Verifica preliminare. Sistema di controllo accessi biometrico facciale - 16 febbraio 2017 [6136705]

[doc. web n. 6136705]

Verifica preliminare. Sistema di controllo accessi biometrico facciale - 16 febbraio 2017

Registro dei provvedimenti
n. 60 del 16 febbraio 2017

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 dott.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

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

VISTE le "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati" (deliberazione n. 53 del 23 novembre 2006 - doc. web n. 1364939);

VISTE le "Linee guida in materia di riconoscimento biometrico e firma grafometrica", allegate al provvedimento del Garante del 12 novembre 2014, come modificato dal provvedimento del 15 gennaio 2015 (doc. web nn. 3556992 e 3701432);

ESAMINATA la richiesta di verifica preliminare presentata da XX S.p.A., ai sensi dell´art. 17 del Codice, e le successive comunicazione inviate dalla Società;

VISTI gli atti d´ufficio;

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;

PREMESSO

1. L´istanza della Società

1.1. XX s.p.a, di seguito "XX" o "la Società", rappresentata dall´avv. Alberto Savi ed elettivamente domiciliata presso il suo studio, con la nota del 10 febbraio 2016, ha presentato all´Autorità, ai sensi dell´art. 17 del Codice, una richiesta di verifica preliminare relativa all´utilizzo di un sistema di "controllo accessi biometrico facciale".

La Società è proprietaria delle unità produttive che in Italia si occupano della realizzazione dei gioielli a marchio "XX" e nel nuovo stabilimento produttivo, in costruzione presso XX, vorrebbe implementare un impianto di controllo accessi biometrico con riconoscimento facciale per consentire l´ingresso allo stabilimento esclusivamente al personale autorizzato.

Il sistema non verrebbe utilizzato per finalità di rilevazione delle presenze del personale ma avrebbe come unica finalità la tutela dell´incolumità dei dipendenti e della sicurezza del patrimonio aziendale.

1.2. XX ha, altresì, chiesto al Garante di poter trattare i dati rilevati dal sistema biometrico senza richiedere il consenso degli interessati, ai sensi dell´art. 24, comma 1, lett. g) del Codice.

2. Il funzionamento del sistema

2.1. Il sistema che la Società intende installare non prevede la memorizzazione delle immagini dei volti durante la fase di enrollement.

Dalla lettura del volto è ricavato unicamente un codice numerico, c.d. template, dal quale vengono rilevate esclusivamente le posizioni reciproche di alcuni punti, c.d. "minuzie", senza identificare in modo univoco alcuna immagine.

Il template, dunque, non può contenere l´immagine del volto e, inoltre, non permette la ricostruzione di quest´ultima partendo dal codice numerico. Il template è sempre diverso per ogni lettura e non ha un valore deterministico ma viene valutato secondo una soglia di probabilità.

Il confronto fra la lettura e il codice numerico effettuato nel lettore verifica unicamente che le posizioni reciproche di almeno un certo numero di minuzie corrispondano.

Nella rete di lettori non transita alcun dato biometrico univoco né il template ma solo il codice identificativo di 8 cifre associato all´utente.

Agli interessati verrà comunque consegnato un badge per l´accesso allo stabilimento attraverso un controllo non biometrico.

La Società ha, infatti, previsto anche l´installazione di un sistema di controllo accessi costituito da un lettore di badge, che sarà posizionato in prossimità del lettore biometrico e che sarà utilizzato unicamente nell´eventualità che il sistema biometrico dovesse avere problemi di funzionamento. I due sistemi sarebbero quindi alternativi e il funzionamento dell´uno escluderà il funzionamento dell´altro.

Ai fini del funzionamento del sistema biometrico non è necessaria la conservazione o registrazione delle immagini rilevate. È tuttavia possibile conservare le immagini relative agli eventi registrati nei log e "tale funzione è disattivabile da configurazione".

