diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

La privacy nei rapporti di lavoro privati

Autore: Policella E. Olimpia
In: Diritto civile e commerciale, Diritto del lavoro

(1 Premessa – 2 Il rapporto tra le Linee Guida privacy e le ulteriori normative – 3 L'articolazione dei ruoli privacy nell'ambito dei gruppi societari
- 4 La pubblicazione dei dati dei dipendenti sulla intranet
– 5 L'utilizzo dei dati biometrici – 5.1 Alcuni precedenti – 5.2 Le finalità lecite –
5.3 Il consenso informato dei dipendenti
- 5.4
L'obbligo di notificazione al garante - 5.5 Il rispetto dello Statuto dei lavoratori - 5.6 Le prescrizioni specifiche richieste dal Garante - 5.7 Le sanzioni conseguenti all'inosservanza delle prescrizioni per il trattamento di dati biometrici - Conclusioni)

1 Premessa

Lo scorso 23 novembre 2006 il Garante privacy ha adottato un primo provvedimento generale avente ad oggetto il trattamento dei dati personali nell'ambito dei rapporti di lavoro con datori di lavoro privati.

Il provvedimento, pubblicato sulla Gazzetta Ufficiale del 7 dicembre 2006 n. 285 e reso noto dall'Authority con comunicato stampa del 13 dicembre 2006, è stato adottato ai sensi dell'art. 154 del Codice privacy comma 1 lett. h), vale a dire nell'esercizio dei poteri dell'Authority di curare la conoscenza, tra il pubblico, della disciplina rilevante in materia di trattamento dei dati personali ivi compresi i profili di sicurezza.

La parte del provvedimento concernente, invece, il trattamento dei dati biometrici da parte dei datori di lavoro è stata adottata anche ai sensi dell'art. 17, inerente il trattamento dei dati che presenta specifici profili di rischiosità meglio noto, tra gli operatori del settore, come prior checking, e dell'art. 154, comma 1, lett. c), del medesimo Codice, avente ad oggetto la prescrizione di misure necessarie ed opportune al fine di rendere i trattamenti conformi alla normativa vigente.

Alle Linee guida sul rapporto di lavoro privato, di cui si propone una breve dissertazione, faranno seguito, verosimilmente entro l'estate 2007, ulteriori provvedimenti generali tesi a dare concreta risoluzione ad alcune problematiche che maggiormente interessano nell'era dell'informazione e che attengono alle nuove forme di controllo elettronico dei dipendenti mediante, si citano a mero titolo esemplificativo, il monitoraggio della navigazione in rete, della posta elettronica, dell'uso del PC o dei costi telefonici. Appare, invece, ancora lontana l'approvazione del codice deontologico sui rapporti di lavoro previsto

dall'art. 111 del Codice privacy.

2 Il rapporto tra le Linee guida del Garante privacy e le ulteriori normative

In via preliminare, il Garante privacy ha ritenuto opportuno evidenziare come l'adozione del provvedimento generale del 23 novembre/6 dicembre 2006 non pregiudica l'applicazione delle altre norme rilevanti in materia di trattamento dei dati personali che maggiormente tutelano i diritti dei soggetti interessati.

L'Authority ha ritenuto di dover richiamare, a scanso di ogni improbabile equivoco, le norme dello Statuto dei lavoratori inerenti il divieto di indagine sulle opinioni dei lavoratori nonché il controllo a distanza degli stessi la cui vigenza, peraltro, era già stata riaffermata da parte dello stesso legislatore del 2003 negli artt. 113 e 114 del Codice privacy.

Alle Linee Guida del Garante privacy sui rapporti di lavoro privati va riconosciuto il merito di aver chiarito talune questioni che sollevavano dei grossi dubbi sotto il profilo giuridico, ci si riferisce, ad esempio, alla tematica relativa alla corretta articolazione dei ruoli privacy nell'ambito dei gruppi societari, alla possibilità per l'azienda di procedere alla pubblicazione dell'immagine e degli altri dati personali dei dipendenti sulla intranet aziendale anche in assenza di un loro specifico consenso ed alla questione inerente il trattamento dei dati biometrici dei dipendenti che necessitano di accedere ad alcune aree sensibili.

In considerazione dell'ampiezza del provvedimento dell'Authority l'ambito di analisi sarà delimitato alle problematiche sopra citate rinviando per le altre tematiche affrontate al medesimo provvedimento, peraltro ricco di riferimenti alla "giurisprudenza" del Garante italiano nonché agli orientamenti espressi da parte del Gruppo dei Garanti europei.

