

VIDEOSORVEGLIANZA, BIOMETRIA E PRIVACY

AVV. ROBERTO LATTANZI
Ufficio del Garante per la Protezione dei dati personali

Provvedimenti del Garante per la protezione dei dati personali

Provvedimento del 21 luglio 2005

Usò delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro

Provvedimento del 27 ottobre 2005

Istituti di credito - Rilevazione di impronte digitali ed immagini: limiti e garanzie

Provvedimento del 23 novembre 2005

Accesso ad aree riservate di particolari aziende: uso proporzionato di impronte digitali

Provvedimento del 23 febbraio 2006

Istituti di credito - Nuove tecnologie per accedere a servizi bancari

Provvedimento del 15 giugno 2006

Trattamento di dati personali biometrici di personale autorizzato per finalità di sicurezza

Provvedimento del 15 giugno 2006

Trattamento di dati personali biometrici nel rapporto di lavoro con finalità di verifica della presenza

Provvedimento del 26 luglio 2006

Sicurezza merci e controlli presenze presso aeroporti

USO DELLE IMPRONTE DIGITALI PER I SISTEMI DI RILEVAMENTO DELLE PRESENZE NEI LUOGHI DI LAVORO

- Provvedimento del 21 luglio 2005

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravallotti vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Esaminata la richiesta di verifica preliminare presentata da Landini S.p.a. ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), relativa al trattamento di dati personali biometrici al fine di verificare le presenze sul luogo di lavoro dei dipendenti;

Visti gli elementi acquisiti a seguito degli accertamenti avviati ai sensi dell'art. 154, comma 1, lettere a), del Codice;

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

Relatore il dott. Mauro Paissan;

PREMESSO:

1. Trattamento di dati personali biometrici nel rapporto di lavoro con finalità di verifica della presenza dei dipendenti

Landini S.p.a., industria di coperture in fibrocemento e metalliche che occupa circa trecento dipendenti, ha presentato a questa Autorità una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, relativa al trattamento di dati biometrici dei propri dipendenti finalizzato ad accertarne la presenza sul luogo di lavoro e commisurare, così, la retribuzione ordinaria e straordinaria da corrispondere.

Il funzionamento di questo sistema presuppone una fase di raccolta di dati biometrici (c.d. *enrollment*) nella quale la società, avvalendosi di apparecchiature elettroniche dotate di lettore di impronte digitali e di apposito *software*, trasformerebbe l'immagine di una porzione dell'impronta digitale dei lavoratori in un codice numerico, associandolo a ciascun lavoratore con la sua memorizzazione nel sistema informativo aziendale (senza sottoporlo a cifratura o ad altre tecniche equivalenti). Tale codice verrebbe utilizzato quale termine di paragone dei codici numerici ricavati dalla lettura delle (parti di) impronte digitali dei lavoratori, rilevate, in occasione di ciascun ingresso e uscita dal luogo di lavoro, attraverso lettori dislocati in diverse aree dell'azienda e connessi al relativo sistema informativo.

Il trattamento dei dati biometrici non perseguirebbe altra finalità che quella ora descritta. Stando alle dichiarazioni rese dalla società titolare del trattamento (e dal produttore del sistema), una volta terminata la fase di *enrollment*, non vi sarebbe ulteriore memorizzazione dell'impronta digitale. Ad avviso della società, non sarebbe possibile, inoltre, risalire all'impronta stessa a partire dal codice numerico generato.

Il trattamento di dati biometrici viene giustificato dall'esigenza di prevenire alcune condotte, anche abusive, da parte di alcuni dipendenti (consistenti nello scambio dei *badge*) e lo smarrimento delle tessere magnetiche attualmente in uso; viene quindi ritenuto che il trattamento dei dati biometrici consentirebbe di ovviare a tali inconvenienti, assicurando un grado elevato di certezza nell'identificazione dei lavoratori.

Stando alle dichiarazioni rese, verrebbe comunque assicurato ai lavoratori che siano impossibilitati a partecipare all'*enrollment* (in ragione delle proprie caratteristiche fisiche) o che non intendano acconsentire al trattamento, di attestare la propria presenza sul luogo di lavoro mediante l'apposizione della propria sottoscrizione in un registro delle presenze ubicato presso l'ufficio del personale con riconoscimento "a vista" o, ancora, ricorrendo ad altri "sistemi convenzionali".

2. Trattamento di dati biometrici e applicabilità della disciplina di protezione dei dati personali

Il caso sottoposto alla verifica preliminare di questa Autorità integra un'ipotesi di trattamento di dati personali.

I dati biometrici che verrebbero rilevati nel caso di specie (porzione dell'impronta digitale) sono informazioni ricavate dalle caratteristiche fisiche di interessati che si vorrebbero identificare in modo univoco, mediante un modello di riferimento (*template*). Quest'ultimo consiste nell'insieme di valori numerici ricavati, attraverso funzioni matematiche, dalle caratteristiche individuali sopra indicate, preordinati all'identificazione personale attraverso opportune operazioni di confronto tra il codice numerico ricavato ad ogni accesso e quello originariamente raccolto.

Sia le impronte dattiloscopiche (cfr. provv. Garante 19 novembre 1999, in *Boll.* n. 10, p. 68), ancorché raccolte in modo parziale e solo ai fini del completamento della fase dell'*enrollment*, sia i codici numerici successivamente utilizzati per le descritte operazioni di confronto, in quanto informazioni riferibili ai singoli lavoratori, sono dati personali (art. 4, comma 1, lett. b), del Codice). Ne discende, pertanto, l'applicazione della disciplina contenuta nel Codice, così nella fase dell'*enrollment*, come pure in relazione alle successive operazioni di confronto (con il correlato tracciamento degli orari di ingresso/uscita dal luogo di lavoro).

3. Qualità dei dati, misure di sicurezza e informativa rispetto al trattamento dei dati biometrici

Con riguardo al principio di qualità dei dati, dall'istruttoria svolta emergono perplessità in ordine al corretto funzionamento del sistema che si intende installare.

Allo stato, non risultano documentati i presupposti per un elevato grado di affidabilità del sistema medesimo, tanto che è stata programmata una fase di prova per testarne l'affidabilità. La società non è inoltre in grado, al momento, di indicare il livello della sua accuratezza ricorrendo ai parametri tecnici idonei ad individuare i "falsi negativi" (FRR–*False Rejection Rate*) e i "falsi positivi" (FAR–*False Acceptation Rate*). I sistemi di rilevazione di dati come quelli in esame devono invece offrire una rigorosa garanzia di affidabilità ed integrità dei dati, anche sulla base di certificazioni od omologazioni dei dispositivi che tengano eventualmente conto delle valutazioni di comitati tecnici indipendenti.

Inoltre, dagli elementi forniti non è possibile ricavare con certezza se siano adeguate le misure di sicurezza predisposte a protezione della rete di comunicazione elettronica sulla quale i dati biometrici sono trasmessi dai singoli lettori al sistema centralizzato di acquisizione dati. A tale proposito, una misura opportuna da parte del titolare del trattamento consisterebbe ad esempio nell'utilizzo di chiavi di cifratura dei dati biometrici, indicato anche a livello europeo (v., ad es., il *Documento di lavoro sulla biometria* del Gruppo per la tutela dei dati personali di cui all'art. 29 della direttiva n. 95/46/Ce del 1° Agosto 2003 (punto 3.6), in http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_it.pdf).

Anche l'informativa predisposta non risulta adeguata rispetto al trattamento che si intende porre in essere: come detto, dalle dichiarazioni acquisite emerge che, i lavoratori sarebbero liberi di aderire o meno al sistema di rilevazione delle presenze basato sull'utilizzo di dati biometrici; strumenti alternativi sarebbero previsti anche per i lavoratori impossibilitati, per ragioni fisiche, a registrare le presenze mediante l'impiego del sistema biometrico.

Tali dichiarazioni, però, non trovano conferma nell'informativa predisposta per gli interessati, secondo la quale il conferimento dei dati, ivi compresi i dati biometrici (espressamente richiamati sotto la voce "*ulteriori specificazioni particolari*"), avrebbe natura obbligatoria. Ciò, ha rilievo anche per la circostanza che il sistema potrebbe operare (con riguardo all'*enrollment* e ai successivi accessi nei luoghi di lavoro) solo con l'attiva collaborazione personale dei lavoratori interessati, i quali dovrebbero rendersi così disponibili –in assenza di una disposizione di legge che lo imponga ed impregiudicati i profili eventualmente connessi al coinvolgimento delle rappresentanze sindacali– a sottoporre una parte del proprio corpo alle operazioni necessarie per la rilevazione biometrica.

Manca, inoltre, nell'informativa ogni riferimento a tecniche alternative per la rilevazione delle presenze, contravvenendosi, così, all'art. 13 del Codice secondo il quale è necessario che le informazioni da rendere agli interessati enuncino chiaramente tutte le modalità impiegate nel trattamento e la tipologia di dati personali utilizzati per ciascuna di esse.

4. Dati biometrici e principi di protezione dei dati personali: finalità, necessità e pertinenza

Se le ragioni illustrate denotano più di un rilievo in ordine al sistema di rilevazione in esame, la sua liceità deve essere verificata altresì, sotto altri profili concernenti i principi di necessità, proporzionalità, finalità e correttezza, nonché di qualità dei dati (artt. 3 e 11 del Codice; art.6, direttiva n. 95/46/Ce).

A questo proposito, se pure rientra tra le legittime facoltà del datore di lavoro sovrintendere all'esecuzione della prestazione lavorativa (art. 2094 cod. civ.) verificando le presenze dei dipendenti e il rispetto dell'orario di lavoro anche ai fini del calcolo della retribuzione, ad esempio attraverso *badge*, non risulta documentato che il trattamento di dati biometrici in esame (con particolare riguardo all'impronta digitale) sia conforme ai principi di necessità e proporzionalità.

L'utilizzo di tali dati in luoghi di lavoro può essere giustificato in casi particolari, in relazione alle finalità e al contesto in cui essi sono trattati (ad esempio, accessi a particolari aree dell'azienda per le quali debbano essere adottati livelli di sicurezza particolarmente elevati in ragione di specifiche circostanze o attività ivi svolte), oppure per finalità di sicurezza del trattamento di dati personali (v. Allegato B) al Codice).

Non può invece ritenersi lecito un uso generalizzato e incontrollato dei medesimi dati, specie se si tratta di impronte digitali per le quali occorre anche prevenire eventuali utilizzi impropri e possibili abusi.

Considerata l'utilizzabilità di idonee modalità alternative per un accertamento parimenti rigoroso dell'identità personale, ma meno problematiche per la dignità stessa dei lavoratori interessati (art. 2 del Codice, modalità di cui non è stata rappresentata l'inefficacia nel caso di specie), l'illustrata finalità di computo dell'orario di lavoro in un'azienda come quella istante non risulta, dagli atti, legittimare la rilevazione di impronte digitali le quali sono comunque associate, contrariamente a quanto rilevato dall'istante, ai relativi interessati.

Al di là dei controlli ordinari e a campione circa la presenza dei lavoratori alle uscite e nei luoghi di lavoro, peraltro di agevole accertamento, non è stata dimostrata l'inefficacia, nel caso di specie, di misure che (senza ricorrere al trattamento di dati biometrici, nel rispetto dell'art. 3 del Codice) possono comunque contenere significativamente il rischio di pratiche abusive.

