplicita e generalizzata, come avvenuto nel provvedimento in commento.

Una volta innalzata la tutela in termini generali, si individuano dei casi di esonero dalla verifica preliminare che riprendono, in buona sostanza, le tipologie di trattamento già vagliate in passato dal Garante e autorizzate, non senza prima aver prescritto misure ed accorgimenti a garanzia dell'interessato nelle singole istanze esaminate.

Ferme restando le disposizioni del Codice *privacy* relative ai princìpi generali (liceità, finalità, necessità e proporzionalità dei trattamenti), nonché l'obbligo di informativa (art. 13) e di notificazione (art. 37), la semplificazione degli adempimenti *privacy* interesserà solo alcune specifiche tipologie di trattamento, che dovranno, sempre e comunque, essere effettuate nel rispetto delle rigorose misure di sicurezza individuate dal Garante.

Le tipologie sono le seguenti: a) autenticazione informatica (impronta digitale o emissione vocale); b) controllo di accesso fisico ad "aree sensibili" dei soggetti addetti e utilizzo di apparati e macchinari pericolosi con utilizzo dell'impronta digitale e topografia della mano (intendendo per aree sensibili aree in cui sono conservati oggetti di particolare valore, aree dove si svolgono processi produttivi pericolosi); c) utilizzo dell'impronta digitale o della topografia della mano a scopi facilitativi (biblioteche pubbliche, aree portuali riservate); d) sottoscrizione di documenti informatici (firma grafometrica, come base per la soluzione di firma elettronica avanzata).

Occorre precisare, in primo luogo, una importante distinzione tra le prime due tipologie di trattamento (*a* e *b*) e le ultime (*c* e *d*). Nel primo

caso si tratta di trattamenti che possono essere effettuati senza il consenso dell'interessato. Questo sia in ambito pubblico, dove il presupposto di legittimità del trattamento è dato dal perseguimento delle finalità istituzionali del titolare, sia in ambito privato, dove, applicando l'istituto del bilanciamento di interessi (art. 24, comma 1, lettera g), del Codice), il trattamento dei dati biometrici può avvenire senza il consenso degli interessati poiché si riconosce un legittimo interesse perseguito dal titolare (legittimo interesse che, ovviamente, è diversamente motivato nei due casi).

Nelle tipologie *c* e *d*), il presupposto di legittimità del trattamento è individuato proprio nel consenso dell'interessato. Tanto è vero che il titolare è tenuto ad assicurare sistemi alternativi di accesso e di firma a quelli che impiegano dati biometrici per i soggetti che intendono negare il proprio consenso al trattamento biometrico (c.d. principio della alternatività o facoltatività).

Sempre in termini generali per ciascuna delle quattro tipologie, secondo un principio che si potrebbe definire di "minimizzazione" (ricavabile dai principi di necessità, pertinenza e non eccedenza sanciti dal Codice *privacy*, artt. 3 e 11, comma 1, lettera d), ogni sistema (dispositivo e collegamenti informatici annessi) dovrà essere configurato in modo tale da raccogliere la minor quantità possibile di dati personali, evitando l'acquisizione di dati ulteriori rispetto a quelli strettamente necessari per il conseguimento della finalità perseguita.

Vi sono poi una serie di misure di sicurezza che il titolare è tenuto ad applicare per usufruire dell'esonero dalla verifica preliminare, intendendosi con l'espressione "misure di sicurezza" tutta una serie di accorgimenti tecnici volti a ridurre al minimo i rischi di distruzione, perdita o

accesso non autorizzato ai dati personali custoditi nei sistemi. Una delle principali misure individuate è quella che obbliga a cifrare il riferimento biometrico con tecniche crittografiche, con una particolare lunghezza delle chiavi, ma anche la costante tracciabilità degli accessi da parte degli amministratori di sistema ai sistemi informatici, così come l'obbligo di conservare sempre separatamente i campioni e riferimenti biometrici dai dati identificativi degli interessati.

Infine un'ultima regola di carattere generale che va evidenziata: qualsiasi trattamento di dati biometrici nei termini finora descritti è esonerato da verifica preliminare, purché questo non comporti in alcun modo una realizzazione di archivi biometrici centralizzati.