3 L'articolazione dei ruoli privacy nei gruppi societari

Con la terminologia "articolazione dei ruoli privacy" si intende fare riferimento alle modalità seguite dall'azienda ai fini dell'individuazione dei ruoli previsti dalla normativa privacy dei diversi soggetti che nell'ambito, ad esempio, di una società eseguono trattamenti di dati personali oppure ne assumono le relative decisioni. In altri termini ci si riferisce ai

Diritto & Diritti ISSN 1127-8579

ruoli di Titolare, Responsabili o Incaricati al trattamento
ricoperti da parte di ciascun soggetto nell'ambito di una società, di un gruppo societario o, comunque, in una determinata operazione che implica il trattamento di dati personali e coinvolge una pluralità di soggetti di diritto.

Nelle persone giuridiche il Titolare del trattamento, da intendersi quale il soggetto che assume le decisioni in ordine alle modalità e finalità del trattamento dei dati (cfr. artt. 4 e 28 del Codice privacy), è la stessa persona giuridica (società, associazione, ente, ecc.), mentre gli incaricati sono necessariamente le persone fisiche che materialmente pongono in essere le operazioni di trattamento dei dati personali su supporti elettronici o cartacei. L'identificazione della figura del Titolare del trattamento non è sempre agevole soprattutto, come rilevato dal Garante nel provvedimento in commento, nei gruppi societari complessi posto che il Titolare coincide con il centro di imputazione di interessi.

L'individuazione del Titolare deve, pertanto, essere effettuata tenendo conto degli effettivi poteri esercitati dai soggetti, a prescindere da un qualsivoglia atto di nomina mentre l'individuazione degli Incaricati deve essere effettuata, da parte del Titolare o del Responsabile, per iscritto secondo le modalità indicate nell'articolo 30 del Codice privacy[1], vale a dire con atto specifico o anche mediante la mera preposizione di un soggetto ad un'unità per la quale si è già provveduto ad individuare l'ambito di trattamento ossia il complesso di operazioni eseguibili per il perseguimento di specifiche finalità indicate e riconducibili in capo al Titolare del trattamento dei dati.

La nomina del Responsabile privacy non costituisce un obbligo di legge seppur va rilevato che essa diviene una scelta obbligata nelle realtà particolarmente complesse. Vengono usualmente individuati due tipologie di responsabili del trattamento dei dati vale a dire i responsabili interni, ossia persone fisiche preposte ai vertici delle singole funzioni o direzioni aziendali nel cui ambito sono trattati dati personali, ed i responsabili esterni del trattamento dei dati che, invece, normalmente coincidono con società di consulenza che prestano la loro attività, ad esempio, di manutenzione dei sistemi informatici, di predisposizione e gestione delle buste paghe, di postalizzazione, ecc..

Possono essere nominati responsabili privacy anche alcune società facenti parte di un gruppo societario da parte delle altre società del gruppo qualora le prime esplichino attività che si risolvono nel trattamento dei dati personali in favore delle altre società del Gruppo. Sovente nell'ambito dei gruppi societari la società capogruppo oppure alcune delle società appartenenti al gruppo prestano determinati servizi in favore di tutte le altre società, è il caso in cui vengono centralizzate le attività di gestione degli adempimenti in materia di lavoro,

Diritto & Diritti ISSN 1127-8579

previdenza ed assistenza dei dipendenti. Le società che svolgono dette attività che implicano il trattamento di dati personali per conto delle altre società del gruppo, indipendentemente dal fatto che le società delegate siano, o meno, società capogruppo, potranno essere
nominate responsabili privacy ai sensi dell'art. 29 del Codice privacy. Nulla, pertanto, osta ai fini giuridici che il soggetto delegato sia la società capogruppo mentre la società delegante sia una società controllata o collegata.

Appare utile richiamare il
provvedimento del Garante del 6 dicembre 2006 laddove si precisa "Tuttavia, nell'ambito dei gruppi, le società controllate e collegate possono delegare la società capogruppo a svolgere adempimenti in materia di lavoro, previdenza ed assistenza sociale per i lavoratori indicati dalla legge: **tale attività implica la designazione** della società capogruppo quale responsabile del trattamento ai sensi dell'art. 29 del Codice. Analoga soluzione (art. 31, comma 2, d. lg. n. 276/2003) **deve essere adottata** per i trattamenti di dati personali, aventi identica natura, effettuati nell'ambito dei consorzi di società cooperative (nei quali a tal fine può essere altresì designata una delle società consorziate)". Il tenore letterale del provvedimento non deve indurre a ritenere che nei casi menzionati da parte del Garante privacy la nomina a responsabile sia divenuta obbligatoria. La modalità di articolazione dei ruoli privacy prospettata dall'Authority, infatti, resta quella maggiormente opportuna e già adottata dalla maggiorparte dei gruppi societari ma non assurge ad obbligo di legge, semmai, come la stessa Authority aveva avuto modo di precisare in precedenti provvedimenti inerenti i soggetti pubblici, costituisce una sorta di "scelta obbligata".