2.2 Nessun dato biometrico viene conservato neanche ai fini di backup. È previsto solo il backup dei template attivi su un server dedicato al controllo accessi rispondente alle seguenti caratteristiche di sicurezza:

- registrazione degli accessi alla postazione da parte degli amministratori di sistema tramite idonei sistemi di raccolta dei log;

- adozione di 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;

- protezione dei sistemi informatici contro l´adozione di malware e adozione di sistemi di firewall per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati;

- adozione di misure e accorgimenti volti a ridurre i rischi di manomissione e accesso fraudolento al dispositivo di acquisizione;

- tecniche crittografiche di cifratura del riferimento biometrico con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati;

- conservazione dei riferimenti biometrici per il tempo strettamente necessario a realizzare le finalità del sistema biometrico;

- conservazione separata dei riferimenti biometrici e dei dati identificativi degli interessati;

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

3. Le valutazioni dell´Autorità

3.1. La raccolta e la registrazione di dati biometrici dei lavoratori dipendenti, ricavati dalle caratteristiche fisiche o comportamentali della persona a seguito di un apposito procedimento e poi risultanti in un modello di riferimento utilizzato per verifiche e raffronti nelle procedure di autenticazione o di identificazione, costituiscono operazioni di trattamento di dati personali alle quali, pertanto, devono applicarsi i principi contenuti nel Codice e richiamati nelle "Linee guida del Garante in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati" e nelle "Linee guida in materia di riconoscimento biometrico e firma grafometrica" allegate al provvedimento del Garante del 12 novembre 2014.

La liceità del sistema deve essere, pertanto, valutata sul piano della conformità ai princìpi di necessità, proporzionalità, finalità e correttezza (artt. 3 e 11 del Codice), tenendo conto della peculiarità dell´attività svolta dalla Società nello stabilimento in questione.

Stando alle dichiarazioni rese da XX, gli ambienti di lavoro in esame si caratterizzano per la loro delicatezza in ragione dell´elevatissimo valore delle materie prime e dei prodotti finiti ivi conservati. Il nuovo sito produttivo, infatti, sarà per la Società il polo produttivo e logistico più grande a livello mondiale e in esso verrà concentrata più della metà della produzione totale XX.

Per tale motivo la Società, al fine di garantire la sicurezza dei materiali e dei prodotti lavorati nonché delle persone che operano all´interno dello stabilimento, ha previsto l´adozione di un insieme articolato di misure di sicurezza quali impianto antincendio, impianto di allarme antintrusione, impianto di videosorveglianza (in relazione al quale, in data 8 luglio 2016, è stato raggiunto un accordo con le rappresentanze sindacali – cfr. nota del 13 luglio 2016), porte e infissi blindati, casseforti e caveaux, pulsanti antirapina, personale di sorveglianza, servizi di vigilanza.

La Società ha dichiarato che il sistema di controllo accessi prescelto consentirebbe di avere "contezza certa" dell´identità del personale presente all´interno dello stabilimento, garantendo un elevato livello di tutela dei beni e delle persone dal pericolo di furti e rapine ma anche da possibili violazioni del marchio e del copyright. E, conseguentemente, costituirebbe un utile strumento di limitazione dei danni, come richiesto anche dalle società assicurative.

Secondo la Società, inoltre, il sistema sottoposto a verifica preliminare, dal punto di vista tecnologico, garantirebbe maggiori vantaggi rispetto ad un sistema alternativo, quale quello basato sul rilevamento delle impronte digitali in associazione all´utilizzo di un impianto di videosorveglianza. Quest´ultimo invero, nel caso specifico, potrebbe vanificare il riconoscimento dell´impronta digitale di molti lavoratori (in particolare degli orafi) in ragione del fatto che tali soggetti quotidianamente svolgono un´attività manuale che presuppone principalmente l´uso dei polpastrelli (Cfr. nota del 18 ottobre 2016).

Pertanto, all´esito della valutazione comparativa effettuata dalla Società tra il sistema proposto e quello basato sul rilevamento dell´impronta digitale, e alla luce delle oggettive e concrete esigenze di sicurezza derivanti dall´ingente valore dei prodotti grezzi, lavorati e custoditi all´interno dello stabilimento, il titolare del trattamento ha ritenuto lecito e proporzionato l´impiego dell´illustrata tecnica biometrica basata sul riconoscimento facciale avente lo scopo di consentire l´accesso alle aree dello stabilimento esclusivamente ai soggetti autorizzati.

XX ha, altresì, assicurato che il sistema di controllo accessi che intende utilizzare rispetta, ad esclusione degli elementi non implementabili per le caratteristiche proprie della tecnologia utilizzata, le prescrizioni impartite dal Garante per i sistemi rientranti nei casi di esonero dall´obbligo di presentare istanza di verifica preliminare, individuati nel Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014.

