VEDI ANCHE: comunicato del 14 ottobre 2016

[doc. web n. 5505689]

Verifica preliminare. Sistema di lettura di dati biometrici mediante parziale identificazione dell'impronta digitale per la rilevazione della presenza in servizio - 15 settembre 2016

Registro dei provvedimenti
n. 357 del 15 settembre 2016

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTO il d.lg. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, di seguito "Codice");

ESAMINATA la richiesta di verifica preliminare presentata dall'Azienda Ospedaliero-Universitaria "San Giovanni di Dio e Ruggi d'Aragona" di Salerno ai sensi dell'articolo 17 del Codice;

VISTE le Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico del 14 giugno 2007 (pubblicate in G.U. n. 161 del 13 luglio 2007, e in www.garanteprivacy.it, doc. web n. 1417809);

VISTO il provvedimento n. 513 del 12 novembre 2014 e all. A recante le Linee guida in materia di riconoscimento biometrico e firma grafometrica (pubblicato in G.U. n. 280 del 4 dicembre 2014 e, doc. web n. 3556992);

ESAMINATE le risultanze istruttorie e la documentazione in atti;

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

RELATORE la dott.ssa Augusta Iannini;

PREMESSO

1.1. L'Azienda ospedaliero-Universitaria "San Giovanni di Dio e Ruggi d'Aragona" di Salerno ha presentato una richiesta di verifica preliminare ai sensi dell'articolo 17 del Codice, in relazione all'installazione di "un sistema di lettura di dati biometrici mediante parziale identificazione dell'impronta digitale", per la finalità di "garantire la sicurezza degli accessi e [la] prevenzione dall'uso fraudolento dei tesserini magnetici" e "allo scopo di contrastare il fenomeno dell'assenteismo"(istanza del 24 settembre 2015 regolarizzata in data 7 giugno 2016, in atti).

RILEVATO

2.1. Alla luce della documentazione disponibile e delle dichiarazioni rese dal titolare del trattamento, emerge che l'Azienda, soggetta a commissariamento, è stata oggetto, fin dal 2014, di indagini da parte della Procura della Repubblica presso il Tribunale di Salerno che hanno interessato centinaia di dipendenti per ipotesi di reato quali truffa aggravata ai danni dello Stato (art. 640 c.p.) e false attestazioni o certificazioni nell'utilizzo del badge da parte dei dipendenti pubblici (art. 55-quinquies, d.lg. n. 165/2001).

Come rappresentato in sede di istanza, la vicenda - con il coinvolgimento in un'indagine giudiziaria di larga parte dei dipendenti dell'Azienda - ha avuto e tutt'ora ha risonanza sulla stampa, non solo locale, e sui più diffusi mezzi di comunicazione di massa (ad esempio, sul web), "con puntualità quotidiana", ingenerando "allarme sociale" e "discredito" per l'Azienda.

Per tali ragioni la struttura commissariale intenderebbe installare un sistema di rilevazione biometrica "al fine di ripristinare il rispetto della legalità e di ristorare la fiducia dell'utenza che si rivolge a questa Azienda affidandole il bene più prezioso: la salute" (cfr. nota 7 giugno 2016).

2.2. Con riferimento alle specifiche ragioni che renderebbero necessario il trattamento di dati biometrici di tutti i dipendenti per finalità di ordinaria gestione del rapporto di lavoro, in particolare allo scopo di rilevazione della presenza in servizio, l'Azienda ha precisato con la richiamata nota del 7 giugno 2016 che :

1) la finalità non è solo quella di "riscontrare con certezza la prestazione lavorativa del dipendente, ma soprattutto, di dare certezza di cura al paziente", tutelando "la salute pubblica come fondamentale diritto dell'individuo e interesse della collettività"; tanto, atteso che la condotta che si intende prevenire, è quella "per cui il dipendente infedele va a marcare al posto di un insieme di colleghi collusi, in realtà assenti sul lavoro" (nota cit., p. 2);