Alcune perplessità degli operatori del settore residuavano in merito alla questione inerente la possibilità per le società controllate di procedere alla nomina delle società capogruppo quali responsabili privacy poiché il rapporto societario controllante – controllata sembrava stridere con un'articolazione dei ruoli privacy in cui la controllante rivestisse il ruolo di Responsabile privacy e non di Titolare del trattamento. Il soggetto nominato responsabile, infatti, soggiace al controllo da parte del Titolare ed appariva piuttosto dubitabile la possibilità, per la società controllata, di eseguire un'attività di controllo effettivo sulle attività di trattamento dei dati personali poste in essere per suo conto e dietro specifica delega da parte della società capogruppo. Al provvedimento dell'Authority privacy va, pertanto, riconosciuto il merito di aver eliminato ogni dubbio in merito alla possibilità di procedere alla nomina della società capogruppo quale società Responsabile privacy in presenza di trattamenti eseguiti dietro delega da parte delle altre società del Gruppo.

4 La pubblicazione dei dati dei dipendenti sulla intranet aziendale

Risultano sempre più diffuse le pratiche dei datori di lavoro privati di pubblicare i dati personali dei propri dipendenti, normalmente comprensivi della fotografia, numero di telefono aziendale ed indirizzo di posta elettronica aziendale oltre che nome e cognome ed ufficio di appartenenza, sulla intranet aziendale al fine di agevolare la comunicazione tra i dipendenti. Detta prassi si è andata consolidando soprattutto nelle

aziende di grandi dimensioni, laddove individuare i soggetti, competenti per lo svolgimento di determinate attività lavorative complementari rispetto alle proprie, risulta particolarmente disagevole.

La pubblicazione dei dati dei dipendenti in Internet, invece, costituisce una pratica limitata, normalmente, ai soggetti che rivestono posizioni apicali all'interno della società.

Il Garante, nel provvedimento del dicembre 2006, ha chiarito come sia nell'uno che nell'altro caso, vale a dire pubblicazione dei dati dei dipendenti sul sito aziendale o sulla intranet, il datore di lavoro privato sia obbligato a raccogliere il consenso specifico dei dipendenti i cui dati sarebbero oggetto di comunicazione sulla intranet oppure di diffusione in Internet.

Si tratta di una soluzione che, a parere della scrivente, appare piuttosto rigida e pregiudizievole per i datori di lavoro privati: si ritiene, infatti che sarebbe stato opportuno, da parte dell'Authority un distinguo tra l'ipotesi di diffusione a mezzo Internet e di comunicazione sulla intranet aziendale.

In caso di diffusione dei dati personali a mezzo internet, infatti, non appare dubbia la necessità di procedere alla raccolta di uno specifico e preventivo consenso informato del dipendente posto che la diffusione a mazzo internet non risulta, di regola, necessaria per adempiere alle obbligazioni scaturenti dal contratto di lavoro.

Un discorso diverso, a parere di chi scrive, doveva essere effettuato per la pubblicazione sulla intranet aziendale di taluni dati personali assolutamente necessari per consentire ai dipendenti di "relazionarsi" per esigenze di carattere lavorativo: in questa specifica ipotesi, infatti, doveva ritenersi applicabile l'esimente dell'esecuzione degli obblighi contrattuali di cui all'art. 24 comma 1 lett. b del Codice privacy purché la pubblicazione fosse stata delimitata, come appena accennato, ai dati personali necessari per assumere contatti e per trasferirsi documentazione (nome e cognome, ufficio di appartenenza, numero di telefono interno,
numero di fax interno e indirizzo di posta elettronica aziendale). L'esimente contrattuale, infatti, non può estendersi all'utilizzo di dati non necessari per adempiere agli obblighi lavorativi quali, ad esempio, i curricula oppure le fotografie.

Peraltro, proprio in relazione alle fotografie va evidenziato che l'utilizzo di questa tipologia di dati personali soggiace anche all'applicazione della normativa sul diritto d'autore (legge 633/1941) che all'art. 96 stabilisce "Il ritratto di una persona non può essere esposto, riprodotto o messo in commercio senza il consenso di questa". L'entrata in vigore della normativa a tutela dei dati personali non ha, infatti, importato l'abrogazione degli articoli inerenti la tutela dell'immagine e contenuti nella LDA. Le previsioni di detta normativa si pongono in termini differenti rispetto a quanto previsto dalla normativa privacy in relazione al principio consensualistico posto che mentre il Codice privacy prevede che il consenso sia necessariamente espresso, la LDA prevede, secondo l'interpretazione giurisprudenziale affermatasi[2], che il consenso possa essere manifestato sia in modo esplicito che implicito[3].

Diritto & Diritti ISSN 1127-8579

Ne consegue che stante l'inapplicabilità dell'esimente contrattuale per la "pubblicazione" sull'intranet delle fotografie dei dipendenti, sussistesse, al pari della diffusione dei dati a mezzo internet, l'obbligo per il datore di lavoro di raccogliere il consenso espresso del dipendente.

