Roma, 5 Marzo 2018

CIRCOLARE N. 05/2018

Prot. 50/2018
Sez. II/1

A TUTTI GLI ISTITUTI ASSOCIATI
LORO SEDI

Oggetto*: Ispettorato del Lavoro. Circolare n. 5 del 19 Febbraio 2018. Strumenti di controllo a distanza dei lavoratori: le nuove indicazioni operative dell'Ispettorato del Lavoro.*

L'Ispettorato Nazionale del Lavoro, di concerto con il Ministero del Lavoro e Politiche Sociali, ha emanato la Circolare n. 5 del 19 Febbraio 2018, (doc. 1) a mezzo della quale fornisce importanti chiarimenti ed indicazioni operative concernenti l'installazione e l'utilizzo di impianti audiovisivi ed altri strumenti di controllo, ai sensi del riformato art. 4 Legge n. 300/1970, già oggetto di nostri precedenti commenti.
Per quanto riguarda le imprese del nostro settore il provvedimento rileva sotto un duplice profilo, posto che i nostri associati, oltre ad essere datori di lavoro, tenuti quindi all'interno delle loro aziende al rispetto di quanto previsto dall'art. 4 Legge n. 300/1970, sono anche soggetti che nella loro attività d'impresa, sempre più spesso, sono chiamati a fornire indicazioni operative ai propri clienti, relativamente all'attività di fornitura, installazione e collegamento, anche a C.O., di impianti audiovisivi e altri strumenti di controllo.

Al punto "***Istruttoria delle Istanze presentate"*** il provvedimento si occupa della questione relativa alle modalità con le quali i vari uffici periferici dovranno valutare le istanze presentate dai datori di lavoro: l'Ispettorato ribadisce come l'istruttoria dell'Ufficio non dovrà, di norma, comportare valutazioni di natura tecnica circa le strumentazioni che l'azienda vuole installare, ma si dovrà concentrare sulla valutazione **dell'effettiva sussistenza delle ragioni per le quali viene richiesta l'autorizzazione**, che dovranno essere esclusivamente ragioni organizzative produttive, di sicurezza sul lavoro **e di tutela del patrimonio aziendale**. Di particolare interesse risulta l'approfondimento relativo alla nozione di "***Tutela del Patrimonio Aziendale***", che, come è noto, proprio la recente novella legislativa ha introdotto fra le ragioni che possono giustificare l'attività di controllo a distanza dei lavoratori. Nella Circolare si precisa che l'attività valutativa dell'Ufficio si concentrerà sulle condizioni poste all'utilizzo delle strumentazioni utilizzate relativamente alla protezione del patrimonio aziendale circoscrivendosi all'ipotesi in cui la richiesta d'installazione riguarda dispositivi operanti **in presenza del personale aziendale,** mentre chiarisce che "***tale problematica non si pone per le richieste che riguardano dispositivi collegati ad impianti antifurto che tutelano il patrimonio aziendale, in quanto tali dispositivi entrando in funzione soltanto quando in azienda non sono presenti lavoratori, non consentono alcuna forma di controllo incidentale degli stessi e pertanto possono essere autorizzati secondo le modalità di cui alla nota n. 299 del 28 Novembre 2017***" **(doc. 2).**

Altro specifico punto esaminato dalla Circolare è quello relativo alla installazione ed utilizzo di "***Telecamere"***.
L'Ispettorato preliminarmente prende atto del fatto che "*le nuove soluzioni video in tecnologia IP hanno rivoluzionato il concetto di videosorveglianza, rendendo possibili funzioni e scenari applicativi inimmaginabili fino a pochi anni fa, (..) con possibilità di installare impianti di videosorveglianza a circuito chiuso, collegati all'internet aziendale o via internet a postazione remota*".
Mutando un precedente orientamento, ad avviso dell'Ispettorato, se sussistono concrete ragioni giustificatrici dell'attività di controllo, (quali ad esempio la tutela del patrimonio aziendale) **nulla impedisce di inquadrare direttamente l'operatore,** senza introdurre condizioni quali ad esempio "l'angolo di ripresa" della telecamera o "l'oscuramento del volto del lavoratore, né appare indispensabile nell'istanza specificare il posizionamento predeterminato e l'esatto numero delle telecamere da installare, **fermo restando, che le riprese effettuate dovranno essere coerenti e strettamente connesse con le ragioni legittimanti il controllo dichiarate nell'istanza o nello specifico accordo con le organizzazioni sindacali.**

Alla luce dei nuovi scenari sopra delineati, nella circolare si forniscono importanti precisazioni circa il fatto che:

(i) ove sussistano le ragioni giustificatrici del provvedimento è autorizzabile da postazione remota sia la visione delle immagini in tempo reale che registrate;

(ii) l'***accesso da postazione remota delle immagini in tempo reale deve essere autorizzato solo in casi eccezionali debitamente motivati***;

(iii) L'accesso alle immagini registrate sia da remoto che in loco, deve essere necessariamente tracciato anche tramite apposite funzionalità che consentano la conservazione dei "log di accesso" per un congruo periodo non inferiore a sei mesi.

Per quanto riguarda il "perimetro" spaziale di applicazione della disciplina, la Circolare rimanda all'orientamento giurisprudenziale prevalente che tende ad identificare come luoghi soggetti alla normativa in questione anche quelli esterni dove venga svolta attività lavorativa in modo saltuario o occasionale, (quali ad esempio zone di scarico/carico merci) mentre sarebbero da escludere dall'ambito di applicazione della norma, le zone estranee alla pertinenza della ditta, anche se antistanti alle zone d'ingresso dell'azienda.
La Circolare detta poi alcune prescrizioni circa l'utilizzo di dispositivi e tecnologie per la raccolta ed il trattamento dei "**Dati biometrici**". Anche in questo caso l'estensore del provvedimento prende atto del fatto che si tratta di tecnologie il cui utilizzo si sta sempre più diffondendo anche sui luoghi di lavoro, con implicazioni di particolare complessità, riportandosi al Provvedimento generale prescrittivo in tema di biometria emanato dal Garante per la protezione dei dati nel Dicembre del 2014 (doc. 3), secondo il quale "***l'adozione di sistemi biometrici basati sulla elaborazione della impronta digitale o topografia della mano può essere consentita per limitare l'accesso ad aree e locali ritenute "sensibili" in cui è necessario assicurare elevati e specifici livelli di sicurezza*** *(..)".*

Sulla scorta di detto provvedimento l'Ispettorato giunge ad una interessante conclusione, stabilendo che l'installazione di apparecchiature per il riconoscimento biometrico, ad esempio per impedir l'utilizzo di macchine a soggetti non autorizzati, potrebbe essere considerato addirittura uno strumento indispensabile a rendere la prestazione lavorativa, che non necessiterebbe per la sua messa in funzione dell'accordo con le RSA o di provvedimento autorizzativo.

Distinti saluti.

Avv. Giovanni Pollicelli

Allegati:

1.Circolare Ispettorato Nazionale del Lavoro n. 5 del 19 Febbraio 2018 "*Indicazioni operative sull'installazione e utilizzazione di impianti audiovisivi e di altri strumenti di controllo ai sensi dell'art. 4 della Legge 300/1970*";
2.Nota Ispettorato del Lavoro n. 299 del 28 Novembre 2017;
3.Provvedimento generale del Garante per la protezione dei dati personali in tema di biometria (G.U. n. 280 del 2 Dicembre 2014).

Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014

Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014

(Pubblicato sulla Gazzetta Ufficiale n. 280 del 2 dicembre 2014)

Registro dei provvedimenti

n. 513 del 12 novembre 2014

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196, di seguito "Codice");

VISTO il Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, pubblicato in G.U.U.E. 2014 L 257, p. 73 (cd. Regolamento eIDAS);

RILEVATO l'elevato numero di notificazioni presentate al Garante relative al trattamento di dati biometrici;

CONSIDERATO che l'evoluzione delle tecnologie biometriche ha generato una significativa diffusione della loro applicazione e ne è prevedibile una ulteriore espansione per il perseguimento di diverse finalità nei più svariati ambiti della società;

VISTE le richieste di verifica preliminare presentate ai sensi dell'art. 17 del Codice in ordine al trattamento dei dati personali effettuati tramite l'utilizzo di tecniche biometriche;

RITENUTA l'opportunità di rendere disponibile un quadro unitario di misure e accorgimenti di carattere tecnico, organizzativo e procedurale per conformare i trattamenti di dati biometrici alla vigente disciplina sulla protezione dei dati personali e per accrescerne i livelli di sicurezza;

RITENUTO, in ragione della specificità dei dati biometrici, di dovere assoggettare il loro trattamento a un regime generale di obbligatoria comunicazione delle eventuali violazioni;

RITENUTA inoltre l'esigenza di individuare, ai sensi dell'art. 17 del Codice, opportune cautele da porre a garanzia degli interessati in relazione ad alcune tipologie di trattamenti di dati biometrici, anche alla luce delle attuali conoscenze tecniche, che potranno essere effettuate senza richiesta di verifica preliminare rivolta al Garante;

VISTE le osservazioni dell'Ufficio formulate dal Segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE la dott.ssa Augusta Iannini;

1. PREMESSA

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.

2. LINEE-GUIDA IN MATERIA DI RICONOSCIMENTO BIOMETRICO E FIRMA GRAFOMETRICA

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" (allegato "A"), 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.

3. COMUNICAZIONE DI VIOLAZIONE DEI 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 .

4. ESONERO DALLA VERIFICA PRELIMINARE DI CUI ALL'ART. 17 DEL CODICE

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.

In ragione di ciò, qualora si intenda provvedere al trattamento di dati biometrici, è necessario presentare al Garante una richiesta di verifica preliminare, ai sensi dell'art. 17 del Codice.

Sulla base dell'esperienza maturata, però, il Garante ha ritenuto di individuare, con il presente provvedimento, talune tipologie di trattamento volte a scopi di riconoscimento biometrico (nella forma di identificazione biometrica o di verifica biometrica) o di sottoscrizione di documenti informatici (firma grafometrica) che, in considerazione delle specifiche finalità perseguite, della tipologia dei dati trattati e delle misure di sicurezza che possono essere concretamente adottate a loro protezione, presentano un livello di rischio ridotto.

In relazione a tali specifiche tipologie di trattamenti non è quindi necessario per i titolari presentare la predetta istanza, a condizione che vengano adottate tutte le misure e gli accorgimenti tecnici idonei a raggiungere gli obiettivi di sicurezza individuati con il presente provvedimento e siano rispettati i presupposti di legittimità contenuti nel Codice e richiamati nel capitolo 4 delle linee-guida (con particolare riferimento ai principi generali di liceità, finalità, necessità e proporzionalità dei trattamenti, e agli adempimenti giuridici quali l'obbligo di informativa agli interessati e di notificazione al Garante).

Il Garante si riserva di prevedere, alla luce dell'esperienza maturata e dell'evoluzione tecnologica, ulteriori ipotesi di esonero.

Le indicazioni relative al trattamento dei dati biometrici contenute nei precedenti provvedimenti del Garante (si vedano, ad esempio, le linee-¬guida in materia di trattamento di dati personali per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati e pubblici (doc. web n. 1364939 e n. 1417809) continuano ad applicarsi in quanto compatibili con le previsioni del presente provvedimento.

I provvedimenti specifici di verifica preliminare sui quali il Garante ha già espresso le proprie valutazioni non dovranno essere oggetto di ulteriori istanze.

I titolari dei trattamenti biometrici in relazione ai quali è previsto l'esonero dalla verifica preliminare, che abbiano già presentato istanza ex art. 17 del Codice alla data di pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica Italiana, sono tenuti a comunicare al Garante, entro trenta giorni dalla stessa data, la conformità del trattamento alle prescrizioni ivi contenute ovvero la propria intenzione di conformarvisi. La presentazione della comunicazione comporta il non luogo a provvedere sulle relative istanze.

Le istanze di verifica preliminare in relazione alle quali non sia stata presentata la comunicazione di cui al periodo che precede verranno invece valutate dal Garante secondo le ordinarie procedure.

4.1 Autenticazione informatica

Le caratteristiche biometriche possono essere utilizzate come credenziali di autenticazione per l'accesso a banche dati e sistemi informatici, 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. Appartengono a tale ambito, ad esempio, le infrastrutture critiche informatiche di cui al D.M. 9 gennaio 2008 del Ministro dell'interno (G.U. n. 101 del 30 aprile 2008).

In questi casi il presupposto di legittimità, che in ambito pubblico è dato dal perseguimento delle finalità istituzionali del titolare, in ambito privato viene individuato nell'istituto del bilanciamento di interessi (art. 24, comma 1, lettera g), del Codice) per cui, in ragione del legittimo interesse perseguito dal titolare, delle prescrizioni imposte dal presente provvedimento, delle finalità connesse a specifiche esigenze di sicurezza commisurate ai rischi incombenti sui dati o sui sistemi informatici che la procedura di autenticazione è destinata a proteggere, anche tenuto conto delle indicazioni normative in materia di misure minime di sicurezza delle banche dati, il trattamento dei dati biometrici può avvenire senza il consenso degli interessati.

Quindi i titolari sono esonerati dall'obbligo di presentare istanza di verifica preliminare se il trattamento è svolto nel rispetto delle seguenti prescrizioni:

a) Le caratteristiche biometriche consistono nell'impronta digitale o nell'emissione vocale.

b) Nel caso di utilizzo dell'impronta digitale, il dispositivo di acquisizione ha la capacità di rilevare la c.d. vivezza.

c) Nel caso di utilizzo dell'emissione vocale, tale caratteristica è utilizzata esclusivamente in combinazione con altri fattori di autenticazione e con accorgimenti che escludano i rischi di utilizzo fraudolento di eventuali registrazioni della voce (prevedendo, per esempio, la ripetizione da parte dell'interessato di parole o frasi proposte nel corso della procedura di riconoscimento).

d) La cancellazione dei dati biometrici grezzi ha luogo immediatamente dopo la loro trasformazione in campioni o in modelli biometrici.

e) I dispositivi per l'acquisizione iniziale (enrolment) e quelli per l'acquisizione nel corso dell'ordinario funzionamento sono direttamente connessi oppure integrati nei sistemi informatici che li utilizzano, siano essi postazioni di enrolment ovvero postazioni di lavoro o sistemi server protetti con autenticazione biometrica.

f) Le trasmissioni di dati tra i dispositivi di acquisizione e i sistemi informatici sono rese sicure con l'ausilio di tecniche crittografiche caratterizzate dall'utilizzo di chiavi di cifratura di lunghezza adeguata alla dimensione e al ciclo di vita dei dati.

g) Nel caso in cui i riferimenti biometrici siano conservati in modalità sicura su supporti portatili (smart card o analogo dispositivo sicuro) dotati di adeguate capacità crittografiche e certificati per le funzionalità richieste in conformità alla norma tecnica ISO/IEC 15408 o FIPS 140-2 almeno level 3:

i. il supporto è rilasciato in un unico esemplare, è nell'esclusiva disponibilità dell'interessato e, in caso di cessazione dei diritti di accesso ai sistemi informatici, è restituito e distrutto con procedura formalizzata;

ii. l'area di memoria in cui sono conservati i dati biometrici è resa accessibile ai soli lettori autorizzati e protetta da accessi non autorizzati;

iii. i campioni o i riferimenti biometrici sono cifrati con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

h) Nel caso di conservazione del campione o del riferimento biometrico sul sistema informatico protetto con autenticazione biometrica:

i. è assicurata, tramite idonei sistemi di raccolta dei log, la registrazione degli accessi da parte degli amministratori di sistema ai sistemi informatici;

ii. sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifiche della configurazione dei sistemi informatici, se non esplicitamente autorizzati;

iii. i sistemi informatici sono protetti contro l'azione di malware;

iv. sono adottate misure e accorgimenti volti a ridurre i rischi di manomissione e accesso fraudolento al dispositivo di acquisizione;

v. i campioni o i riferimenti biometrici sono cifrati con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati;

vi. i campioni o i riferimenti biometrici sono conservati per il tempo strettamente necessario a realizzare le finalità del sistema biometrico;

vii. i campioni o i riferimenti biometrici sono conservati separatamente dai dati identificativi degli interessati;

viii. sono previsti meccanismi di cancellazione automatica dei dati, cessati gli scopi per i quali sono stati raccolti e trattati.

i) E' esclusa la realizzazione di archivi biometrici centralizzati.

j) E' predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico. Tale relazione è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante.