2) stante l'entità del fenomeno e il numero dei dipendenti interessati dalle indagini ("850 dipendenti su 2000 in servizio nel plesso oggetto di indagini"), e stante l'inefficacia dei sistemi di rilevazione delle presenze in uso, "l'uso generalizzato di un sistema di rilevazione biometrica è necessario nel caso di questa Azienda, a causa del generalizzato sistema di illegalità messo in luce dall'attività investigativa della magistratura";

3) l'eventuale installazione del sistema si collocherebbe "in un più ampio quadro di iniziative" quali, in particolare, l'irrogazione di sanzioni disciplinari (il licenziamento senza preavviso sarebbe già stato disposto nei confronti dei dipendenti interessati da misure cautelari) e l'adozione di uno specifico regolamento per la disciplina dell'orario di lavoro (deliberazione del direttore generale n. 1030 del 27.11.2014) "recante disposizioni, tra l'altro, in materia di utilizzo del badge marcatempo; responsabilità del Direttore di struttura nella vigilanza e regime sanzionatorio delle inosservanze";

4) stando a quanto rappresentato le specifiche responsabilità poste in capo al Direttore di Struttura, tuttavia, non sono da considerarsi sufficienti essendo questo "impegnato per gran parte del tempo lavorativo nella pratica medica o chirurgica è, spesso, nell'oggettiva difficoltà di verificare puntualmente e sistematicamente l'effettiva presenza di tutti gli operatori sanitari, potendosi, questi, anche allontanare dal reparto per esigenze connesse al servizio";

5) in tale quadro, l'Azienda ritiene che, oltre all'attività sanzionatoria repressiva, "più efficace può risultare l'azione che, preventivamente, cerca di porre un freno all'illecito" con "strumenti integrativi per la rilevazione della presenza";

6) è stata valutata anche la possibilità di prevedere dei varchi o "sistemi che consentano il passaggio di una persona per volta (c.d. tornelli), in prossimità dei marcatempo". Tale soluzione non è stata tuttavia ritenuta praticabile in concreto, tenuto conto della "topologia delle sedi ospedaliere, che impedisce l'efficace incalanamento e controllo dei flussi di traffico pedonale: ciascun plesso ospedaliero è costituito da più corpi di fabbrica costruiti in epoche successive (fino agli anni '80), in assenza di misure costruttive apposite"; ciascun edificio presenta un numero elevato di varchi di accesso "utilizzati dal personale anche per spostamenti durante il servizio, oltre che dall'utenza per l'accesso ai vari reparti e servizi"; inoltre, per alcuni edifici sussiste un "vincolo d'interesse storico-culturale"(ad esempio, quello di Cava dè Tirreni, risalente al sec. XVI).

2.3. Con specifico riguardo alle caratteristiche del sistema l'Azienda ha dichiarato che il sistema "non memorizza in alcun modo il dato biometrico, residente sul badge e letto solo al momento della timbratura": "il dipendente [dovrebbe apporre] sia il badge che il dito sul marcatempo che confronta le informazioni lette trasmettendo al sistema centrale, in caso positivo, le sole informazioni di timbratura (matricola, data e ora, causale)". Sono state fornite assicurazioni sulla "volatilità del dato" ("non c'è memorizzazione del dato biometrico in alcun database, né sotto forma di codifica numerica né tantomeno, sotto forma di immagine"). Non vi sarebbe inoltre trasmissione in rete del dato biometrico il quale verrebbe ad essere "residente in forma numerica crittografata sul badge in possesso e ad uso esclusivo del dipendente". Il sistema è in grado di rilevare il c.d. "dito vivo", "ad evitare comportamenti fraudolenti (copia dell'impronta in silicone, etc.) [ma] non prevede l'associazione dei dati biometrici con ulteriori informazioni riferite al dipendente"(cfr. n. nota 18 marzo 2016, cit.). Più nel dettaglio, alla luce di quanto emerge dalle relazioni tecniche predisposte dal fornitore del sistema (cfr. relazione allegata alla nota del 18 marzo 2016 e quella allegata alla nota 8 giugno 2016):