Per quanto concerne la
pubblicazione sulla intranet del curriculum del dipendente va osservato che, in termini generali, detta pubblicazione contrasta con il principio di pertinenza cui si ispira il cosiddetto principio del need to know in base al quale i dati personali siano trattati esclusivamente in caso di necessità da parte dei soli soggetti che hanno necessità di accedervi.

5 L'utilizzo dei dati biometrici in azienda

I dati biometrici sono le informazioni che possono essere ricavate dalle caratteristiche fisiche o comportamentali di una persona. Queste informazioni vengono ricavate per il tramite dell'utilizzo di procedimenti in parte automatizzati e risultanti in un modello di riferimento che si risolve in un insieme di valori numerici ricavati dalle caratteristiche individuali. Sono, ad esempio, dati biometrici i dati ricavati dalle impronte digitali, dalla lettura dell'iride e dal riconoscimento vocale.

5.1 Alcuni precedenti

Sulla tematica del trattamento dei dati biometrici il Garante è già intervenuto con numerosissimi provvedimenti ed ha emesso, nell'ottobre del 2005, un provvedimento generale concernente l'uso di dati biometrici da parte degli istituti di credito[4]. Nel maggio 2006, peraltro, l'Authority riprendendo sostanziamente anche quanto già previsto nei confronti delle banche, ha emesso un comunicato stampa avente ad oggetto un decalogo da rispettare circa il corretto utilizzo dei dati biometrici. I dieci punti del Garante, illustrati dal consigliere Giuseppe Fortunato, in occasione del Forum della Pubblica Amministrazione, si sostanziano nei seguenti:

1)

sistemi di rilevazione dei dati biometrici affidabili da sottoporre a rigidi controlli;

2)

Diritto & Diritti ISSN 1127-8579

informativa chiara
da rilasciare ai soggetti interessati che avranno la possibilità di aderire o meno al sistema biometrico e potranno utilizzare tecniche alternative all'utilizzo dei sistemi di controllo biometrici;

3)

liceità del sistema tramite l'adozione di una verifica preventiva della necessità proporzionalità, correttezza, adeguatezza e qualità dei dati con l'obbligo, per il titolare, di non dimostrare l'inefficacia di pratiche alternative ma meno intrusive nella sfera della persona;

4)

la deroga deve essere motivata e va verificata successivamente anche alla luce del progresso scientifico, non deve essere attuato un uso incontrollato o indifferenziato delle tecniche biometriche;

5)

i dati biometrici vanno memorizzati non in archivi centralizzati e debbono sempre essere disponibili per il soggetto interessato;

6)

i dati biometrici vanno conservati per un periodo di tempo limitato e nel caso in cui siano associati alle immagini la conservazione non potrà avere una durata superiore ad una settimana;

7)

Diritto & Diritti ISSN 1127-8579

adozione di scrupolose misure di sicurezza dei dati mediante l'interposizione di una figura di "vigilatore dei dati" nelle banche che incrocino dati biometrici e dati raccolti mediante il sistema di videosorveglianza, tale figura deve essere nominata da parte di organismi indipendenti e deve presiedere all'eventuale operazione di decifrazione dei dati;

8)

garantire la piena ed immediata conoscibilità dei dati biometrici da parte dei soggetti interessati;

9)

rispettare gli obblighi di verifica preliminare del Garante previsti dall'art 17 nonché quelli di notificazione ai sensi dell'art. 37 del medesimo Codice privacy;

10)
prevedere la disattivazione automatica delle funzioni di smart card o altre funzioni analoghe in caso di smarrimento o furto.

Nel provvedimento del 6 dicembre 2006 il Garante ha indicato, anche ai sensi dell'art. 17 del Codice privacy, le misure e le prescrizioni che il Titolare del trattamento è tenuto ad adottare al fine di eseguire correttamente il trattamento di dati biometrici.

Ne consegue che i datori di lavoro privati che intendano avvalersi, nelle proprie strutture, di strumenti biometrici per le finalità indicate nel provvedimento in disamina non saranno tenuti a presentare una specifica richiesta di verifica preliminare ai sensi dell'art. 17 del Codice privacy qualora osservino anche le misure e le prescrizioni di cui al medesimo provvedimento.

Al contrario, come evidenziato dallo stesso Garante, i datori di lavoro saranno tenuti a presentare una specifica richiesta di verifica preliminare laddove intendano utilizzare strumenti biometrici per il perseguimento di finalità non considerate nel provvedimento posto che nello stesso si può leggere: "Resta salva, per fattispecie particolari o in ragione di situazioni eccezionali non considerate in questa sede, la presentazione da parte di Titolari del trattamento che intendano discostarsi dalle presenti prescrizioni, di apposito interpello al Garante, ai sensi dell'art. 17 del Codice".

