diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

ISSN 1127-8579

Pubblicato dal 13/07/2012

All'indirizzo http://www.diritto.it/docs/33728-la-firma-grafometrica-e-l-opinione-dei-garanti-privacy-europei-sui-dati-biometrici

Autori: Marcoccio Gloria , Manca Giovanni

La firma grafometrica e l'Opinione dei Garanti Privacy Europei sui dati biometrici

La firma grafometrica e l'Opinione dei Garanti Privacy Europei sui dati biometrici

Luglio 2012

Giovanni Manca, Gloria Marcoccio

Il Working Party 29 (WP 29), consesso dei Garanti privacy europei, a fine Aprile 2012 ha pubblicato l'Opinione 3/2012 riguardo gli sviluppi delle tecniche biometriche ed i conseguenti aspetti che occorre tenere presenti ai fini della normativa EU in materia di protezione dati personali e privacy.[1] Già nel 2003 il WP 29 aveva dedicato all'argomento un primo "documento di lavoro" con il quale si evidenziavano, rispetto alle soluzioni tecnologiche di allora, le criticità derivanti dal trattamento di dati biometrici e le possibili aree di intervento in termini di contromisure. L'Opinione attuale aggiorna il quadro esaminato precedentemente nel 2003, individua specifici settori di utilizzo del trattamento dei dati biometrici, ed indica linee guida e raccomandazioni indirizzate al settore industriale interessato, agli utenti di tali tecnologie, ed alle autorità europee e nazionali competenti per la relativa legislazione. In questo senso nell'Opinione si legge, a livello europeo, l'attenzione del WP 29 per la nuova regolamentazione privacy EU attualmente in corso di esame (avviato ufficialmente il 25 gennaio 2012, nella quale i dati biometrici sono espressamente referenziati) e, a livello nazionale, qualcosa di più di un invito ai singoli Garanti privacy nel predisporre le prescrizioni di misure ed accorgimenti in sintonia con quanto riportato nell'Opinione stessa.

Tra i vari contesti di utilizzo e di tecnologie elencate nell'Opinione, vi è anche l'esplicito riferimento alla firma cosiddetta grafometrica (vedasi paragrafo 4.4.6 dell'Opinione), e dunque alle soluzioni tecnologiche ed ai procedimenti che consentono di firmare un documento informatico, in base alla rilevazione di determinate caratteristiche biometriche della persona che appone la firma. Sono già presenti sul mercato italiano le prime soluzioni tecnologiche e proposte commerciali per la firma grafometrica ed è comprensibile che queste vengano accolte con favore: infatti l'esperienza di firmare un documento informatico apponendo, di fatto, la propria firma "a mano", è facilmente apprezzabile da chiunque, posto che la soluzione tecnica/organizzativa offra nel suo complesso accettabili garanzie di affidabilità e sicurezza. A tale proposito l'interesse riguardo la firma grafometrica è certamente destinato ad aumentare in particolare considerando il suo utilizzo come "firma elettronica avanzata", alla quale gli aggiornamenti normativi portati da D.Lgs 235/2010[2] in materia di firma elettronica riconoscono, rispetto al passato, un maggiore valore legale. Infatti la "firma elettronica avanzata" definita alla lettera q-bis del comma 1 dell'art. 1 del D.Lgs 82/2005 (Codice dell'amministrazione digitale) come:

"*insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati*"

ha il valore legale riconosciuto con il comma 2 dell'art. 21 del D.Lgs 82/2005:

"Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702[3] *del codice*

---

1 "Opinion 3/2012 on developments in biometric technologies
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

2 DECRETO LEGISLATIVO 30 dicembre 2010, n. 235: Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69. *GU n.6 del 10-1-2011 - Supplemento. Ordinario n. 8)*

3 *"La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro*

civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria."

In termini di condizioni di sicurezza ed affidabilità della firma elettronica avanzata (FEA), le regole tecniche previste dal comma 3 art. 20 del D.Lgs 235/2010, ne devono fissare i termini ed i limiti da rispettare, sotto il profilo tecnico e quello organizzativo procedurale. Tali regole non sono state ancora pubblicate in Gazzetta Ufficiale (dovrebbe avvenire a breve), ma è comunque possibile consultare il testo dello schema notificato a Bruxelles secondo le usuali procedure europee, disponibile presso:

http://ec.europa.eu/enterprise/tris/pisa/app/search/index.cfm?fuseaction=recent&lang=IT

Peraltro il testo è stato restituito dai compenti Uffici dell'UE senza alcuna modifica e quindi si può ritenere definitivo il testo notificato.

Lo schema è già stato oggetto di vari commenti disponibili in rete e su riviste specializzate[4] e da questi è interessante riportare che per la FEA sono state predisposte prescrizioni notevoli, sicuramente con l'obiettivo di predisporre tutele, con adeguate misure tecniche ed organizzative, in considerazione del suo nuovo e maggiore valore legale.