Il titolare del trattamento, per verificare la puntuale osservanza dell'orario di lavoro da parte dei lavoratori, impedendo in pari tempo condotte abusive dei medesimi, può disporre di altri sistemi meno invasivi della sfera

personale, della libertà individuale e che non coinvolgano il corpo del lavoratore –aspetti entrambi costitutivi della dignità personale, a presidio della quale sono dettate le discipline di protezione dei dati personali (art. 2 del Codice)–

Il trattamento in esame deve ritenersi sproporzionato anche in considerazione delle modalità tecniche prefigurate (centralizzazione dei codici identificativi derivati dall'esame del dato biometrico), ben potendosi adottare, anche da questo punto di vista, misure tecnologiche meno invasive. Infatti, anche a mente della disposizione contenuta nell'art. 3 del Codice, è da ritenere comunque preferibile, laddove sia ammesso il ricorso a dati biometrici, la memorizzazione del codice identificativo su un supporto che resti nell'esclusiva disponibilità dell'interessato (una volta completato il c.d. *enrollment*), piuttosto che la registrazione dello stesso a livello centralizzato nel sistema informativo aziendale (con conseguenti più gravi ripercussioni per i diritti individuali in caso di violazione delle misure di sicurezza, di accessi di persone non autorizzate o, comunque, di abuso delle informazioni memorizzate, anche ad opera di terzi).

In conformità con il quadro comunitario (il quale prescrive, non a caso, che i trattamenti di dati che comportano rischi specifici per i diritti e le libertà fondamentali degli interessati, come quello in esame, siano consentiti solo in presenza di una verifica preliminare volta ad appurare la liceità e correttezza del trattamento e ad impartire misure ed accorgimenti a garanzia degli interessati: art. 20 direttiva n. 95/46/Ce; art. 17 del Codice), deve pertanto riscontrarsi l'assenza nel caso di specie nei presupposti di legge per un trattamento di dati corrispondenti ad impronte digitali.

In conclusione, il trattamento oggetto di richiesta non può ritenersi lecito, nei termini di cui in motivazione.

TUTTO CIÒ PREMESSO, IL GARANTE:

ai sensi e per gli effetti di cui agli artt. 3, 11, 17 e 154, comma 1, lett. d) del Codice dichiara che il trattamento che Landini S.p.a. intenderebbe effettuare non risulta lecito, nei termini di cui in motivazione, e ne vieta pertanto lo svolgimento se effettuato per le finalità e con le modalità ivi descritte.

Roma, 21 luglio 2005

**ISTITUTI DI CREDITO - RILEVAZIONE DI IMPRONTE DIGITALI ED IMMAGINI:
LIMITI E GARANZIE**

- Provvedimento del 27 ottobre 2005 (G.U. n. 68 del 22-3-2006)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Vista la normativa internazionale e comunitaria in materia di protezione dei dati personali (direttiva n. 95/46/CE);

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), con particolare riguardo all'art. 17;

Visti i provvedimenti del Garante del 29 aprile 2004, in materia di videosorveglianza, e del 28 settembre 2001, relativo alle rilevazioni biometriche presso gli istituti di credito;

Esaminate le richieste di verifica preliminare presentate da vari istituti di credito ai sensi dell'art. 17 del Codice, relative al trattamento di dati personali biometrici in relazione ad esigenze di sicurezza presso sportelli bancari; vista la bozza di linee-guida che l'Associazione bancaria italiana intende inoltrare alle banche e che ha sottoposto all'attenzione di questa Autorità;

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

Relatore il dott. Giuseppe Fortunato;

PREMESSO

1. Introduzione

Alcuni istituti di credito hanno inoltrato a questa Autorità una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, relativa a trattamenti di dati personali consistenti nell'associazione di dati biometrici di clienti (risultanti, in particolare, dall'acquisizione di impronte digitali tramite scanner collegati o integrati in un sistema informatico) con altri dati personali, relativi anch'essi alla clientela, raccolti avvalendosi di sistemi di ripresa.

Le richieste sono state presentate, anche in relazione a quanto prescritto dal Garante con il provvedimento in materia di videosorveglianza del 29 aprile 2004 (punto 3.2.1), per consentire la raccolta di elementi di prova suscettibili di utilizzazione in caso di comportamenti delittuosi.

L'Associazione bancaria italiana, nel fornire alcuni dati statistici relativi a fenomeni criminosi posti in essere nei confronti di dipendenze bancarie (in particolare, a rapine), ha rappresentato a sua volta che l'esigenza di dotare di impianti di rilevazione biometrica talune filiali maggiormente esposte alla commissione di reati è condivisa da una pluralità di istituti.

All'esito della complessa istruttoria preliminare, il Garante ritiene necessario adottare un nuovo provvedimento di carattere generale che, sulla base dei principi generali già enunciati nel provvedimento del 28 settembre 2001 (in Bollettino n. 22/2001, p. 82), tenga conto delle novità sopravvenute con il Codice entrato in vigore il 1° gennaio 2004 (con particolare riguardo alle disposizioni contenute negli artt. 17, 24, comma 1, lett. g) e 154, comma 1, lett. c)). In relazione ai trattamenti di dati personali (diversi da quelli sensibili e giudiziari) che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, il Garante ha infatti il compito di individuare misure ed accorgimenti rivolti "a determinate categorie di titolari o di trattamenti" nell'ambito di una verifica preliminare all'inizio del trattamento (art. 17 del Codice).

Nel caso in esame (come già rilevato nel menzionato punto 3.2.1. del provvedimento del 2004), i rischi specifici sono determinati dall'installazione di "sistemi di videosorveglianza che prevedono una raccolta delle immagini collegata e/o incrociata e/o confrontata con altri particolari dati personali", e dalla particolare natura di alcuni dati trattati, segnatamente di quelli derivanti dalla rilevazione delle impronte digitali.

Il presente provvedimento mira, pertanto, ad individuare le misure e gli accorgimenti a garanzia degli interessati che dovranno essere posti in essere da tutti gli istituti di credito operanti sul territorio nazionale che intendano avvalersi dei sistemi descritti, qualora ne ricorrano i presupposti di seguito indicati e rispettando i principi contenuti nel Codice.

2. Liceità, finalità, necessità e proporzionalità

L'utilizzo generalizzato ed indiscriminato di sistemi che consentono l'identificazione degli interessati mediante la combinazione di diversi sistemi di rilevazione dati non è consentito, in quanto contrasta con il principio di necessità che impone di configurare i sistemi informativi e i programmi informatici escludendo il trattamento di dati personali non necessari -nel caso di specie, biometrici- in rapporto alle finalità che si intende perseguire (art. 3 del Codice).

Un'attività di raccolta indifferenziata di dati particolarmente significativi (quali quelli relativi alle impronte digitali), imposta all'intera clientela degli istituti bancari, non è lecita, tanto più se giustificata solo da una generica esigenza di sicurezza.

In mancanza di specifici elementi che comprovino una concreta situazione di elevato rischio, tale attività comporta infatti un sacrificio sproporzionato della sfera di libertà e della dignità delle persone interessate, esponendo, altresì, le stesse a pericolo di abusi in relazione a dati a sé riferibili particolarmente delicati quali sono le impronte digitali.

Il trattamento di tali dati personali è consentito, con l'osservanza di adeguate garanzie, soltanto quando debba essere perseguita l'esclusiva finalità di elevare il grado di sicurezza di beni e persone (segnatamente, del personale dipendente degli istituti di credito e della clientela). A tal fine è necessaria la ricorrenza di specifici elementi riconducibili a circostanze obiettive che devono evidenziare una concreta situazione di elevato rischio e che l'istituto bancario deve valutare con particolare cautela (cfr. Provv. 11 dicembre 2000, in Boll. n. 14-15/2000, p. 30; Provv. 7 marzo 2001).

Tali particolari condizioni, risultanti anche da concordanti valutazioni da parte degli organi competenti in materia di tutela dell'ordine e della sicurezza pubblica, possono derivare, in particolare, dalla localizzazione dello sportello bancario (ad esempio, ove lo stesso sia situato in aree ad alta densità criminale, o isolate o, comunque, poste nell'immediata prossimità di "vie di fuga"). Può altresì venire in considerazione la circostanza che lo sportello bancario, o altri sportelli siti nella medesima zona, abbiano subito rapine. Possono inoltre rilevare altre contingenti vicende che esponano a reale pericolo una o più filiali determinate (come ad esempio rilevato in passato, con riguardo alla maggiore "liquidità" presso gli sportelli bancari in corrispondenza dell'introduzione della moneta unica europea: cfr. Provv. 28 settembre 2001).

La sussistenza di tali circostanze deve essere altresì valutata periodicamente in rapporto a fattori suscettibili di incidere sulla soglia di esposizione a rischio (si pensi, ad esempio, all'istituzione di una postazione di pubblica sicurezza nelle immediate vicinanze, oppure al rafforzamento di servizi di sorveglianza privata all'interno della filiale). All'esito di tale valutazione periodica i trattamenti di dati non più giustificati devono essere cessati o sospesi.

3. Informativa

Gli interessati devono essere informati adeguatamente della presenza dei sistemi di acquisizione delle impronte digitali e dell'associazione di queste ultime con immagini raccolte (art. 13 del Codice). Ciò, prima che i dati siano rilevati e, comunque, prima dell'accesso a varchi a doppia porta o bussole.

L'informativa deve fornire gli elementi previsti dal Codice (art. 13) anche con formule sintetiche, ma chiare e senza ambiguità. Deve essere ben evidenziata la libertà di accedere in banca senza consentire il rilevamento dell'impronta digitale, sulla base di un procedimento alternativo basato anche su un'identificazione del cliente eventualmente necessaria.

Il Garante ha individuato un modello di informativa "minima" che i titolari del trattamento potranno utilizzare in corrispondenza dei varchi di accesso alle strutture della banca, che dovrà essere integrato con un'informativa più ampia esposta all'interno della dipendenza bancaria. Entrambi i modelli sono allegati in facsimile al presente provvedimento.

4. Misure ed accorgimenti

L'utilizzazione dei sistemi di rilevazione delle impronte digitali associata a sistemi di videosorveglianza deve avvenire nel rispetto degli ulteriori accorgimenti e misure a garanzia degli interessati, di seguito elencati.

a) modalità alternative di accesso alla banca

La rilevazione delle impronte digitali non può comportare una contrazione della libertà e della dignità degli utenti degli sportelli bancari. L'accesso tramite i descritti sistemi di rilevazione deve avvenire predisponendo un meccanismo che, in presenza di una difforme volontà del cliente, oppure dell'impossibilità del medesimo di prestarsi alle operazioni di trattamento in ragione di proprie condizioni personali, gli permetta di accedere comunque all'istituto bancario attraverso un ingresso alternativo (o comunque senza dover essere obbligato a rilasciare dati personali), con l'eventuale adozione di cautele rimesse alla ragionevole valutazione dei responsabili della filiale (come, ad esempio, con la richiesta di esibizione di un documento). Come già rilevato nel richiamato provvedimento del 2001, sono da ritenersi precluse eventuali pratiche vessatorie o comunque elusive dell'obbligo di consentire l'ingresso senza rilevazione dell'impronta.

b) modalità di raccolta

I sistemi di videosorveglianza installati devono essere orientati esclusivamente verso l'area di accesso all'istituto di credito, senza riprendere altri immobili e, in particolare, i loro ingressi.