Diritto & Diritti ISSN 1127-8579

5.2 Le finalità lecite

In via preliminare l'Authority, richiamando anche precedenti provvedimenti adottati sull'argomento, ha evidenziato che un uso generalizzato dei dati biometrici dei dipendenti debba escludersi e che la liceità del trattamento di questa particolare tipologia di dati debba essere valutata in considerazione della finalità e del contesto del trattamento nonché in relazione ai luoghi di lavoro. Sono, ad esempio, stati considerati legittimi:

-

il trattamento di dati biometrici per presidiare
l'accesso ad aree aziendali particolarmente sensibili in considerazione delle attività che vi si svolgono come i luoghi in cui si svolgono processi produttivi pericolosi al fine di tutelare, anche in esecuzione degli obblighi del datore di lavoro di cui all'art. 2087 c.c., la stessa incolumità dei soggetti non tenuti ad accedervi per motivi lavorativi[5];

-

il trattamento di dati biometrici per presidiare l'accesso ad aree aziendali in cui sono custoditi segreti di varia natura (es. programma avionico di rilevanza nazionale ed internazionale[6]);

-

Diritto & Diritti ISSN 1127-8579

il trattamento di dati biometrici per presidiare l'accesso a locali in cui sono custoditi beni, documenti segreti o riservati o, ancora, oggetti di valore (es. uffici di presidenza e di direzione generale in cui sono presenti fascicoli e documenti riservate ed opere d'arte[7], caveau e magazzini di stoccaggio per evitare l'introduzione nelle stive di aeromobili di oggetti pericoli ed a tutela della sicurezza dei terzi[8]).

Al contrario il Garante in più occasioni ha avuto modo di evidenziare come non possa essere considerato legittimo l'utilizzo dei dati biometrici dei dipendenti al fine di verificare l'osservanza dell'orario lavorativo; detto trattamento, infatti, sarebbe sproporzionato rispetto alla finalità di organizzazione del lavoro[9].

5.3 Il consenso informato dei dipendenti e l'obbligo di notificazione

Fermo restando quanto sopra detto in ordine alla liceità della finalità del trattamento dei dati biometrici, l'utilizzo degli stessi richiede il rilascio di un consenso preventivo libero ed informato prestato da parte dei dipendenti ai datori di lavoro.

Affinché detto consenso sia effettivamente libero è necessario che il datore di lavoro abbia provveduto alla predisposizione di misure alternative rispetto al trattamento di dati biometrici per l'accesso ai locali.

In caso contrario il consenso sarebbe viziato quindi nullo.

Il datore di lavoro è, pertanto, tenuto a rilasciare un'informativa completa che vada ad integrare l'informativa dipendenti già rilasciata eventualmente all'atto dell'assunzione o predisporre un unico documento per i nuovi assunti nel quale dia evidenza del trattamento dei dati biometrici, delle specifiche modalità e finalità di trattamento degli stessi, delle modalità alternative predisposte dal datore di lavoro per il perseguimento della medesima finalità, del consenso specifico, espresso, libero ed informato rilasciato da parte del dipendente.

La violazione dell'obbligo di informativa espone il datore di lavoro, come noto, alla sanzione amministrativa che va fino ad un massimo di novantamila euro mentre il trattamento eseguito in mancanza del consenso, quando è necessario come in questa ipotesi tenuto conto di quanto rappresentato dall'Authority, espone il datore di lavoro alla reclusione fino a tre anni in presenza delle altre condizioni di cui al delitto, perseguibile d'ufficio, di illegittimo trattamento dei dati personali di cui all'at. 167 del Codice privacy.

5.4 L'obbligo di notificazione al Garante

Un ulteriore obbligo previsto dalla normativa privacy in caso di trattamento di dati biometrici è costituito dall'obbligo di notificazione cui sono tenuti, in virtù dell'art. 37, comma 1, lett. a), tutti i Titolari del trattamento dei dati che intendano procedere al trattamento di dati biometrici.

L'inosservanza dell'obbligo di notificazione espone il Titolare del trattamento, che nel caso in analisi coincide con il datore di lavoro:

-

alla sanzione amministrativa che va da 10.000 a 60.000 euro di cui all'art. 163 del Codice privacy;

-

alla reclusione da sei mesi a tre anni, salvo che il fatto costituisca più grave reato, in caso di invio di informazioni false stante l'integrazione del delitto di cui all'art. 168 del medesimo Codice di "falsità nelle informazioni e notificazioni rese al Garante";

-

Diritto & Diritti ISSN 1127-8579

alla sanzione accessoria
della pubblicazione dell'ordinanza di ingiunzione di pagamento nella prima ipotesi, ex art. 163 ult. parte e di pubblicazione della sentenza di condanna ai sensi dell'art. 172 del Codice.

5.5 Il rispetto dello Statuto dei lavoratori

Il consenso informato degli interessati, tuttavia, non costituisce l'unica condizione di liceità del trattamento posto che ordinariamente l'utilizzo di strumenti biometrici per l'accesso ad aree riservate si risolve in uno strumento di controllo a distanza dei dipendenti.

