AREA TEMATICA
PRIVACY

L'area tratta delle problematiche legate alla gestione della privacy dei lavoratori.

INDICE DEI DOCUMENTI PRESENTI NELL'AREA TEMATICA

Nota all'utilizzo del documento.
Su richiesta dei soci dal 01.10.2012 i documenti vengono inseriti in ordine cronologico, con l'indicazione della data di inserimento. I documenti antecedenti invece seguono l'ordine cronologico inverso, ovvero dal più vecchio al più recente.

Nota del 20.03.2014 - Accesso alle dichiarazioni rese dai lavoratori in sede di ispezione: avv. Paolo Ricchiuto.

Un datore di lavoro che abbia subito una ispezione, e che voglia articolare la propria difesa, ha diritto di accedere ai verbali relativi alle dichiarazioni rese dai dipendenti agli ispettori ?

La risposta a questo non semplice quesito, dopo anni di oscillazioni interpretative, è oggi compendiata in due recenti documenti di grande importanza, che devono essere letti congiuntamente:

- il nuovo *Codice di comportamento ad uso degli ispettori del lavoro approvato con d.m. 15.01.2014*, prevede espressamente all'art. 12 comma 9 che gli stessi non debbano rilasciare né al lavoratore né all'azienda copia delle dichiarazioni rese dai lavoratori, limitandosi se del caso a segnalare al richiedente che l'eventuale accesso può essere richiesto direttamente all'Amministrazione;
- specularmente, la *circolare n. 43 del 8.11.13 inviata dal Ministero del Lavoro* a tutti gli organismi territoriali, richiamando espressamente (ed allegando !) la sentenza del Consiglio di Stato n. 4035/2013, afferma un principio che tenta di comporre il diritto di difesa dell'azienda con quello alla riservatezza (in chiave di tutela da possibili ritorsioni) del lavoratore: l'accesso va di regola negato, e può essere concesso solo e soltanto in specifici casi, nei quali l'amministrazione ravvisi una "prevalenza delle esigenze difensive", comunque previa adozione di specifiche misure (come l'oscuramento del nominativo del dichiarante).

Alla luce di tutto ciò, in sede di richiesta di accesso, non sarà possibile addurre generiche esigenze difensive, ma sarà necessario indicare specifiche motivazioni a sostegno della istanza. Quali ?

L'esperienza applicativa ci dirà se un principio apparentemente così virtuoso sarà gestito sulla base di criteri oggettivi ed uniformi, o se, come accade ogni volta che ci si misura con disposizione troppo "aperte", il tema rimarrà esposto a potenziali arbitri interpretativi.

Quello che è certo, è che continua ad essere incomprensibile, almeno a chi scrive, un sistema che inibisce all'azienda nella fase del contenzioso amministrativo di conoscere il contenuto di dichiarazioni che, nella stragrande maggioranza dei casi, nella successiva fase del vaglio giudiziale, vengono comunque prodotte dalla difesa dell'amministrazione a corredo della propria posizione difensiva.

L'esistenza di questo doppio binario, quindi, non tutela affatto il lavoratore, ma semplicemente (ed un po' ipocritamente) sposta in avanti la ostensione delle sue dichiarazioni, non mettendolo affatto al riparo da azioni ritorsive del datore di lavoro, di tal che sembra tradursi, inutilmente, in una duplice lesione del diritto di difesa dell'azienda, costretta ad articolare il proprio ricorso amministrativo, prima, e quello avanti al Giudice del Lavoro, dopo, senza conoscere il contenuto analitico delle dichiarazioni dei lavoratori, con tutte le potenziali decadenze che ciò può peraltro determinare.

Torna al sommario

Nota dell'11.06.2013 - Il nuovo Vademecum del Garante per le imprese: avv. Paolo Ricchiuto: *Coordinatore scientifico Sezione Protezione dei Dati Personali*

Continuando nella meritoria (ed ancora, assolutamente necessaria !) opera di divulgazione delle regole privacy che ogni azienda è tenuta a rispettare, il Garante ha appena pubblicato sul proprio sito istituzionale (http://www.garanteprivacy.it/documents/10160/2416443/Vademecum-privacy-e-imprese.pdf) un nuovo, snellissimo Vademecum, nel quale sono compendiati principi di riferimento che è sempre opportuno avere ben presenti.

