

Privacy: Garante, impronte digitali lavoratori solo in casi particolari

Garante Privacy , verifica preliminare 17.11.2010

<http://www.altalex.com/index.php?idnot=13078>

ASCA) - Roma, 4 feb - Le imprese che intendono adottare sistemi di lettura delle impronte digitali per verificare la presenza in servizio dei dipendenti devono prima dimostrare che le finalita' di controllo non possano essere realizzate con sistemi meno invasivi. Questa la decisione Garante che ha respinto le richieste di verifica preliminare con le quali due societa' - una impresa di autotrasporti e la sua capogruppo - chiedevano di poter usare un meccanismo di autenticazione biometrico.

E' quanto si legge nella newsletter del Garante per la protezione dei dati personali. In base alla documentazione presentata, si legge ancora, tale procedura avrebbe dovuto riguardare in primo luogo i lavoratori addetti al controllo degli automezzi e del personale di guida. Secondo le societa', il rilevamento delle impronte avrebbe evitato eventuali condotte irregolari, come lo scambio di badge attestanti la presenza in servizio, e avrebbe di conseguenza determinato anche maggiori garanzie per l'incolumita' degli utenti e del personale viaggiante. Nel corso dell'istruttoria e' pero' emerso che i tradizionali metodi di controllo si erano dimostrati piu' che sufficienti a garantire la verifica della presenza in servizio dei dipendenti, evidenziando la mancata necessita' di introdurre sistemi cosi' invasivi. L'uso dei sistemi biometrici era stato richiesto dalle due societa' anche per accedere ai locali dove sono custoditi le banche dati cartacee e informatiche contenenti i dati personali dei dipendenti. Anche in questo caso, dagli accertamenti effettuati dal Garante e' pero' emerso che tali dati non richiedevano particolari sistemi di controllo, trattandosi di informazioni solitamente elaborate dagli uffici amministrativi di qualsiasi azienda. Nei provvedimenti con i quali ha respinto la richiesta delle due societa' di autotrasporti, l'Autorita' ha ritenuto opportuno sottolineare che l'utilizzo di sistemi di riconoscimento basati su dati biometrici e' possibile solo in casi particolari, per i quali sia dimostrato che non siano sufficienti strumenti alternativi e che dunque la raccolta delle impronte digitali risulti davvero necessaria e proporzionata.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Verifica preliminare 17 novembre 2010

Trasporto: impronte digitali solo in casi particolari. (art. 17 del Codice) [doc. web n. 1779745]

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. Daniele De Paoli, segretario generale;

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

Visto il provvedimento adottato dal Garante in data 23 novembre 2006, recante le "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati" (doc. web n. 1364939), con particolare riferimento al punto 3.2;

Esaminata la documentazione acquisita agli atti;

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

Relatore il dott. Giuseppe Chiaravalloti;

PREMESSO

1. Trattamento di dati personali dei dipendenti attraverso un sistema di autenticazione su base biometrica (impronte digitali).

Autotrasporti Irpini S.p.a. (A.IR. S.p.a.), società che effettua il servizio di trasporto pubblico di persone su tutto il territorio della Regione Campania e, in parte, in altre regioni limitrofe, intende adottare un sistema di rilevazione di dati biometrici basato sulla elaborazione di template originati dalla lettura delle impronte digitali di alcuni dipendenti della società. In particolare, si tratterebbe di un "dispositivo di rilevazione delle presenze per il personale addetto al controllo degli automezzi e del personale di guida e per quello autorizzato ad entrare nelle aree ad accesso controllato (...) finalizzato ad assicurare, inequivocabilmente, la presenza del suddetto personale in servizio", con esclusione della sua utilizzazione "per verificare l'orario di lavoro ai fini del calcolo della retribuzione ordinaria e straordinaria".