I titolari dotati di certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) secondo la norma tecnica ISO/IEC 27001 che inseriscono il sistema biometrico nel campo di applicazione della certificazione sono esentati dall'obbligo di redigere la relazione di cui al precedente periodo, potendo

utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico.

4.2 Controllo di accesso fisico ad aree "sensibili" dei soggetti addetti e utilizzo di apparati e macchinari pericolosi

L'adozione di sistemi biometrici basati sull'elaborazione dell'impronta digitale o della topografia della mano può essere consentita per limitare l'accesso ad aree e locali ritenuti "sensibili" in cui è necessario assicurare elevati e specifici livelli di sicurezza oppure per consentire l'utilizzo di apparati e macchinari pericolosi ai soli soggetti qualificati e specificamente addetti alle attività.

Appartengono a tale ambito, in particolare:

• le aree destinate allo svolgimento di attività aventi carattere di particolare segretezza, ovvero prestate da personale selezionato e impiegato in specifiche mansioni che comportano la necessità di trattare informazioni riservate e applicazioni critiche;

• le aree in cui sono conservati oggetti di particolare valore o la cui disponibilità è ristretta a un numero circoscritto di addetti;

• le aree preposte alla realizzazione o al controllo di processi produttivi pericolosi che richiedono un accesso selezionato da parte di personale particolarmente esperto e qualificato;

• l'utilizzo di apparati e macchinari pericolosi, laddove sia richiesta una particolare destrezza onde scongiurare infortuni e danni a cose o persone.

In questi casi il presupposto di legittimità, che in ambito pubblico è dato dal perseguimento delle finalità istituzionali del titolare, in ambito privato viene individuato nell'istituto del bilanciamento di interessi (art. 24, comma 1, lettera g), del Codice) per cui, in ragione del legittimo interesse perseguito dal titolare, delle prescrizioni imposte dal presente provvedimento e delle finalità connesse a specifiche esigenze di sicurezza, il trattamento può avvenire senza il consenso degli interessati.

In relazione a tali finalità, il titolare è esonerato dall'obbligo di presentare istanza di verifica preliminare se il trattamento è svolto nel rispetto delle seguenti prescrizioni:

a) Le caratteristiche biometriche consistono nell'impronta digitale o nella topografia della mano.

b) Nel caso di utilizzo dell'impronta digitale, il dispositivo di acquisizione ha la capacità di rilevare la c.d. vivezza.

c) La cancellazione dei dati biometrici grezzi e dei campioni biometrici ha luogo immediatamente dopo la loro trasformazione in modelli biometrici.

d) I dispositivi per l'acquisizione iniziale e quelli per l'acquisizione nel corso dell'ordinario funzionamento sono direttamente connessi o integrati, rispettivamente, nelle postazioni informatiche di enrolment e nelle postazioni di controllo ai varchi di accesso.

e) Le trasmissioni di dati tra i dispositivi di acquisizione e le postazioni di lavoro o le postazioni di controllo sono rese sicure con l'ausilio di tecniche crittografiche caratterizzate dall'utilizzo di chiavi di cifratura con lunghezza adeguata alla dimensione e al ciclo di vita dei dati.

f) Nel caso di esclusiva conservazione del riferimento biometrico in modalità sicura su supporti portatili (smart card o analogo dispositivo sicuro) dotati di adeguate capacità crittografiche e certificati per le funzionalità richieste in conformità alla norma tecnica ISO/IEC 15408 o FIPS 140-2 almeno level 3:

i. il supporto è rilasciato in un unico esemplare, è nell'esclusiva disponibilità dell'interessato e, in caso di cessazione dei diritti di accesso alle aree sensibili, è restituito e distrutto con procedura formalizzata;

ii. l'area di memoria in cui sono conservati i dati biometrici è accessibile ai soli lettori autorizzati ed è protetta da accessi non autorizzati;

iii. il riferimento biometrico è cifrato con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

g) Nel caso di conservazione del riferimento biometrico su un dispositivo-lettore o una postazione informatica dedicata (controller di varco) dotata di misure di sicurezza di cui alla precedente lettera e):

i. è assicurata la registrazione degli accessi alla postazione da parte degli amministratori di sistema, tramite idonei sistemi di raccolta dei log;

ii. sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione della postazione informatica, se non esplicitamente autorizzati;

iii. i sistemi informatici sono protetti contro l'azione di malware e sono, inoltre, adottati sistemi di firewall per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati;

iv. sono adottate misure e accorgimenti volti a ridurre i rischi di manomissione e accesso fraudolento al dispositivo di acquisizione;

v. il riferimento biometrico è cifrato con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati;

vi. i riferimenti biometrici sono conservati per il tempo strettamente necessario a realizzare le finalità del sistema biometrico;

vii. i riferimenti biometrici sono conservati separatamente dai dati identificativi degli interessati;

viii. sono previsti meccanismi di cancellazione automatica dei dati, cessati gli scopi per i quali sono stati raccolti e trattati.

h) E' esclusa la realizzazione di archivi biometrici centralizzati.

i) E' predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico. Tale relazione tecnica è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante.

I titolari dotati di certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) secondo la norma tecnica ISO/IEC 27001 che inseriscono il sistema biometrico nel campo di applicazione della certificazione sono esentati dall'obbligo di redigere la relazione di cui al precedente periodo, potendo

utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico.

4.3 Uso dell'impronta digitale o della topografia della mano a scopi facilitativi

Le tecniche biometriche possono anche prestarsi a essere utilizzate per consentire, regolare e semplificare l'accesso fisico di utenti ad aree fisiche in ambito pubblico (es. biblioteche) o privato (es. aree aeroportuali riservate) o a servizi.

In questi casi il presupposto di legittimità del trattamento dei dati biometrici è dato dal consenso effettivamente libero degli interessati e dall'utilizzo di sistemi alternativi di accesso non basati su dati biometrici.

Il titolare è esonerato dall'obbligo di presentare istanza di verifica preliminare se il trattamento è svolto nel rispetto delle seguenti prescrizioni:

a) Le caratteristiche biometriche consistono nell'impronta digitale o nella topografia della mano.

b) La cancellazione dei dati biometrici grezzi e dei campioni biometrici ha luogo immediatamente dopo la loro raccolta e trasformazione in modelli biometrici.

c) I dispositivi per l'acquisizione iniziale e quelli per l'acquisizione nel corso dell'ordinario funzionamento sono direttamente connessi o integrati, rispettivamente, nelle postazioni informatiche di enrolment e nelle postazioni di controllo o nei dispositivi di acquisizione.

d) Le trasmissioni di dati tra i dispositivi di acquisizione e le altre componenti del sistema biometrico sono rese sicure con l'ausilio di tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

e) Nel caso di esclusiva conservazione del riferimento biometrico in modalità sicura su supporti portatili (smart card o analogo dispositivo sicuro) dotati di adeguate capacità crittografiche e certificati per le funzionalità richieste in conformità alla norma tecnica ISO/IEC 15408 o FIPS 140-2 almeno level 3:

i. il supporto è rilasciato in un unico esemplare, è nell'esclusiva disponibilità dell'interessato e, in caso di cessazione dei diritti di accesso, è restituito e distrutto con procedura formalizzata;

ii. l'area di memoria in cui sono conservati i riferimenti biometrici è accessibile ai soli lettori autorizzati ed è protetta da accessi non autorizzati;

iii. il riferimento biometrico è cifrato con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

f) Nel caso di conservazione del riferimento biometrico su un dispositivo-lettore o su postazioni informatiche:

i. è assicurata la registrazione degli accessi alla postazione da parte degli amministratori di sistema, tramite idonei sistemi di raccolta dei log;

ii. sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione dei dispositivi o delle postazioni informatiche, se non esplicitamente autorizzati;

iii. sono adottate misure e accorgimenti volti a ridurre i rischi di manomissione e accesso fraudolento al dispositivo di acquisizione;

iv. il riferimento biometrico è cifrato con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati;

v. i riferimenti biometrici sono conservati per il tempo strettamente necessario a realizzare le finalità del sistema biometrico;

vi. i riferimenti biometrici sono conservati separatamente dai dati identificativi degli interessati.

g) E' esclusa la realizzazione di archivi biometrici centralizzati.

h) E' predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico rispetto ai suoi fini facilitativi. Tale relazione tecnica è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante.

I titolari dotati di certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) secondo la norma tecnica ISO/IEC 27001 che inseriscono il sistema biometrico nel campo di applicazione della certificazione sono esentati dall'obbligo di redigere la relazione di cui al precedente periodo, potendo utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico.

4.4 Sottoscrizione di documenti informatici

Il trattamento di dati biometrici costituiti da informazioni dinamiche associate all'apposizione a mano libera di una firma autografa avvalendosi di specifici dispositivi hardware è ammesso in assenza di verifica preliminare laddove si utilizzino sistemi di firma grafometrica posti a base di una soluzione di firma elettronica avanzata, così come definita dal Decreto Legislativo 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale" che non prevedono la conservazione centralizzata di dati biometrici.

L'utilizzo di tali sistemi, da un lato, si giustifica al fine di contrastare eventuali tentativi di frode e il fenomeno dei furti di identità e, dall'altro, ha lo scopo di rafforzare le garanzie di autenticità e integrità dei documenti informatici sottoscritti, anche in vista di eventuale contenzioso legato al disconoscimento della sottoscrizione apposta su atti e documenti di tipo negoziale in sede giudiziaria.

In tali casi, il presupposto di legittimità del trattamento dei dati biometrici è dato dal consenso, effettivamente libero degli interessati ovvero, in ambito pubblico, dal perseguimento delle finalità istituzionali del titolare. Il consenso è espresso dall'interessato all'atto di adesione al servizio di firma grafometrica e ha validità, fino alla sua eventuale revoca, per tutti i documenti da sottoscrivere.

Il titolare è esonerato dall'obbligo di presentare istanza di verifica preliminare se il trattamento è svolto nel rispetto delle seguenti prescrizioni e limitazioni:

a) Il procedimento di firma è abilitato previa identificazione del firmatario.

b) Sono resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione, che non comportino l'utilizzo di dati biometrici.

c) La cancellazione dei dati biometrici grezzi e dei campioni biometrici ha luogo immediatamente dopo il completamento della procedura di sottoscrizione, e nessun dato biometrico persiste all'esterno del documento informatico sottoscritto.

d) I dati biometrici e grafometrici non sono conservati, neanche per periodi limitati, sui dispositivi hardware utilizzati per la raccolta, venendo memorizzati all'interno dei documenti informatici sottoscritti in forma cifrata tramite sistemi di crittografia a chiave pubblica con dimensione della chiave adeguata alla dimensione e al ciclo di vita dei dati e certificato digitale emesso da un certificatore accreditato ai sensi dell'art. 29 del Codice dell'amministrazione digitale. La corrispondente chiave privata è nella esclusiva disponibilità di un soggetto terzo fiduciario che fornisca idonee garanzie di indipendenza e sicurezza nella conservazione della medesima chiave. La chiave può essere frazionata tra più soggetti ai fini di sicurezza e integrità del dato. In nessun caso il soggetto che eroga il servizio di firma grafometrica può conservare in modo completo tale chiave privata. Le modalità di generazione, consegna e conservazione delle chiavi sono dettagliate nell'informativa resa agli interessati e nella relazione di cui alla lettera k) del presente paragrafo, in conformità con quanto previsto all'art. 57, comma 1 lettere e) ed f) del d.P.C.M. 22 febbraio 2013.

e) La trasmissione dei dati biometrici tra sistemi hardware di acquisizione, postazioni informatiche e server avviene esclusivamente tramite canali di comunicazione resi sicuri con l'ausilio di tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

f) Sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione delle postazioni informatiche e dei dispositivi, se non esplicitamente autorizzati.

g) I sistemi informatici sono protetti contro l'azione di malware e sono, inoltre, adottati sistemi di firewall per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati.

h) Nel caso di utilizzo di sistemi di firma grafometrica nello scenario mobile o BYOD (Bring Your Own Device), sono adottati idonei sistemi di gestione delle applicazioni o dei dispositivi mobili, con il ricorso a strumenti MDM (Mobile Device Management) o MAM (Mobile Application Management) o altri equivalenti al fine di isolare l'area di memoria dedicata all'applicazione biometrica, ridurre i rischi di installazione abusiva di software anche nel caso di modifica della configurazione dei dispositivi e contrastare l'azione di eventuali agenti malevoli (malware).

i) I sistemi di gestione impiegati nei trattamenti grafometrici adottano certificazioni digitali e policy di sicurezza che disciplinino, sulla base di criteri predeterminati, le condizioni di loro utilizzo sicuro (in particolare, rendendo disponibili funzionalità di remote wiping applicabili nei casi di smarrimento o sottrazione dei dispositivi).

j) L'accesso al modello grafometrico cifrato avviene esclusivamente tramite l'utilizzo della chiave privata detenuta dal soggetto terzo fiduciario, o da più soggetti, in caso di frazionamento della chiave stessa, e nei soli casi in cui si renda indispensabile per l'insorgenza di un contenzioso sull'autenticità della firma e a seguito di richiesta dell'autorità giudiziaria. Le condizioni e le modalità di accesso alla firma grafometrica da parte del soggetto terzo di fiducia o da parte di tecnici qualificati sono dettagliate nell'informativa resa agli interessati e nella relazione di cui alla lettera k) del presente paragrafo, in conformità con quanto previsto all'art. 57, comma 1, lettere e) ed f) del d.P.C.M. 22 febbraio 2013.

k) E' predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico rispetto alle finalità. Tale relazione tecnica è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante.

I titolari dotati di certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) secondo la norma tecnica ISO/IEC 27001 che inseriscono il sistema biometrico nel campo di applicazione della certificazione sono esentati dall'obbligo di redigere la relazione di cui al precedente periodo, potendo utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico.

TUTTO CIÒ PREMESSO IL GARANTE

1. adotta ai sensi dell'art. 154, comma 1, lettera h) del Codice l'allegato "A", recante le "Linee-guida in materia di riconoscimento biometrico e firma grafometrica", che forma parte integrante della presente deliberazione, al fine di informare i titolari di trattamento, i produttori di tecnologie biometriche, i fornitori di servizi e gli interessati sui diversi aspetti connessi alla protezione dei dati personali, ivi compresi quelli relativi alla sicurezza, e sui presupposti di legittimità dei trattamenti dei dati biometrici;

2. prescrive, ai sensi dell'art. 154, comma 1, lettera c) del Codice, che i titolari di trattamenti biometrici comunichino al Garante, entro ventiquattro ore dalla conoscenza del fatto, le violazioni dei dati biometrici secondo le modalità di cui al paragrafo 3;

3. individua, nei termini di cui al paragrafo 4, i casi di esonero dalla presentazione di istanza di verifica preliminare, e prescrive ai soggetti che intendano procedere in qualità di titolari a tali trattamenti, ai sensi dell'art. 17 del Codice, di adottare le misure e gli accorgimenti tecnici, organizzativi e procedurali descritti nel medesimo paragrafo, nonché di rispettare i presupposti di legittimità e le indicazioni contenute nelle allegate linee-guida con particolare riferimento al capitolo 4 "Principi generali e adempimenti giuridici";

4. prescrive ai titolari di trattamenti biometrici che non abbiano richiesto la verifica preliminare al Garante:

a. di adottare – entro centottanta giorni dalla pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica Italiana – le misure e gli accorgimenti di cui al paragrafo 4, qualora i trattamenti siano compresi nei casi di esonero dall'obbligo di verifica preliminare;

ovvero

b. di sospendere – entro il medesimo termine – i trattamenti e di sottoporre gli stessi a verifica preliminare, con interpello al Garante ai sensi dell'art. 17 del Codice;

5. invita i titolari dei trattamenti biometrici compresi nei casi di esonero dall'obbligo di verifica preliminare, i quali abbiano già presentato istanza, tuttora pendente, ex art. 17 del Codice, a comunicare al Garante – entro trenta giorni dalla pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica Italiana – la conformità del trattamento alle prescrizioni ivi contenute ovvero la propria intenzione di conformarvisi. La presentazione della comunicazione comporta il non luogo a provvedere sulle relative istanze. Le istanze di verifica preliminare in relazione alle quali non sia stata presentata la comunicazione di cui al periodo che precede verranno valutate dal Garante secondo le ordinarie procedure;

6. dispone, ai sensi dell'art. 143, comma 2, del Codice, che copia del presente provvedimento sia trasmessa al Ministero della giustizia – Ufficio pubblicazione leggi e decreti – per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica Italiana.