Quanto ai dati biometrici da raccogliere, è sufficiente rilevare solo l'impronta dattiloscopica di una delle dita dell'interessato.

c) misure di sicurezza

I sistemi per la raccolta delle immagini (fisse o in movimento) e delle impronte digitali devono prevedere l'immediata cifratura dei dati, prima della loro registrazione in una banca dati comunque configurata, e devono garantire un livello elevato di sicurezza.

Deve essere assicurata l'associazione univoca tra le immagini e le impronte digitali, per evitare errori di identificazione.

Particolare attenzione deve essere dedicata alle tecniche crittografiche applicate alle immagini e alle impronte.

I dati devono essere trattati con sistemi di cifratura "robusti" con l'utilizzo, anche congiunto, di algoritmi crittografici simmetrici o asimmetrici.

In particolare, qualora si ricorra a tecniche di crittografia simmetrica per la cifratura dei dati e a crittografia asimmetrica o a chiave pubblica per la cifratura delle chiavi simmetriche relative a ciascun dato o a ciascuna porzione di dato, l'intero processo crittografico deve essere garantito dall'interposizione di un vigilatore dei dati (individuato nel titolare di una funzione di controllo interno in posizione di indipendenza, o da un soggetto parimenti indipendente da questi designato), depositario delle chiavi crittografiche idonee a decifrare le informazioni conservate dalla banca.

Deve essere infatti evitata la possibilità, anche solo tecnica, di decifrare le informazioni acquisite senza l'intervento del predetto vigilatore dei dati.

L'accesso alle informazioni "in chiaro", sia per esigenze di giustizia, sia in caso di esercizio dei diritti dell'interessato (art. 7 del Codice), deve avvenire solo tramite il medesimo vigilatore dei dati.

Resta fermo l'obbligo di adottare, in conformità al Codice, misure di sicurezza anche minime corrispondenti ai parametri previsti (art. 31 ss. e Allegato B del Codice), in particolare per quanto riguarda l'accesso degli incaricati o amministratori di sistema che abbiano un ruolo nella conduzione o nella manutenzione dei sistemi utilizzati.

I sistemi di rilevazione devono infine offrire una garanzia rigorosa di affidabilità e di integrità dei dati, anche sulla base di eventuali certificazioni od omologazioni dei dispositivi. In questa cornice, gli istituti presso i quali vengono installati i sistemi oggetto del presente provvedimento devono farsi rilasciare dall'installatore, e conservare, l'attestato di cui alla regola n. 25 del disciplinare tecnico in materia di misure minime di sicurezza (Allegato "B" al Codice).

d) conservazione dei dati

I dati cifrati relativi alle impronte e alle eventuali immagini devono essere conservati per un periodo non superiore ad una settimana e devono essere registrati cronologicamente in modo tale da consentire il loro pronto reperimento anche sulla base di un' opportuna organizzazione per giorni di rilevazione.

Devono essere predisposti meccanismi di integrale cancellazione automatica delle informazioni allo scadere del termine previsto. Deve essere altresì evitato un prolungamento surrettizio dei tempi di conservazione attraverso la creazione di copie di sicurezza.

Resta fermo che la banca, in presenza di una richiesta di accesso da parte dell'interessato, oppure di eventi criminosi verificatisi o, ancora, di una richiesta da parte dell'autorità giudiziaria, potrà assicurare la disponibilità dei dati raccolti, evitandone l'automatica cancellazione alla scadenza del periodo di conservazione previsto.

Da ultimo, non può ritenersi consentito alcun sistema di interconnessione dei dati raccolti con altri dati in possesso dell'istituto bancario o di terzi, o di creazione di ulteriori database, come pure di sistemi di riconoscimento facciale.

e) conoscibilità dei dati

Possono decifrare ed accedere alle informazioni raccolte con i sistemi di rilevazione soltanto le autorità giudiziarie e di polizia, con riferimento a specifiche attività investigative connesse all'accertamento o alla prevenzione di reati svolte in conformità al codice di procedura penale. Ciò, avvalendosi anche della cooperazione del predetto vigilatore dei dati, il quale può, se necessario, venire lecitamente a conoscenza di dati qualora presti la propria opera anche in caso di esercizio del diritto d'accesso da parte dell'interessato ai dati personali a sé riferiti.

Il personale, anche esterno alla banca, selettivamente preposto all'utilizzo e alla manutenzione delle apparecchiature, non deve invece poter accedere in alcun modo "in chiaro" alle informazioni cifrate (immagini ed impronte).

5. Bilanciamento di interessi

In presenza dei presupposti e delle condizioni sopra indicati, il trattamento dei dati personali potrà ritenersi lecito anche in assenza del consenso degli interessati, ai sensi dell'art. 24, comma 1, lett. g), del Codice.

Ciò, attesa la particolare finalità perseguita e considerando sia la temporaneità e le modalità del trattamento da effettuarsi nella rigorosa osservanza delle misure e degli accorgimenti prescritti con il presente provvedimento, sia le ulteriori finalità perseguite dagli altri titolari del trattamento ai quali i dati possono essere comunicati (identificati nell'autorità giudiziaria e nelle forze di polizia).

Il consenso dell'interessato deve ritenersi non necessario anche con riguardo alle operazioni di decrittazione dei dati trattati ad opera del vigilatore dei dati, le cui ulteriori operazioni di trattamento devono esaurirsi nella sola comunicazione dei dati "in chiaro" ai soggetti sopra individuati o all'interessato che abbia esercitato il diritto d'accesso riconosciuto dall'art. 7 del Codice.

6. Adempimenti

Resta in primo luogo fermo l'obbligo di notificare al Garante il trattamento dei dati secondo le modalità previste (art. 37, comma 1, lett. a) del Codice).

Ciascun istituto di credito è altresì tenuto ad inviare a questa Autorità, entro il 31 gennaio 2006^[4] e con un'unica comunicazione riguardante tutti i propri sportelli bancari, l'elenco di quelli per i quali i dispositivi in esame siano stati già attivati prima del presente provvedimento.

Ogni istituto di credito che intenda installare nuove apparecchiature, oppure modificare quelle esistenti, dovrà invece inoltrare, sempre al Garante, una specifica richiesta di verifica preliminare utilizzando i modelli riprodotti in allegato, verifica da svolgere una tantum ai sensi dell'art. 17 del Codice, prima dell'inizio del trattamento. A tal fine potrà essere effettuata un'unica comunicazione riguardante tutti gli sportelli della banca, indicando l'elenco di quelli per i quali intende attivare i dispositivi menzionati e le condizioni di concreto rischio poste a fondamento della loro installazione valutate in rapporto alle altre misure adottabili.

Da ultimo, in aggiunta alle predette prescrizioni, presso ogni sportello bancario dovrà essere comunque conservata e tenuta aggiornata, anche in previsione di verifiche disposte da questa Autorità, la seguente documentazione:

- a) copia della richiesta di verifica preliminare inviata al Garante;
- b) eventuale documentazione dalla quale si possa desumere l'esistenza di condizioni di rischio concreto dello sportello;
- c) documentazione tecnica relativa all'installazione dei sistemi biometrici e di videosorveglianza adottati, dal quale risulti la conformità dei medesimi alle condizioni indicate nel presente provvedimento. Dalla medesima devono evincersi:
 - le caratteristiche dell'impianto di ripresa (ad esempio, localizzazione della/e telecamera/e con l'indicazione delle caratteristiche tecniche);
 - le caratteristiche dell'impianto di raccolta del dato biometrico;
 - le caratteristiche del sistema informatico di gestione delle immagini e dei dati biometrici, con particolare riguardo alle fasi del processo crittografico;
 - l'indicazione del tempo massimo di conservazione dei dati;
- d) copia dell'informativa resa alla clientela;
- e) documentazione dalla quale si possano desumere le modalità alternative di accesso alla struttura della banca.

TUTTO CIÒ PREMESSO, IL GARANTE

1. ai sensi dell'art. 154, comma 1, lett. c), del Codice prescrive a tutti i titolari del trattamento di adottare le misure necessarie indicate nel presente provvedimento al fine di rendere il trattamento conforme alle disposizioni vigenti;
2. individua nei termini di cui in motivazione, ai sensi dell'art. 24, comma 1, lett. g) del Codice, i casi nei quali il trattamento dei dati personali nell'ambito dei sistemi informativi oggetto del presente provvedimento può essere effettuato dagli istituti di credito, nei limiti e alle condizioni indicate, per perseguire legittimi interessi senza richiedere il consenso degli interessati;
3. dispone che copia del presente provvedimento sia trasmesso al Ministero della giustizia–Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica Italiana ai sensi dell'art. 143, comma 2, del Codice.

Roma, 27 ottobre 2005

**ACCESSO AD AREE RISERVATE DI PARTICOLARI AZIENDE:
USO PROPORZIONATO DI IMPRONTE DIGITALI**

- Provvedimento del 23 novembre 2005

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Esaminata la richiesta di verifica preliminare presentata da Galileo Avionica S.p.a. ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), relativa al trattamento di dati personali biometrici al fine di controllare gli accessi di alcuni dipendenti ad un'area aziendale ad accesso limitato;

Visti gli elementi acquisiti a seguito degli accertamenti avviati ai sensi dell'art. 154, comma 1, lettere a), del Codice;

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

Relatore il dott. Mauro Paissan;

PREMESSO

1. Trattamento di dati personali biometrici di dipendenti con finalità di accesso a particolari aree aziendali

Galileo Avionica S.p.a., fornitrice di tecnologie per la difesa nel settore avionico ed elettronico (e controllata italiana della holding SELEX Sensors and Airborne Systems S.p.a.), ha presentato a questa Autorità una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, relativa al trattamento di dati biometrici di un numero ristretto di dipendenti non superiore a quindici unità, finalizzato a controllarne gli accessi in un'area aziendale circoscritta di superficie pari a circa trenta mq.

Tale misura, reputata dalla società capace di assicurare un grado elevato di certezza nell'identificazione del personale abilitato all'accesso, sarebbe a suo avviso conforme ai livelli di "sicurezza e riservatezza richiesti in ambiente NATO" (cfr. comunicazione Galileo Avionica S.p.A. del 30 settembre 2005) che dovrebbero essere rispettati per realizzare un particolare programma avionico. Al riguardo la Società ha dichiarato che il numero di lavoratori coinvolti non subirà variazioni trattandosi di personale in possesso di nulla osta di sicurezza (Nos) rilasciato dall'Autorità nazionale di sicurezza (A.n.s.) per trattare informazioni classificate al massimo livello di segretezza.

Il sistema che si intende utilizzare presuppone, in particolare, una raccolta di dati biometrici mediante apparecchiature dotate di lettore di impronte digitali e un apposito software; i dati verrebbero trasformati in un codice numerico (template), utilizzato esclusivamente per la raccolta e il successivo trattamento dei dati ai fini predetti (cfr. comunicazione Galileo Avionica S.p.A. del 30 settembre 2005).

2. Dati biometrici e disciplina di protezione dei dati personali: principi di liceità, finalità e pertinenza nel trattamento

Il caso sottoposto alla verifica preliminare di questa Autorità integra un'ipotesi di trattamento di dati personali.