a) con riguardo alla fase di registrazione ("enrollment"):

tale fase viene svolta avvalendosi di un personal computer e di un sensore ottico ad esso collegato attraverso una interfaccia "USB"; l'immagine dell'impronta non viene memorizzata ("se non per il tempo necessario alla sua elaborazione - un paio di secondi") o inviata al personal computer, ma gestita completamente all'interno del dispositivo stesso; l'impronta digitale rilevata, in sede di registrazione, è immediatamente trasformata dal sensore stesso in una stringa di bits crittografati ed inviata al personal computer che provvede a registrarla sotto forma di template sul supporto personale di identificazione (tessera "smart card" dotata di micro chip cui è preventivamente associato un codice di identificazione personale c.d. "matricola") e consegnata ad ogni utilizzatore. Quando il dipendente appone il dito per la rilevazione dell'impronta ne viene memorizzata un'immagine soltanto per il tempo necessario all'elaborazione, volta ad ottenere la stringa di caratteri rappresentativa (il template), a partire dalle caratteristiche dell'impronta (le "minuzie"). Sono state fornite assicurazioni in ordine alla "irreversibilità del processo", in quanto "non è possibile in alcun modo ottenere l'immagine dell'impronta digitale a partire dalla stringa di bits ("template") memorizzata sulla smartcard" data in uso e custodia al dipendente. "la stringa di bits ("template") è protetta da due livelli di crittografazione: il 1°livello è insito nelle logiche di trasformazione (proprietarie) il 2° livello utilizza la "chiave" di autenticazione della smart card stessa".

b) con riguardo alla fase di rilevamento di presenza:

la "testa di lettura", denominata DOR50, in fase di riconoscimento del dipendente, ha 2 input: il dito del dipendente e la card data in uso a questi. L'utilizzatore "fa leggere la carta MIFARE al lettore RFID integrato nella testa di lettura, quindi pone il suo dito sul sensore biometrico" il quale esegue l'elaborazione dell'immagine dell'impronta che la rappresenta al fine di ottenere il "template" e lo confronta con quello presente sulla card (autenticazione);"i sensori biometrici utilizzati dal lettore DOR30 e dai terminali serie ON sono in grado di verificare la "vivezza" dell'impronta"; se il confronto/riconoscimento avviene con successo, il numero di matricola del dipendente viene trasmesso al sistema di rilevazione che deve dare il consenso all'ingresso; anche in questa fase non vi è memorizzazione e tantomeno trasmissione né di immagini dell'impronta né del template, a parte la memorizzazione temporanea e locale al dispositivo al solo fine del riconoscimento ("i dati biometrici restano confinati nel sensore stesso ed eliminati alla fine del processo"). Con riguardo a ciascun utente "viene registrato, in caso di transito e autenticazione, solo il numero della tessera (analogamente a quanto avviene già normalmente nei sistemi di controllo degli accessi e/o di rilevazione delle presenze che utilizzano terminali dotati di lettore badges magnetici o di prossimità)".

CONSIDERATO

3.1. Il descritto sistema di rilevazione di dati biometrici, allo stato non attivo, rientra nell'ambito di applicazione della disciplina posta in materia di protezione dei dati personali, nella misura in cui l'Azienda intende acquisire nella fase di enrollment le informazioni desumibili dall'impronta dei dipendenti –memorizzandole sul badge affidato nella disponibilità di questi ultimi– per utilizzarle quindi in procedure di identificazione. Quelli biometrici, infatti, sono dati personali "direttamente, univocamente e in modo tendenzialmente stabile nel tempo, collegati all'individuo e denotano la profonda relazione tra corpo, comportamento e identità della persona" e il loro impiego per la specifica finalità di rilevazione delle presenze in servizio, che l'Azienda intende perseguire e per la quale correttamente è stata presentata al Garante apposita istanza ai sensi dell'articolo 17 del Codice, non è contemplato tra le ipotesi di trattamento "esonerato" dalla presentazione di istanza di verifica preliminare (cfr. provvedimento generale prescrittivo in tema di biometria n. 513 del 2014 cit., punto 4).