Nel segnalare agli associati la opportunità di una attenta lettura di tutto il documento (per qualcuno, sarà un mero ripasso; per altri, l'occasione per scoprire la esistenza di tante soluzioni utili a semplificare la gestione di determinati adempimenti), va sottolineata la parte n. 4 del documento dedicata al trattamento dei dati contenuti nel curriculum vitae del candidato alla assunzione.

Ancora una volta, e facendo giustizia di ridondanti prassi operative (es: il consenso espresso in calce al curriculum) o di vere e proprie leggende (es: è sempre e comunque necessario un consenso), l'Autorità ribadisce con estrema chiarezza come:

- l'azienda che lancia una selezione di personale e che in esito alla stessa raccoglie i curriculum inviati dagli aspiranti al posto offerto è sì, sempre tenuta a dare una informativa, ma la stessa può essere scritta o orale;

- il consenso non è affatto necessario (a meno che il curriculum non contenga dati sensibili, come ad esempio quelli relativi alla appartenenza a categorie protette);

- quando il curriculum venga spontaneamente inviato dal candidato (al di fuori, quindi, di una selezione strutturata), l'onere della informativa non scatta automaticamente, ma solo e soltanto nel momento in cui l'azienda decida di prendere in considerazione il curriculum e di contattare il candidato (ed è in quel momento che il potenziale datore di lavoro può adempiere all'onere di informare sulle caratteristiche e finalità del trattamento, anche mediante una informativa orale).

Ecco allora una buona opportunità per verificare se all'interno della propria azienda esistano zone scoperte o (come sempre più spesso accade) inutili ingessature operative che è agevole superare conoscendo le regole.

Torna al sommario

Esistono ancora i controlli difensivi? avv. Paolo Ricchiuto: *Coordinatore scientifico Sezione Protezione dei Dati Personali*

Con la recentissima sentenza n. 16622 del 01.10.12, la Cassazione torna sul tema dei controlli difensivi, ed afferma con stentorea chiarezza principi che, a primissima vista, appaiono in grado di annichilire quella categoria esegetica.
Nel rimandare alla integrale lettura della interessante, e sorprendente, pronuncia, ecco il passaggio che può assumere un rilievo veramente critico,
"l'effettività del divieto di controllo a distanza dell'attività dei lavoratori richiede che anche per i ed. controlli difensivi trovino applicazione le garanzie del citato art. 4, secondo comma, e che, comunque, quest'ultimi, così come la altre fattispecie di controllo ivi previste, non si traducano in forme surrettizie di controllo a distanza dell'attività lavorativa dei lavoratori. Se per l'esigenza di evitare attività illecite o per motivi organizzativi o produttivi, possono essere installati impianti ed apparecchiature di controllo che rilevino dati relativi anche alla attività lavorativa dei lavoratori, la previsione che siano osservate le garanzie procedurali di cui all'art. 4, secondo comma, non consente che attraverso tali strumenti, sia pure adottati in esito alla concertazione con le r.s.a., si possa porre in essere, anche se quale conseguenza mediata, un controllo a distanza dei lavoratori che, giova ribadirlo, è vietato dall'art. 4, comma 1. cit."
Ciò equivale a dire che se l'illecito compiuto dal lavoratore attiene, in qualsiasi forma, alla sua attività lavorativa, il datore di lavoro vede inibita la possibilità di farlo emergere con strumenti di controllo a distanza (come un sistema di filtraggio delle telefonate).
Seguendo questo ragionamento, se una cassiera ruba il denaro dalla cassa, un sistema di videosorveglianza installato senza il previo accordo con le RSA sarebbe sempre e comunque illegittimo, atteso che la condotta illecita fatta oggetto di accertamento sarebbe intimamente connessa con lo svolgimento della prestazione lavorativa.
Esattamente il contrario, di quanto affermato anche recentemente dalla Cassazione penale (fra le altre, cfr. sentenza n. 20722 del 01.06.10)
Molto ci sarà da meditare sui contenuti di questa pronuncia. Quello che è certo, è che su questo importantissimo tema, la confusione regna sovrana, e la sentenza in commento introduce un ulteriore tassello grigio, nel già sufficientemente disorganico quadro disegnato dalle sentenze della Cassazione penale (che continuano a "difendere" i controlli difensivi"), dalle pronunce del Garante per la protezione dei dati personali (che lavorano, da anni, per abbattere quella categoria) e dai precedenti della Sezione Lavoro del Supremo Collegio (che, a parere di chi scrive, mai si erano spinte a negare con tanta chiarezza la esistenza di una categoria contigua, ma estranea, all'area dell'art. 4 L. 300/70).