Sia le impronte digitali, sia i dati da esse ricavati successivamente utilizzati per verifiche e raffronti nelle procedure di autenticazione o di identificazione sono informazioni personali riconducibili ai singoli interessati (art. 4, comma 1, lett. b), del Codice), alle quali trova applicazione la disciplina contenuta nel Codice (cfr. provvedimenti del Garante 19 novembre 1999, in Boll. n. 10, p. 68, doc. web n. 42058 e 21 luglio 2005, in Boll. n. 63, doc. web n. 1150679; in merito v. pure il documento di lavoro sulla biometria del Gruppo art. 29, direttiva n. 95/46/Ce -WP80-, punto 3.1).

L'uso generalizzato e incontrollato di dati biometrici dei lavoratori non è in linea di principio lecito, in particolare quando si tratta di impronte digitali le quali, per la loro particolare natura, impongono che siano prevenuti eventuali utilizzi impropri, nonché possibili abusi.

Tuttavia, gli elementi acquisiti nel caso di specie consentono di ritenere che il trattamento di dati oggetto dell'odierna verifica preliminare sia configurabile in termini leciti. Ciò, tenendo conto delle specifiche finalità perseguite nel contesto esaminato e di alcuni accorgimenti che la società intende adottare, nonché di quelli prescritti con il presente provvedimento rispetto alle concrete modalità di identificazione biometrica.

Nel caso di specie, la finalità perseguita dalla società titolare del trattamento (identificare in modo certo i soggetti abilitati all'accesso in un'area riservata e che vi hanno fatto ingresso) è lecita alla luce della fattispecie, del tutto peculiare, descritta in atti.

La stessa evidenza l'obiettivo necessità di effettuare un accertamento particolarmente rigoroso sia della legittimazione all'ingresso nella predetta area aziendale dei dipendenti autorizzati, sia dell'identità dei singoli lavoratori coinvolti (cfr. già, a questo proposito, Provv. del Garante 21 luglio 2005 cit.): le attività per le quali sono approntate le misure di identificazione sopra descritte richiedono infatti standard di sicurezza specifici ed elevati, nonché un quadro di certezza riguardo all'identificazione dei soggetti che vi partecipano, in quanto coinvolgono progetti industriali rilevanti per attività di difesa.

Il sistema è destinato ad operare unicamente per accedere ad un'area riservata e specificamente individuata, adibita alla realizzazione di un particolare programma avionico di rilevanza nazionale ed internazionale nel settore della difesa.

Formano oggetto di trattamento solo i dati pertinenti e non eccedenti rispetto alla finalità perseguita, riferiti (non alla generalità dei dipendenti ma soltanto) ad un numero ridotto di lavoratori interessati, individuati tra quelli in possesso di nulla osta di sicurezza ed impiegati in attività che comportano la necessità di trattare informazioni rigorosamente riservate.

Il sistema è, inoltre, realizzato in modo tale da contenere fino ad un massimo di 900 transazioni in entrata e in uscita; oltre tale soglia, i dati più risalenti vengono eliminati automaticamente.

Il trattamento di dati biometrici per lo scopo prefissato è così configurabile in termini proporzionati rispetto ai diritti individuali degli interessati, alla luce della finalità in concreto perseguita e delle modalità di trattamento che saranno adottate.

A tal fine, il meccanismo che la società potrà utilizzare dovrà essere basato – senza creare un archivio centralizzato di impronte digitali o di template - su un efficace sistema di verifica e di identificazione, improntato sulla lettura delle impronte digitali cifrate su uno strumento disponibile al lavoratore (smart card o analoghi dispositivi).

Un connesso dispositivo potrà però permettere alla società di annotare nel sistema informativo, tra le predette 900 transazioni in entrata e in uscita, altri dati personali univocamente identificativi dei lavoratori, che siano ritenuti necessari per registrare temporaneamente anche l'identità dei lavoratori che hanno fatto ingresso, di volta in volta, nell'area riservata, anziché la sola circostanza che vi siano entrate persone autorizzate, ma non specificamente individuate in relazione ai singoli accessi.

Dovranno essere impartite istruzioni riguardo all'eventuale perdita e sottrazione dei dispositivi affidati al lavoratore (anche rispetto alle tempestive comunicazioni dovute alla società), nonché al ciclo di utilizzazione dei dispositivi di autenticazione e, infine, alle procedure interne per verificare il sistema ed aggiornare, ove necessario, i dispositivi affidati ai lavoratori.

3. Qualità dei dati e misure di sicurezza rispetto al trattamento dei dati biometrici

Il sistema oggetto di verifica preliminare appare caratterizzabile in base ad un adeguato livello di affidabilità (risultante dai test di controllo realizzati dal produttore) e di sicurezza.

Con riguardo a quest'ultimo aspetto, le misure predisposte a protezione dei dati trasmessi dai singoli lettori al sistema centralizzato di acquisizione dei dati (separato dai sistemi informativi aziendali) risultano adeguate: i dati contenuti nell'archivio ad essi espressamente dedicato sono crittografati e protetti da password per impedirne l'accesso e il trattamento da parte di soggetti non autorizzati.

In attuazione dell'obbligo di adottare ogni misura anche minima di sicurezza prescritta dal Codice (art. 31 ss. e Allegato B), la società resta obbligata a farsi rilasciare dall'installatore del sistema, e conservare presso la propria struttura, l'attestato di cui alla regola n. 25 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato "B" al Codice), nonché ogni altra idonea certificazione od omologazione dei dispositivi impiegati.

Resta parimenti ferma, con particolare riguardo all'accesso ai dati da parte del responsabile per la gestione delle reti aziendali, la necessità di designare per iscritto tale soggetto come incaricato o, eventualmente, responsabile delle relative operazioni di trattamento, impartendogli idonee istruzioni alle quali attenersi.

4. Conservazione dei dati

I dati devono essere conservati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali sono stati raccolti e trattati (art. 11, comma 1, lett. e) del Codice).

Ne deriva anche l'obbligo per la società di eliminare i dati trattati al termine del programma, come peraltro anticipato dalle dichiarazioni in atti secondo cui i dati verranno appunto conservati per il tempo necessario alle lavorazioni e agli studi connessi al programma e successivamente cancellati.

5. Informativa agli interessati e notificazione del trattamento

La società ha dichiarato che i lavoratori interessati all'utilizzo del sistema in esame riceveranno un'ideale informativa scritta e che coloro che non vorranno o non potranno, anche in ragione delle proprie caratteristiche fisiche, avvalersi del sistema saranno interdetti dall'accesso all'area riservata ovvero potranno accedere solo se accompagnati da altro personale abilitato all'ingresso mediante l'impiego del descritto sistema di rilevazione biometrica.

L'informativa che la società dovrà rendere rispetto al trattamento che intende porre in essere nei confronti di tutti i lavoratori interessati deve risultare completa degli elementi previsti dal Codice (art. 13).

La società è, infine, tenuta a notificare al Garante il trattamento dei dati biometrici prima che abbia inizio (art. 37, comma 1, lett. a), del Codice).

TUTTO CIÒ PREMESSO IL GARANTE:

prescrive al titolare del trattamento, ai sensi degli artt. 17 e 154, comma 1, lett. c) del Codice, al fine di conformarsi alle disposizioni vigenti, di adottare le misure e gli accorgimenti a garanzia degli interessati nei termini di cui in motivazione e, con particolare riguardo a quanto indicato al punto 2) del provvedimento:

- di predisporre un sistema di verifica basato sul confronto tra le impronte rilevate ad ogni accesso all'area riservata e il template memorizzato e cifrato su un supporto che resti nell'esclusiva disponibilità dei lavoratori interessati, senza creare a tal fine un archivio centralizzato di impronte digitali o di template;
- di dotarsi di un dispositivo che permetta alla società di registrare nel sistema informativo dedicato all'archiviazione degli accessi all'area riservata le informazioni personali (anche in forma di codice) necessarie ad identificare univocamente i lavoratori che vi accedono.

Roma, 23 novembre 2005

ISTITUTI DI CREDITO - NUOVE TECNOLOGIE PER ACCEDERE A SERVIZI BANCARI

- Provvedimento del 23 febbraio 2006

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Esaminata la richiesta di verifica preliminare presentata da San Paolo Imi S.p.a. ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), relativa all'introduzione, in via sperimentale, di modalità di trattamento di dati personali biometrici e dell'utilizzo di una tessera-servizi che si avvale della tecnologia Rfid;

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 il dott. Giuseppe Fortunato;

PREMESSO

1. Trattamento di dati personali dei clienti attraverso il servizio sperimentale denominato "Service card"

San Paolo Imi S.p.A. ha presentato al Garante una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice in relazione al progetto sperimentale Filiale "High Tech".

In base ad esso, i clienti che lo richiedano verranno dotati di una smart card con microprocessore Rfid denominata Service Card, volta a facilitare la fruizione di taluni servizi rendendo immediatamente visibile sul terminale del personale operante presso la banca la "posizione" del cliente, e agevolando l'accesso diretto a talune aree dedicate (ad es., "chiosco banca diretta").

Nella smart card sarebbero memorizzate unicamente talune informazioni, non immediatamente correlabili al cliente (numero seriale precodificato della tessera, codice Abi della banca e codice del contratto di Internet Banking), conoscibili da parte del personale della banca all'atto di prestare servizi mediante la tecnologia Rfid (semplicemente accostando la "service card" ad un lettore). La service card non consentirebbe di tracciare la posizione geografica del detentore.

Inoltre, nel caso di operazioni bancarie poste in essere avvalendosi del sistema di Internet banking disponibile presso il "chiosco banca diretta" sito nella Filiale "High Tech", verrebbe attribuita al cliente la facoltà di identificarsi, oltre che ricorrendo alle tradizionali credenziali di autenticazione (Personal identification number-Pin), anche previo procedimento di controllo biometrico dell'identità. I dati biometrici verrebbero conferiti facoltativamente. Resterebbe altresì attribuito alla libera scelta del cliente l'utilizzo di un codice numerico di identificazione personale, in luogo del sistema biometrico (cfr. comunicazione San Paolo Imi S.p.A. del 14 novembre 2005, all. 1, punti 5 e 20).

Il procedimento biometrico volto ad identificare il cliente sarebbe basato sulla previa rilevazione dell'impronta digitale dell'interessato, sulla successiva trasformazione della medesima in sede di enrolment in un codice numerico (tramite una procedura che si asserisce essere "irreversibile", denominata one-way hashing, che renderebbe impossibile, ad avviso della richiedente, risalire non solo all'immagine dell'impronta digitale, ma anche al template da questa generato) e sulla memorizzazione di quest'ultimo in un archivio centralizzato della banca. Il template così registrato verrebbe quindi utilizzato quale termine di paragone rispetto ai dati biometrici rilevati in occasione di ciascuna autenticazione da parte del cliente nell'ambito dei servizi resi disponibili nella Filiale "High Tech". I dati biometrici dell'interessato, ove collimanti con quelli memorizzati nel database centralizzato, verrebbero dunque utilizzati per sostituire le credenziali di autenticazione più tradizionali.