Roma, 12 novembre 2014

IL PRESIDENTE

Soro

IL RELATORE

Iannini

IL SEGRETARIO GENERALE

Soro

Rettifica alla Deliberazione n. 513 del 12 novembre 2014 recante 'Provvedimento generale prescrittivo in tema di biometria' - 15 gennaio 2015

(Pubblicato sulla Gazzetta Ufficiale n. 34 dell'11 febbraio 2015)

Registro dei provvedimenti

n. 16 del 15 gennaio 2015

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della prof.ssa Licia Califano e della dott.ssa Giovanna Bianchi Clerici, componenti e del dott. Giuseppe Busia, segretario generale;

VISTO il d.lgs. 30 giugno 2003, 196 (Codice in materia di protezione dei dati personali);

VISTA la deliberazione n. 513 del 12 novembre 2014 del Garante per la protezione dei dati personali, pubblicata nella Gazzetta Ufficiale della Repubblica italiana – serie generale – n. 280 del 2 dicembre 2014 recante "Provvedimento generale prescrittivo in tema di biometria";

CONSIDERATO che in fase di redazione del testo per mero errore materiale sono state richiamate in modo non corretto talune norme tecniche;

RITENUTO pertanto necessario apportare le dovute correzioni alla citata deliberazione;

VISTE le osservazioni formulate dal Segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE la dott.ssa Augusta Iannini;

TUTTO CIO' PREMESSO, IL GARANTE:

dispone la correzione degli errori materiali contenuti nella citata deliberazione n. 513 del 12 novembre 2014 nei termini di seguito indicati:

1) ovunque si leggano nel testo le parole: "… alla norma tecnica UNI CEI ISO/IEC 15408…" devono intendersi correttamente riportate le parole: "… alla norma tecnica ISO/IEC 15408 …";

2) ovunque si leggano nel testo le parole: "… secondo la norma tecnica UNI CEI ISO/IEC 27001:2005 e successive modificazioni …" devono intendersi correttamente riportate le parole: "… secondo la norma tecnica ISO/IEC 27001 …".

La presente deliberazione è pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 15 gennaio 2015

IL PRESIDENTE

Soro

IL RELATORE

Iannini

IL SEGRETARIO GENERALE

Busia

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

ENGLISH VERSION

LINEE-GUIDA IN MATERIA DI RICONOSCIMENTO BIOMETRICO E FIRMA GRAFOMETRICA

Allegato A al Provvedimento del Garante del 12 novembre 2014

SOMMARIO

1. PREMESSA

L'utilizzo di dispositivi e tecnologie per la raccolta e il trattamento di dati biometrici sta andando incontro a crescente diffusione, in particolare per l'accertamento dell'identità personale, per accedere a servizi digitali e sistemi informativi, per il controllo degli accessi a locali e aree, per l'apertura di serrature elettromeccaniche, per l'attivazione di dispositivi elettronici anche di uso personale o di macchinari, per la sottoscrizione di documenti informatici.

La diffusione dell'utilizzo di dati biometrici 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 le autorità degli Stati membri dell'Unione europea.

In ambito nazionale, il Garante è intervenuto più volte, su interpello di titolari di trattamento ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice"), con propri provvedimenti di verifica preliminare che hanno in alcuni casi vietato e in altri ammesso, pur nel rispetto di prescrizioni di natura tecnica od organizzativa, i trattamenti prefigurati.

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". Rientrando, quindi, nell'ambito di applicazione del Codice (art. 4, comma 1, lett. b), le operazioni su di essi compiute con strumenti elettronici sono a tutti gli effetti trattamento di dati personali.

Nell'attuale contesto di rapida evoluzione tecnologica, con crescente disponibilità commerciale e diffusione dell'uso di dispositivi biometrici, anche incorporati in prodotti di largo consumo, il Garante intende definire, tramite le presenti linee-guida e sulla base della pregressa esperienza, un quadro unitario di misure e accorgimenti di carattere tecnico, organizzativo e procedurale per accrescere i livelli di sicurezza dei trattamenti biometrici e per conformarli alla vigente disciplina della protezione dei dati personali.

Saranno oggetto di esame i trattamenti svolti da soggetti pubblici e privati per finalità di riconoscimento biometrico o di sottoscrizione di documenti informatici, restando esclusi quelli svolti per finalità di pubblica sicurezza, di giustizia e di ricerca scientifica.

2. DEFINIZIONI

Pur non esistendo, allo stato, una definizione normativa concernente i "dati biometrici", questi 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*"[1].

Per esigenze di armonizzazione dei termini usati in un contesto caratterizzato da notevole tecnicismo, si ritiene tuttavia necessario utilizzare le definizioni fornite dallo standard internazionale ISO/IEC 2382-37 *"Information technology — Vocabulary — Part 37: Biometrics"*.

Sono di seguito riportati i principali termini utilizzati:

- **caratteristica biometrica**: caratteristica biologica o comportamentale di un individuo da cui possono essere estratti in modo ripetibile dei **tratti biometrici** (*biometric features*) distintivi e idonei al **riconoscimento biometrico**;
- **riconoscimento biometrico**: si intende il riconoscimento di individui basato su loro caratteristiche biologiche o comportamentali, includendo in tale accezione le nozioni di **verifica biometrica** e di **identificazione biometrica**;
- **verifica biometrica**: confronto tra un modello biometrico acquisito nel momento in cui l'interessato interagisce con il sistema biometrico e un modello biometrico previamente memorizzato e (presuntivamente) a lui corrispondente; questo tipo di verifica è detta **confronto uno a uno** (*one-to-one comparison*);
- **enrolment:** iscrizione in un sistema, nel caso in oggetto, in un sistema biometrico. La fase di *enrolment* va dall'acquisizione del campione biometrico alla sua memorizzazione, all'estrazione dei tratti fino alla generazione del riferimento biometrico da archiviare per i confronti successivi;
- **identificazione biometrica**: ricerca in un archivio, per confronto biometrico, di uno o più modelli biometrici corrispondenti al dato acquisito. Questo tipo di operazione è detta anche **confronto uno a molti** (*one-to-many comparison*) e non prevede una fase assertiva;
- **tratto biometrico** (*biometric feature*): informazione estratta da un campione biometrico a fini di confronto;
- **campione biometrico** (*biometric sample*): rappresentazione analogica o digitale di una caratteristica biometrica ottenuta al termine del processo di acquisizione (*biometric capture* e *biometric acquisition)* costituita, per esempio, dalla riproduzione dell'immagine di un polpastrello;
- **confronto biometrico** (*biometric comparison*): confronto, usualmente basato su metodi statistici e metriche tipiche del contesto tecnologico e del sistema biometrico

[1] V. Gruppo per la tutela dei dati personali Articolo 29 costituito da rappresentanti delle Autorità di protezione dati dei diversi stati membri, Parere 3/2012 sugli sviluppi nelle tecnologie biometriche, WP193, adottato il 27 aprile 2012.

prescelto, fra dati biometrici con l'obiettivo di stabilirne il grado di somiglianza o di dissomiglianza;

- **modello biometrico** (*biometric template*): insieme di tratti biometrici memorizzati informaticamente e direttamente confrontabile con altri modelli biometrici;
- **istanza biometrica** (*biometric probe)*[2]: modello biometrico generato ogni volta che l'interessato interagisce con il sistema biometrico;
- **riferimento biometrico** (*biometric reference*): modello biometrico utilizzato come termine di confronto e registrato in modo persistente e invariabile nel tempo (a meno di aggiornamenti resi necessari dalle variazioni anche naturali della caratteristica biometrica da cui è estratto).

Per semplicità, nelle presenti linee guida, si farà riferimento a **modelli biometrici** anche nei casi in cui si dovrebbe utilizzare, rispettivamente, **riferimento biometrico** o **istanza biometrica**, mentre con il termine generico di "dati biometrici" ci si riferirà a campioni, modelli, riferimenti, tratti e ad ogni altro dato ricavato con procedimento informatico dalle caratteristiche biometriche degli interessati.

[2] Dal punto di vista tecnico-informatico, il *biometric reference* e il *biometric probe* possono coincidere del tutto, differenziandosi soltanto per il momento del loro uso e per la circostanza che i *biometric reference* vengono acquisiti e memorizzati in modo persistente, mentre i *biometric probe* sono generati ogni volta che l'interessato interagisce con il sistema biometrico, potendo quindi essere soggetti a lievi differenziazioni sulla base delle condizioni di loro acquisizione.

3. PRINCIPALI CARATTERISTICHE BIOMETRICHE E LORO PROPRIETÀ

Alcune proprietà delle caratteristiche, dei dati e delle tecniche biometriche consentono di effettuare classificazioni di carattere generale che si propongono qui di seguito in quanto funzionali a una valutazione dei loro aspetti di protezione dei dati personali.

Sistemi biometrici interattivi e sistemi biometrici passivi

I sistemi biometrici sono detti interattivi o partecipativi laddove prevedono la cooperazione dell'interessato e richiedono la sua consapevole partecipazione durante la fase di raccolta del dato biometrico (si pensi, ad esempio, alla scansione della retina o all'apposizione della firma autografa). I sistemi biometrici passivi, invece, raccolgono il dato biometrico senza che l'interessato ne abbia piena percezione o consapevolezza (si pensi, ad esempio, all'acquisizione delle immagini del volto o alla registrazione della voce senza che l'interessato ne sia a conoscenza).

Caratteristiche biometriche biologiche e comportamentali

Altra distinzione praticabile è quella tra caratteristiche biometriche biologiche, legate a tratti fisici, biochimici, morfologici o fisiologici, e caratteristiche biometriche comportamentali legate ad azioni e atteggiamenti dell'individuo, quali, a esempio, la dinamica di apposizione della firma, il tipo di andatura o anche, per alcuni aspetti, l'emissione della voce.

Caratteristiche biometriche traccianti e non traccianti

Alcune caratteristiche biometriche lasciano tracce nell'ambiente rispetto ad altre (*traceless)* che non ne lasciano. Una caratteristica biometrica che può lasciare tracce sugli oggetti è l'impronta digitale così come le fattezze del volto che possono essere rilevate all'insaputa dell'interessato. Esempi di caratteristiche biometriche del secondo tipo sono la topografia della mano e la struttura venosa del dito.

Altre proprietà

Le caratteristiche biometriche sono connotate, seppure in modo diversificato, da univocità (cioè capacità distintiva per ogni persona) e universalità (presenza in ogni individuo), e sono tendenzialmente dotate di una certa stabilità temporale. Tuttavia, sono soggette a decadimento per cause naturali, ad alterazioni accidentali o a lesioni che possono incidere sull'operatività dei sistemi biometrici.

Di seguito sono brevemente descritte le principali caratteristiche utilizzate in sistemi biometrici, evidenziandone la modalità di rilevazione (interattiva o passiva), l'eventuale suscettibilità alla dispersione di tracce nell'ambiente, la possibilità di ricavarne dati sensibili e il loro grado di stabilità nel tempo.

3.1. Impronte digitali

Il trattamento biometrico delle impronte digitali prevede il rilevamento, tramite dispositivi di acquisizione ottica, di un campione biometrico che riproduca la disposizione delle *creste di Galton* e delle valli cutanee presenti sui polpastrelli delle dita fin dalla fase prenatale.

Le *minutiae* dell'impronta, ovvero i suoi tratti biometrici, sono costituite da vortici, biforcazioni, creste, valli e terminazioni, e la loro individuazione nel campione biometrico acquisito consente di ottenere un modello biometrico che fornisca una rappresentazione sintetica numerica dell'impronta di partenza e che si presti alla realizzazione di efficienti algoritmi di confronto.

L'univocità del modello in una base dati biometrica non è garantita poiché, soprattutto in grandi archivi dattiloscopici, a più di una impronta può corrispondere un medesimo modello; l'utilizzo di una rappresentazione sintetica della caratteristica biometrica consente comunque di effettuare in modo molto efficiente delle ricerche automatizzate, in cui il modello biometrico svolge la funzione di indice per la ricerca di corrispondenze in un *data base*.

Queste capacità di indicizzazione sono alla base del funzionamento dei moderni sistemi di riconoscimento automatico delle impronte digitali (*Automatic Fingerprint Identification Systems – AFIS*) utilizzati su scala globale, in particolare dalle forze di polizia e da agenzie investigative.

Le impronte digitali lasciano tracce, e possono, in alcuni casi, fornire indicazioni sui dati sensibili dell'interessato (secondo alcuni studi le impronte digitali possono consentire di individuare l'etnia del soggetto cui appartengono), sono tendenzialmente stabili nell'individuo adulto e hanno un elevato grado di unicità nella popolazione, differendo perfino tra gemelli omozigoti: queste ultime proprietà, in particolare, le hanno rese spesso utilizzate per finalità giudiziarie e di polizia.

La rilevazione dell'impronta digitale in un sistema biometrico è solitamente effettuata con la partecipazione attiva dell'interessato, tuttavia è possibile acquisire impronte apposte da una persona su oggetti e farne, almeno in linea teorica, uso in un sistema biometrico.

3.2. Dinamica di apposizione della firma autografa

Le caratteristiche dinamiche della firma autografa appartengono al novero delle caratteristiche biometriche comportamentali, e vengono acquisite tramite speciali tavolette di acquisizione (*tablet grafometrici*), o anche su dispositivi *tablet* di uso generale equipaggiati con opportuni sensori e programmi *software*. I dispositivi di acquisizione utilizzati sono in grado di elaborare, oltre che il tratto grafico, anche una serie di parametri dinamici associati all'atto della firma (velocità di tracciamento, accelerazione, pressione, inclinazione, *salti in volo* …).

L'acquisizione delle caratteristiche dinamiche di firma può essere funzionale a procedure di riconoscimento biometrico, anche se presenta tassi elevati di *falsi negativi* (risultati erronei di mancato riconoscimento) che possono rendere tali procedure poco efficienti e imprecise al di fuori di contesti particolari in cui sia possibile sopperire con intervento

umano agli inevitabili errori di riconoscimento; il suo uso più frequente è invece la cosiddetta firma grafometrica.

Tale caratteristica comportamentale non lascia traccia e non ha elevata stabilità nel tempo.

La sua rilevazione deve essere effettuata con la partecipazione attiva dell'interessato.

3.3. Caratteristiche dell'emissione vocale

L'evoluzione delle tecniche *hardware* e *software* di elaborazione dei segnali consente oggi di eseguire analisi dell'emissione vocale in modo sufficientemente efficiente da prestarsi a operazioni di riconoscimento biometrico dell'individuo (*speaker recognition*) effettuate tramite interlocuzione telefonica tradizionale, o via Internet, oppure su scala locale interagendo con un dispositivo connesso o integrato in un *personal computer* o altro dispositivo informatico.

Le caratteristiche dell'emissione della voce sono, infatti, strettamente legate all'anatomia del tratto vocale, alla sua lunghezza, alle risonanze, alla morfologia della bocca e delle cavità nasali.

Il riconoscimento dell'individuo viene usualmente realizzato non solo tramite l'elaborazione e l'analisi dei segnali vocali (*signal processing*), ma anche tramite procedure di *sfida* dipendenti dalle modalità con le quali l'interessato viene invitato a ripetere delle frasi, nomi o numeri (c.d. *sfida*).

E' possibile realizzare il riconoscimento anche senza sfida, nel caso in cui l'interessato è invitato a parlare senza uno schema prefissato.

Normalmente il riconoscimento biometrico consiste in una verifica d'identità (confronto *uno a uno*), in cui è previsto che venga comunque fornita dall'utente un'informazione aggiuntiva nella sua disponibilità cognitiva (codice identificativo, codice utente…) o a lui associata (identificativo della linea telefonica chiamante).

Il segnale vocale, opportunamente elaborato per costruire e registrare un modello biometrico della voce, è successivamente utilizzato per il confronto con il modello acquisito in fase di *enrolment* al sistema, corrispondente alle informazioni aggiuntive fornite dall'utente.

Tale caratteristica può lasciare traccia e la sua rilevazione può essere effettuata senza la partecipazione attiva dell'interessato e senza l'uso di sensori specializzati (essendo sufficiente in molti casi un normale microfono anche telefonico).