Cassazione Sezione Lavoro — 01.10.2012 n. 16622

Svolgimento del processo

1. La Corte d'Appello di Roma, con la sentenza n. 1970, del 12 novembre 2009, resa sull'impugnazione proposta da M.R. nei confronti della società A.G. spa, in ordine alla sentenza emessa dal Tribunale di Roma n. 11651 del 2007, rigettava l'appello e compensava tra le parti le spese di giudizio.

2. H R. aveva adito il Tribunale per sentire dichiarare l'illegittimità del licenziamento intimatogli in data 23 dicembre 2004, con l'adozione delle conseguenti statuizioni di cui all'art. 18 Statuto dei lavoratori.

Esponeva che con contestazioni del 2 e del 23 novembre 2004 era stato a lui addebitato, quale operatore telefonico di centrale di prima assistenza stradale e automobilistica, di aver intrattenuto, nel periodo 1° agosto- 29 ottobre 2004, n. 460 contatti telefonici inferiori a 15 secondi (tempo non sufficiente per sentire le richieste degli utenti e rispondere) e di aver effettuato 136 telefonate personali.

Il Tribunale di Roma rigettava la domanda.

3. La Corte d'Appello, con la sentenza sopra richiamata, in via preliminare rigettava l'eccezione di improcedibilità dell'appello e, nel merito, riteneva, come già il giudice di primo grado, che il sistema di rilevamento delle telefonate attraverso il software Blue's 2002 non fosse in contrasto con l'art. 4 dello Statuto dei lavoratori, in quanto relativo al cd. controllo difensivo.

Affermava, altresì, la tempestività della contestazione e la sussistenza della prova in fatto, in ragione dei tabulati, delle condotte ascritte al R.; riteneva, quindi, sussistente la responsabilità di quest'ultimo in ordine ai fatti contestati, nonché la gravità degli stessi.

4. Ricorre, per la cassazione della suddetta sentenza d'appello, il R., prospettando tre motivi di ricorso.

5.Resiste con controricorso la società A.G. spa

6. Il R. ha depositato memoria ai sensi dell'art. 378 cpc.

Motivi della decisione

1. Con il primo motivo di ricorso è dedotta la violazione dell'art. 2909 c.c.

Il ricorrente ricorda che con decreto del 6 giugno 2005, adottato ex art. 28 della legge n. 300 del 1970, nel giudizio promosso da FISAC (recte: FILT) CGIL di Roma nei confronti della società A.G. spa, il Tribunale di Roma accertava l'illegittimità dell'installazione ed utilizzo del sistema informatico Blue's 2002.

Tale pronuncia, ad avviso del ricorrente costituirebbe giudicato nel presente giudizio, anche non era parte del suddetto procedimento.

1.1. Il motivo non è fondato e deve essere rigettato. Ed infatti, le statuizioni assunte nel decreto ex art. 28, del 6 giugno 2005, come si evince dall'esame dello stesso e dalla sentenza del Tribunale di Roma dell'8-11 gennaio 2007 resa nel relativo giudizio di opposizione, non sono intervenute sulle complessive medesime questioni di fatto e di diritto dell'odierno giudizio, né tra le stesse parti, sancendo le stesse una condotta antisindacale nell'installazione del programma Blue's 2002 senza il previo confronto con le 00.SS.

2. Con il secondo motivo di ricorso è dedotta violazione dell'art. 4 della legge n. 300 del 1970.

Erroneamente, la Corte d'Appello (nel richiamare Cass., n. 4746 del 2002 e Cass., n. 15892 del 2007), avrebbe ritenuto legittimi gli accertamenti compiuti dalla società A.G. spa con il sistema informatico Blue's 2002, nonostante il fatto che lo stesso consentisse un controllo a distanza sull'attività lavorativa e fosse installato in assenza di accordo con le OO.SS., o autorizzazione dell'Ispettore del lavoro, affermando che si trattava di controllo difensivo, in quanto tale sottratto all'ambito di applicazione del citato art. 4.