2. Dati biometrici e disciplina di protezione dei dati personali: principi di liceità, finalità e pertinenza nel trattamento

La richiesta di verifica preliminare relativa all'utilizzo di dati biometrici riguarda un'ipotesi di trattamento di dati personali. Sia le impronte digitali, sia i dati biometrici da esse ricavati e successivamente utilizzati per verifiche e raffronti nelle procedure di autenticazione o di identificazione, sono informazioni personali riconducibili ai singoli interessati (art. 4, comma 1, lett. b), del Codice), alle quali trova applicazione la disciplina contenuta nel Codice (cfr. Prov. Garante 19 novembre 1999, in Boll. n. 10, p. 68, doc. web n. 42058; 21 luglio 2005, in Boll. n. 63, doc. web n. 1150679; 23 novembre 2005, in Boll. n. 66, doc. web n. 1202254; in merito v. pure Gruppo Art. 29, Documento di lavoro sulla biometria-Wp80, punto 3.1.).

La finalità perseguita dalla banca richiedente (titolare del trattamento), consistente nell'identificare i soggetti abilitati a svolgere attività negoziale presso aree della banca appositamente attrezzate ("chiosco banca diretta"), è lecita. Pur

potendo, a tal fine, essere utilizzati dati biometrici –assicurando i medesimi, allo stato, un elevato grado di attendibilità nel procedimento di identificazione–, risulta sproporzionata, invece, la centralizzazione in un database delle informazioni personali (in forma di template ricavati dalla rilevazione delle impronte digitali) trattate nell'ambito del descritto procedimento di riconoscimento biometrico: in ossequio al principio di necessità (art. 3 del Codice), i sistemi informativi devono essere infatti configurati in modo da ridurre al minimo l'utilizzazione di dati personali, e da escluderne il trattamento, quando le finalità perseguite nei singoli casi possono essere realizzate con altre modalità (in particolare, mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità).

Nella fattispecie sottoposta a verifica preliminare la banca, senza (aver la necessità di) creare un archivio centralizzato di impronte digitali o di template, e fatte salve le operazioni necessarie a generare il template in fase di enrolment, potrà avvalersi comunque di un sistema efficace di verifica e di identificazione biometrica, improntato però sulla lettura delle impronte digitali memorizzate sotto forma di template cifrato su uno strumento posto nell'esclusiva disponibilità del cliente (smart card o dispositivo analogo) –che ben potrebbe essere la stessa "service card"– in luogo della prospettata centralizzazione in un database.

Tale modalità di riconoscimento biometrico è parimenti idonea a garantire un adeguato livello di accuratezza in ordine all'accertamento dell'identità del detentore della smart card (il confronto delle impronte digitali con il template memorizzato sulla carta potrà essere realizzato, infatti, ricorrendo a procedure di matching on card o di matching on device), senza la costituzione di un archivio di informazioni personali –peraltro particolarmente delicate–, prevenendo così il rischio di eventuali utilizzi impropri o possibili abusi (in questo senso, v. Prov. Garante 23 novembre 2005, in <http://www.garanteprivacy.it>, doc. web n. 1202254).

3. Qualità dei dati e misure di sicurezza rispetto al trattamento dei dati biometrici

In attuazione dell'obbligo di adottare ogni necessaria misura di sicurezza, anche minima (art. 31 ss. e Allegato B al Codice), la banca resta obbligata a farsi rilasciare dall'installatore del sistema il previsto attestato di conformità, e a conservarlo presso la propria struttura (regola n. 25 dell'Allegato B al Codice).

Resta parimenti ferma, con particolare riguardo alla raccolta dei dati da parte degli incaricati operanti sotto la diretta autorità del responsabile del trattamento (che verrebbe individuato nel "responsabile pro tempore della Direzione Macchina Operativa Integrata": comunicazione San Paolo Imi del 14 novembre 2005, all. 1, punto 20), la necessità di designarli per iscritto, impartendo loro idonee istruzioni alle quali attenersi.

4. L'utilizzo della tecnologia Rfid

Non emergono, con riguardo alla "service card", profili di illiceità del trattamento. La tessera è sprovvista di informazioni immediatamente identificative (essendo la sola banca in grado di associarle al cliente). I dati personali in essa inseriti risultano pertinenti e non eccedenti, trattandosi di informazioni funzionali all'esecuzione delle operazioni bancarie. Anche in relazione alle modalità trasmissive delle informazioni mediante il sistema Rfid non risultano, allo stato, rischi specifici in relazione ai dati personali trattati: la tecnica utilizzata non caratterizza significativamente la modalità d'uso della tessera stessa rispetto alle tradizionali smart card, e la ridotta distanza operativa di lettura (non superiore a 2 centimetri) appare precludere l'acquisizione anche inconsapevole dei dati contenuti nella tessera da parte di soggetti estranei al trattamento.

Quale accorgimento aggiuntivo a garanzia dell'interessato (cfr. art. 17 del Codice), la banca dovrà attuare, dandone comunicazione a questa Autorità entro il 20 aprile 2006, le misure idonee affinché vengano inibite immediatamente, in modo automatico, tutte le funzioni connesse all'uso della carta in caso di smarrimento o furto della "service card".

Va rilevato che, stante il quadro emergente dal progetto, il personale della banca può comunque richiedere l'esibizione di documenti d'identità in corrispondenza dell'esecuzione di operazioni bancarie (cfr. in merito la decisione del Garante del 27 ottobre 2005, in <http://www.garanteprivacy.it>, doc. web n. 1189435).

5. Informativa, consenso e notificazione del trattamento

L'informativa che la banca ha predisposto (acquisita agli atti) include gli elementi previsti dalla legge (art. 13 del Codice).

Si constata altresì che la banca raccoglie uno specifico consenso degli interessati (sia per i trattamenti effettuati mediante la service card, sia per l'utilizzo di dati biometrici) e che provvederà a notificare al Garante il trattamento dei dati biometrici prima che abbiano inizio le operazioni di trattamento (art. 37, comma 1, lett. a), del Codice).

6. Considerazioni conclusive

I trattamenti di dati personali oggetto della presente verifica preliminare potranno essere effettuati nel rispetto delle misure e degli accorgimenti riassunti nel seguente dispositivo.

Esaurita la fase sperimentale realizzata presso la "Filiale High Tech", San Paolo Imi S.p.A. dovrà darne comunicazione a questa Autorità indicandone gli esiti per quanto attiene i profili di protezione dei dati personali. Valutata da parte del Garante l'adeguatezza degli accorgimenti e delle misure adottati e riscontrato, sempre da parte dell'Autorità, che non si siano manifestate controindicazioni per i diritti degli interessati, San Paolo Imi S.p.a. potrà

chiedere di attivare analoghi sistemi presso altre dipendenze senza che sia necessario sottoporli a nuova verifica preliminare, sempreché ne restino inalterate le caratteristiche.

TUTTO CIÒ PREMESSO IL GARANTE

prescrive al titolare del trattamento, ai sensi degli artt. 17 e 154, comma 1, lett. c) del Codice, al fine di conformarsi alle disposizioni vigenti, di adottare le misure e gli accorgimenti a garanzia degli interessati nei termini di cui in motivazione, dandone comunicazione a questa Autorità entro il 20 aprile 2006, ed in particolare:

- a) in relazione a quanto indicato al punto 2 di cui in motivazione, predisporre un sistema di verifica basato sul confronto tra le impronte rilevate ad ogni accesso al sistema e il template memorizzato e cifrato su un supporto che resti nell'esclusiva disponibilità degli interessati, senza creare un archivio centralizzato di template tratti dalle impronte digitali;
- b) in relazione a quanto indicato al punto 4, attuare le misure idonee affinché vengano immediatamente inibite, in modo automatico, tutte le funzioni connesse all'uso della "service card", in caso di smarrimento o furto.

Roma, 23 febbraio 2006

- Provvedimento del 15 giugno 2006

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Esaminata la richiesta di verifica preliminare presentata dalla Cassa di risparmio di Ferrara S.p.a. ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

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 il dott. Mauro Paissan;

PREMESSO

1. Trattamento di dati personali biometrici di personale autorizzato per finalità di sicurezza, riservatezza e protezione dei beni in una particolare area della sede dell'istituto bancario

La Cassa di risparmio di Ferrara S.p.a. ha presentato una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, relativa al trattamento di dati biometrici di un numero ristretto di soggetti (complessivamente non superiore a trenta unità, comprendenti amministratori e dipendenti della banca) autorizzati all'accesso ad un'area particolare della sede nella quale sono situati gli uffici della presidenza e la direzione generale della banca. Si tratta, segnatamente, di un piano dell'edificio (non aperto al pubblico e privo di sportelli e uffici operativi) al quale allo stato si accede, previo riconoscimento da parte del personale di portineria, cui è rimesso il compito di azionare l'arresto degli ascensori al piano sopra indicato.

Le finalità di tale sistema sono di garantire la sicurezza del personale della direzione (evitando che persone estranee accedano a tale area: come accaduto in passato: cfr. richiesta di verifica preliminare), la riservatezza di documenti e fascicoli, nonché la protezione di opere d'arte ivi custodite.

Il sistema di riconoscimento, isolato e non comunicante con altri, non verrebbe utilizzato per ulteriori finalità; la sua adozione consentirebbe ai soggetti autorizzati –che su base volontaria e previa informativa intendano avvalersene– di salire al piano senza l'intervento del personale di portineria, utilizzando i menzionati ascensori dotati al proprio interno di un apposito lettore delle impronte digitali. Una volta raccolta, l'immagine dell'impronta dell'ultima falange del dito destro o sinistro verrebbe trasformata in un algoritmo matematico, successivamente confrontato con il modello registrato in un database dedicato, nel quale sarebbero centralizzati i template dei soggetti autorizzati.

A giudizio della banca non sarebbe possibile ricostruire il dato biometrico originario, tenendo conto del fatto che il codice numerico generato verrebbe criptato.

Le informazioni relative agli accessi al piano (data ed ora) verrebbero conservate per un periodo di sette giorni e, con cadenza semestrale, verrebbero aggiornati i nominativi dei soggetti autorizzati ad avvalersi della descritta procedura (cfr. comunicazioni della banca del 27 dicembre 2005 e del 20 marzo 2006).

2. Dati biometrici e disciplina di protezione dei dati personali: principi di liceità, finalità e pertinenza nel trattamento

2.1. Il caso sottoposto alla verifica preliminare di questa Autorità integra un'ipotesi di trattamento di dati personali. Sia le impronte digitali, sia i dati da esse ricavati e successivamente utilizzati per verifiche e raffronti nelle procedure di autenticazione o di identificazione sono informazioni personali riconducibili ai singoli interessati (art. 4, comma 1, lett. b), del Codice), alle quali trova applicazione la disciplina contenuta nel Codice (cfr. Provv. 19 novembre 1999, in Boll. n. 10, p. 68, doc. web n. 42058 e 21 luglio 2005, in Boll. n. 63, doc. web n. 1150679; in merito v. pure il documento di lavoro sulla biometria del Gruppo art. 29, direttiva n. 95/46/Ce -wp80-, punto 3.1.).

L'uso generalizzato e incontrollato di dati biometrici, specie se ricavati dalle impronte digitali, non è in linea di principio lecito. Tali dati, per la loro peculiare natura, richiedono l'adozione di elevate cautele al fine di prevenire possibili pregiudizi ai danni degli interessati, con particolare riguardo a condotte illecite che determinino l'abusiva "ricostruzione" dell'impronta partendo dal template e la sua ulteriore "utilizzazione" all'insaputa degli stessi.