Sul versante della normativa italiana in materia di protezione dati personali le soluzioni tecnologiche ed i processi di utilizzo delle firme grafometriche, indipendentemente dal loro sfruttamento come FEA, trovano già nel Codice Privacy - D.Lgs 196/03 (ed applicabili autorizzazioni e provvedimenti del Garante privacy italiano) il diretto riferimento normativo. In estrema sintesi…

> In termini di adempimenti occorre ricordare la preventiva Notifica al Garante (lettera a del comma 1 art. 37 del Codice Privacy) e, tenendo conto dei "*rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare*", la Verifica preliminare del Garante ai sensi dell'art. 17 del Codice Privacy.
>
> Nei riguardi degli interessati (coloro ai quali si riferiscono i dati biometrici) è sempre necessaria l'informativa (art 13 Codice Privacy) ed il consenso (art 23 Codice Privacy) a meno di non rientrare nei casi di esclusione previsti nel Codice Privacy, art.24.
>
> Sempre poi da porre in essere quanto richiesto per la regolamentazione della figura degli Incaricati e dei Responsabili (rispettivamente art. 30 e 29 del Codice Privacy) ed eventuali trasferimenti di dati all'estero (artt. 42-45 del Codice Privacy).
>
> Sul fronte delle misure di sicurezza, occorre in ogni caso predisporre le misure minime di sicurezza (artt. 33-36 del Codice Privacy e suo allegato B), le misure e gli accorgimenti previsti dal Provvedimento del Garante sul ruolo dell'Amministratore di sistema (sono trattamenti effettuati mediante "strumenti elettronici") e le misure derivanti dall'analisi dei rischi (art 31 e successivi del Codice Privacy).
>
> In termini di prescrizioni generali riguardo i dati biometrici, già emesse dal nostro Garante privacy, occorre menzionare quella presente nelle "Linee-guida per il trattamento di dati dei dipendenti privati - 23 novembre 2006 *(G.U. 7 dicembre 2006, n. 285)*" e relativa a 'Dati biometrici e accesso ad "aree riservate"' (paragrafo 4 dell'allegato 1 alle Linee-guida).

Le organizzazioni che intendono realizzare e/o utilizzare soluzioni di firma grafometrica come firma elettronica avanzata dovranno in ogni caso osservare le prescrizioni:

- derivanti dalla normativa privacy (per gli aspetti di trattamento di dati biometrici)
- dettate con le regole tecniche previste dal comma 3 art. 20 del D.Lgs 235/2010.

In tale contesto le linee guida e le raccomandazioni portate dalla Opinione 3/2012 del WP 29, rilette sotto la prospettiva della firma grafometrica e come base a supporto di quanto richiesto delle regole tecniche di cui al

il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta. "

4 Vedasi "Commenti allo schema normativo relativo alla firma elettronica avanzata (FEA)" di G. Manca, pubblicato su Information Security n° 11, maggio 2012

D.Lgs 235/2010 per la FEA, forniscono un quadro d'assieme sicuramente di notevole valore, e che vale la pena di tenere presente sebbene, come noto, le opinioni del WP 29 non abbiano di per se una diretta efficacia come obbligo di legge.

PIA – Privacy Impact Assessment

Il WP 29 pone l'accento sulla necessità di seguire un approccio strutturato e sistematico nell'individuare i rischi e determinare le misure necessarie in considerazione dello specifico contesto d'uso: non solo quindi le misure squisitamente tecniche ma anche quelle derivanti dal contesto organizzativo/pratico nel quale lo strumento di firma sarà utilizzato e relativi e specifici adempimenti di legge. Tanto per fare un esempio una firma grafometrica adottata da un istituto bancario con i suoi clienti, ha caratteristiche ed aspetti normativi e profili di rischi diversi dal contesto di firma adottata all'interno di un'azienda, per cui gli utilizzatori sono dipendenti, consulenti e magari anche fornitori dell'azienda stessa.

L'approccio indicato è quello della cosiddetta PIA – Privacy Impact Assessment. Il WP 29 si è già espresso sulla necessità di adottare la PIA nel settore della tecnologia RFID con diversi lavori ed opinioni a riguardo[5]. Anche la nuova proposta di regolamentazione privacy in fase di esame a livello UE prevede espressamente un simile approccio (per ora con la dizione: data protection assessment)

La PIA dovrà prendere in considerazione:

- la natura dei dati che si intende raccogliere
- le finalità e scopi del loro trattamento
- l'accuratezza dei sistemi che si intende utilizzare, nella consapevolezza dell'importanza di una firma grafometrica nel suo contesto d'uso (e suo valore probatorio qualora sia utilizzata come FEA)
- i presupposti legali per il suo utilizzo, con particolare attenzione agli adempimenti di legge richiesti (Notifica,…) ed in modo particolare gli aspetti del consenso
- l'accesso agli strumenti nei quali sono conservati i dati biometrici e le esigenze di scambi di informazioni che li riguardano all'interno dell'organizzazione che ne farà uso e le conseguenti necessarie misure di sicurezza per consentire l'accesso in chiaro ai dati solo agli aventi diritto
- le decisioni che riguardano i tempi di conservazione e le modalità della completa cancellazione quando non più necessari, dei dati biometrici e delle altre informazioni a corredo necessarie per l'utilizzo di una firma grafometrica

Da evidenziare che la PIA si propone come base naturale ed essenziale per soddisfare il principio di "Accountability" e dunque la capacità di dimostrare le scelte fatte e le misure predisposte ai fini della conformità della normativa in oggetto.