3. Con il terzo motivo di ricorso è dedotta omessa motivazione circa fatti controversi e decisivi riguardanti la ritenuta sussistenza e riferibilità al ricorrente degli addebiti posti a fondamento del licenziamento.

Ed infatti, l'acquisizione dei tabulati, nonché la documentazione acquisita con il sistema di controllo, posti dal giudice di appello a fondamento della prova delle condotte contestate al R., sarebbe illegittima e illecita (art. 171 del d.lgs. n. 196 del 2003), con la conseguente illegittimità della contestazione disciplinare e del successivo licenziamento. Inoltre, contrariamente a quanto ritenuto dalla Corte d'Appello, in nessuna lettera di reclamo, né nelle deposizioni dei testi L.C. e

E.B. vi era un qualunque elemento che consentisse dì riferire i fatti/disservizi denunciati a comportamenti di esso ricorrente, neppure in via indiretta o indiziaria.

4.1Il secondo ed il terzo motivo di ricorso devono essere esaminati congiuntamente in ragione della loro connessione. Gli stessi sono fondati e devono essere accolti.

4.1. L'art. 4 della legge n. 300 del 1970, commi 1 e 2, stabilisce il divieto di apparecchiature di controllo a distanza, e subordina ad accordo con le r.s.a., o a specifiche disposizioni dell'ispettorato del lavoro, l'installazione di quelle apparecchiature rese necessarie da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dalle quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori.

Le richiamate disposizioni fanno parte di quella complessa normativa diretta a regolamentare le manifestazioni del potere organizzativo e direttivo del datore di lavoro che, per le modalità di attuazione incidenti nella sfera della persona, si ritengono lesive della dignità e della riservatezza del lavoratore.

La garanzia procedurale prevista per impianti ed apparecchiature ricollegabili ad esigenze produttive contempera l'esigenza di tutela del diritto dei lavoratori a non essere controllati a distanza e quello del datore dì lavoro o, se si vuole, della stessa collettività, relativamente alla organizzazione, produzione e sicurezza del lavoro, individuando una precisa procedura esecutiva e gli stessi soggetti ad essa partecipi (Cass., n. 15982 del 2007).

La possibilità di effettuare tali controlli incontra un limite nel diritto alla riservatezza del dipendente, tanto che anche l'esigenza di evitare condotte illecite dei dipendenti non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore (cfr. Cass., 4375 del 2010).

4.2. La giurisprudenza di legittimità è intervenuta più volte sull'applicazione di detta disposizione, modificando il proprio iniziale orientamento, ed affermando i seguenti principi di diritto.

Con la sentenza n. 4746 del 2002 si era statuito che, ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori, era necessario che il controllo riguardasse (direttamente o indirettamente) l'attività lavorativa, mentre dovevano ritenersi certamente fuori dell'ambito di applicazione della norma ì controlli diretti ad accertare condotte illecite del lavoratore, cd. controlli difensivi.

Tale giurisprudenza, quindi escludeva, i cd. controlli difensivi, dall'ambito di applicazione dell'art. 4, comma 2.

Con la successiva pronuncia n. 15892 del 2007, volta a sostanziare l'effettività del divieto di cui all'art. 4, comma 1, cit. si è poi affermato che il riferimento all'attività lavorativa, oggetto della fattispecie astratta, non riguardava solo le modalità del suo svolgimento, ma anche il quantum della prestazione, il controllo sull'orario di lavoro, risolvendosi in un accertamento circa quantità di lavoro svolto.

Si è poi statuito, correggendo l'impostazione sopra richiamata di Cass., n. 4746 del 2002, che riteneva in ogni caso legittimi i cd. controlli difensivi, che l'insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore (Cass. 15982 del 2007).