3.2. La Società ha, inoltre, dichiarato che i lavoratori interessati all´utilizzo del sistema in esame riceveranno l´informativa ai sensi dell´art. 13 del Codice, (cfr. "informativa controllo accessi biometrico" - Allegato 1 alla istanza della Società), mentre idonea segnaletica sarà apposta in prossimità delle aree soggette a rilevamento biometrico.

Con riferimento alla richiesta di XX di poter effettuare il trattamento dei dati connesso all´utilizzo del sistema biometrico, senza il consenso dei dipendenti, per perseguire un legittimo interesse del titolare, ai sensi dell´art. 24, comma 1, lett. g) del Codice, si rileva che il controllo biometrico dell´accesso fisico ad uno stabilimento che ospiterà entro il 2018 più di 600 dipendenti e che rappresenterà per la Società il polo produttivo e logistico più grande a livello mondiale risulta condizione atta a giustificare la richiesta della Società volta ad ottenere tale esonero (peraltro riconosciuto dal Garante nel citato provvedimento generale in relazione all´ipotesi di accesso ad aree sensibili mediante impronte digitali).

Valutato quindi il legittimo interesse della società a implementare un sistema efficace di controllo degli accessi limitatamente allo stabilimento di cui si tratta, per esigenze di tutela dell´incolumità delle persone e di sicurezza del patrimonio aziendale, si ritiene

necessario prendere in considerazione ogni utile ed opportuno intervento volto a rafforzare la protezione dei dati personali trattati, considerate le caratteristiche tecniche del sistema biometrico che si intende implementare e le specifiche modalità del trattamento sottoposto a verifica preliminare, secondo quanto disposto nel successivo punto 3.3.

Pertanto, ferma restando la necessità di adottare le misure e gli accorgimenti illustrati di seguito, con il presente provvedimento il Garante, ai sensi dell´art. 24, comma 1, lett. g) del Codice, individua nel descritto trattamento di dati un´ipotesi in cui non è richiesto il consenso degli interessati, ritenendo il medesimo trattamento necessario per perseguire un legittimo interesse della Società,.

3.3. La Società resta tenuta a designare per iscritto tutti i soggetti che effettueranno le operazioni di trattamento (con particolare riguardo alla raccolta dei dati durante la fase di enrollement) quali incaricati o, eventualmente, responsabili, impartendo loro idonee istruzioni alle quali attenersi (artt. 29 e 30 del Codice).

La Società dovrà, inoltre, adottare le seguenti misure, se non già previste:

- l´accesso ai dati e al sistema deve essere consentito ai soli soggetti incaricati, muniti di specifiche credenziali o dispositivi di autenticazione forte; gli accessi ai dati devono essere tracciati e le 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 degli amministratori di sistema;

- le trasmissioni di dati tra i dispositivi di acquisizione e le postazioni di lettura devono essere 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;

- il sistema di controllo accessi, costituito dai dispositivi di acquisizione, dai lettori e dal server, deve utilizzare una LAN o VLAN dedicata, e deve essere separato dagli altri sistemi che trattano dati personali dei dipendenti per altre finalità;

- la funzione di configurazione del sistema che consente di conservare nei log le immagini relative agli eventi registrati deve essere disattivata.

Nulla viene detto in ordine all´obbligo di notificazione del trattamento ai sensi degli artt. 37 e 38 del Codice al quale la Società dovrà conformarsi, provvedendo a tale adempimento prima dell´entrata in funzione dell´impianto.

TUTTO CIÒ PREMESSO IL GARANTE

1) ai sensi dell´art. 17 del Codice, accoglie la richiesta di verifica preliminare presentata da XX s.p.a., nei termini di cui in motivazione, e a tal fine prescrive alla Società l´adozione delle misure di cui al punto 3.3 del presente provvedimento;

2) ai sensi dell´art. 24, comma 1, lett. g), del Codice, individua nel trattamento dei dati, correlato all´utilizzo del sistema di controllo accessi biometrico facciale, un´ipotesi in cui non è richiesto il consenso degli interessati.

Avverso il presente provvedimento può essere proposta opposizione ai sensi degli artt. 152 del Codice e 10 del d.lgs. n. 150 del 2011 con ricorso dinanzi all´autorità giudiziaria ordinaria, da presentarsi entro il termine di trenta giorni dalla data della sua comunicazione ovvero di sessanta giorni se il ricorrente risiede all´estero.

Roma, 16 febbraio 2017

IL PRESIDENTE
Soro

IL RELATORE
Iannini

IL SEGRETARIO GENERALE
Busia