Ne consegue che la liceità dell'installazione di siffatti strumenti richiede, sotto il profilo giuslavorista, il rispetto della procedura di cui al comma 2 dell'art. 4 dello Statuto dei lavoratori la cui vigenza è stata espressamente richiamata dall'art. 114 del Codice privacy[10].

La procedura prevista dalla citata disposizione costituita dal conseguimento di un accordo preventivo con le rappresentanze sindacali aziendali ed, in mancanza di esse, con la Direzione provinciale del lavoro. Il mancato rispetto degli obblighi di cui sopra importa l'applicabilità nei confronti della società di un'ammenda sino a lire tre milioni nonché l'arresto da 15 giorni ad un anno e la sanzione accessoria della pubblicazione della sentenza di condanna[11]. La sanzione penale ritrova attualmente il proprio fondamento normativo nell'art. 171 del Codice privacy che ha operato un rinvio all'art. 38 dello Statuto dei lavoratori. La sanzione pecuniaria può essere aumentata
fino al quintuplo qualora il giudice la ritenga inefficace in considerazione delle condizioni economiche del contravventore. Il reato di cui sopra non sarebbe un reato proprio, pertanto, autore dello stesso potrà essere non solo il datore di lavoro ma anche i soggetti addetti agli impianti vietati[12].

5.6 Le prescrizioni specifiche richieste dal Garante

Fatto salvo quanto sopra detto in merito alle ulteriori condizioni di liceità del trattamento di dati biometrici va evidenziato che detto trattamento è subordinato, inoltre, al rispetto di una pluralità di misure e prescrizioni indicate dall'Authority nel provvedimento in commento e sintetizzabili nei termini che seguono:

-

Diritto & Diritti ISSN 1127-8579

evitare la centralizzazione dei dati biometrici in specifiche banche dati nel rispetto degli obblighi previsti dagli artt. 3 e 11 del Codice; in via particolareggiata l'art. 3 stabilisce che i sistemi informativi ed i programmi informatici vadano configurati con modalità tali da ridurre al minimo l'utilizzo di dati personali diretti ed indiretti in modo da escluderne il trattamento quando la medesima finalità possa essere perseguita tramite dati anonimi oppure l'identificazione dell'interessato sia possibile solo in caso di necessità. La violazione di questo articolo espone, peraltro, al rischio di inutilizzabilità dei dati previsto dal comma 2 dell'art. 11 del Codice privacy.

-

considerare adeguati e sufficienti i sistemi biometrici basati sulla lettura delle impronte digitali memorizzate tramite un modello cifrato su un supporto che deve essere posto nell'esclusiva disponibilità dell'interessato (smart card) e privo di identificazioni nominative, il citato supporto dovrà essere "bloccato" in caso di perdita o smarrimento al fine di ridurre al minimo il rischio di utilizzi da parte di soggetti non autorizzati;

-

attuare il confronto tra il modello memorizzato e le impronte digitali mediante comuni procedure di confronto sulla carta o sul dispositivo stesso;

-

Diritto & Diritti ISSN 1127-8579

trattare i dati personali necessari per realizzare il modello esclusivamente durante la fase di registrazione;

-

impartire agli incaricati specifiche istruzioni scritte cui attenersi con particolare riferimento alle misure da adottare per evitare la perdita o
la sottrazione delle carte o dispositivi loro affidati dal datore di lavoro;

-

attuare delle misure che consentano l'acceso ai dati biometrici memorizzati al personale preposto alla verifica del rispetto delle misure di sicurezza all'interno dell'impresa esclusivamente per il perseguimento di questa finalità;

-

conservare i dati per un periodo di tempo non superiore ai sette giorni salvo la possibilità di protrarre questo periodo in presenza di limitate circostanze;

-

Diritto & Diritti ISSN 1127-8579

garantire idonei meccanismi di cancellazione automatica dei dati.

Il Garante non cita specifiche ipotesi in cui la conservazione dei dati biometrici registrati possa aver luogo per un periodo superiore ai sette giorni ma si deve ragionevolmente ritenere che non sarà dovuta la cancellazione (né su istanza di parte né automatica) in caso di richiesta dell'AG (si pensi alle ipotesi di sequestro) oppure nel caso in cui la cancellazione vada irrimediabilmente a ledere il diritto di difesa del datore di lavoro o di terzi.