L'utilizzo di dati biometrici può essere, quindi, giustificato in casi particolari, tenuto conto delle finalità e del contesto in cui essi sono trattati e, in relazione ai luoghi di lavoro, per presidiare accessi ad "aree sensibili", considerata la natura delle attività ivi svolte (si pensi, ad esempio, a processi produttivi pericolosi o sottoposti a segreti, di varia natura: cfr. Provv. 23 novembre 2005, in <http://www.garanteprivacy.it>, doc. web n. 1202254) o in ragione della documentazione o dei beni ivi custoditi (quali, documenti segreti o riservati, oggetti di valore, etc.).

2.2. Nella fattispecie in esame, la finalità perseguita dalla banca è, in termini generali, lecita. La centralizzazione in un database delle informazioni personali (in forma di template) trattate nell'ambito del descritto procedimento di riconoscimento biometrico risulta, tuttavia, sproporzionata e non necessaria, atteso che i sistemi informativi devono

essere configurati in modo da ridurre al minimo l'utilizzazione di dati personali e da escluderne il trattamento, quando le finalità perseguite possono essere realizzate con modalità tali da permettere di identificare l'interessato solo in caso di necessità (artt. 3 e 11 del Codice).

In luogo della prospettata centralizzazione, deve ritenersi adeguato e sufficiente avvalersi di un sistema efficace di verifica e di identificazione biometrica basato sulla lettura delle impronte digitali memorizzate, sotto forma di template cifrato, su un supporto posto nell'esclusiva disponibilità dell'interessato (smart card o dispositivo analogo) e privo di indicazioni nominative a quest'ultimo riferibili (quale un codice individuale).

Tale modalità di riconoscimento, infatti, è parimenti idonea ad assicurare che possano accedere all'area riservata solo coloro che, previamente autorizzati, decidano su base volontaria di avvalersi della smart card –in relazione alla quale il confronto delle impronte digitali con il template memorizzato sulla carta potrà essere realizzato ricorrendo a procedure di matching on card o di matching on device–; è possibile così evitare la costituzione di un archivio di dati biometrici (come detto particolarmente delicati), prevenendo il rischio di eventuali utilizzi impropri dei dati o di possibili abusi (in questo senso, v. Provv. 23 novembre 2005, in <http://www.garanteprivacy.it>, doc. web n. 1202254).

3. Informativa agli interessati e notificazione del trattamento

L'informativa che la banca dovrà rendere rispetto al trattamento che intende porre in essere deve risultare completa degli elementi previsti dal Codice (art. 13).

In particolare, tenuto conto del diverso sistema suscettibile di impiego secondo l'avviso di questa Autorità (indicato al punto 2.2.), l'informativa (in atti) predisposta dalla banca –nella quale è, peraltro, chiaramente rappresentato il carattere volontario del ricorso al sistema di riconoscimento biometrico–, dovrà essere integrata con riguardo al profilo relativo alle modalità del trattamento.

4. Misure ed accorgimenti

4.1. La banca resta tenuta a designare per iscritto tutti i soggetti che effettuino operazioni di trattamento dei dati (con particolare riguardo alla registrazione dei template sui menzionati supporti), quali incaricati o, eventualmente, responsabili delle operazioni di trattamento, impartendo loro idonee istruzioni alle quali attenersi.

Tali istruzioni dovranno riguardare anche le misure da adottare in caso di eventuale perdita e sottrazione dei dispositivi, nonché al ciclo di utilizzazione dei dispositivi di autenticazione e le procedure interne per verificare il sistema ed aggiornare, ove necessario, i dispositivi affidati.

4.2. In attuazione dell'obbligo di adottare ogni misura anche minima di sicurezza prescritta dal Codice (art. 31 ss. e Allegato B), la banca dovrà farsi rilasciare dall'installatore del sistema il prescritto attestato di conformità e conservarlo presso la propria struttura (regola n. 25 del Disciplinare tecnico in materia di misure minime di sicurezza - Allegato "B" al Codice).

4.3. La società dovrà notificare al Garante il trattamento dei dati biometrici prima che abbiano inizio le operazioni di trattamento (art. 37, comma 1, lett. a), del Codice).

5. Conservazione dei dati

I dati personali necessari alla realizzazione del template potranno essere trattati esclusivamente durante tale fase (c.d. enrollment).

I dati relativi agli orari di accesso dei soggetti che utilizzeranno il descritto sistema di riconoscimento biometrico, accessibili al personale preposto al rispetto delle misure di sicurezza all'interno della banca e per l'esclusiva finalità dell'osservanza delle medesime, potranno essere conservati per il tempo massimo di sette giorni, assicurando, oltre il predetto arco temporale meccanismi di cancellazione automatica dei dati. Tale intervallo temporale, peraltro indicato nella richiesta formulata dalla banca, appare ragionevole tenendo conto della documentazione e dei beni custoditi nell'area riservata (che si intendono con tale sistema proteggere), la cui sottrazione potrebbe essere scoperta a distanza di tempo.

TUTTO CIÒ PREMESSO IL GARANTE

prescrive al titolare del trattamento, ai sensi degli artt. 17 e 154, comma 1, lett. c), del Codice, di adottare le misure e gli accorgimenti a garanzia degli interessati nei termini di cui in motivazione, ed in particolare:

- di predisporre un sistema di riconoscimento basato sul confronto tra le impronte rilevate ad ogni accesso all'area riservata e il template memorizzato e cifrato su un supporto che resti nell'esclusiva disponibilità degli interessati, senza creare a tal fine un archivio centralizzato di impronte digitali o di template individuali (punto 2.2.);
- di riformulare l'informativa resa agli interessati, con riferimento alle modalità impiegate nel trattamento, descritte al punto 2.2 del presente provvedimento (punto 3.);
- di conservare i dati relativi agli orari di accesso all'area riservata per il tempo massimo di sette giorni (punto 5).

Roma, 15 giugno 2006

- Provvedimento del 15 giugno 2006

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Esaminata la richiesta di verifica preliminare presentata da Molino Casillo Francesco s.r.l. ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

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 il dott. Giuseppe Fortunato;

PREMESSO

1. Trattamento di dati personali biometrici nel rapporto di lavoro con finalità di verifica della presenza dei dipendenti e di accesso a particolari aree produttive

Molino Casillo Francesco s.r.l., società che svolge attività industriale di carattere molitorio (lavorazione di grano duro finalizzata a produrre semola per pastificazione), ha presentato a questa Autorità una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, relativa al trattamento di dati biometrici (ricavati dalla lettura delle impronte digitali) di un numero circoscritto di dipendenti (trentadue unità su circa sessanta che accedono all'area produttiva) finalizzato, contestualmente, a controllarne gli accessi a due stabilimenti ove si effettua l'attività molitoria e a rilevarne la presenza per determinare la retribuzione da corrispondere.

Il sistema ipotizzato, installato in corrispondenza delle porte di accesso agli stabilimenti, è ritenuto dalla società idoneo ad identificare il personale addetto alle lavorazioni svolte senza interruzioni presso "impianti classificati come molitori e a rischio di incendio medio a norma del d.m. l. del 16 febbraio 1982", nonché "soggetti alla direttiva Atex riguardante luoghi con pericolo di esplosione per la presenza di polveri" (cfr. punto 18 della comunicazione Molino Casillo Francesco s.r.l. del 20 febbraio 2006).

La società ha dichiarato che i lavoratori interessati alla rilevazione biometrica sarebbero solo gli operai addetti agli impianti, che operano in due turni diurni ed uno notturno. Ciò in quanto l'accesso di personale non specializzato esporrebbe a rischio l'incolumità di tutti i lavoratori. Resterebbe escluso il personale impiegatizio, il quale accede ai soli uffici amministrativi –ubicati nello stesso edificio di uno dei due impianti di lavorazione, ma "senza diritto di accesso all'impianto"– e la cui presenza giornaliera verrebbe rilevata mediante una tessera magnetica di prossimità.

Il sistema che si intenderebbe utilizzare presuppone, in particolare, una raccolta di dati biometrici mediante apparecchiature dotate di lettore di impronte digitali e di un apposito software. I dati verrebbero trasformati in un template cifrato su una smart card posta nell'esclusiva disponibilità del lavoratore. Il template sarebbe confrontato con altro codice numerico ricavato dall'impronta rilevata in occasione di ogni ingresso del lavoratore all'impianto. L'associazione tra i due codici, preceduta da una lettura della tessera di prossimità (effettuata mediante il menzionato lettore), consentirebbe l'accesso all'impianto, mentre l'uscita sarebbe "sempre possibile per motivi di sicurezza" (cfr. punti 8-14 della comunicazione Molino Casillo Francesco s.r.l. del 20 febbraio 2006; cfr., inoltre, la comunicazione della società del 10 dicembre 2005).

2. I principi di necessità, liceità, finalità e pertinenza nel trattamento di dati biometrici dei lavoratori

2.1. La raccolta e la registrazione di impronte digitali e dei dati biometrici ricavati e successivamente utilizzati per verifiche e raffronti nelle procedure di autenticazione o di identificazione, sono operazioni di trattamento di dati personali riconducibili ai singoli interessati (art. 4, comma 1, lett. b), del Codice), alle quali trova applicazione la normativa contenuta nel Codice (v. Provv. 19 novembre 1999, in Boll. n. 10, p. 68, doc. web n. 42058; 21 luglio 2005, in Boll. n. 63, doc. web n. 1150679; 23 novembre 2005, in Boll. n. 66, doc. web n. 1202254; in merito v. pure il documento di lavoro sulla biometria del Gruppo art. 29, direttiva 95/46/Ce –Wp 80–, punto 3.1.).

La liceità del sistema deve essere pertanto valutata sul piano della conformità ai principi di necessità, proporzionalità, finalità e correttezza (artt. 3 e 11 del Codice).

2.2. Con riguardo al trattamento di dati biometrici allo scopo di regolare l'accesso ad aree particolari dell'azienda deve rilevarsi che, in base alle dichiarazioni rese dalla società, gli ambienti di lavoro in esame, per la natura e le modalità di svolgimento delle lavorazioni in essi effettuate, si caratterizzano per la loro pericolosità. In ragione di ciò, essi sono inclusi nell'elenco delle attività soggette a visite e controlli periodici dei vigili del fuoco

al fine del rilascio del certificato di prevenzione incendi (v. il punto 35 del decreto del Ministero dell'interno 16 febbraio 1982) e sono soggetti all'ambito applicativo di due direttive europee denominate "ATEX-ATmosfere EXplosive", relative al rischio di presenza di atmosfera esplosiva in ambienti di lavoro, nonché alle successive norme di attuazione (cfr. direttiva 94/9/Ce, in vigore dal 1° luglio 2003, relativa alle attrezzature e/o strumenti di lavoro; direttiva 99/92/Ce, in vigore dal 10 settembre 2003, relativa all'uomo e all'ambiente di lavoro in cui opera; d.lg. 12 giugno 2003, n. 233 di attuazione della direttiva 99/92/Ce).

Atteso che rientra tra gli obblighi del datore di lavoro adottare le misure necessarie a tutelare l'integrità fisica dei lavoratori (art. 2087 c.c.; v. anche d.lg. n. 626/1994 e successive modifiche ed integrazioni), l'accesso ai predetti impianti può essere limitato al solo personale addetto, tecnicamente specializzato. Ciò, anche attraverso la verifica dell'identità di coloro i quali accedono a tali luoghi di lavoro, resa in tal caso possibile, con maggiore accuratezza, grazie all'impiego di sistemi biometrici.