3.4. Struttura venosa delle dita o della mano

Le caratteristiche della rete venosa delle dita e della mano si sviluppano antecedentemente alla nascita.

La loro acquisizione avviene tramite sensori che rilevano la forma e la disposizione delle vene delle dita, del dorso o del palmo della mano utilizzando una sorgente luminosa a lunghezza d'onda prossima all'infrarosso.

Rispetto ad altri sistemi, non è richiesto il contatto del corpo con la superficie del sensore, rendendo così il procedimento maggiormente accettato dagli utilizzatori. L'uso di tale caratteristica, allo stato, non trova un grande favore da parte di chi realizza sistemi biometrici.

I sistemi biometrici che utilizzano questa caratteristica hanno un'accuratezza elevata, in genere superiore a quelli basati sulle impronte digitali, e sono adatti sia per l'identificazione sia per la verifica biometrica.

Tale caratteristica non lascia traccia, non fornisce indicazioni su dati sensibili e ha un'elevata stabilità nel tempo.

La sua rilevazione deve essere effettuata con la partecipazione attiva dell'interessato.

3.5. Struttura vascolare della retina

Le tecniche biometriche basate sul rilevamento della struttura vascolare della retina prevedono l'utilizzo di un fascio di luce a infrarosso a bassa intensità che illumini la parte posteriore dell'occhio. I sistemi che si basano su di essa sono soggetti a possibili malfunzionamenti nel caso siano presenti patologie oculari.

La scansione della retina è solitamente usata in ambiti che richiedono un livello di sicurezza particolarmente elevato: non sono, infatti, noti meccanismi efficaci per replicare la struttura vascolare della retina e non è possibile utilizzare tessuti di persone decedute, poiché il sensore rileva la circolazione sanguigna.

Tale caratteristica biologica non lascia traccia, è altamente distintiva dell'individuo e ha elevata stabilità nel tempo.

La sua rilevazione deve essere effettuata con la partecipazione attiva dell'interessato.

3.6. Forma dell'iride

Il procedimento di lettura dell'iride è una tecnica biometrica che consente la rilevazione della forma della pupilla e della parte anteriore dell'occhio mediante immagini ad alta risoluzione.

Si tratta di un procedimento di elevata accuratezza e velocità di comparazione.

Il tasso di falsi positivi è piuttosto basso rispetto ad altre caratteristiche biometriche, anche se si segnalano tassi elevati di falsi negativi che comporterebbero il mancato riconoscimento dell'individuo da parte del sistema.

Tale caratteristica biologica non lascia traccia, è altamente distintiva dell'individuo (differisce tra gli occhi di una stessa persona) e ha elevata stabilità nel tempo.

La sua rilevazione può essere effettuata senza la partecipazione attiva dell'interessato, anche se i sensori più utilizzati prevedono una partecipazione attiva all'atto del rilevamento.

3.7. Topografia della mano

Le tecniche biometriche basate sulla topografia della mano consistono nella rilevazione delle proprietà geometriche dell'arto (bidimensionali o tridimensionali), acquisite mediante un apposito dispositivo di ripresa che coglie determinate caratteristiche quali la forma, la larghezza e lunghezza delle dita, la posizione e la forma delle nocche o del palmo della mano.

Le caratteristiche della mano di un individuo non sono descrittive al punto da risultare uniche, per cui non sono adatte ad essere utilizzate nell'identificazione biometrica tra un numero ampio di persone ma, nel contempo, sono sufficientemente descrittive per essere impiegate efficacemente ai fini della verifica biometrica.

Il costo dei sensori è mediamente più elevato rispetto ai sensori per altre caratteristiche e l'ingombro è tale da richiedere adeguato spazio per l'installazione e da non renderli integrabili in altri dispositivi o utilizzabili nel contesto mobile.

Tale caratteristica non lascia traccia, può fornire indicazioni sullo stato di salute (potendo svelare la presenza di patologie degenerative o di altra natura) e non ha elevata stabilità nel tempo.

La sua rilevazione deve essere effettuata con la partecipazione attiva dell'interessato.

3.8. Caratteristiche del volto

Il riconoscimento automatico di un individuo tramite l'analisi delle sue sembianze facciali è un procedimento complesso che utilizza immagini video in luce visibile o "termiche" a infrarosso.

I confronti biometrici sono resi complicati dalla presenza di capigliatura, di occhiali e dalla posizione assunta dalla testa durante la ripresa, nonché dalle condizioni di illuminazione.

Le stesse tecniche basate su riprese a infrarosso non sono invece influenzate dall'illuminazione e sono efficaci anche al buio.

Possono essere ottenute anche immagini di tipo tridimensionale, per fusione di più immagini o con tecniche di *computer graphics* basate sull'elaborazione dell'ombreggiatura.

Dal campione biometrico facciale tramite algoritmi, talvolta basati sulle c.d. reti neurali, vengono estratti un certo numero di tratti, quali la posizione degli occhi, del naso, delle narici, del mento, delle orecchie, al fine di costruire un modello biometrico.

Laddove il procedimento avvenga in un contesto cooperativo il riconoscimento facciale può essere molto accurato, al punto da poter essere utilizzato in funzione di controllo di accesso logico o fisico.

Le fattezze del volto possono lasciare tracce, potendo essere acquisite automaticamente, per esempio, da sistemi di videosorveglianza, e possono fornire indicazioni sui dati sensibili. Esse mantengono elevata stabilità nel tempo e la loro rilevazione può essere effettuata anche senza la partecipazione attiva dell'interessato

4. PRINCIPI GENERALI E ADEMPIMENTI GIURIDICI

Il trattamento dei dati biometrici si deve svolgere in conformità alle disposizioni del Codice, e a condizione che non si determini un'ingerenza ingiustificata e sproporzionata nei confronti degli interessati.

4.1. Liceità

In via prioritaria, occorre verificare che i dati biometrici siano trattati tenendo presenti i diversi presupposti di liceità stabiliti dal Codice in ragione della natura del titolare del trattamento, fermo restando gli ulteriori ed eventuali obblighi di legge e provvedimenti prescrittivi del Garante.

In ambito pubblico, il trattamento dei dati personali è consentito unicamente per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dal Codice in relazione alla specifica tipologia di dati utilizzati, nonché dalla legge e dai regolamenti (artt. 18 e ss.); in tali casi, i soggetti pubblici non operano in base al consenso dell'interessato, a differenza dei soggetti privati ed enti pubblici economici.

Questi ultimi, prima di iniziare il trattamento, devono, di regola, acquisire il consenso informato dell'interessato, che è sempre revocabile e deve essere manifestato in forma libera ed espressa, ossia deve essere scevro da eventuali pressioni o condizionamenti, fermi restando i casi in cui si è in presenza di uno dei presupposti equipollenti (artt. 23 e 24 del Codice). In particolare, il consenso non è richiesto nei casi in cui il Garante, con proprio specifico provvedimento, abbia già operato un cd. bilanciamento di interessi ed abbia ritenuto prevalente il perseguimento di un legittimo interesse del titolare, come in alcune delle ipotesi per le quali l'Autorità ha ritenuto non essere necessaria la richiesta di verifica preliminare ai sensi dell'art. 17 del Codice (es. controllo di accesso fisico ad aree "sensibili" e controllo dell'identità per l'utilizzo di apparati e macchinari pericolosi; v. al riguardo provvedimento generale contestuale all'adozione delle presenti Linee guida).

4.2. Necessità

I sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi. Prima di procedere all'utilizzo di un sistema biometrico, pertanto, occorre valutare se le stesse finalità possano essere perseguite mediante dati anonimi oppure tramite il sistema biometrico ma con modalità tali da permettere l'individuazione dell'interessato solo in caso di necessità (art. 3 del Codice).

In tale quadro, i sistemi biometrici devono essere predisposti, laddove tecnicamente possibile in coerenza con la finalità perseguita, in modo da cancellare immediatamente, e possibilmente in modo automatico, i dati biometrici e le informazioni a essi correlate in caso di cessazione del trattamento, ferme restando eventuali disposizioni che prevedano una disciplina differente per casi specifici.

4.3. Finalità

I dati oggetto di trattamento per mezzo di sistemi biometrici devono essere raccolti in maniera accurata e trattati per le sole finalità che il titolare intende legittimamente

perseguire, previamente indicate nell'informativa che verrà resa agli interessati, e non possono essere utilizzati in altre operazioni di trattamento che siano con queste incompatibili (art. 11, comma 1, lett. *a*, *b*, *c* ed *e*, del Codice).

In base a tale principio, ad esempio, se la finalità perseguita nel caso concreto è quella di garantire la sicurezza di persone o beni, potrebbero essere utilizzati sistemi biometrici per controllare l'accesso, da parte dei soli dipendenti autorizzati, a luoghi particolarmente pericolosi; gli stessi dati, tuttavia, non possono essere utilizzati a diversi fini come, per esempio, la verifica del rispetto dell'orario di lavoro dei dipendenti.

E ancora, si potrebbero utilizzare dati biometrici per identificare, senza margine di dubbio e in modo da escludere (o ridurre) ipotesi di frode, un soggetto che voglia effettuare operazioni bancarie, ma senza che dagli stessi dati si possano desumere altre informazioni per verificare anche l'accesso in banca del cliente.

4.4. Proporzionalità

Possono essere trattati i soli dati pertinenti e non eccedenti in relazione alle finalità perseguite (art. 11, comma 1, lett. *d*, del Codice).

Pertanto, il sistema di rilevazione deve essere configurato in modo tale da raccogliere un numero circoscritto di informazioni (principio di minimizzazione), escludendo l'acquisizione di dati ultronei rispetto a quelli necessari per la finalità perseguita nel caso concreto: ad esempio, se la finalità è quella dell'autenticazione informatica, i dati biometrici non devono essere trattati in modo da poter desumere anche informazioni di natura sensibile dell'interessato.

Occorre evitare, se non per motivate ed eccezionali esigenze, di ricorrere a sistemi che impieghino più di una caratteristica biometrica dell'interessato.

4.5. Adempimenti giuridici

Nel caso in cui, alla luce dei principi generali precedentemente illustrati, la valutazione abbia avuto esito positivo, il titolare deve porre in essere i seguenti adempimenti richiesti dal Codice.

4.5.1. Informativa

Prima dell'inizio del trattamento (cioè antecedentemente alla fase di *enrolment*, laddove prevista), il titolare deve fornire agli interessati un'informativa idonea e specifica relativa all'utilizzo dei dati biometrici. Nell'informativa, contenente tutti gli elementi previsti dall'art. 13 del Codice, occorre puntualizzare, in particolare, la finalità perseguita e la modalità del trattamento (anche enunciando, sia pure sinteticamente, le cautele adottate, i tempi di conservazione dei dati, l'eventuale loro centralizzazione).

L'informativa deve dare adeguata rilevanza alla natura obbligatoria o facoltativa del conferimento dei dati rispetto al perseguimento delle finalità del trattamento. Laddove sia previsto un sistema alternativo ovvero gli interessati non vogliano o non possano, anche in ragione di proprie caratteristiche fisiche, servirsi del sistema di riconoscimento biometrico, oppure successivamente decidano di non usufruirne più, nell'informativa deve

essere precisata anche la facoltà di utilizzare modalità diverse per avvalersi comunque del servizio nel cui ambito è prevista una procedura biometrica. Nel caso in cui il dato biometrico sia registrato in un dispositivo posto nell'esclusiva disponibilità dell'interessato, l'informativa dovrà fornire adeguate istruzioni sulla sua corretta custodia e sugli adempimenti connessi ad un eventuale suo smarrimento, sottrazione, malfunzionamento.

Nel caso in cui i sistemi utilizzati in determinate sedi siano potenzialmente idonei al rilevamento di dati biometrici dell'interessato senza la sua cooperazione (come può avvenire in alcuni casi di riconoscimento facciale, vocale o comportamentale), occorre informare gli interessati dando loro la possibilità di scelta relativamente all'accesso a una zona soggetta a tale tipo di controlli biometrici. L'informativa può essere resa mediante apposita segnaletica in prossimità delle aree soggette a rilevamento biometrico o delle postazioni di rilevamento, oppure può essere fornita con altri mezzi prima dell'interazione dell'interessato con il sistema biometrico (es. riconoscimento vocale tramite telefono preceduto da un avviso).

Analogamente, nei casi in cui il trattamento su base biometrica operi in sinergia con un altro sistema (es. videosorveglianza), l'informativa deve evidenziare tale circostanza in maniera chiara e adeguata, anche con le opportune semplificazioni richieste dallo specifico mezzo utilizzato.

4.5.2. Notificazione

Il titolare del trattamento dei dati biometrici è tenuto ad effettuare la notificazione al Garante ai sensi degli artt. 37, comma 1, lett. *a*), e 38, del Codice. In tale ambito, vanno considerati i casi di esonero dall'obbligo di notificazione riguardanti talune categorie di soggetti in ragione delle attività da essi svolte[3].

4.5.3. Verifica preliminare

L'art. 17 del Codice prevede che il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta 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, è ammesso nel rispetto di misure ed accorgimenti, a garanzia dell'interessato, rivolti anche "*a determinate categorie di titolari o di trattamenti*", ove prescritti.

I dati biometrici sono, per loro natura, direttamente e univocamente collegati all'individuo e denotano in generale un'intrinseca, universale e irreversibile relazione tra corpo e identità, per cui è necessario garantire particolari cautele in caso di trattamento.

L'utilizzo di sistemi biometrici rientra, pertanto, tra i trattamenti che presentano rischi specifici e dovrà essere svolto previa richiesta di verifica preliminare al Garante ai sensi

---

[3] Si richiama il Provvedimento relativo ai casi da sottrarre all'obbligo di notificazione, 31 marzo 2004 (in G.U. n. 81 del 6 aprile 2004, doc. web n. 85261); il provvedimento recante "Chiarimenti sui trattamenti da notificare al Garante" 23 aprile 2004 (doc. web n. 993385) ed il provvedimento riguardante le "Notificazioni in ambito sanitario: precisazioni del Garante" 26 aprile 2004 (doc. web n. 996680).

dell'art. 17 del Codice. Attraverso la verifica preliminare, che deve essere presentata dal titolare prima dell'inizio del trattamento, il Garante ha il compito di prescrivere, ove necessario, misure e accorgimenti specifici per consentire il corretto utilizzo di dati così delicati nel contesto del trattamento prospettato.

Nella istanza di verifica preliminare il titolare dovrà fornire elementi informativi inerenti l'analisi dei rischi effettuata e le modalità con cui intende garantire il rispetto delle misure di carattere generale, degli adempimenti giuridici e delle misure descritte nel par. 8 delle presenti linee-guida.

In particolare, l'istanza dovrà recare i seguenti elementi informativi:

- la tipologia di dati biometrici trattati;
- il contesto e le specifiche finalità perseguite mediante il sistema biometrico che si intende installare;
- le ragioni in base alle quali si ritengono inidonei rispetto agli scopi perseguiti sistemi alternativi che pongono minori rischi per i diritti e le libertà fondamentali degli interessati;
- le modalità di funzionamento del sistema nonché le modalità di acquisizione, utilizzo e archiviazione dei dati biometrici e la durata della loro eventuale conservazione;
- l'eventuale idoneità del dato biometrico raccolto a rivelare informazioni relative allo stato di salute degli interessati;
- gli eventuali vantaggi per gli interessati e per i titolari del trattamento derivanti dall'utilizzo di dati biometrici;
- i rischi individuati e gli accorgimenti tecnici e organizzativi messi in atto per mitigarli;
- le modalità di acquisizione del consenso, ove previsto, i sistemi alternativi, il testo dell'informativa.

Tanto premesso, il Garante – con provvedimento generale contestuale all'adozione delle presenti linee-guida – ha individuato alcune specifiche tipologie di trattamenti in relazione alle quali non ritiene necessaria la presentazione della predetta richiesta di verifica preliminare, a condizione che vengano rispettati i presupposti di legittimità contenuti nel Codice e nelle presenti linee-guida e che vengano adottate tutte le misure e gli accorgimenti tecnici descritti nel medesimo provvedimento. I trattamenti in questione sono:

- autenticazione informatica;
- controllo di accesso fisico ad aree "sensibili" dei soggetti addetti e utilizzo di apparati e macchinari pericolosi;
- uso delle impronte digitali o della topografia della mano a scopi facilitativi;
- sottoscrizione di documenti informatici.