Le principali categorie di rischio individuate dal WP 29 riguardano:

1. furto dell'identità digitale (nel caso di interesse da leggersi come furto in relazione alla firma grafometrica)
2. utilizzo dei dati biometrici per un uso diverso dallo scopo per i quali sono stati raccolti
3. violazione dei dati (che in funzione della gravità delle violazione potrebbe comportare la necessità di darne comunicazione ai diretti interessati e/o alle autorità competenti)

MISURE ED ACCORGIMENTI

In termini di misure ed accorgimenti l'Opinione del WP 29 evidenzia l'importanza di prevedere:

come misure tecniche (di interesse per gli aspetti di firma grafometrica):

5 Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications -http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf

utilizzo di "biometric template", ossia informazioni chiave estratte dai dati biometrici raccolti e successivamente trattate in luogo dei dati biometrici stessi. È chiaro che questa indicazione va accolta come "laddove applicabile": per esempio nel caso di firma grafometrica i dati raccolti (pressione impressa al tratto, velocità e accelerazione della scrittura, …) potrebbero dare luogo al relativo "biometric template" che è l'oggetto di trattamento

conservazione dei dati biometrici su dispositivi ad uso esclusivo dell'interessato, se non realmente indispensabile utilizzare database centralizzati, **prevedendo di:**

- eseguire le necessarie operazioni di confronti/lettura dei dati (crittografati) direttamente sui dispositivi in uso esclusivo dell'interessato
- conservare su tali dispositivi il minor numero possibile di dati identificativi dell'interessato (per limitare i rischi di furto d' identità digitale)
- comunque di mantenere sempre i dati crittografati qualora sia effettivamente necessaria la conservazione di dati biometrici in database centralizzati

rinnovabilità e revocabilità

- possibilità tecnica/organizzativa di rigenerare i dati in modo sicuro a seguito di una violazione dei dati stessi o a seguito di evoluzioni tecnologiche
- possibilità per l'interessato di esercitare il diritto di revoca della connessione tra la sua identità e i dati biometrici elaborati

crittografia

- necessità di mantenere sempre crittografati i dati biometrici
- assegnare le chiavi di decrittazione esclusivamente a coloro che hanno effettiva necessità di conoscere i dati

antispoofing

- ai produttori è indicato di implementare sistemi in grado di determinare la genuinità dei dati biometrici conservati ed il loro collegamento alla persona fisica, ai fini della affidabilità dello specifico sistema biometrico

Il WP 29 considera come meritevole di interesse le tecniche di crittografia/decrittografia biometrica, ossia basate sull'utilizzo di dati biometrici per creare le chiavi di crittazione/decrittazione

metodi automatizzati per la cancellazione dei dati

- la cancellazione del dato, allo scadere del termine entro il quale è necessaria la sua conservazione, è considerata una delle più importanti misure nel trattamento biometrico per limitare i rischi di furti di identità ed uso improprio dei dati

come misure organizzative:

procedure interne

- stabilire chiare procedure per determinare i limiti e le modalità di accesso esclusivamente per gli aventi diritto nonché prevedere meccanismi per tracciare tutte le attività condotte sui dati (non solo quindi log di accesso come è in Italia per il caso degli amministratori di sistema)

policy di controllo dei fornitori

- definire policy per controllare gli eventuali fornitori di servizi coinvolti nel trattamento dei dati biometrici, prevedendo ispezioni e controlli adeguati nei loro riguardi, richiedendo garanzie sul rispetto delle misure per gli incaricati di loro responsabilità e sulle procedure da attivare quando un interessato esercita i propri diritti previsti dalla legge, in merito al trattamento dei suoi dati

Molte delle indicazioni proposte nell'Opinione del WP 29 trovano riscontro e sostengono i requisiti presenti nelle regole tecniche italiane di prossima pubblicazione in materia di firma elettronica avanzata.
E' comunque utile che un eventuale futuro provvedimento di carattere generale del Garante per la protezione dei dati personali, relativo al trattamento dei dati biometrici, incluse le firme grafometriche, stabilisca prescrizioni di misure e accorgimenti che possano favorire la conformità alle regole tecniche per la FEA da parte dei produttori di soluzioni e coloro che intendano erogare ai propri utenti servizi di FEA.