In tema di controllo del lavoratore, le garanzie procedurali imposte dall'art. 4, secondo comma, della legge n. 300 del 1970 (espressamente richiamato anche dall'art. 114 del d.lgs. n. 196 del 2003 e non modificato dall'art. 4 della legge n. 547 del 1993, che ha introdotto il reato dì cui all'art. 615-ter cp) per l'installazione di impianti ed apparecchiature di controllo richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, trovano applicazione anche ai controlli ed. difensivi, ovverosia a quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino l'esatto adempimento delle obbligazioni

discendenti dal rapporto di lavoro e non la tutela dei beni estranei al rapporto stesso Cass., n. 2722 del 2012, ti. 4375 del 2010).
4.3. Così richiamato il quadro normativo e giurisprudenziale occorre precisare che il giudice di merito ha ritenuto che il sistema informatico Bluès 2002 non fosse in contrasto con l'art. 4 dello statuto dei lavoratori per un duplice ordine di ragioni.
In primo luogo, perché la circostanza che a seguito del cd. controllo difensivo a cui era finalizzato il suddetto sistema informatico, risultasse l'inesatto adempimento della prestazione di lavoro del lavoratore non è che una conseguenza indiretta dell'illecito che il datore di lavoro ha diritto di controllare proprio nella forma del ed. controllo difensivo.
In secondo luogo, perché anche la rilevazione di telefonate ingiustificate mira ad evitare illeciti e ben può con la scoperta dell'illecito emergere il relativo inadempimento contrattuale, se ciò che è vietato è solo il controllo sull'orario di lavoro e sul "quantum" della prestazione, e non già sugli illeciti comportamenti dei dipendenti.
4.4. Dette statuizioni della Corte d'Appello non fanno corretta e congrua applicazione dei principi di diritto di cui alla sentenza Cass., n. 4375 del 2010, sopra richiamata ai quali si intende dare continuità.
Ed infatti, l'effettività del divieto di controllo a distanza dell'attività dei lavoratori richiede che anche per i ed. controlli difensivi trovino applicazione le garanzie del citato art. 4, secondo comma, e che, comunque, quest'ultimi, così come la altre fattispecie di controllo ivi previste, non si traducano in forme surrettizie di controllo a distanza dell'attività lavorativa dei lavoratori.
Se per l'esigenza di evitare attività illecite o per motivi organizzativi o produttivi, possono essere installati impianti ed apparecchiature di controllo che rilevino dati relativi anche alla attività lavorativa dei lavoratori, la previsione che
siano osservate le garanzie procedurali di cui all'art. 4, secondo comma, non consente che attraverso tali strumenti, sia pure adottati in esito alla concertazione con le r.s.a., si possa porre in essere, anche se quale conseguenza mediata, un controllo a distanza dei lavoratori che, giova ribadirlo, è vietato dall'art. 4, comma 1. cit.
Il divieto di controlli a distanza ex art. 4, della legge n. 300 del 1970, implica, dunque, che i controlli difensivi posti in essere con il sistema informatico Blue's 2002, ricadono nell'ambito dell'art. 4, comma 2, della legge n. 300 del 1970, e, fermo il rispetto delle garanzie procedurali previste, non possono impingere la sfera della prestazione lavorativa dei singoli lavoratori; qualora interferenze con quest'ultima vi siano, e non siano stati adottati dal datore di lavoro sistemi di filtraggio delle telefonate per non consentire, in ragione della previsione dell'art. 4, comma 1, di risalire all'identità del lavoratore, i relativi dati non possono essere utilizzati per provare l'inadempimento contrattuale del lavoratore medesimo.
5. Il ricorso, quindi, deve essere accolto con riguardo al secondo e al terzo motivo di impugnazione, rigettato il primo. Cassa la sentenza impugnata e rinvia anche per le spese del presente giudizio alla Corte d'Appello di Roma in diversa composizione, che si atterrà ai suddetti principi di diritto.
P.Q.M.
Accoglie il secondo ed il terzo motivo di ricorso. Rigetta il primo motivo. Cassa la sentenza impugnata in relazione ai motivi accolti e rinvia alla Corte d'Appello di Roma in diversa composizione anche per le spese del presente giudizio.

Torna al sommario

Provvedimento del 23 dicembre 2010 del Garante della Privacy
Avv. Paolo Ricchiuto - *Coordinatore scientifico Sezione Protezione dei Dati Personali*

Un dipendente licenziato per aver distolto il know how aziendale in favore di un concorrente, si rivolge al Garante per opporsi al trattamento da parte del datore di lavoro dei dati contenuti nel portatile che aveva in uso. L'opposizione si riferisce in particolare ai dati inseriti in una directory che in sede di riconsegna dell'apparecchio il lavoratore aveva espressamente indicato esser dedicata soltanto ad informazioni private, ed estranee all'attività lavorativa. Il Garante accoglie il ricorso, ed inibisce all'azienda di accedere a quei dati (che quindi, si arguisce, non essendo accessibili, non potranno nemmeno esser utilizzati per finalità difensive nel giudizio avente ad oggetto la impugnazione del recesso).

