[doc. web n. 1318582]

Biometria per sicurezza merci e controllo delle presenze presso aeroporti - 26 luglio 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 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 un 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. *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. 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 (*Provv*. 15 giugno 2006, in , 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. *Provv*. 23

novembre 2005, in , 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 delle 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), giustifichino 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 addotto 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. *Provv*. 21 luglio 2005, doc. *web* n. 1150679; da ultimo *Provv.ti* del 15 giugno 2006, in , docc. *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 Disciplinare 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 dell'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

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli