Uso delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro
21 luglio 2005

Parere - 21 luglio 2005 [doc. web n. 1150679]

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 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 Acception 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/...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 bometrico.

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

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

stampa
chiudi