5.7 Le sanzioni conseguenti all'inosservanza delle prescrizioni per il trattamento di dati biometrici

La violazione delle prescrizioni di cui al provvedimento del 6 dicembre 2006 inerenti il trattamento dei dati biometrici potrebbe importare l'integrazione del delitto di illecito trattamento dei dati personali di cui all'art. 167, comma 2, del Codice per violazione dell'art. 17 del medesimo Codice. Come si è, infatti, avuto modo di evidenziare nelle premesse di questo breve elaborato il Garante ha emanato le prescrizioni inerenti il trattamento dei dati biometrici in attuazione dell'art. 17 del Codice che così recita: "1 Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti. 2 Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare." Non appare dubbio, pertanto, che i dati biometrici rientrano tra quelle categorie di dati il cui trattamento presenta specifici rischi per i diritti e le libertà fondamentali. Nel caso di specie, pertanto, il Garante ha provveduto d'ufficio (e non dietro richiesta specifica dei titolari del trattamento) ad indicare le misure e gli accorgimenti che i datori di lavoro, che intendono utilizzare i dati biometrici dei loro dipendenti per esigenze lavorative, debbono osservare. Inoltre l'art. 167, comma 2 del Codice prevede: "Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, [omissis] è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni."

Con specifico riguardo al combinato di cui agli artt. 17 e 167 del Codice privacy va evidenziato come una parte della dottrina ha avanzato seri dubbi di legittimità costituzionale in relazione all'art. 167 nella parte in cui lo stesso richiama l'art. 17 del Codice[13].

Nello specifico il menzionato orientamento dottrinale, con il quale si concorda, ha avuto modo di rappresentare come il precetto penalistico in questo caso viene individuato
mediante il richiamo ad una norma extrapenale dai contenuti generici che, a sua volta, rinvia ad un

Diritto & Diritti ISSN 1127-8579

provvedimento amministrativo dell'Authority privacy. L'utilizzo del metodo cd. a Matrioska nell'attività legislativa penalistica esporrebbe, secondo quanto sostenuto dal citato orientamento dottrinale, la normativa di cui all'art. 167 del codice privacy, nella parte in cui richiama l'art. 17, a seri dubbi di legittimità costituzionale.

Nel caso specifico il Garante ha provveduto ad emettere un provvedimento indicativo delle misure e delle prescrizioni seppur va rilevato che il medesimo provvedimento risulta in taluni punti carente, basti pensare all'indicazione delle misure di sicurezza da adottare a protezione dei dati biometrici laddove l'Autorhity se per un verso evidenzia la non sufficienza dell'adozione delle misure minime di sicurezza di cui all'Allegato B del Codice privacy, per altro verso omette di effettuare un'indicazione puntuale e dettagliata delle misure di sicurezza ulteriori da ritenersi adeguate rispetto al trattamento dei dati biometrici, se non effettuando taluni generici riferimenti che si è avuto modo di esporre precedentemente.

La "genericità" del provvedimento del Garante del dicembre 2006 non elimina i dubbi di incostituzionalità del combinato di cui agli artt. 17 e 167 del Codice privacy sopra indicati. Pertanto, nonostante il principio del favor rei costituisca uno dei capisaldi del sistema penalistico vigente, in presenza di dubbi, da parte del datore di lavoro, circa la "riconducibilità" del trattamento dei dati biometrici da porre in essere alle relative prescrizioni di cui alle Linee guida, è opportuno avanzare una specifica richiesta di verifica preliminare ai sensi dell'art. 17 al Garante privacy al fine di scongiurare ogni pericolo di attivazione di un procedimento penale per il delitto, perseguibile d'ufficio, di illegittimo trattamento dei dati personali di cui al citato art. 167 del Codice privacy.

6 Conclusioni

In conclusione al provvedimento generale del Garante del dicembre 2006 seppur va riconosciuto il merito di aver risolto talune questioni, quali la necessità di raccogliere il consenso espresso dei dipendenti i cui dati vengono pubblicati sulla intranet aziendale nonché abbia emesso, in via preliminare, una valutazione positiva del trattamento dei dati biometrici dei dipendenti nel rispetto delle prescrizioni indicate nel medesimo provvedimento, per altro verso va osservato che detto provvedimento presta al fianco a numerose critiche.

Resta fermo l'auspicio della pronta emanazione del Codice deontologico per il trattamento dei dati personali nell'ambito del rapporto di lavoro o di altri provvedimenti generali che vadano a risolvere talune questioni prioritarie per la corretta gestione del rapporto di lavoro (es. monitoraggio elettronico dei dipendenti per scopi difensivi).

Avv. Eulalia Olimpia Policella del Foro di Roma

Per maggiori informazioni sull'argomento olimpia.policella@policella.info

Diritto & Diritti ISSN 1127-8579

[1] L'individuazione degli Incaricati costituisce una misura minima di sicurezza la cui mancata adozione può importare l'applicazione della contravvenzione di mancata adozione delle misure minime di sicurezza di cui all'art. 169 del Codice privacy.

[2] I giudici di legittimità, infatti, sin dagli anni settanta, hanno escluso l'abuso di immagine in presenza di un consenso implicito o esplicito del soggetto interessato (Cass. Civ. 73/3290). Si pensi alle ipotesi dei soggetti che hanno partecipato a trasmissioni televisive

[3] Circa la tutela dell'immagine tra il diritto alla privacy e la normativa sul diritto d'autore ci si permette di richiamare l'articolo "La tutela dell'immagine tra privacy e copyright" pubblicato in www.diritto.it all'URL: https://www.diritto.it/materiali/privacy/policella1.html.