La società ha affermato che il trattamento di dati biometrici che intenderebbe effettuare per verificare la presenza in servizio del personale addetto al controllo sugli automezzi e sul personale di guida, oltre ad essere connesso alla sicurezza del trasporto pubblico, sarebbe giustificato dall'esigenza di prevenire condotte irregolari poste in essere da alcuni dipendenti, tra cui lo scambio dei badge attestanti la presenza in servizio; secondo la società, detti inconvenienti sarebbero ovviabili attraverso il sistema di rilevazione biometrica che si intenderebbe installare, perché in grado di assicurare un elevato grado di certezza nell'identificazione dei lavoratori e, di conseguenza, di impedire eventuali false attestazioni relative a controlli effettuati sull'efficienza dei mezzi e sullo stato di salute del personale addetto alla guida, con evidenti benefici per l'incolumità degli utenti e del personale viaggiante.

L'azienda ha precisato che il controllo preliminare sull'efficienza degli automezzi – avente ad oggetto, in particolare, le parti elettriche, le parti meccaniche, l'usura delle gomme e la funzionalità delle porte - viene effettuato da meccanici, mentre quello sugli autisti – concernente il rispetto dei turni di lavoro e la verifica sommaria delle loro condizioni psico-fisiche – viene effettuato da personale con qualifica di capo servizio.

Per quanto concerne, invece, il controllo degli accessi dei lavoratori ad alcuni locali dove sono custodite le banche dati cartacee ed informatiche, la società ha dichiarato che le stesse conterrebbero dati sensibili relativi ai dipendenti, informazioni concernenti eventuali procedimenti disciplinari, dati giudiziari relativi a partecipanti a gare, informazioni "su utenti colpiti da multe e terzi coinvolti in sinistri", "dati relativi ai turni di servizio del personale viaggiante" e informazioni connesse a transazioni commerciali (contratti e fatture). Da qui deriverebbe l'esigenza di un dispositivo di verifica degli accessi assolutamente affidabile, che dovrebbe riguardare 48 dipendenti appositamente incaricati del trattamento di tali dati.

1.2. Caratteristiche tecnico-organizzative del sistema

Il sistema oggetto di verifica preliminare comporterebbe un trattamento di dati personali biometrici (impronta del dito indice), i quali, al termine della fase di enrollment, verrebbero memorizzati su una card rilasciata in possesso esclusivo degli interessati, priva dei dati anagrafici di costoro.

Nella fase di enrollment, la predisposizione delle card verrebbe affidata al responsabile della sicurezza informatica (designato anche responsabile del trattamento dei dati ex art. 29 del d.lgs. 196/03), il quale, dopo la consegna della card, avrebbe anche il compito di verificare l'inesistenza di tracce dei dati biometrici rilevati sulle apparecchiature informatiche aziendali.

Per prevenire accessi non autorizzati al sistema, sarebbero state previste alcune misure di sicurezza, consistenti in:

- utilizzazione di un computer "stand alone", non collegato quindi ad alcuna rete;
- cancellazione dal computer dei dati al termine dell'operazione di enrollment;
- esecuzione dell'operazione a cura del solo responsabile della sicurezza informatica (ingegnere informatico dirigente dell'azienda) particolarmente formato sul d.lgs 196/2003.

I dipendenti sottoposti al rilevamento biometrico, inserirebbero la card in un'apposita fessura, poggiando l'indice in un alloggiamento predisposto dell'apparecchio. Il dispositivo rileverebbe la corrispondenza dei dati contenuti nella card con quelli dell'indice e, conseguentemente, poiché ad essa sarebbe associato un numero di identificazione del dipendente, ne rileverebbe la presenza al lavoro.

Il sistema, tuttavia, non verrebbe utilizzato per verificare il rispetto dell'orario di lavoro ai fini del calcolo della retribuzione ordinaria e straordinaria.

Stando a quanto dichiarato dalla società, il personale tenuto a servirsi del sistema di autenticazione, una volta informato, sarebbe invitato a prestare il proprio consenso al trattamento dei dati sin dalla fase di enrollment; inoltre, sarebbe comunque previsto un sistema di rilevazione delle presenze alternativo, da utilizzare nel caso in cui i dipendenti fossero impossibilitati a partecipare all'enrollment (in ragione delle proprie caratteristiche fisiche) o non intendessero acconsentire al trattamento.