Allo stato attuale delle conoscenze tecnologiche, nel caso di specie non appare sproporzionato l'uso di dati biometrici tratti dalle impronte digitali, atteso che il template viene memorizzato su un supporto, privo di indicazioni nominative riferibili all'interessato (essendo sufficiente inserire un codice individuale), destinato a restare nell'esclusiva disponibilità di quest'ultimo. Inoltre, come dichiarato dalla società (cfr. punto 12 della comunicazione Molino Casillo s.r.l. del 20 febbraio 2006) il template memorizzato sulla smart card (senza che ricorrano, peraltro, esigenze di interoperabilità) risulta essere protetto con una chiave crittografica e con un codice alfanumerico per la lettura.

- 2.3. Il trattamento di dati biometrici sopra descritto non risulta invece lecito in rapporto al perseguimento della diversa finalità di rilevazione della presenza dei dipendenti, rispetto alla quale la società non ha peraltro addotto ragioni specifiche volte a chiarire la necessità dell'utilizzo di tali peculiari modalità di trattamento per verificare il puntuale adempimento della prestazione lavorativa. Verifica che, dato il numero esiguo di lavoratori presenti per ciascun turno nei due impianti molitori, può essere ad esempio svolta agevolmente dal responsabile di ciascun turno sì da apparire, oltre che non necessario, anche sproporzionato il ricorso ai dati biometrici per la descritta finalità (artt. 3 e 11 del Codice).

Peraltro, tale peculiare modalità di verifica dell'osservanza dell'orario di lavoro verrebbe ad essere introdotta solo nei confronti di un gruppo di dipendenti, anziché ai restanti lavoratori per i quali la società non pone in discussione le modalità di rilevazione delle presenze in uso che continuerebbero, quindi, ad essere utilizzate.

La finalità in esame può dunque essere legittimamente perseguita, nel caso di specie, senza ricorrere ad alcun trattamento di dati biometrici (nel rispetto dell'art. 3 del Codice), avvalendosi del sistema già in uso o di un altro idoneo sistema.

3. Informativa e consenso degli interessati, misure di sicurezza e notificazione del trattamento

- 3.1. L'informativa allo stato predisposta dalla società –peraltro non chiara in ordine alle finalità che si intenderebbero perseguire (non menzionando chiaramente la finalità di commisurazione del tempo di lavoro che, nel caso di specie, non può peraltro essere perseguita con le modalità ipotizzate dalla società)– dovrà essere riformulata (nei soli confronti dei lavoratori interessati) in modo da tener conto delle misure sopra indicate e da includere tutti gli elementi previsti all'art. 13 del Codice.
- 3.2. Preso atto che la società raccoglie un consenso specifico degli interessati (per l'utilizzo di dati biometrici), in relazione all'eventualità che alcuni lavoratori non possano o non intendano aderire alla rilevazione biometrica effettuata nei termini di cui in motivazione, risulta praticabile il sistema di identificazione alternativo prospettato dalla società, consistente nel riconoscimento del personale entrante negli impianti da parte di quello uscente.
- 3.3. La società dovrà notificare al Garante il trattamento dei dati biometrici prima che abbiano inizio le operazioni di trattamento (art. 37, comma 1, lett. a), del Codice).
- 3.4. In attuazione dell'obbligo di adottare ogni misura di sicurezza, anche minima, prescritta dal Codice (art. 31 ss. e Allegato B), la società dovrà farsi rilasciare dall'installatore del sistema il prescritto attestato di conformità e conservarlo presso la propria struttura (regola n. 25 dell'Allegato B al Codice).
- 3.5. La società resta tenuta a designare per iscritto tutti i soggetti che effettuino operazioni di trattamento dei dati (con particolare riguardo alla registrazione del template sul supporto assegnato al dipendente), quali incaricati o, eventualmente, responsabili delle operazioni di trattamento, impartendo loro idonee istruzioni alle quali attenersi (artt. 29 e 30 del Codice).

4. Conservazione dei dati

I dati personali necessari alla realizzazione del template potranno essere trattati esclusivamente durante tale fase.

I dati relativi agli orari di ingresso agli impianti molitori, accessibili al personale preposto al rispetto delle misure di sicurezza all'interno dell'azienda e per l'esclusiva finalità dell'osservanza delle medesime, potranno essere conservati

per il tempo massimo di 48 ore, assicurando, oltre il predetto arco temporale, meccanismi di cancellazione automatica dei dati.

TUTTO CIÒ PREMESSO IL GARANTE

preso atto del trattamento di dati biometrici effettuato mediante un sistema di verifica basato sul confronto tra le impronte rilevate ad ogni accesso all'area riservata e il template, memorizzato e cifrato su un supporto che resti nell'esclusiva disponibilità dei lavoratori interessati (punto 2.1. e 2.2.), prescrive a Molino Casillo s.r.l., ai sensi degli artt. 17 e 154, comma 1, lett. c), del Codice, di adottare le misure e gli accorgimenti a garanzia degli interessati nei termini di cui in motivazione e, in particolare:

- di riformulare l'informativa resa ai lavoratori interessati dal trattamento dei dati biometrici, indicando con chiarezza nella medesima le finalità perseguite e gli ulteriori elementi indicati all'art. 13 del Codice (punto 3.1.);
- di conservare i dati relativi agli orari di accesso agli impianti molitori per il tempo massimo di 48 ore (punto 4);
- vieta, ai sensi dell'art. 154, comma 1, lett. d), del Codice, il trattamento dei dati biometrici mediante il sistema descritto in narrativa per le finalità di rilevazione della presenza dei lavoratori (punto 2.3.).

Roma, 15 giugno 2006

SICUREZZA MERCI E CONTROLLI PRESENZE PRESSO AEROPORTI

- Provvedimento del 26 luglio 2006

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravallotti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Esaminata la richiesta di verifica preliminare presentata da Alha Airport S.p.a. ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

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 il dott. Giuseppe Fortunato;

PREMESSO

1. Trattamento di dati personali biometrici di lavoratori con finalità di accesso ad aree riservate aeroportuali e di verifica della presenza dei dipendenti

- 1.1. Alha Airport S.p.a. –società che, in possesso della qualifica di "Agente di handling autorizzato" rilasciata dal Servizio vigilanza prevenzione di polizia e procedure aeroportuali dell'E.n.a.c., svolge attività di movimentazione a terra di merci e passeggeri in ambito aeroportuale (ora disciplinata dal d.lg. 13 gennaio 1999, n. 18)– ha presentato a questa Autorità una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, relativa al trattamento di dati biometrici (ricavati dalla lettura delle impronte digitali) del personale che ha accesso ad alcuni locali della propria sede operativa dell'aeroporto di Milano-Malpensa: si tratterebbe, in particolare, di un magazzino di stoccaggio delle merci e di un caveau (nel quale sono depositati beni di particolare valore). Tali ambienti sono ubicati nelle c.d. aree "sterili" ("security restricted area"), soggette a controlli e procedure inerenti la tutela della sicurezza e dell'ordine pubblico previsti dal "Programma nazionale di sicurezza" per esigenze "[...] di tutela di persone e cose e di prevenzione del rischio [...] di atti terroristici [...]" (cfr. d.P.R. 4 luglio 1985, n. 461); analogo sistema verrebbe altresì installato per accedere agli uffici della società presenti nell'area aeroportuale.

La società ha dichiarato e documentato di dover rispettare, oltre alle procedure del Programma nazionale di sicurezza che mirano a "[...] prevenire l'introduzione illecita, nelle stive degli aeromobili, di armi non autorizzate, di ordigni, di esplosivi e di ogni altro oggetto in grado di causare grave turbativa al normale svolgimento del traffico aereo civile", anche ulteriori prescrizioni di sicurezza impartite dalla Direzione di aeroporto a seguito di deliberazioni del Comitato di sicurezza aeroportuale, con particolare riferimento all'art. 5 dell'ordinanza n. 8/2006 dell'E.n.a.c. Direzione Aeroportuale Milano-Malpensa che prevede la possibilità di ingressi a soggetti autorizzati attraverso varchi "configurati in modo da consentire l'accesso, ad una persona per volta, dopo aver inserito il proprio badge, associato ad un P.I.N., nell'apposito lettore". In luogo di questo sistema la medesima disposizione ammette, previa approvazione dell'E.n.a.c., l'utilizzo di sistemi biometrici.

L'installazione contribuirebbe inoltre a scongiurare il reiterarsi di episodi di indebita sottrazione di merci di vari vettori aerei già avvenuti nell'aeroporto di Malpensa "[...] a causa della mancanza di sistemi di sicurezza ausiliari rispetto a quelli già imposti [...]" dal Programma nazionale di sicurezza (cfr. comunicazione Alha Airport S.p.a. del 31 gennaio 2006).

Il sistema biometrico (da installare a presidio di cinque accessi ai locali sopra menzionati, e che secondo la società garantirebbe un accertamento più rigoroso dell'identità del personale autorizzato ad accedere ai locali sopra menzionati) sarebbe altresì preordinato alla rilevazione della presenza dei dipendenti della società.

- 1.2. La società ha dichiarato che i lavoratori interessati alla rilevazione biometrica (circa 190 dipendenti di Alha Airport S.p.a., oltre ai componenti della Direzione di Firenze della società e 100 soci/lavoratori delle cooperative "La Corsica" e "Riz") sarebbero quelli che "[...] per necessità operative hanno l'esigenza di transitare/accedere nelle aree sterili (magazzino e caveau) [...]"; il personale della società "[...] che presta il proprio lavoro in ufficio (impiegati) e che non ha necessità d'accesso in magazzino e/o caveau, non sarà obbligato ad entrare da varchi regolati da sistema biometrico" (cfr. comunicazione Alha Airport s.p.a. del 14 giugno 2006).
- 1.3. Il sistema di verifica biometrica sarebbe costituito da dispositivi di lettura di impronte digitali non centralizzati, ma totalmente autonomi nello svolgimento della procedura di identificazione biometrica (in quanto dotati di un proprio microprocessore e di una propria memoria di lavoro), nonché da un software per la trasformazione in un codice numerico dell'impronta rilevata in occasione di ogni ingresso all'area riservata, codice poi confrontato con il template precedentemente ricavato dalla lettura dell'impronta dell'interessato e cifrato "[...] solo su una smart card, anziché nella memoria interna dei dispositivi [...]" posta nell'esclusiva disponibilità del

lavoratore. L'associazione tra i due codici, preceduta dalla lettura della tessera, consentirebbe l'accesso all'area riservata (cfr. comunicazione Alha Airport S.p.a. del 31 gennaio 2006 e punto 8 della comunicazione Alha Airport S.p.a. del 14 giugno 2006).

I dati trattati, oltre a quelli biometrici estratti dall'analisi delle impronte digitali, sarebbero nome e cognome, numero di matricola, codice assegnato al badge utilizzato quale supporto del template e profilo di autorizzazione individuale.