3.2. Il trattamento dei dati personali relativi alla rilevazione delle presenze e dell'orario di lavoro è riconducibile alle finalità perseguite dai soggetti pubblici quali datori di lavoro all'interno di un preciso quadro normativo che prevede specifici obblighi di controllo e conseguenti responsabilità in capo alle competenti funzioni delle pubbliche amministrazioni nell'ambito delle finalità e dei compiti istituzionali ad essi normativamente assegnate tra cui anche, nei casi in cui ne ricorrano i presupposti, la promozione delle conseguenti azioni disciplinari, salve le eventuali responsabilità sul piano penale e contabile (cfr. artt. 55 e ss., d.lg. n. 165/2001 e, in particolare, art. 54-quater nel testo introdotto dal d.lg. 20 giugno 2016, n. 116; e artt. 18, 19, comma 1 del Codice; sul punto, seppure con riferimento al caso, in parte diverso, di trattamento di dati a scopo di verifica sulle assenze, Provv. 5 giugno 2014, n. 281, doc. web n. 3275942).

3.3.Con riferimento all'uso di tecnologie biometriche per finalità di rilevazione delle presenze si osserva che la legittima finalità volta ad accertare il rispetto dell'orario di lavoro anche "mediante forme di controlli obiettivi e di tipo automatizzato (e in taluni casi a garantire speciali livelli di sicurezza)" deve, in ogni caso, essere effettuato nel pieno rispetto della disciplina in materia di protezione dei dati personali, anzitutto con riguardo all'osservanza dei principi di necessità e proporzionalità (cfr. punto 7.1., Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico 14.6.2007, doc. web n. 1417809; v. anche Gruppo dei garanti europei previsto dall'art. 29 della direttiva 95/46/Ce WP193, Parere 3/2012 sugli sviluppi nelle tecnologie biometriche, adottato il 27 aprile 2012, p. 12, secondo cui "il datore di lavoro è sempre tenuto a cercare i mezzi meno invasivi scegliendo, se possibile, un procedimento non biometrico").

Tali principi impongono che siano preventivamente considerati altri sistemi, dispositivi e misure di sicurezza fisiche e logicistiche che possano assicurare parimenti una puntuale e attendibile verifica delle presenze e degli ingressi sul luogo di lavoro senza fare ricorso al trattamento dei dati biometrici (artt. 2, 3 e 11 del Codice).

4. Tanto premesso, al fine di procedere ad una valutazione complessiva del caso in esame alla stregua dei principi e delle regole in materia di protezione dei dati personali, si osserva che i circostanziati elementi forniti dal titolare del trattamento, riguardanti i ripetuti e concreti episodi di violazione dei doveri d'ufficio da parte dei dipendenti e il fondato timore della perpetrazione degli abusi, unitamente ai possibili benefici derivanti alla collettività dall'effettiva rilevazione della presenza in servizio e dall'osservanza dell'orario di lavoro da parte dei dipendenti della struttura sanitaria, rendono il caso in esame assolutamente peculiare, tenuto altresì conto della specifica realtà lavorativa e dell'elevato numero di lavoratori coinvolti dagli accertamenti interni e dalle indagini dell'autorità giudiziaria.

Ai fini della medesima valutazione, risultano rilevanti anche altri aspetti che hanno orientato la scelta della Azienda verso il descritto sistema di rilevazione delle presenze mediante trattamento di dati biometrici, quali, la toponomastica e l'estensione dell'area sulla quale insistono i diversi padiglioni dell'ospedale, peraltro ad accesso promiscuo da parte di utenti e personale medico, paramedico ed ausiliario, e tali da non consentire un agevole controllo sulla presenza e sull'osservanza dell'orario di lavoro da parte degli interessati.