5. UTILIZZO DELLE TECNICHE BIOMETRICHE

L'uso delle tecniche biometriche, nella maggior parte dei casi, è volto a realizzare procedure di **riconoscimento biometrico** di un individuo.

Il riconoscimento può essere basato su **verifica biometrica** (processo in cui il soggetto dichiara la sua identità e il sistema effettua un confronto fra il modello biometrico rilevato e quello memorizzato e corrispondente all'identità dichiarata) oppure su **identificazione biometrica** (processo in cui il sistema confronta il modello rilevato con tutti i modelli disponibili per individuare l'identità del soggetto), mentre i principali campi di applicazione riguardano il controllo degli accessi, sia logico (autenticazione informatica) sia fisico.

Costituiscono un caso a parte i sistemi di *firma grafometrica*, finalizzati alla sottoscrizione di documenti informatici senza che necessariamente sia effettuato un riconoscimento biometrico.

5.1. Riconoscimento biometrico: verifica e identificazione biometrica

Nel caso dei processi biometrici basati sulla verifica dell'identità dell'interessato il confronto viene effettuato tra un determinato modello biometrico associato all'identità dichiarata dall'utente nella fase assertiva (per esempio, mediante l'inserimento di un codice d'utente o l'utilizzo di un *badge* a varia tecnologia) e il modello biometrico generato al momento della richiesta di riconoscimento. Questo tipo di riconoscimento viene detto anche "confronto *uno-a-uno*".

Qualora il confronto risulti positivo l'identità potrà dirsi verificata e si otterrà la conseguente abilitazione alla successiva azione tecnica (apertura di un varco, nel caso di accesso fisico, abilitazione all'accesso a un sistema informatico, nel caso dell'accesso logico) la cui corretta esecuzione costituisce la finalità del trattamento biometrico.

Laddove il trattamento sia invece volto all'identificazione biometrica dell'interessato, il modello biometrico estratto dovrà essere confrontato o utilizzato come indice per la consultazione nella banca dati dei modelli biometrici di riferimento (confronto *uno-a-molti*). In tale ipotesi, la complessità dell'operazione è certamente superiore, dipendendo dalla dimensione della banca dati in termini di numerosità dei dati in essa presenti e dagli algoritmi di ricerca e confronto utilizzati.

5.2. Controllo biometrico dell'accesso logico

Le tecniche di riconoscimento biometrico sono talvolta adottate, anche in applicazione della regola 2 del Disciplinare tecnico in materia di misure minime di sicurezza, allegato B al Codice, per finalità di sicurezza, in aggiunta o in sostituzione degli ordinari sistemi di autenticazione informatica basati su informazioni nella disponibilità cognitiva (*password, user id*) o su dispositivi *(badge, token)* nel materiale possesso dell'interessato.

Le credenziali di autenticazione ordinarie, basate sull'associazione di un codice identificativo (*username, login-name...*) e di una parola chiave (*password*), quest'ultima da mantenere riservata, possono infatti essere facilmente smarrite, dimenticate, sottratte.

Anche i sistemi basati su tessere a varia tecnologia (magnetica, ottica, a contatto, a radiofrequenza) o su dispositivi di autenticazione di tipo OTP (*one-time password*) con cui si realizzano i cosiddetti sistemi di autenticazione forte o a due fattori, pur introducendo un maggior livello di sicurezza rispetto alle normali credenziali testuali, non sono tuttavia esenti da inconvenienti a seguito di smarrimento, cessione illegittima o furto dei dispositivi di autenticazione, cui si può accompagnare la perdita di confidenzialità delle informazioni di sicurezza eventualmente necessarie per il loro utilizzo (PIN, *password…*), al punto da consentire anche in questo caso la violazione dei dati trattati (*data breach*).

Con l'autenticazione biometrica, in cui vengono invece sottoposte a elaborazione informatica alcune caratteristiche biometriche, si cerca di scongiurare il rischio di cessione illegittima o di furto di credenziali, e di perseguire il raggiungimento di un maggior grado di certezza dell'identità del soggetto legittimato all'utilizzo di sistemi informatici.

5.3. Controllo dell'accesso fisico

Le diverse tecniche biometriche si prestano, con maggiore o minore efficacia a seconda del tipo di procedimento adottato, a utilizzazione in contesti differenti da quello informatico anche se comunque caratterizzati da una qualche interazione con sistemi tecnologici. In particolare, è rilevante l'uso di sistemi biometrici per il controllo dell'accesso fisico ad aree ristrette o riservate, per l'apertura di varchi o di serrature a protezione di locali o per l'uso di determinati apparati e macchinari.

Le finalità del trattamento biometrico sono principalmente di sicurezza, per la protezione patrimoniale o la tutela dell'incolumità di persone, ma le stesse tecniche biometriche possono anche prestarsi a scopi "facilitativi", in scenari che variano dall'accesso a biblioteche, all'apertura di armadietti in palestre o di cassette di sicurezza.

In ogni caso, le procedure biometriche per queste applicazioni ricadono nelle categorie dell'identificazione biometrica o della verifica biometrica.

5.4. Sottoscrizione di documenti informatici

Le tecniche biometriche basate sul rilevamento della dinamica di apposizione della firma autografa (firma grafometrica) possono essere utilizzate per la sottoscrizione di documenti informatici anche al fine di dare maggiore certezza ai rapporti giuridici.

Si tratta di un caso in cui i dati biometrici non sono funzionali, come tutti quelli finora esaminati, al riconoscimento biometrico di un individuo (anche se sono possibili e sono stati riscontrati utilizzi in questo senso), ma sono incorporati all'interno di documenti informatici per realizzare, laddove ne ricorrano i presupposti tecnici e normativi, delle soluzioni di firma elettronica avanzata, introdotta dal decreto legislativo 7 marzo 2005, n. 82 recante il "Codice dell'amministrazione digitale", e disciplinata con le regole tecniche di cui al d.P.C.M. 22 febbraio 2013, oppure, più in generale, per incorporare nel documento informatico delle informazioni strettamente connesse al soggetto firmatario e al

documento firmato che consentano comunque, al di là della valenza giuridica della sottoscrizione così ottenuta, di effettuare delle verifiche sull'integrità e autenticità del documento informatico.

Nella firma grafometrica si costituisce, infatti, un *set* di informazioni biometriche che, con l'ausilio di tecniche crittografiche, viene strettamente associato a un determinato documento informatico, in modo tale da consentire *ex post* lo svolgimento di analisi grafologiche da parte di un perito calligrafo sulla genuinità della sottoscrizione, analogamente a quanto avviene con le firme sui documenti cartacei (tipicamente, a seguito di contenzioso contrattuale o di disconoscimento della sottoscrizione).

L'utilizzo della firma grafometrica per la sottoscrizione di documenti non richiede, in genere, la creazione di una banca dati biometrica, poiché le singole firme grafometriche sono volta per volta acquisite e incorporate, con le opportune protezioni crittografiche, nel documento informatico sottoscritto, eventualmente archiviato in un sistema di gestione documentale.

6. IL CICLO DI VITA DEI DATI BIOMETRICI

6.1. Rilevamento e acquisizione biometrica

I trattamenti biometrici possono essere descritti come una sequenza di fasi di elaborazione a partire dal rilevamento, tramite sensori specializzati o dispositivi di uso generale, di una determinata caratteristica biometrica, biologica o comportamentale, di un individuo, al fine di creare un campione biometrico. Ottenuto il campione, la fase di acquisizione biometrica si considera conclusa.

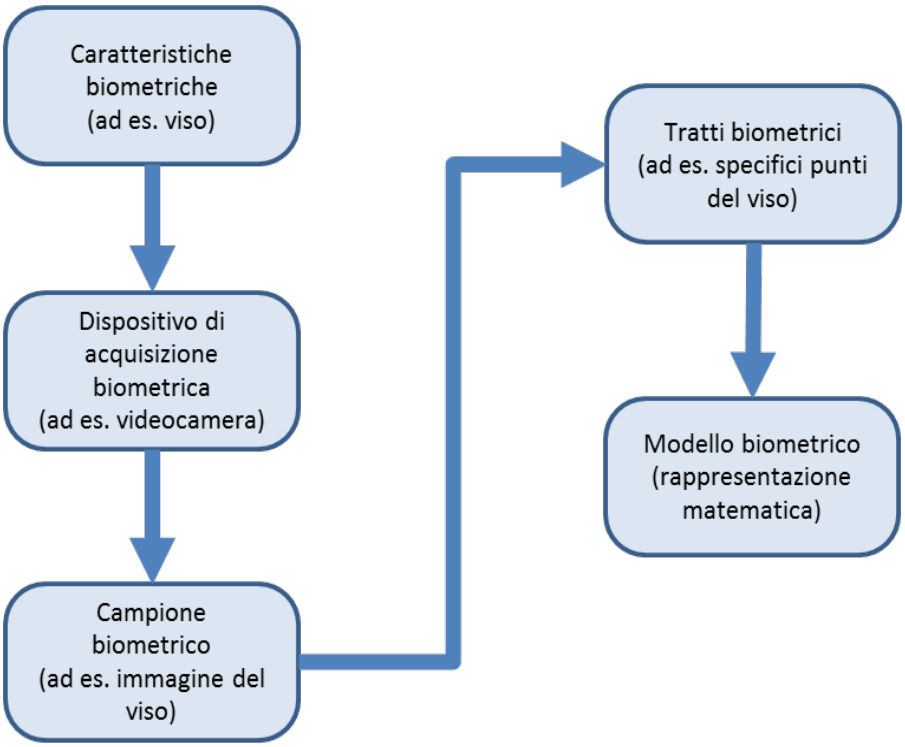

Figura 1: Fasi del processo di acquisizione di una caratteristica biometrica e di enrolment al sistema biometrico

I sensori biometrici possono essere *specializzati* (scanner per il rilevamento dell'impronta digitale, scanner per la lettura dell'iride, dispositivi per il rilevamento della topografia della mano, della vascolarizzazione delle dita, delle mani o del fondo oculare, tavolette grafometriche per l'acquisizione delle caratteristiche dinamiche delle firme autografe) o *non specializzati* (videocamere o microfoni con cui si possono acquisire immagini del volto di una persona o registrazioni della voce, da sottoporre poi a trattamento informatizzato; dispositivi di tipo *tablet* o similari dotati di schermo sensibile al tatto, con cui è possibile realizzare procedure semplificate di acquisizione a mezzo software delle caratteristiche dinamiche della firma, senza ricorrere a periferiche specializzate; *webcam* e microfoni incorporati in dispositivi mobili o in computer portatili che, usualmente adibiti alla videocomunicazione, possono fungere da sensori per il riconoscimento facciale e vocale).

I campioni biometrici acquisiti tramite i sensori consistono in *file* di dimensioni variabili a seconda del tipo di sistema biometrico e di sensore utilizzato. Si tratta quindi di dati che

mantengono una stretta correlazione, anche di tipo analogico, con la caratteristica biometrica da cui sono tratti, essendone una rappresentazione digitale la cui fedeltà all'originale dipende dall'accuratezza e dalla sofisticazione del sensore utilizzato.

Le eventuali elaborazioni successive agiranno su tali dati biometrici, e saranno anch'esse dipendenti dalla specifica tecnica biometrica e funzionali agli usi prescelti.

6.2. Enrolment e creazione del modello biometrico

Per consentire il riconoscimento biometrico è necessario acquisire la caratteristica biometrica con una procedura che garantisca la correttezza dell'accreditamento nel sistema biometrico *(biometric enrolment)*, il legame con il soggetto che si sottopone all'*enrolment* e la qualità del campione biometrico risultante.

I dati biometrici possono essere trattati e conservati, oltre che nella forma di campione biometrico, anche in forma di modello biometrico, cioè di descrizione informatica sintetica della caratteristica biometrica ottenuta estraendo dal campione biometrico soltanto gli elementi salienti predefiniti.

Dai campioni biometrici è infatti possibile estrarre tratti distintivi (per esempio, misurazioni del volto da un'immagine) e conservarli per sottoporli a un successivo utilizzo al posto degli stessi campioni. La definizione delle dimensioni del modello biometrico è una questione fondamentale: da un lato le dimensioni devono essere sufficientemente ampie per garantire un livello di accuratezza adeguato nel riconoscimento biometrico, evitando sovrapposizioni fra dati biometrici diversi o sostituzioni d'identità; dall'altro non devono essere eccessive per evitare il rischio di ricostruzione del campione biometrico.

In generale, è opportuno che le dimensioni e la ricchezza di tratti identificativi del modello siano commisurate all'ambito e alle finalità di utilizzo.

Il modello biometrico estratto dal campione biometrico va poi conservato per le successive operazioni di confronto.

Le rilevazioni successive, propedeutiche ai confronti biometrici, devono essere effettuate con le medesime garanzie previste per la fase di *enrolment* iniziale, avendo cura che i modelli da confrontare non viaggino su reti insicure o che restino privi di protezione crittografica.

6.3. Riconoscimento biometrico

I sistemi per l'identificazione biometrica richiedono necessariamente la costituzione di banche dati centralizzate di modelli biometrici per determinare l'identità dell'interessato. Il risultato del confronto (*match*) è positivo e consente di identificare l'interessato se vi è corrispondenza fra il modello biometrico di riferimento, conservato in banca dati, e il modello biometrico ricavato dalla caratteristica presentata.

Per la verifica biometrica è invece possibile, in linea di principio, adottare sia la conservazione centralizzata, che prevede l'accentramento di tutti i modelli biometrici di riferimento in un'unica banca dati, che la conservazione decentralizzata, in cui i riferimenti biometrici sono conservati direttamente sui dispositivi di rilevazione, su cui

avviene il confronto, oppure su dispositivi sicuri affidati alla custodia dell'interessato. Il confronto *uno a uno* è, per sua natura, estremamente rapido, non presentando alcuna apprezzabile complessità computazionale anche in presenza di tecniche biometriche sofisticate.

Alcune tipologie di *smart card* permettono di attuare il confronto biometrico addirittura all'interno del dispositivo stesso (*comparison on card*), senza la necessità di estrarre il riferimento biometrico, ma vanno incontro a forti limitazioni in termini di prestazioni e di costo a causa della loro limitata capacità elaborativa.

Come conseguenza della differente complessità computazionale, i "tempi di risposta" di un sistema di identificazione possono essere notevolmente superiori a quelli di un sistema di verifica biometrica, rendendo la procedura concretamente utilizzabile, laddove sia richiesta una elevata interattività, solo nei casi in cui la base dati contente i riferimenti biometrici sia di modeste dimensioni. Occorre quindi valutare, laddove sia tecnicamente possibile la scelta tra *verifica biometrica* e *identificazione biometrica*, se il vantaggio ergonomico di non richiedere una fase assertiva della propria identità non sia pregiudicato dal maggior tempo richiesto dalla procedura di riconoscimento, rendendo il processo inefficiente e inadatto agli scopi per cui si intende farvi ricorso.

6.4. Conservazione dei dati biometrici

Il dato biometrico (usualmente in forma di modello biometrico, ma in alcuni casi anche di campione biometrico) può trovarsi nella disponibilità del titolare del trattamento ed essere conservato in un'unica banca dati centralizzata, anche in forma di *Hardware Security Module* (HSM), nelle postazioni di lavoro informatiche oppure sugli stessi dispositivi di acquisizione biometrica.

In alternativa, è possibile memorizzare il dato biometrico in dispositivi sicuri (es. *token*, *smart card*) affidati alla diretta ed esclusiva disponibilità degli interessati, in modo che il titolare non debba conservare il dato biometrico (*template on card*). Tuttavia, in caso di furto, smarrimento o distruzione del dispositivo, l'interessato potrebbe essere temporaneamente impossibilitato all'utilizzo del sistema biometrico.

I *filesystem* di *smart card* e *token* biometrici devono essere leggibili dai soli lettori autorizzati, quantomeno nella porzione contenente i dati biometrici, che vanno resi inintelligibili al di fuori del contesto in cui se ne prevede l'uso tramite l'adozione di accorgimenti crittografici.

7. ANALISI DEI RISCHI

L'uso generalizzato della biometria, in virtù della delicatezza dei dati oggetto di trattamento, può presentare rischi per gli interessati, con potenziali gravi ripercussioni sulla loro sfera personale, in caso di impropria utilizzazione.

Il rischio, intenzionale o accidentale, consiste nella vulnerabilità di un *asset* o di un gruppo di *asset* tecnologici in grado di causare un trattamento illecito dei dati e il pericolo di furti di identità per l'interessato.