[4] Cfr. Provvedimento generale sul trattamento dei dati biometrici da parte degli **Istituti di credito - Rilevazione di impronte digitali ed immagini: limiti e garanzie - 27 ottobre 2005** pubblicato sulla G.U. n. 68 del 22-3-2006.

[5] Sono stati considerati tali, dal Garante privacy con decisione del 15 giugno 2006 rinvenibile all'URL http://www.garanteprivacy.it/garante/doc.jsp?ID=1306523, l'ambiente produttivo molitorio poiché ritenuto estremamente pericoloso tanto che risulta

Diritto & Diritti ISSN 1127-8579

incluso nell'elenco delle attività soggette a visite e controlli periodici dei vigili del fuoco al fine del rilascio del certificato di prevenzione incendi (v. il punto 35 del decreto del Ministero dell'interno 16 febbraio 1982) nonché soggetto a due direttive europee denominate "ATEX–ATmosfere EXplosive", relative al rischio di presenza di atmosfera esplosiva in ambienti di lavoro, ed alle successive norme di attuazione (cfr. direttiva 94/9/Ce, in vigore dal 1° luglio 2003, relativa alle attrezzature e/o strumenti di lavoro; direttiva 99/92/Ce, in vigore dal 10 settembre 2003, relativa all'uomo e all'ambiente di lavoro in cui opera; D. Lg. 12 giugno 2003, n. 233 di attuazione della direttiva 99/92/Ce). In questo specifico caso il datore di lavoro ha richiesto al Garante, ai sensi dell'art. 17, di eseguire una verifica preliminare della liceità del trattamento dei dati biometrici di una parte limitata dei dipendenti che aveva accesso a dette aree al fine di evitare che personale non autorizzato possa accederVi con enorme esposizione al rischio. L'Authority ha ritenuto proporzionato rispetto alla finalità perseguita da parte del medesimo datore di lavoro posto che lo scopo è quello della tutela dell'integrità fisica dei dipendenti (art. 2087 c.c.; v. anche D. Lg. n. 626/1994 e successive modifiche ed integrazioni), è stato, pertanto, ritenuto corretto che l'accesso ai predetti impianti possa essere limitato al solo personale addetto, tecnicamente specializzato. L'impiego dei sistemi biometrici, in tal caso rende possibile con maggiore accuratezza l'accertamento dell'identità dei soggetti effettivamente autorizzati.

[6] Cfr. Verifica preliminare ex art. 17 Codice privacy del novembre 2005 in Bollettino n. 66/2005 rinvenibile all'URL http://www.garanteprivacy.it/garante/doc.jsp?ID=1202254.

[7] Cfr. Verifica preliminare del 15 giugno 2006 in Bollettino n. 73/2006 che considera lecita la finalità di voler tutelare la documentazione segreta ma richiama l'istituto di credito richiedente ad evitare la prevista centralizzazione de dati biometrici prescrivendo ulteriori misure di sicurezza. Il documento è disponibile all'URL: http://www.garanteprivacy.it/garante/doc.jsp?ID=1306098.

[8] Cfr. Provvedimento del 26 luglio 2006 in Bollettino n. 74/2006 pubblicato all'URL http://www.garanteprivacy.it/garante/doc.jsp?ID=1318582. in questo specifico provvedimento di verifica preliminare il Garante ha riconosciuto la liceità solo di alcune delle finalità che la società intendeva perseguire mediante l'utilizzo di dati biometrici escludendo espressamente la liceità del trattamento per finalità di controllo degli orari lavorativi poiché sproporzionato nonché di accesso agli uffici della società poiché non erano stati addotti elementi che dimostravano la presenza di documentazione riservata o di altre circostanze che legittimassero il trattamento de quo.

Diritto & Diritti ISSN 1127-8579

[9] Cfr. cfr. Provv.
21
luglio
2005, doc. web n.
1150679; da ultimo Provv.ti del 15 giugno 2006, in http://www.garanteprivacy.it, docc. web nn.
1306523,
1306530
e
1306551).

[10] L'art. 4 comma 2 dello Statuto dei lavoratori recita: "Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze
organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali deriva anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati
soltanto previo accordo
con le rappresentanze sindacali aziendali (RSU), oppure, in mancanza di queste, con la Commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti".

[11] Detta pubblicazione sarà eseguita nelle forme di cui all'art. 39 del codice penale.

[12] V. Secco. Il controllo del traffico telematico in azienda, dicembre 2003, in www.diritto.it.

[13] Cfr. D. Ielo e V. Saponara, Codice della privacy, op.cit. Tomo II, pag. 2153.

https://www.diritto.it/la-privacy-nei-rapporti-di-lavoro-privati/

Diritto & Diritti ISSN 1127-8579