PROVVEDIMENTO DEL 30 LUGLIO 2019 SULLA NOTIFICA DELLE VIOLAZIONI DEI DATI PERSONALI

L'utilizzo di dispositivi e tecnologie per la raccolta e il trattamento di dati biometrici è soggetto a una crescente diffusione, in particolare per l'accertamento dell'identità personale nell'ambito dell'erogazione di servizi della società dell'informazione e dell'accesso a banche dati informatizzate, per il controllo degli accessi a locali e aree, per l'attivazione di dispositivi elettromeccanici ed elettronici, anche di uso personale, o di macchinari, nonché per la sottoscrizione di documenti informatici.

Tale diffusione ha suscitato la massima attenzione delle autorità di protezione dati, testimoniata anche dall'elaborazione di pareri da parte del Working Party Article 29 (WP29) che costituiscono un significativo punto di riferimento per ogni analisi e studio del fenomeno. I dati biometrici sono infatti dati personali, poiché possono sempre essere considerati come "informazione concernente una persona fisica identificata o identificabile (...)" prendendo in considerazione "l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona". Essi rientrano quindi nell'ambito di applicazione del Codice (art. 4, comma 1, lettera b), e le operazioni su essi compiute con strumenti elettronici sono a tutti gli effetti trattamenti nel senso delineato dalla disciplina sulla protezione dei dati personali.

Sono considerati dati biometrici nel presente contesto, coerentemente con i pareri del WP29, i campioni biometrici, i modelli biometrici, i riferimenti biometrici e ogni altro dato ricavato con procedimento informatico da caratteristiche biometriche e che possa essere ricondotto, anche tramite interconnessione ad altre banche dati, a un interessato individuato o individuabile.

Il Garante è intervenuto più volte, a seguito di specifiche richieste di verifica preliminare ai sensi dell'art. 17 del Codice, con provvedimenti che hanno in alcuni casi negato e in altri ammesso, nel rispetto di prescrizioni di natura tecnica od organizzativa, i trattamenti sottoposti alla valutazione dell'Autorità.

A fronte della complessità della materia in rapporto alla disciplina sul trattamento dei dati personali, con l'adozione delle "Linee-guida in materia di riconoscimento biometrico e firma grafometrica", che formano parte integrante del presente provvedimento, il Garante intende fornire un quadro di riferimento unitario sulla cui base i titolari possano orientare le proprie scelte tecnologiche, conformare i trattamenti ai principi di legittimità stabiliti dal Codice, rispettare elevati standard di sicurezza.

Le linee-guida introducono altresì la terminologia essenziale per la descrizione degli aspetti tecnologici, con il ricorso a standard internazionali, e individuano i principali profili di rischio associati al trattamento di dati biometrici.

Le peculiari caratteristiche dei dati biometrici, unitamente ai rischi su di essi incombenti illustrati nelle linee-guida, fanno ritenere necessario assoggettare il loro trattamento, anche in coerenza con le previsioni del Regolamento europeo eIDAS in tema di identificazione, autenticazione e firma elettronica, all'obbligo di comunicare al Garante il verificarsi di violazioni dei dati (data breach) o incidenti informatici (accessi abusivi, azione di malware...) che, pur non avendo un impatto diretto su di essi, possano comunque esporli a rischi di violazione.

A questo fine, entro ventiquattro ore dalla conoscenza del fatto i titolari comunicano all'Autorità tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici o sui dati personali ivi custoditi. Tali comunicazioni devono essere redatte secondo lo schema riportato nell'allegato "B" al presente provvedimento e quindi inviate tramite posta elettronica o posta elettronica certificata all'indirizzo: databreach.biometria@pec.gpdp.it.