7.1. Controllo sociale e usi discriminatori

Molte caratteristiche biometriche hanno un elevato grado di unicità nella popolazione: ciò le rende adatte a essere utilizzate come una sorta di identificatore universale, con il rischio, se non opportunamente gestito, di un futuro in cui soggetti privati e istituzioni potrebbero acquisire o dedurre informazioni sui singoli individui incrociando e collegando dati provenienti da più banche dati, per finalità differenti da quelle per cui tali dati biometrici sono stati in origine raccolti.

Le caratteristiche biometriche che possono essere acquisite senza la consapevolezza o la partecipazione di un individuo potrebbero essere utilizzate per il suo tracciamento, ad esempio per seguirne gli spostamenti tramite l'utilizzo di tecnologie completamente automatizzate, tanto ubique quanto invasive, ledendo così il diritto alla riservatezza.

Utilizzi di questo tipo, quindi, trasformerebbero la biometria da risorsa per la sicurezza o per l'accesso facilitato (in sostituzione di carte, codici, *password* e firme), in uno strumento di controllo generalizzato.

L'attitudine di alcune caratteristiche biometriche a rivelare informazioni sensibili quali lo stato di salute, l'etnia o la razza, rende la discriminazione un ulteriore rischio concreto da tener sempre presente.

7.2. Furto di identità biometrica

Il furto di identità biometrica può causare effetti lesivi rilevanti nei confronti degli interessati in quanto non può essere fornita una nuova identità biometrica che utilizzi la stessa tipologia di dato biometrico, diversamente dai sistemi di riconoscimento tradizionali.

Le caratteristiche biometriche, infatti, poiché normalmente non modificabili e inscindibilmente legate all'individuo (seppur soggette in misura variabile a deterioramento in base all'età, al tipo di caratteristica, alle attività e agli stili di vita dell'interessato), costituiscono una sorta di credenziale di autenticazione non revocabile e non sostituibile la cui appropriazione da parte di soggetti non legittimati può prestarsi alla realizzazione di azioni fraudolente e compromettere l'efficacia di sistemi di sicurezza basati sul riconoscimento biometrico.

Le caratteristiche biometriche che lasciano traccia (es. impronte digitali) o che possono essere acquisite senza la cooperazione dell'interessato (es. la registrazione della voce, il

riconoscimento facciale o la scansione dell'iride eseguita con una telecamera a distanza o nascosta) possono comportare il rischio acquisizione indebita e prestarsi, in via teorica, a frodi e furti di identità. Tuttavia tali rischi rilevano solo nei casi in cui si utilizzino procedure il cui funzionamento sia basato esclusivamente sulla componente biometrica, mentre sono marginali se l'utilizzo della biometria avviene nell'ambito di un sistema *multi-factor* (che preveda, per esempio, l'uso di informazioni aggiuntive quali le *password* o analoghi codici, o l'impiego di un *token*).

7.3. Accuratezza del riconoscimento biometrico

Il riconoscimento biometrico avviene generalmente su base statistica e non deterministica, ed è dunque suscettibile di errore. Due dei più importanti parametri tecnici da considerare, connessi a un sistema biometrico, sono il tasso dei falsi rigetti (*false rejection rate – FRR*) o "falsi negativi" e il tasso delle false accettazioni (*false acceptance rate – FAR*) o "falsi positivi". Per questo motivo, le prestazioni del sistema biometrico vanno attentamente valutate in funzione delle finalità d'uso: un alto tasso di falsi positivi, abilita, erroneamente, l'accesso a utenti non autorizzati creando situazioni di pericolo per persone, cose o informazioni.

7.4. Falsificazione biometrica

L'estrazione di modelli biometrici comporta sempre una perdita di informazione rispetto a quella contenuta nel campione.

La creazione del modello dovrebbe essere sempre, qualora tecnicamente possibile, un processo univoco e non reversibile: non dovrebbe essere possibile, infatti, ricreare il campione biometrico a partire dal modello, dando luogo a una "ricostruzione" non autorizzata di una caratteristica biometrica.

Il caso largamente più dibattuto è quello delle impronte digitali: in linea teorica risulta possibile, con particolari algoritmi, generare, a partire da un modello biometrico, un campione biometrico che, sottoposto allo stesso processo di estrazione delle minuzie, produca un modello biometrico molto simile a quello iniziale. Tuttavia i campioni biometrici sintetici, affidati all'analisi dattiloscopica di un esperto, possono rivelare la loro natura di "falso" per via della scarsa verosimiglianza anatomica con campioni reali. Gli stessi modelli biometrici ottenuti, inoltre, non sono perfettamente corrispondenti a quello iniziale, recando spesso tracce di distorsioni e caratteristiche spurie.

Non appare quindi fondata l'ipotesi di ricostruzione più o meno fedele del campione biometrico originario e tantomeno della caratteristica biometrica da cui è stato ottenuto, a partire dal modello biometrico corrispondente.

Recentemente è stata dimostrata la possibilità di creare campioni biometrici dattiloscopici "artificiali" di elevata qualità da cui, utilizzando il procedimento di estrazione delle *minutiae* e provvedendo alla generazione del corrispondente modello biometrico tramite gli algoritmi utilizzati in normali sistemi biometrici, si può ottenere un modello biometrico del tutto corrispondente al riferimento biometrico originario. Il modello così ottenuto, utilizzato in sede di confronto biometrico, produrrebbe un risultato positivo.

Questa acclarata possibilità di ricostruzione di un campione biometrico corrispondente a un modello biometrico di partenza comporta certamente dei potenziali rischi, mitigati tuttavia da alcuni accorgimenti di sicurezza largamente utilizzati nei sistemi e in continua evoluzione.

Oltre al rischio di ricostruzione del campione esiste quello della falsificazione di alcune caratteristiche biometriche derivante dalla creazione di una caratteristica biometrica artificiale (*spoofing* biometrico) a partire da impronte rilevate al di fuori del sistema biometrico.

L'esempio tipico è quello delle impronte digitali, mediante creazione di una sorta di "dito artificiale" che riproduca le sembianze anatomiche del polpastrello, reso possibile oggi con maggiore facilità con la diffusione di tecniche di stampa tridimensionale a basso costo: il polpastrello artificiale così ottenuto è comunque un falso grossolano, contro cui sono ben efficaci misure tecniche in grado di garantire la genuinità della caratteristica rilevata dal dispositivo di acquisizione (come le funzioni di *liveness detection* presenti in alcuni sensori per il rilevamento dell'impronta digitale).

7.5. Amplificazione del rischio nel contesto mobile e BYOD

Si registra un significativo sviluppo nel settore IT rispetto all'utilizzo, per finalità aziendali, di dispositivi mobili di proprietà del dipendente o collaboratore. In tale contesto, il lavoratore può connettersi a risorse informative e documentali o a servizi dell'organizzazione di appartenenza, secondo il paradigma "*Bring Your Own Device*" (BYOD), accedendo ad applicazioni installate, con il suo consenso, sul proprio dispositivo, che gli permettano il trattamento di dati aziendali per lo svolgimento della propria attività lavorativa.

Tali scenari, che ENISA[4] include tra quelli su cui concentrare gli sforzi evolutivi sulle architetture e gli approcci alla sicurezza, assumono un significativo rilievo e lo stesso Garante ha avuto contezza della crescente diffusione, nei più importanti settori produttivi, di modelli di lavoro fortemente caratterizzati da mobilità abbinata a interazione con i sistemi informativi aziendali (soprattutto nel caso del settore bancario con lo sviluppo della firma grafometrica).

Un trattamento biometrico effettuato con dispositivi mobili (es. *tablet*), può andare incontro, in assenza di adeguate e specifiche misure di sicurezza, a rischi maggiori rispetto allo svolgersi del trattamento all'interno del perimetro di sicurezza aziendale.

L'accentuata possibilità di uso promiscuo dello strumento e, addirittura, dell'uso personale e familiare, per motivi ludici e ricreativi, non si concilia con la sicurezza dei dati anche in considerazione dell'accresciuta esposizione al rischio e all'utilizzo di applicativi non selezionati e installabili in modo incontrollato dall'utente.

Raramente, infatti, in questi contesti vengono adottati meccanismi di controllo degli accessi anche di tipo basilare, come il blocco automatico per inattività, né vengono offerte

[4] European Union Agency for Network and Information Security, https://www.enisa.europa.eu/

modalità di connessione sicura con protocolli avanzati per proteggere i dati in mobilità che rimangono esposti poiché trasmessi su canali insicuri.

8. MISURE DI CARATTERE GENERALE APPLICABILI AI TRATTAMENTI DI DATI BIOMETRICI

Ferma restando l'adozione delle misure previste agli artt. 31 – 35 e all'allegato B del Codice, al trattamento di dati biometrici devono essere applicate specifiche misure dipendenti dalla tipologia di dato, dall'architettura del sistema, dalla finalità perseguita, dal contesto ambientale in cui il sistema biometrico è introdotto, dalla modalità di raccolta e conservazione del dato.

Alla luce dell'esperienza maturata e dei provvedimenti adottati in materia, vengono di seguito illustrate le principali misure e accorgimenti di carattere generale che si ritiene debbano essere osservate a garanzia degli interessati, fermo restando l'obbligo del titolare di individuare compiutamente, ai sensi dell'art. 31 del Codice, le misure in concreto idonee agli specifici trattamenti che si intendono porre in essere. Tali misure, qualora si discostino da quelle qui richiamate, dovranno essere opportunamente motivate e documentate.

8.1. Misure di sicurezza dei trattamenti biometrici

Il titolare del trattamento svolto con sistemi elettronici è tenuto ad adoperarsi, utilizzando i mezzi tecnici che lo stato dell'arte nel settore informatico rende disponibili, per proteggere i dati personali trattati con le misure di sicurezza previste dal Codice. Tali misure comprendono, oltre alle misure minime di cui agli artt. 33-34 del Codice e all'allegato B, anche le misure idonee e preventive rispetto al trattamento di cui all'art. 31, la cui predisposizione richiede una valutazione del rischio incombente sui dati e sull'adeguatezza delle soluzioni tecniche predisposte per contrastarlo.

8.2. Scelta del sistema biometrico e accorgimenti di sicurezza

Per quanto riguarda le caratteristiche dei sensori, deve essere privilegiata, laddove tecnicamente praticabile, la capacità di rilevamento della vivezza della caratteristica biometrica, basata sul rilevamento di differenti parametri di forma e fisiologici (nel caso delle impronte digitali, il controllo di vivezza prende in considerazione la deformabilità, il comportamento in torsione dell'impronta all'atto della sua apposizione sul sensore, la presenza di circolazione sanguigna, la temperatura, la conduttività elettrica…) in modo da impedire grossolane falsificazioni della caratteristica biometrica impiegata.

Nella scelta dei processi biometrici si deve privilegiare l'uso di quelli che richiedono la cooperazione consapevole dell'interessato.

Laddove tecnicamente possibile, vanno utilizzati modelli biometrici con la minore quantità di informazioni, in modo da ridurre o annullare il rischio di ricostruzione del campione biometrico originario in qualunque fase del trattamento.

I dati biometrici grezzi (*raw data*) generati nel corso del procedimento di acquisizione biometrica (*biometric capture*) andranno cancellati da aree di memoria temporanea, centrale e secondaria e dal *filesystem* del sistema utilizzato per l'acquisizione immediatamente dopo la generazione del campione biometrico.

Il dato biometrico andrà possibilmente cifrato al momento della sua acquisizione dal sensore per ridurre il rischio di acquisizione fraudolenta con attacchi di tipo di *third in the middle* sul sensore o sui suoi canali di comunicazione con il sistema biometrico.

La trasmissione del dato andrà comunque effettuata, sia in fase di *enrolment* sia in fase di riconoscimento, su canali di comunicazione cifrati tra il dispositivo di acquisizione e il sistema su cui sono effettuati i confronti biometrici o l'eventuale conservazione dei campioni o dei modelli biometrici di riferimento.

Nel caso di adozione di sistemi biometrici in contesti *mobile* o BYOD è opportuno lo svolgimento di attività di *audit* periodiche e l'adozione di strumenti per accrescere la sicurezza dei dispositivi mobili come i sistemi *software* per *Mobile Device Management* (*MDM*) o *Mobile Device Auditing* (*MDA*).

Eventuali scelte in difformità dalle indicazioni contenute nel presente paragrafo andranno opportunamente descritte e motivate nell'istanza di verifica preliminare.

8.3. Gestione informatica e memorizzazione dei dati

I campioni o i modelli biometrici, laddove indispensabile per consentire i confronti, andranno conservati in aree di *filesystem* protette con strumenti crittografici o in *database* che supportino la cifratura a livello di *record* o di colonna. Laddove il sistema biometrico renda non praticabile l'utilizzo di tecniche crittografiche a chiave pubblica o la partecipazione di un soggetto terzo fiduciario, la cifratura dovrà comunque garantire elevati standard di sicurezza con lunghezza delle chiavi adeguate alla dimensione e alla criticità della banca dati[5].

Andrà privilegiata, laddove tecnicamente possibile, la conservazione dei soli modelli biometrici in dispositivi nell'esclusiva disponibilità dell'utente, evitandone l'archiviazione centralizzata in banche dati accessibili su reti anche di tipo locale.

I dati identificativi degli utenti andranno conservati separatamente dai relativi dati biometrici.

Se il dato biometrico si trova nella disponibilità del titolare del trattamento ed è conservato in un'unica banca dati, nelle postazioni di lavoro informatiche oppure su dispositivi di acquisizione biometrica, il titolare deve sempre prendere le massime precauzioni e implementare tutti i presidi necessari alla tutela del dato, riducendo al minimo il rischio di accesso non autorizzato, il furto, la sostituzione o la compromissione dei dati biometrici.

In alternativa, e preferibilmente laddove realizzabile, se il dato biometrico è memorizzato in dispositivi sicuri affidati alla diretta ed esclusiva disponibilità degli interessati, il titolare non deve conservare copia del dato biometrico.

---

[5] Si vedano in proposito le raccomandazioni ENISA contenute nel rapporto "Algorithms, Key Sizes and Parameters Report", October 2013 (https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report

Smart card e *token* biometrici devono essere leggibili dai soli lettori autorizzati, quantomeno relativamente all'area di memoria contenente dati biometrici.

8.4. Registrazione degli accessi ai dati biometrici

Nei casi eventuali di conservazione centralizzata dei dati biometrici in un *server* devono essere adottati sistemi idonei alla registrazione degli accessi da parte dei soggetti specificatamente abilitati a svolgere mansioni tecniche connesse alla manutenzione e alla gestione del *server* medesimo, che dovranno essere designati quali amministratori di sistema. Tali registrazioni devono comprendere i riferimenti temporali e avere caratteristiche di completezza, integrità, inalterabilità e durata della conservazione analoghe a quelle richieste per i *log* degli accessi di cui al provvedimento del Garante del 27 novembre 2008 sugli amministratori di sistema[6].

8.5. Tempi di conservazione dei dati biometrici

I dati biometrici rilevati, riferiti al dato grezzo d'origine, al campione biometrico, oppure ai dati ottenuti tramite elaborazione di quelli precedentemente citati (modelli o riferimenti biometrici), saranno oggetto di trattamento per il periodo di tempo strettamente necessario a perseguire gli scopi per i quali sono stati raccolti e trattati, fatta salva l'eventuale applicabilità di specifiche disposizioni in casi particolari.

In particolare, i campioni biometrici impiegati nella realizzazione del modello biometrico possono essere trattati solo durante le fasi di registrazione e di acquisizione necessarie al confronto biometrico, e non devono essere memorizzati se non per il tempo strettamente necessario alla generazione del modello stesso.

Venuta meno la necessità di trattare il dato questo deve essere cancellato in modo sicuro anche dalle aree di memoria volatile oltre che dai supporti di memorizzazione.

---

[6] V. "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", 27 novembre 2008 (pubblicato in G.U. n. 300 del 24 dicembre 2008; doc. web n. 1577499), come rivisto dal provvedimento recante "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento", 25 giugno 2009 (pubblicato in G.U. n. 149 del 30 giugno 2009, doc. web n. 1626595).

APPENDICE

A. GLOSSARIO

Vengono qui descritte le principali voci tecniche utilizzate nel testo delle presenti linee-guida e in altri documenti tecnici. Alcune voci sono già state introdotte nelle definizioni di cui al paragrafo 2, e si ripropongono qui unitamente ad altre voci di interesse nel presente contesto.

