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

23 novembre 2005

Verifica preliminare (art. 17 del Codice) - 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 evidenzia l'obiettiva 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'idonea 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 accedervi 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

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

stampa
chiudi