2. I principi di necessità, liceità, finalità e pertinenza nel trattamento di dati biometrici dei lavoratori. Insussistenza di tali presupposti fuori delle "aree sensibili"

- 2.1. La raccolta e la registrazione di impronte digitali e dei dati biometrici da esse ricavati e successivamente utilizzati per l'autenticazione o l'identificazione degli interessati sono operazioni di trattamento di dati personali (art. 4, comma 1, lett. b), del Codice), alle quali trova applicazione la normativa contenuta nel Codice (v. Prov. 19 novembre 1999, in Boll. n. 10, p. 68, doc. web n. 42058; 21 luglio 2005, in Boll. n. 63, doc. web n. 1150679; 23 novembre 2005, in Boll. n. 66, doc. web n. 1202254; in merito, v. pure il documento di lavoro sulla biometria del Gruppo art. 29, direttiva 95/46/Ce-Wp 80-, punto 3.1.).

La liceità del sistema deve essere pertanto valutata sul piano della conformità ai principi di necessità, proporzionalità, finalità e correttezza (artt. 3 e 11 del Codice).

- 2.2. Gli elementi acquisiti nel caso di specie consentono di ritenere che, in relazione ai soli accessi al magazzino e al caveau, sia lecito e proporzionato il trattamento di dati biometrici consistente nell'identificazione (per quanto possibile) certa dei dipendenti della società medesima abilitati all'accesso (oltre che dei soci/lavoratori facenti capo alle società cooperative "La Corsica" e "Riz" che cooperano con Alha Airport S.p.a.).

Come già affermato da questa Autorità (Prov. 15 giugno 2006, in <http://www.garanteprivacy.it>, doc. web n. 1306098), l'utilizzo di dati biometrici può risultare infatti giustificato solo in casi particolari. Occorre a tal fine tenere conto delle finalità e del contesto in cui essi sono trattati. In relazione a luoghi di lavoro come quelli in esame, risulta proporzionato utilizzare i sistemi in esame per presidiare accessi ad "aree sensibili", considerata la natura delle attività ivi svolte (si pensi, ad esempio, a processi produttivi pericolosi o sottoposti a segreti, di varia natura: cfr. Prov. 23 novembre 2005, in <http://www.garanteprivacy.it>, doc. web n. 1202254) o in ragione dei beni ivi custoditi (quali, documenti segreti o riservati o oggetti di valore) oppure, nella situazione in esame, per assicurare la sicurezza di terzi.

Nel caso di specie, i locali dove la società svolge le proprie attività di assistenza a terra (correlate all'ordinato svolgimento del traffico aeroportuale) risultano allo stato richiedere l'adozione di standard di sicurezza specifici ed elevati, nonché di affidabili sistemi di identificazione dei soggetti deputati ad accedervi in conformità alle procedure previste dalla vigente normativa a garanzia della sicurezza di persone e cose (cfr. d.P.R. 4 luglio 1985, n. 461).

Alla luce delle circostanze menzionate, non risulta quindi sproporzionato l'uso di dati biometrici tratti dalle impronte digitali nei locali sopra indicati, tenendo conto anche del fatto che il template, memorizzato sulla smart card e che verrebbe protetto con una chiave crittografica (cfr. punto 11 della comunicazione Alha Airport S.p.a. del 14 giugno 2006), è destinato a restare nell'esclusiva disponibilità dell'interessato.

- 2.3. Analoga valutazione non può essere invece estesa nei confronti del trattamento di dati biometrici previsto per l'accesso ad uffici della società rispetto ai quali, allo stato degli atti, non è stata fornita dalla società idonea prova della sussistenza di analoghe stringenti esigenze di sicurezza che, in conformità ai principi di necessità e proporzionalità (artt. 3 e 11 del Codice), giustificano l'utilizzo di dati biometrici in luogo di altri strumenti meno invasivi.
- 2.4. Il trattamento di dati biometrici sopra descritto non risulta altresì lecito per perseguire la diversa finalità di rilevazione della presenza dei dipendenti della società. Ciò, sia in quanto la società non ha adottato ragioni specifiche a sostegno della necessità di ricorrere a tale peculiare modalità di verifica dell'osservanza dell'orario di lavoro, già dichiarata sproporzionata in passato dal Garante (cfr. Prov. 21 luglio 2005, doc. web n. 1150679; da ultimo Prov. del 15 giugno 2006, in <http://www.garanteprivacy.it>, doc. web nn. 1306523, 1306530 e 1306551) –limitandosi ad accennare all'esigenza, che parrebbe essere di natura prettamente organizzativa, di evitare la contemporanea presenza di due sistemi di controllo concorrenti–, sia perché ne sarebbe prevista l'introduzione nei soli confronti dei dipendenti destinati ad accedere all'area riservata, ad esclusione dei restanti lavoratori della società.

La verifica dell'esatto adempimento della prestazione lavorativa può essere quindi legittimamente perseguita, nel caso di specie, senza ricorrere ad alcun trattamento di dati biometrici (nel rispetto dell'art. 3 del Codice), avvalendosi pertanto di altro idoneo sistema a tal fine predisposto.

3. Qualità dei dati e misure di sicurezza rispetto al trattamento dei dati biometrici, informativa agli interessati e notificazione del trattamento. Necessità dello scrupoloso rispetto di prescrizioni nelle "aree sensibili"

- 3.1. Nelle "aree sensibili", e nella misura in cui il trattamento in esame risulti proporzionato nei termini predetti, occorre comunque avvalersi di un sistema efficace di verifica e di identificazione biometrica basato solo sulla lettura delle impronte digitali memorizzate, sotto forma di template cifrato, su un supporto posto nell'esclusiva disponibilità dell'interessato (smart card o dispositivo analogo). Diversamente da quanto prefigurato dalla società tale supporto dovrà essere poi privo di indicazioni nominative (essendo sufficiente l'attribuzione a ciascun dipendente di un codice individuale), sì che, pure in caso di smarrimento del medesimo, siano remote le possibilità di abuso rispetto ai dati biometrici memorizzati.
- 3.2. Le misure di sicurezza che si intende predisporre a protezione dei dati sono conformi alle disposizioni fissate dal Codice, alla luce di quanto dichiarato dalla società con riguardo al fatto che: i template verrebbero crittografati; il software di gestione (protetto da password) e i dispositivi di creazione delle tessere saranno ubicati in una central room sorvegliata permanentemente per prevenire accessi non autorizzati al sistema ed operazioni di trattamento da parte di soggetti non autorizzati; l'attestato di cui alla regola n. 25 del Disciplinary tecnico in materia di misure minime di sicurezza (Allegato "B" al Codice) ed ogni altra idonea certificazione od omologazione dei dispositivi impiegati verranno rilasciati dall'installatore del sistema e conservati dalla società presso la propria struttura; la società designerà per iscritto il responsabile del centro elaborazione dati (deputato alla raccolta dei dati biometrici) e la persona preposta all'attivazione delle smart card assegnate ai lavoratori quali incaricati delle relative operazioni di trattamento, impartendo loro idonee istruzioni alle quali attenersi (art. 30 del Codice).

In aggiunta alle misure di sicurezza prescritte dal Codice, la società dovrà adottare ulteriori accorgimenti a protezione dei dati, impartendo agli interessati apposite istruzioni scritte alle quali attenersi, con particolare riguardo al caso di perdita o sottrazione delle smart card loro affidate (cfr. punto 19 della comunicazione Alha Airport S.p.a. del 14 giugno 2006).

- 3.2. Si prende poi atto di quanto dichiarato dalla società circa il fatto che tutti i lavoratori interessati all'utilizzo del sistema in esame riceveranno un'informativa scritta completa degli elementi previsti dal Codice (art. 13) rispetto al trattamento di dati biometrici che intende porre in essere; la medesima dovrà tener conto delle modifiche al sistema biometrico derivanti dal presente provvedimento.
- 3.3. La società resta altresì tenuta a raccogliere il consenso degli interessati (per l'utilizzo di dati biometrici); in relazione all'eventualità che alcuni lavoratori non possano o non intendano aderire alla rilevazione biometrica effettuata nei termini di cui in motivazione, risulta comunque praticabile il sistema alternativo di identificazione, peraltro espressamente richiesto all'art. 5 dell'ordinanza n. 8/2006 dell'E.n.a.c.–Direzione aeroportuale Milano–Malpensa (che riconosce come facoltativo, il sistema biometrico), consistente, come detto, nell'utilizzo unitamente al badge, di un codice individuale (P.I.N.). L'esistenza di tale sistema alternativo deve essere evidenziata nell'informativa agli interessati.
- 3.4. La società resta parimenti tenuta a notificare al Garante il trattamento dei dati biometrici prima che abbiano inizio le operazioni di trattamento (art. 37, comma 1, lett. a), del Codice), a rispettare, sussistendone i presupposti, la disciplina del controllo a distanza dei lavoratori (art. 4, comma 2, l. 20 maggio 1970, n. 300; art. 114 del Codice) e a richiedere la formale approvazione da parte dell'E.n.a.c., in conformità all'art. 5 della menzionata ordinanza n. 8/2006 della Direzione aeroportuale Milano–Malpensa.

4. Conservazione dei dati

I dati personali necessari per realizzare il template potranno essere trattati esclusivamente durante la fase di enrollment.

I dati memorizzati dovranno essere accessibili al personale preposto al rispetto delle misure di sicurezza all'interno della società per l'esclusiva finalità dell'osservanza delle medesime; potranno essere inoltre conservati per il tempo massimo di sette giorni assicurando, oltre tale arco temporale, meccanismi di cancellazione automatica dei dati. Il medesimo intervallo temporale, in assenza di disposizioni di legge o di provvedimenti dell'autorità aeroportuale e, comunque, più precise indicazioni da parte della società, appare ragionevole, tenendo conto dei beni custoditi nell'area riservata (che si intendono con tale sistema proteggere), la cui sottrazione potrebbe essere scoperta a distanza di tempo.

5. Conclusioni

La società potrà effettuare il trattamento di dati personali dichiarati qualora rispetti le misure e gli accorgimenti a garanzia degli interessati prescritti con il presente provvedimento, in attuazione del Codice, i quali vanno osservati affinché il medesimo trattamento sia lecito e corretto anche ai fini dell'eventuale applicazione di sanzioni penali (artt. 17 e 167 del Codice).

TUTTO CIÒ PREMESSO IL GARANTE

preso atto del trattamento di dati biometrici effettuato mediante un sistema di verifica basato sul confronto tra le impronte rilevate ad ogni accesso all'area riservata e il template, memorizzato e cifrato su un supporto che resti nell'esclusiva disponibilità dei lavoratori interessati (punti 1. e 2.2.), prescrive ad Alha Airport S.p.a., ai sensi degli artt. 17 e 154, comma 1, lett. c), del Codice, di adottare tutte le misure e gli accorgimenti a garanzia degli interessati nei termini di cui in motivazione fra cui, in particolare:

- di trattare, oltre ai dati biometrici estratti dall'analisi delle impronte digitali, i soli dati necessari al funzionamento del sistema biometrico: un codice identificativo individuale, un codice assegnato al badge utilizzato quale supporto del template e il profilo di autorizzazione individuale;
- di indicare l'esistenza del sistema alternativo di identificazione nell'informativa agli interessati;
- di conservare i dati relativi agli orari di accesso alle aree riservate per il tempo massimo di sette giorni (punto 4);
- vieta, ai sensi dell'art. 154, comma 1, lett. d), del Codice, il trattamento dei dati biometrici fuori delle aree riservate, nonché il trattamento effettuato mediante il sistema descritto in narrativa per le finalità di rilevazione della presenza dei lavoratori (punto 2.4.).

Roma, 26 luglio 2006