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

La raccolta e la registrazione di impronte digitali e dei dati biometrici ricavati e successivamente utilizzati per verifiche e raffronti nelle procedure di autenticazione sono operazioni di trattamento di dati personali riconducibili ai singoli interessati [art. 4, comma 1, lett. b) del Codice], operazioni alle quali trova applicazione la normativa contenuta nel Codice.

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; art. 6, direttiva n. 95/46/Ce).

Secondo il costante orientamento del Garante, l'utilizzo dei dati biometrici può essere giustificato solo in casi particolari, in relazione alle finalità e al contesto in cui essi sono trattati e, in relazione ai luoghi di lavoro, per presidiare accessi ad "aree sensibili", in considerazione della natura delle attività ivi svolte: si pensi, ad esempio, a processi produttivi pericolosi o sottoposti a segreti di varia natura o al fatto che particolari locali siano destinati alla custodia di beni, documenti segreti o riservati e/o oggetti di valore (in tal senso, vedi il punto 4.1 delle "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati", emanate dall'Autorità in data 23 novembre 2006 (doc. web n. 1364939).

Con riferimento al caso di specie, dagli elementi forniti dalla società nel corso dell'istruttoria non sono emerse circostanze atte a giustificare la necessità di un trattamento di dati biometrici in vista dell'accesso ai locali dove sarebbero custodite le banche dati aziendali. Infatti, i dati che risultano conservati negli archivi cartacei ed informatici, lungi dall'essere caratterizzati da specifiche peculiarità, si sostanziano in informazioni che solitamente sono trattate negli uffici amministrativi di qualsiasi azienda, mentre le loro attuali modalità di custodia, "in appositi locali ove è stato permesso l'accesso al solo personale dipendente che deve lavorare su di esse", risultano più che sufficienti per impedire la loro presa di conoscenza da parte di soggetti diversi dai singoli incaricati del trattamento. Pertanto, allo stato, tenuto conto della natura e della tipologia delle informazioni conservate nelle banche dati ubicate nei predetti locali, si deve ritenere che la procedura di accesso selezionato attualmente adottata dalla società sia adeguata per garantirne la riservatezza, senza che possano ravvisarsi ragioni per ritenere giustificato l'impiego di un delicato sistema di rilevazione delle impronte digitali nei confronti di un numero limitato di dipendenti (48 unità).

Con particolare riferimento all'esigenza di verificare la presa di servizio dei dipendenti addetti ai controlli di sicurezza sugli autisti e sui mezzi di trasporto pubblico, la società ha sostenuto che essa scaturirebbe da "una realtà lavorativa alquanto delicata e, comunque, tale da indurre l'azienda a cercare misure di controllo più efficaci" di quelle attuali. In particolare, la società ha dichiarato di aver ricevuto reclami con i quali era stato lamentato "lo stato di ubriachezza di alcuni autisti evidentemente non controllati da chi era preposto a farlo risultando, comunque, regolarmente in servizio", nonché di essere stata impossibilitata a verificare tardive partenze dei mezzi dal deposito per assenza del preposto "alla registrazione e alla verifica", il quale, però, risultava regolarmente in servizio; infine, la società ha dichiarato che "a seguito di controlli effettuati da Funzionari aziendali, sono stati rilevati arrivi in servizio in ritardo con i badge marcatempo che segnalavano orari precedenti a quello dell'effettivo ingresso in azienda, badge utilizzati dalla Guardia Giurata ivi preposta per assicurare il servizio notturno di guardiania". Tali comportamenti sono stati oggetto di procedimenti disciplinari, definiti con l'irrogazione, nei confronti dei responsabili, di provvedimenti disciplinari di sospensione dal servizio e dalla paga.

Ciò premesso, occorre sottolineare che, pur rientrando tra le legittime facoltà del datore di lavoro quella di sovrintendere all'esecuzione della prestazione lavorativa (art. 2094 cod. civ.), verificando le presenze dei dipendenti e il rispetto dell'orario di lavoro, nel caso di specie non risulta dimostrata la necessità e proporzionalità del trattamento dei dati biometrici che si intenderebbe attuare.