*

Con riferimento all'uso da parte dei dipendenti degli strumenti elettronici assegnati in dotazione dall'azienda, la giurisprudenza del Garante degli ultimi anni (soprattutto quella formatasi a seguito della emanazione delle cd. Linee Guida per posta elettronica ed internet del 01.03.07) sta rendendo sempre più chiaro come tutti i datori di lavoro pubblici e privati, per poter esercitare le naturali prerogative connesse alla sovraodinazione gerarchica, debbano necessariamente dotarsi di un compiuto regolamento interno che chiarisca cosa i lavoratori possono o non possono fare.

Il provvedimento sotto riportato si segnala proprio per la sua portata generale: se è infatti certamente vero che la adozione di un cd. "disciplinare interno" sia ad oggi obbligatoria soltanto relativamente all'uso di internet e della posta elettronica (cfr. prescrizione ex art. 154 comma 1 lett. c del Codice Privacy, impartita dal Garante nelle Linee Guida citate), l'Autorità, inibendo nel caso di specie all'azienda la possibilità di accedere ai dati contenuti sul portatile assegnato in dotazione ad un ex-dipendente perché contenuti in una directory utilizzata per dichiarate esclusive finalità non professionali, indirettamente sembra affermare che tale problematica non si sarebbe posta, laddove fosse esistita una policy interna che avesse inibito a monte l'uso del computer per motivi estranei alla attività lavorativa.

L'assenza di chiarezza in sede di assegnazione dello strumento al lavoratore, quindi, si risolve in una sostanziale paralisi delle facoltà datoriali di controllo, ivi comprese quelle finalizzate all'accertamento di un illecito.

Sul punto il provvedimento de quo segna pertanto un ulteriore avanzamento delle tesi più oltranziste in termini di inibizione delle facoltà di controllo. Se infatti già il Garante, ai fini della applicazione dell'art. 4 comma 2 L. 300/70, ha da anni sostanzialmente by-passato la categoria dei controlli difensivi (con buona pace dei pur recentissimi interventi sul punto della Suprema Corte di Cassazione che continuano al contrario ad affermare la esistenza ed utilizzabilità di tale categoria esegetica), con il provvedimento qui indicato l'Autorità va ancora più in là, sostenendo che la dedotta non attinenza delle informazioni alla attività lavorativa faccia scattare *ex se*, ed a prescindere dall'applicabilità o meno della norma statutaria, la conseguenza della impossibilità per il datore di lavoro di accedere a tali dati, anche se tale accesso sia finalizzato, come nel caso di specie, ad accertare il compimento di un illecito.

Ecco quindi un ulteriore tassello che deve spingere ogni datore di lavoro ad affrontare preventivamente il problema, per non trovarsi nella spiacevole situazione di vedersi inibito il potere di controllare il compimento di illeciti sempre più agevolmente perpetrabili mediante gli

strumenti elettronici (soprattutto se il Garante dovesse, come nel caso di specie, ritenere sufficiente che il lavoratore dichiari la non attinenza all'attività lavorativa dei dati contenuti in una directory, nella quale siano magari in realtà nascoste le prove dell'illecito).

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

[doc. web n. 1786116]

NELLA riunione odierna, in presenza del prof. Francesco Pizze tti, presidente, del dott. Giuseppe Chiaravallo ti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Daniele De Paoli, segretario generale;