In tale quadro, deve altresì essere presa in considerazione, in termini di proporzionalità rispetto alle finalità in concreto perseguite, sia l'effettiva necessità di una continua reperibilità degli interessati i quali, per ragioni di servizio, sono tenuti a spostarsi frequentemente da un reparto all'altro, sia la particolare condotta che l'Azienda intende prevenire, ossia quella "per cui il dipendente infedele va a marcare al posto di un insieme di colleghi collusi, in realtà assenti sul lavoro"(cfr. nota 7 giugno 2016 cit.).

Infatti, il menzionato trattamento di dati biometrici risulta proporzionato rispetto alla predetta finalità, diversamente dai casi in cui il Garante ha messo in luce l'inidoneità dell'utilizzo in via esclusiva di un sistema biometrico al fine di scongiurare condotte diverse da quella in esame.

Quanto a tale ultimo profilo, l'Azienda ha documentato le ragioni in base alle quali strumenti automatizzati alternativi sono risultati inefficaci nonché le difficoltà in concreto riscontrate nello svolgimento del controllo sulla corretta esecuzione della prestazione dei dipendenti anche attraverso gli strumenti posti dall'ordinamento a disposizione del personale dirigenziale o direttivo in genere, sul quale incombe in ogni caso la verifica quotidiana della presenza del personale agli stessi assegnato (cfr. Regolamento adottato con deliberazione del direttore generale n. 1030 del 27.11.2014 che disciplina anche le responsabilità del Direttore di struttura nella vigilanza ed il regime sanzionatorio delle inosservanze). In particolare, è stata rappresentata l'impossibilità per alcune figure apicali di garantire un monitoraggio costante sui propri collaboratori essendo esse per prime impegnate nella pratica medica o chirurgica negli ambulatori e nei reparti dell'ospedale.

5. Tutto ciò considerato, alla luce delle descritte circostanze e delle scelte di configurazione del sistema nonché delle modalità di utilizzo che l'Azienda intende porre in essere, all'interno di un più ampio quadro di misure (alcune delle quali già implementate), per contrastare il diffuso fenomeno di assenteismo nei termini sopra precisati, si ritiene che il trattamento dei dati biometrici dei lavoratori possa essere effettuato nel rispetto delle finalità e degli accorgimenti che l'Azienda si è impegnata ad adottare (cfr. punto n. 2) in quanto lecito e idoneo a soddisfare i principi di necessità e proporzionalità in relazione alla finalità perseguita (artt. 3, 11, comma 1, lett. a) e d), 18 e 19, comma 1, del Codice).

6. Resta fermo che l'Azienda, prima dell'inizio dei descritti trattamenti, è tenuta in base alla normativa vigente a:

a. effettuare la notificazione al Garante ai sensi dell'articolo 37, comma 1, lett. a), del Codice;

b. fornire ai dipendenti coinvolti dai descritti trattamenti, un'informativa comprensiva di tutti gli elementi contenuti nell'articolo 13

del Codice (tipologia di dati, finalità e modalità del trattamento, compresi i tempi di conservazione), con riferimento, ovviamente, al trattamento dei dati biometrici, integrando sul punto il modello di informativa trasmesso (cfr., nota 8 giugno 2016);

c. adottare le misure di sicurezza previste dagli articoli 31 e seguenti del Codice al fine di preservare l'integrità dei dati trattati e prevenire l'accesso agli stessi da parte di soggetti non autorizzati;

d. predisporre misure al fine di garantire agli interessati l'esercizio dei diritti previsti dagli articoli 7 e seguenti del Codice.

TUTTO CIÒ PREMESSO IL GARANTE

preso atto della richiesta di verifica preliminare presentata dall'Azienda ospedaliero-Universitaria "San Giovanni di Dio e Ruggi d'Aragona" di Salerno, stabilisce, ai sensi dell'articolo 17 del Codice, che il trattamento dei dati personali biometrici dei dipendenti possa essere effettuato nei termini di cui in motivazione.

Ai sensi degli articoli 152 del Codice e 10 del decreto legislativo n. 150 del 2011, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 15 settembre 2016

IL PRESIDENTE
Soro

IL RELATORE
Iannini

IL SEGRETARIO GENERALE
Busia