In primo luogo va rilevato che benché il personale della società ammonti a ben 409 dipendenti, il sistema biometrico sarebbe preordinato a verificare la presenza in servizio di un numero limitato di unità lavorative (53 operai per il controllo sui mezzi e 12 capi servizio per il controllo sugli autisti, pari al solo "20% dell'intera forza lavoro"), obiettivo questo certamente perseguibile attraverso l'utilizzazione dei tradizionali e meno invasivi sistemi di controllo, quali l'uso di un normale badge accompagnato da accorgimenti tecnici ed organizzativi (es. disponendo ulteriori controlli da affidare a corpi di vigilanza esterna) atti a scongiurare manomissioni del congegno marcatempo o sostituzioni nell'impiego del supporto stesso.

Inoltre, dalla documentazione prodotta dalla società, non si traggono elementi da cui possa desumersi con certezza la mancata presa di servizio da parte dei controllori di turno, semmai soltanto alcuni "arrivi in servizio in ritardo" da parte di addetti/collaboratori di esercizio dislocati presso il "box" del deposito di

Torrette di Mercogliano; inoltre, in tali casi (uno dei quali addirittura risalente al 1999!), risulta che gli accertamenti sull'orario di effettiva presa di servizio sono stati effettuati direttamente da personale gerarchicamente sovraordinato ("addetti A.M.T."), che ha curato l'invio di specifici rapporti ai vertici aziendali. A ciò aggiungasi che gli ulteriori documenti prodotti dalla società fanno riferimento a contestazioni disciplinari mosse direttamente nei confronti degli operatori d'esercizio (autisti), i quali avrebbero osservato condotte (es. guida in stato di ubriachezza) non conformi ad una regolare esecuzione della prestazione lavorativa, senza che però risulti dimostrato un mancato controllo sulla loro apparente condizione psico/fisica al momento della loro presa di servizio. Pertanto, alla luce delle acquisizioni istruttorie, i controlli attualmente effettuati dalla società appaiono sufficienti a garantire una verifica sulla presa di servizio degli addetti e dei collaboratori d'esercizio, mentre i precedenti disciplinari cui la società ha fatto riferimento per giustificare la propria richiesta non risultano –sia dal punto di vista numerico, sia dal punto di vista qualitativo- significativi per dimostrare l'esistenza di una diffusa situazione di disobbedienza da parte del personale, tale da rendere necessaria l'adozione di un sistema di rilevazione biometrica delle presenze.

Da ultimo si rileva che il trattamento di dati biometrici non risulterebbe conforme a legge anche in ragione del fatto che, allo stato, non risulta neanche osservata la procedura prevista dall'art. 4, comma 2 della legge 20 maggio 1970, n. 300 (cui fa espresso riferimento l'art. 114 del Codice), che trova applicazione anche in relazione all'installazione di apparecchiature che consentano "di controllare il rispetto o non degli orari di entrata e uscita e presenza sul luogo di lavoro da parte dei dipendenti" (cfr. Cass., 17 luglio 2007, n. 15892).

Da quanto detto deriva che la richiesta di verifica preliminare dev'essere rigettata.

L'odierna pronuncia, resa sulla scorta delle attuali acquisizioni istruttorie, non preclude all'Autorità di adottare una diversa determinazione nel caso in cui la Autotrasporti Irpini S.p.a. offra una più documentata motivazione delle ragioni atte a giustificare l'adozione del rappresentato sistema di rilevazione biometrica, da valutare alla luce della normativa esistente.

TUTTO CIÒ PREMESSO, IL GARANTE

rigetta la richiesta di verifica preliminare presentata dalla Autotrasporti Irpini S.p.a. (A.IR. S.p.a.).

Roma, 17 novembre 2010

IL PRESIDENTE

Pizzetti

IL RELATORE

Chiaravalloti

IL SEGRETARIO GENERALE

De Paoli