Accuratezza: grado di corrispondenza del dato teorico, desumibile da una serie di valori misurati (campione di dati), con il dato reale o di riferimento.

Archivio dattiloscopico: struttura che raccoglie, inventaria e conserva modelli biometrici di impronte digitali.

Campione biometrico: rappresentazione analogica o digitale di una caratteristica biometrica ottenuta al termine del processo di acquisizione costituita, per esempio, dalla riproduzione dell'immagine di un polpastrello.

Caratteristica biometrica: caratteristica biologica e comportamentale di un individuo da cui possono essere estratti in modo ripetibile dei tratti biometrici idonei al riconoscimento biometrico.

Confronto biometrico: confronto, usualmente basato su metodi statistici e metriche tipiche del contesto tecnologico e del sistema biometrico prescelto, fra dati biometrici.

Creste cutanee: rilievi lineari, per lo più irregolarmente paralleli, determinati in alcune regioni del corpo (palma delle mani, pianta dei piedi) dalla sporgenza, attraverso l'epidermide, delle papille dermiche allineate e descrivono disegni caratteristici e assolutamente individuali (anse, archi, vortici). Le creste si formano nel corso della dodicesima settimana, si completano dopo il sesto mese di vita intrauterina e si conservano anche nei cadaveri sino alla sussistenza del supporto epidermico.

Dispositivo di acquisizione ottica: sensore utilizzato per acquisire le impronte digitali, costituito da un prisma di vetro o materiale plastico, sul quale viene appoggiato il dito. La luce che attraversa il prisma è riflessa nelle valli (l'immagine appare bianca) e assorbita dalle creste (l'immagine appare nera).

Enrolment: processo attraverso cui un soggetto si accredita al sistema biometrico, attraverso la acquisizione di una sua caratteristica biometrica.

Falso negativo: risultato di un confronto che porta erroneamente ad un rigetto/confronto fallito.

Falso positivo: risultato di un confronto che porta erroneamente ad una accettazione/confronto riuscito.

Identificazione biometrica: ricerca in un archivio, per confronto biometrico automatizzato, di uno o più dati biometrici corrispondenti al dato acquisito. Questo tipo di operazione è detta anche confronto uno a molti e non prevede una fase assertiva.

Impronta digitale: impronta lasciata dai dermatoglifi (risultato dell'alternarsi di creste e valli) dell'ultima falange delle dita delle mani.

Minuzie: discontinuità delle creste cutanee (chiamate anche "dettagli di Galton") costituite da biforcazioni e terminazioni. Le minuzie sono molto importanti per la discriminazione delle impronte, e pertanto vengono usate nella maggior parte dei sistemi di confronto automatico.

Modello biometrico: insieme di tratti biometrici memorizzati informaticamente e direttamente confrontabile con altri modelli biometrici.

One-time password: parola-chiave valida solo per una singola sessione di accesso o una transazione

Istanza biometrica: modello biometrico generato ogni volta che l'interessato interagisce con il sistema biometrico.

Rete neurale: rete di neuroni artificiali che intende simulare, all'interno di un sistema informatico, il funzionamento dei neuroni biologici tra loro interconnessi.

Riconoscimento biometrico: si intende il riconoscimento automatico di individui basato su loro caratteristiche biologiche o comportamentali, includendo in tale accezione le nozioni di verifica biometrica e di identificazione biometrica.

Riferimento biometrico: modello biometrico utilizzato come termine di confronto e registrato in modo persistente e invariabile nel tempo (a meno di aggiornamenti resi necessari dalle variazioni anche naturali della caratteristica biometrica da cui è estratto).

Sensore: dispositivo che misura una grandezza fisica in ingresso e fornisce un segnale in uscita a fini di misurazione o di controllo del sistema in cui è impiegato.

Sistema crittografico a chiave asimmetrica: La crittografia asimmetrica (nota anche come crittografia a coppia di chiavi, crittografia a chiave pubblica/privata o crittografia a chiave pubblica) è un tipo di crittografia dove ad ogni attore coinvolto nella comunicazione è associata una coppia di chiavi:

- la chiave pubblica, che deve essere distribuita, serve a cifrare un documento destinato alla persona che possiede la relativa chiave privata;
- la chiave privata, personale e segreta, utilizzata per decifrare un documento cifrato con la chiave pubblica;

evitando così il problema connesso alla distribuzione delle chiavi.

Smart card: dispositivo costituito da un supporto di plastica nel quale è incastonato un *microchip* che possiede potenzialità di elaborazione e memorizzazione dati, e integra diverse tecnologie, comprendenti circuiti integrati, microprocessori, memorie RAM, ROM, EEPROM, antenne.

Third in the middle: in crittografia è un tipo di attacco (noto anche come *man in the middle*, MIM) nel quale il soggetto "attaccante" (colui che tenta di violare la sicurezza del sistema) è in grado di leggere, inserire o modificare a piacere messaggi scambiati tra le due parti comunicanti senza che nessuna delle due sia in grado di sapere se il collegamento che li unisce reciprocamente sia stato effettivamente compromesso. L'attaccante è così in grado di osservare, intercettare e replicare verso la destinazione prestabilita il transito dei messaggi tra le due parti comunicanti.

Two-factors authentication: l'autenticazione a due fattori (nota anche come *strong authentication*) è un metodo che si basa sull'utilizzo congiunto di due metodi di autenticazione individuale (es. *PIN/password* e *smart c*ard, come nel caso del bancomat).

Token: dispositivo portatile utilizzato per effettuare l'autenticazione ad un sistema informatico. Tipicamente è un generatore di numeri casuali, che utilizza lo stesso algoritmo di generazione installato sul server di autenticazione.

Tratto biometrico: informazione estratta da un campione biometrico a fini di confronto.

Valli cutanee: area dell'epidermide di alcune regioni del corpo (palma delle mani, pianta dei piedi) priva di sporgenze delle papille dermiche e quindi non in rilievo.

Verifica biometrica: confronto automatizzato tra un modello biometrico acquisito nel momento in cui l'interessato interagisce con il sistema biometrico e un modello biometrico previamente memorizzato e (presuntivamente) a lui corrispondente; questo tipo di verifica è detta *confronto uno a uno*.

B. PROVVEDIMENTI DEL GARANTE IN TEMA DI TRATTAMENTO DEI DATI BIOMETRICI

- Sistema automatizzato di cassette di sicurezza basato sul rilevamento dell'impronta digitale dei clienti. Verifica preliminare richiesta da Banca degli Ernici di credito coop. ScpA - 6 febbraio 2014 [doc. web n. 3000045]
- Sistema automatizzato di cassette di sicurezza basato sul rilevamento dell'impronta digitale dei clienti. Verifica preliminare richiesta da Banca Patrimoni Sella & C. S.p.a. - 6 febbraio 2014 [doc. web n. 2986091]
- Servizio di firma digitale remota con autenticazione biometrica. Verifica preliminare richiesta da Telecom Italia Trust Technologies s.r.l. e Banca Generali S.p.A. - 23 gennaio 2014 [doc. web n. 2938921]
- Ordinanza di ingiunzione nei confronti di Associazione culturale Koala - 5 dicembre 2013 [doc. web n. 2997038]
- Ordinanza di ingiunzione nei confronti di Axa società cooperativa a responsabilità limitata - 28 novembre 2013 [doc. web n. 2996788]
- Provvedimento del 28 novembre 2013 [doc. web n. 2951732]
- Sistema per l'accesso della clientela in modalità self service, 24 ore su 24, alle cassette di sicurezza, con trattamento di dati biometrici - Verifica preliminare richiesta da Credito Lombardo Veneto S.p.A. - 19 settembre 2013 [doc. web n. 2710934]
- Sistema per la sottoscrizione in forma elettronica di atti, contratti e altri documenti relativi a prodotti e servizi offerti da una banca - 12 settembre 2013
- Sistema biometrico di rilevazione delle presenze dei dipendenti in una scuola - 1° agosto 2013 [doc. web n. 2578547]
- Videosorveglianza e biometria all'interno di una scuola per la rilevazione delle presenze dei dipendenti - 30 maggio 2013
- Installazione in un istituto scolastico di un dispositivo a riconoscimento biometrico (impronta digitale) per finalità di controllo del rispetto dell'orario di servizio - 30 maggio 2013 [doc. web n. 2503101]
- Installazione in un istituto scolastico di un dispositivo a riconoscimento biometrico (impronta digitale) per finalità di controllo del rispetto dell'orario di servizio - 30 maggio 2013 [doc. web n. 2502951]
- Sistema per l'accesso della clientela in modalità c.d. self service, 24 ore su 24 alle cassette di sicurezza che può prevedere il trattamento di dati biometrici. Verifica preliminare richiesta da Banca di credito cooperativo di Vigevano - 14 febbraio 2013 [doc. web n. 2375735]
- Sistemi di rilevazione biometrica. Verifica preliminare richiesta da IT Telecom s.r.l. e Cassa di Risparmio di Parma e Piacenza S.p.A. - 31 gennaio 2013 [doc. web n. 2311886]
- Trattamento di dati biometrici. Verifica preliminare richiesta da Unicredit S.p.A. - 31 gennaio 2013 [doc. web n. 2304808]
- Trattamento di dati biometrici per finalità di rilevazione delle presenze dei dipendenti: verifica preliminare richiesta dal Comune di Boscoreale - 31 gennaio 2013 [doc. web n. 2304669]
- Sistema di rilevazione di dati biometrici dei lavoratori basato sulla lettura della geometria della mano - 10 gennaio 2013 [doc. web n. 2354574]

- Ordinanza di ingiunzione nei confronti di G & W Invest s.r.l. - 29 novembre 2012 [doc. web n. 2315593]
- Sistema di rilevazione di dati biometrici dei passeggeri. Verifica preliminare richiesta da Alitalia–Compagnia Aerea Italiana S.p.A. - 4 ottobre 2012
- Installazione di un sistema completamente automatizzato di cassette di sicurezza. Verifica preliminare richiesta da Cassa Raiffeisen di Lagundo Soc. coop", 13 settembre 2012 [doc. web n. 1927441]
- Trattamento dei dati biometrici riferiti ai lavoratori presso un cantiere edile - 13 settembre 2012, [doc. web n. 1927456]
- Dati biometrici: illecito raccogliere e utilizzare le impronte digitali degli iscritti per l'accesso ad una palestra - 29 marzo 2012 [doc. web n. 1891999]
- Dati biometrici: illecito raccogliere e utilizzare le impronte digitali degli iscritti per l'accesso ad una palestra - 16 febbraio 2012 [doc. web n. 1894570]
- Divieto di trattamento dei dati biometrici dei dipendenti per finalità di rilevazione della presenza sul posto di lavoro - 20 ottobre 2011 [doc. web n. 1851657]
- Trattamento di dati biometrici ricavati dalla lettura delle impronte digitali - Verifica preliminare - 10 giugno 2011 [doc. web n. 1835792]
- Trattamento sproporzionato di dati biometrici dei dipendenti per finalità di accesso alla sede aziendale - 10 marzo 2011 [doc. web n. 1807683]
- Trasporto: impronte digitali solo in casi particolari - 17 novembre 2010 [doc. web n. 1779745]
- Trasporto: impronte digitali solo in casi particolari - 17 novembre 2010 [doc. web n. 1779758]
- Banche: cassette sicure con le impronte digitali - 15 aprile 2010 [doc. web n. 1719879]
- Nuove tecnologie e aree a rischio - 10 dicembre 2009 [doc. web n. 1689698]
- Divieto all'uso di dati biometrici per rilevare la presenza sul luogo di lavoro - 29 ottobre 2009 [doc. web n. 1682066]
- Imprese: vietato l'uso della biometria per la rilevazione delle presenze e dei tempi di lavoro - 15 ottobre 2009 [doc. web n. 1664257]
- Vigilanza più "vigilata" negli aeroporti - 17 settembre 2009 [doc. web n. 1655708]
- Biometria e rilevamento della presenza del personale aeroportuale - 12 giugno 2008 [doc. web n. 1635731]
- Videosorveglianza e biometria per esigenze di sicurezza: impiego non conforme - 4 giugno 2009 [doc. web n. 1629975]
- Rilevazione di impronte digitali ed immagini per accedere agli istituti di credito: verifica preliminare - 14 maggio 2009 [doc. web n. 1617735]
- Trattamento di dati biometrici per finalità di autenticazione di accesso a particolari aree aziendali - 8 aprile 2009 [doc. web n. 1610018]
- Dati biometrici: vietati per la rilevazione dell'orario di lavoro - 2 ottobre 2008 [doc. web n. 1571502]
- Uso di dati biometrici nelle operazioni di trasfusione - 19 giugno 2008 [doc. web n. 1532480]
- Più sicurezza in ospedale con le impronte digitali - 15 aprile 2008 [doc. web n. 1523435]
- Riconoscimento vocale e gestione di sistemi informatici - 28 febbraio 2008 [doc. web n. 1501094]

- Trattamento dei dati biometrici di dipendenti per incrementare la sicurezza della rete idrica - 15 febbraio 2008 [doc. web n. 1497675]
- Trattamento di dati biometrici in Banca (Cariprato S.p.A.) - 23 gennaio 2008 [doc. web n. 1490382]
- Trattamento di dati biometrici in banca (Monte dei Paschi di Siena) - 23 gennaio 2008 [doc. web n. 1490463]
- Trattamento di dati biometrici in banca (Banca nazionale del lavoro) - 23 gennaio 2008 [doc. web n. 1490477]
- Trattamento di dati biometrici in banca (Banca San Paolo Imi S.p.A.) - 23 gennaio 2008 [doc. web n. 1490533]
- Rivelazioni biometriche per verificare la presenza a corsi di formazione - 23 gennaio 2008 [doc. web n. 1487903]
- Rilevazioni biometriche per l'accesso alla sala operativa di una soprintendenza archeologica - 8 novembre 2007 [doc. web n. 1461908]
- Verifica preliminare: trattamento dei dati biometrici per l'accesso ad un complesso polifunzionale nel settore orafo - 1 febbraio 2007 [doc. web n. 1381983]
- Biometria per sicurezza merci e controllo delle presenze presso aeroporti - 26 luglio 2006 [doc. web n. 1318582]
- Verifica preliminare: uso della biometria per identificazione del personale nelle banche - 15 giugno 2006 [doc. web n. 1306098]
- Trattamento di dati biometrici per la verifica della presenza dei dipendenti e l'accesso ad aree produttive (mulino) - 15 giugno 2006 [doc. web n. 1306530]
- Istituti di credito - Modifica del termine per gli adempimenti sulla rilevazione di impronte digitali ed immagini - 2 marzo 2006 [doc. web n. 1248850]
- Verifica preliminare: dati biometrici e Rfid nelle banche - 23 febbraio 2006 [doc. web n. 1251535]
- Accesso ad aree riservate di azienda operante nel settore avionico ed elettronico: uso proporzionato di dati biometrici - 23 novembre 2005 [doc. web n. 1202254]
- Rilevazione di impronte digitali ed immagini per accedere agli istituti di credito: limiti e garanzie - 27 ottobre 2005 [doc. web n. 1246675]
- Uso delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro", 21 luglio 2005 [doc. web n. 1150679]
- Indicazioni sullo schema di decreto interministeriale sui documenti di soggiorno elettronici - 4 marzo 2004 [doc. web n. 1054853]
- Videosorveglianza e dati biometrici - Rilevazioni biometriche presso istituti di credito ' 28 settembre 2001 [doc. web n. 39704]
- Videosorveglianza - Raccolta di impronte digitali associate ad immagini per l'accesso a banche - 7 marzo 2001 [doc. web n. 30947]
- Videosorveglianza - Videosorveglianza e rilevazione di impronte digitali all'ingresso di banche - 28 febbraio 2001 [doc. web n. 40181]
- Videosorveglianza - Impronte digitali per l'accesso in banca - 11 dicembre 2000 [doc. web n. 30903]
- Videosorveglianza e biometria - Trattamento dati personali mediante utilizzo di impronte digitali - 19 novembre 1999 [doc. web n. 42058]

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Allegato B al Provvedimento n.513 del Garante del 12 novembre 2014

VIOLAZIONE DI DATI BIOMETRICI
MODELLO DI COMUNICAZIONE AL GARANTE

A seguito del Provvedimento del 12 novembre 2014, i titolari di trattamento di dati biometrici sono tenuti a comunicare al Garante le violazioni di tali dati (*data breach*) che si verificano nell'ambito dei propri sistemi.

La comunicazione deve essere effettuata in base al presente modello, allegando eventualmente ulteriore documentazione ritenuta utile.

Titolare del trattamento di dati biometrici

Denominazione o ragione sociale _____

Provincia _____ **Comune** _____

Cap _____ **Indirizzo** _____

Nome persona fisica addetta alla comunicazione _____

Cognome persona fisica addetta alla comunicazione _____

Funzione rivestita _____

Indirizzo Email/PEC per eventuali comunicazioni _____

Recapito telefonico per eventuali comunicazioni _____

Eventuali Contatti (altre informazioni) _____

Natura della comunicazione

- ☐ Nuova comunicazione
- ☐ Inserimento ulteriori informazioni sulla precedente comunicazione (Numero di riferimento)

Breve descrizione del trattamento di dati biometrici (finalità, caratteristiche biometriche utilizzate..)

Breve descrizione della violazione di dati biometrici

Quando si è verificata la violazione di dati biometrici?

- ☐ Il _____
- ☐ Tra il _____ e il _____
- ☐ È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio?

Tipo di violazione

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- ☐ Altro :

Dispositivo oggetto della violazione

- ☐ Postazione di lavoro
- ☐ Dispositivo di acquisizione o dispositivo-lettore
- ☐ Smart card o analogo supporto portatile
- ☐ Dispositivo mobile
- ☐ File o parte di un file
- ☐ Strumento di *backup*
- ☐ Rete
- ☐ Altro :

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione di dati biometrici?

- ☐ N. _____ di persone
- ☐ Circa _____ persone
- ☐ Un numero (ancora) sconosciuto di persone

Altri dati coinvolti nella violazione

- ☐ Dati anagrafici
- ☐ Numero di telefono (fisso o mobile)
- ☐ Indirizzo di posta elettronica
- ☐ Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)
- ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
- ☐ Altri dati di personali (sesso, data di nascita, età, ...), dati sensibili e giudiziari
- ☐ Ancora sconosciuto
- ☐ Altro :

Livello di gravità della violazione dei dati biometrici (secondo le valutazioni del titolare)?

- ☐ Basso/trascurabile
- ☐ Medio
- ☐ Alto
- ☐ Molto alto

Misure tecniche e organizzative applicate ai dati colpiti dalla violazione

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

La violazione è stata comunicata anche agli interessati?

- ☐ Sì, è stata comunicata il
- ☐ No, perché

La violazione coinvolge interessati che si trovano in altri Paesi UE?

- ☐ Sì
- ☐ No

La comunicazione è stata effettuata alle competenti autorità di altri Paesi UE?

- ☐ No
- ☐ Sì

Ispettorato del Lavoro
Nota n. 299 del 28 novembre 2017

Indicazioni operative sull'installazione e utilizzazione di impianti audiovisivi e di altri strumenti di controllo ai sensi dell'art. 4 della legge n. 300/1970

Pervengono a questo Ispettorato numerose istanze da parte di imprese che intendono procedere all'installazione di impianti di allarme o antifurto dotati anche di videocamere o fotocamere che si attivano, automaticamente, in caso di intrusione da parte di terzi all'interno dei luoghi di lavoro.

L'installazione di tali impianti, finalizzati alla tutela del patrimonio aziendale, prevedendo comunque la presenza di videocamere o fotocamere, rappresenta una fattispecie rientrante nell'ambito di applicazione dell'art. 4 della legge n. 300/1970 ed è soggetta pertanto alla preventiva procedura di accordo con RSA o RSU ovvero all'autorizzazione da parte dell'Ispettorato del Lavoro.

Al fine di uniformare l'operatività degli Uffici Territoriali, si ritiene però opportuno fornire le seguenti indicazioni operative finalizzate a rendere più celeri le procedure autorizzative connesse a tali particolari impianti.

In primo luogo si ritiene che questi ultimi, essendo evidentemente finalizzati alla tutela del patrimonio aziendale, trovano la loro legittimazione nella previsione di cui al primo comma del citato art. 4.

Quanto alle modalità operative va tenuto presente che, qualora le videocamere o fotocamere si attivino esclusivamente con l'impianto di allarme inserito, non sussiste alcuna possibilità di controllo "preterintenzionale" sul personale e pertanto non vi sono motivi ostativi al rilascio del provvedimento.

Conseguentemente, in relazione alla evidente esigenza di celerità nell'attivazione dei predetti impianti, si invitano codesti Uffici a rilasciare il provvedimento autorizzativo in tempi assolutamente rapidi stante l'inesistenza di qualunque valutazione istruttoria.

CIRCOLARE N. 5/2018

Agli Ispettorati interregionali e territoriali del lavoro

Al Comando Carabinieri per la Tutela del Lavoro

e, p.c.

Alla Provincia Autonoma di Trento

Alla Provincia Autonoma di Bolzano

All' Ispettorato regionale del Lavoro di Palermo

Oggetto: indicazioni operative sull'installazione e utilizzazione di impianti audiovisivi e di altri strumenti di controllo ai sensi dell'art. 4 della legge n. 300/1970.

L'art. 23 del d.lgs. n. 151/2015 e il successivo art. 5, comma 2, del d.lgs. n. 185/2016 hanno modificato l'art. 4 della legge n. 300/1970 adeguando l'impianto normativo e le procedure preesistenti alle innovazioni tecnologiche nel frattempo intervenute. Lo scopo della norma, dunque, rimane quello di contemperare, da un lato, l'esigenza afferente all'organizzazione del lavoro e della produzione propria del datore di lavoro e, dall'altro, tutelare la dignità e la riservatezza dei lavoratori.

Con la presente circolare, condivisa con il Ministero del lavoro e delle politiche sociali, si forniscono indicazioni operative in ordine alle problematiche inerenti l'installazione e l'utilizzazione di impianti audiovisivi e di altri strumenti di controllo.

Istruttoria delle istanze presentate

Una prima questione riguarda le modalità secondo cui effettuare l'istruttoria in ordine alle istanze presentate per il rilascio del provvedimento e, in particolare, la valutazione dei presupposti legittimanti il controllo a distanza dei lavoratori.

Va premesso che tale istruttoria **non coinvolge normalmente aspetti tecnici particolari che debbano essere valutati da personale con la qualifica di "ispettore tecnico"** e, pertanto, tale attività va demandata al personale ispettivo ordinario o amministrativo operante all'interno delle varie unità

Ispettorato Nazionale del Lavoro
Via Fornovo, 8 - 00192 Roma
Tel. 06 46837270
capoispettorato@pec.ispettorato.gov.it
segreteriacapoispettoratoi@ispettorato.gov.it

organizzative dell'Ufficio e, solo in casi assolutamente eccezionali comportanti valutazioni tecniche di particolare complessità, anche al personale ispettivo tecnico.

L'oggetto dell'attività valutativa, infatti, va concentrata sulla effettiva sussistenza delle ragioni legittimanti l'adozione del provvedimento, tenendo presente in particolare la specifica finalità per la quale viene richiesta la singola autorizzazione e cioè le ragioni organizzative e produttive, quelle di sicurezza sul lavoro e quelle di tutela del patrimonio aziendale.

Conseguentemente, le eventuali condizioni poste all'utilizzo delle varie strumentazioni utilizzate devono essere **necessariamente correlate alla specifica finalità individuata nell'istanza** senza, però, particolari ulteriori limitazioni di carattere tecnico che talvolta finiscono per vanificare l'efficacia dello stesso strumento di controllo. L'eventuale ripresa dei lavoratori, di norma, dovrebbe avvenire in via incidentale e con carattere di occasionalità ma nulla impedisce, se sussistono le ragioni giustificatrici del controllo (ad esempio tutela della "sicurezza del lavoro" o del "patrimonio aziendale"), di inquadrare direttamente l'operatore, senza introdurre condizioni quali, per esempio, "l'angolo di ripresa" della telecamera oppure "l'oscuramento del volto del lavoratore".

Parimenti, sempre in tema di videosorveglianza, **non appare fondamentale specificare il posizionamento predeterminato e l'esatto numero delle telecamere da installare** fermo restando, comunque, che le riprese effettuate devono necessariamente essere **coerenti e strettamente connesse con le ragioni legittimanti il controllo** e dichiarate nell'istanza, ragioni la cui effettiva sussistenza va sempre verificata in sede di eventuale accertamento ispettivo. Ciò in quanto lo stato dei luoghi e il posizionamento delle merci o degli impianti produttivi è spesso oggetto di continue modificazioni nel corso del tempo (si pensi ad esempio alla rotazione delle merci nelle strutture della grande distribuzione) e **pertanto rendono scarsamente utile una analitica istruttoria basata su planimetrie che nel corso del breve periodo non sono assolutamente rappresentative del contesto lavorativo**.

Del resto, un provvedimento autorizzativo basato sulle esibizione di una documentazione che "fotografa" lo stato dei luoghi in un determinato momento storico rischierebbe di perdere efficacia nel momento stesso in cui tale "stato" venga modificato per varie esigenze, con la conseguente necessità di un aggiornamento periodico dello specifico provvedimento autorizzativo, pur in presenza delle medesime ragioni legittimanti l'installazione degli strumenti di controllo.

Da ultimo va precisato che il provvedimento autorizzativo viene rilasciato sulla base delle specifiche ragioni dichiarate dall'istante in sede di richiesta. L'attività di controllo, pertanto, **è legittima se strettamente funzionale alla tutela dell'interesse dichiarato**, interesse che non può essere modificato nel corso del tempo nemmeno se vengano invocate le altre ragioni legittimanti il controllo stesso ma non dichiarate nell'istanza di autorizzazione.

Gli eventuali controlli ispettivi successivi al rilascio del provvedimento autorizzativo, pertanto, dovranno innanzitutto verificare che le modalità di utilizzo degli strumenti di controllo siano assolutamente conformi e coerenti con le finalità dichiarate.

Tutela del patrimonio aziendale.

Fra le ragioni giustificatrici del controllo a distanza dei lavoratori l'elemento di novità introdotto dalla più recente normativa è rappresentato dalla **tutela del patrimonio aziendale** che in precedenza veniva considerato come unico criterio legittimante delle visite personali di controllo di cui all'art. 6 della stessa legge.

Tale presupposto necessita però di una attenta valutazione in quanto l'ampiezza della nozione di "patrimonio aziendale" rischia di non trovare una adeguata delimitazione e, conseguentemente, non fungere da "idoneo filtro" alla ammissibilità delle richieste di autorizzazione.

In primo luogo va chiarito che tale problematica **non si pone per le richieste che riguardano dispositivi collegati ad impianti di antifurto** che tutelano il patrimonio aziendale in quanto tali dispositivi, entrando in funzione soltanto quando in azienda non sono presenti lavoratori, non consentono alcuna forma di controllo incidentale degli stessi e pertanto possono essere autorizzati secondo le modalità di cui alla nota n. 299 del 28 novembre 2017.

Diversa invece è l'ipotesi in cui la richiesta di installazione riguardi dispositivi operanti in presenza del personale aziendale, in quanto in tal caso la generica motivazione di "tutela del patrimonio" va necessariamente declinata per non vanificare le finalità poste alla base della disciplina normativa.

In tali fattispecie, come ricorda il garante della privacy, i principi di legittimità e determinatezza del fine perseguito, nonché della sua proporzionalità, correttezza e non eccedenza, **impongono una gradualità nell'ampiezza e tipologia del monitoraggio**, che rende assolutamente residuali i controlli più invasivi, legittimandoli solo a fronte della rilevazione di specifiche anomalie e comunque all'esito dell'esperimento di misure preventive meno limitative dei diritti dei lavoratori.

Del resto, anche secondo la Corte di Cassazione, la sussistenza dei presupposti legittimanti la tutela del patrimonio aziendale mediante le visite personali di controllo, va valutata in relazione ai mezzi tecnici e legali alternativi attuabili, all'intrinseca qualità delle cose da tutelare, alla possibilità per il datore di lavoro di prevenire ammanchi attraverso l'adozione di misure alternative (Cass. sent. n. 84/5902).

Inoltre, tra gli elementi che devono essere tenuti presenti nella comparazione dei contrapposti interessi, non possono non rientrare anche quelli relativi all'intrinseco valore e alla agevole asportabilità dei beni costituendi il patrimonio aziendale.

Telecamere

I sistemi di videosorveglianza di più recente introduzione si basano su tecnologie digitali adatte all'elaborazione su PC e trasmissione su rete dati (tipo internet). Le nuove soluzioni video in tecnologia IP hanno rivoluzionato il concetto di videosorveglianza, rendendo possibili funzioni e scenari applicativi inimmaginabili fino a pochi anni fa.

I sistemi di videosorveglianza che utilizzano tale tecnologia sono caratterizzati dall'utilizzo di una rete IP, cablata oppure wireless, che consente il trasporto dei dati video e audio digitali da un computer all'altro attraverso internet; è anche possibile registrare, visualizzare e mantenere le informazioni video e audio in qualsiasi punto della rete opportunamente dimensionata. Inoltre è possibile installare impianti di videosorveglianza a circuito chiuso, collegati all'intranet aziendale o via internet a postazione remota.

A tal proposito si precisa che, ove sussistano le ragioni giustificatrici del provvedimento, è autorizzabile da postazione remota sia la visione delle immagini "in tempo reale" che registrate.

Tuttavia, l'accesso da postazione remota alle immagini "in tempo reale" deve essere autorizzato solo in casi eccezionali debitamente motivati.

L'accesso alle immagini registrate, sia da remoto che "in loco", deve essere necessariamente tracciato anche tramite apposite funzionalità che consentano la conservazione dei "log di accesso" per un congruo periodo, non inferiore a sei mesi; pertanto non va più posta più come condizione, nell'ambito del provvedimento autorizzativo, l'utilizzo del sistema della "doppia chiave fisica o logica".

Quanto invece al "perimetro" spaziale di applicazione della disciplina in esame, l'orientamento giurisprudenziale tende ad identificare come luoghi soggetti alla normativa in questione anche quelli esterni dove venga svolta attività lavorativa in modo saltuario o occasionale (ad es. zone di carico e scarico merci). La Corte di Cassazione penale (sent. n. 1490/1986) afferma infatti che l'installazione di una telecamera diretta verso il luogo di lavoro dei propri dipendenti o su spazi dove essi hanno accesso anche occasionalmente, **deve essere preventivamente autorizzata da uno specifico accordo con le organizzazioni sindacali ovvero da un provvedimento dell'Ispettorato del lavoro**.

Sarebbero invece da escludere dall'applicazione della norma quelle zone esterne estranee alle pertinenze della ditta, come ad es. il suolo pubblico, anche se antistante alle zone di ingresso all'azienda, nelle quali non è prestata attività lavorativa.

Dati biometrici

L'utilizzo di dispositivi e tecnologie per la raccolta e il trattamento di dati biometrici sta andando incontro ad una crescente diffusione. Il Garante per la protezione dei dati personali ha emanato un Provvedimento generale prescrittivo in tema di biometria, pubblicato sulla Gazzetta Ufficiale n. 280 del 2

dicembre 2014. Il Garante evidenzia, al punto 4.2, come "*l'adozione di sistemi biometrici basati sull'elaborazione dell'impronta digitale o della topografia della mano può essere consentita per limitare l'accesso ad aree e locali ritenuti "sensibili" in cui è necessario assicurare elevati e specifici livelli di sicurezza oppure per consentire l'utilizzo di apparati e macchinari pericolosi ai soli soggetti qualificati e specificamente addetti alle attività*".

Ne consegue che il riconoscimento biometrico, installato sulle macchine con lo scopo di impedire l'utilizzo della macchina a soggetti non autorizzati, necessario per avviare il funzionamento della stessa, **può essere considerato uno strumento indispensabile a "*...rendere la prestazione lavorativa...*"** e pertanto si possa prescindere, ai sensi del comma 2 dell'art. 4 della L. n. 300/1970, sia dall'accordo con le rappresentanze sindacali sia dal procedimento amministrativo di carattere autorizzativo previsto dalla legge.

IL CAPO DELL'ISPETTORATO

Paolo Pennesi

Ispettorato Nazionale del Lavoro
Via Fornovo, 8 - 00192 Roma
Tel. 06 46837270
capoispettorato@pec.ispettorato.gov.it
segreteriacapoispettoratoi@ispettorato.gov.it