VISTO il ricorso presentato al Garante il 30 luglio 2010 nei confronti di T.E.R. s.r.l. (rappresentata e difesa dall'avv. Giulio De Carolis) con il quale XY (rappresentato e difeso dall'avv. Luca Nisi), ex dipendente della predetta società, ha ribadito la richiesta, già avanzata ai sensi dell'art. 7 del Codice in materia di protezione dei dati personali (d. lgs. 30 giugno 2003, n. 196), volta a ottenere la cancellazione dei dati che lo riguardano conservati in alcune ***directory*** (dallo stesso espressamente indicate in un ***"verbale di riconsegna beni e dati"***) contenute nell'***hard disk*** del ***notebook*** datogli in uso dalla società e restituito alla stessa a seguito del proprio licenziamento, opponendosi al loro ulteriore trattamento; ciò tenuto conto che tali dati non farebbero alcun riferimento all'attività lavorativa prestata, essendo esclusivamente relativi alla propria vita privata (tra essi, ad esempio, il ricorrente cita ***"numerose foto delle nipotine (...), foto della fidanzata (...) e di altri parenti e amici, le buste paga recapitate dalla società T .E.R. s.r.l. in formato elettronico, (...), e-mail scambiate con familiari, parenti ed amici a mezzo del proprio indirizzo e-mail personale"***, per il quale lo stesso ha dichiarato di utilizzare un ***"client di posta elettronica"*** distinto da quello utilizzato per la casella di posta attribuitagli dalla società resistente); rilevato che il ricorrente ha chiesto la liquidazione in proprio favore delle spese del procedimento;

VISTI gli ulteriori atti d'ufficio e, in particolare, la nota del 9 agosto 2010, con la quale questa Autorità, ai sensi dell'art. 149, comma 1 del Codice ha invitato il predetto titolare del trattamento a fornire riscontro alle richieste dell'interessato, nonché il verbale dell'audizione del 27 settembre 2010 e la nota del 12 novembre 2010 con la quale è stata disposta, ai sensi dell'art. 149, comma 7, la proroga dei termini del procedimento;

VISTA la memoria inviata via fax il 23 settembre 2010 con la quale la società resistente, nel dichiarare che il computer in questione ***"non è stato mai riassegnato ad altri, né è stato mai acceso dal momento della consegna da parte del ricorrente a seguito della sospensione dall'attività lavorativa"*** e che lo stesso sarebbe ***"conservato in luogo appartato, dedicato e sicuro presso la sede dell'azienda, a disposizione dell'autorità giudiziaria"***, ha rappresentato di voler conservare tutti i dati (personali e non) contenuti nel notebook poiché gli stessi, a proprio avviso, sarebbero necessari per far valere e difendere in giudizio i propri diritti, costituendo ***"gli elementi probatori posti a fondamento delle circostanze che hanno prodotto il licenziamento"***; in particolare, la società ha sostenuto che, attraverso "***l'account registrato nel computer aziendale (...)"*** del ricorrente emergerebbe ***"un preciso intento criminoso che coinvolge"*** alcuni ex dipendenti e soci della resistente e volto ***"a creare, attraverso attività di concorrenza sleale, vantaggio illegittimo per sé e per altri e precisamente (...) a spostare le risorse tecniche, economiche ed il know how dell'azienda TER (...) verso un'altra azienda"***; rilevato che, alla luce di ciò, la resistente ha rappresentato che ***"la cancellazione dei dati così come genericamente richiesta creerebbe una inevitabile compressione delle garanzie di difesa dell'azienda che, sul punto, ha già avviato denuncia-querela"*** e che gli stessi dati comunque evidenzierebbero altresì "***l'illegittimo utilizzo da parte del dipendente dello strumento aziendale"*** alla luce delle disposizioni impartite al riguardo con regolamento di cui la società ha allegato copia;

VISTA la memoria depositata il 27 settembre 2010 con la quale il ricorrente ha insistito nelle richieste formulate e, allegando copia di alcune sue comunicazioni ***e-mail*** depositate dalla società

in un giudizio attualmente in corso a seguito di opposizione a un decreto ingiuntivo relativo al riconoscimento di indennità da fine rapporto, ha ipotizzato che la stessa abbia già, contrariamente a quanto sostenuto, avuto accesso ai dati conservati nel ***notebook*** aziendale; rilevato che il ricorrente ha altresì dichiarato di non aver ***"attivato formale impugnazione del licenziamento innanzi all'Autorità giudiziaria (...), avviando semplicemente la preliminare e tassativa procedura di conciliazione innanzi alla competente Direzione provinciale del lavoro"*** e di non vedere la ragione della paventata ***"compressione del diritto di difesa"*** della società;
VISTE le note datate 8 ottobre, 4 e 29 novembre 2010 con le quali la resistente ha ribadito di non aver avuto accesso al ***notebook*** del ricorrente, ma di aver recuperato le ***e-mail*** in questione da altro ***"hard disk aziendale di back-up lasciato in azienda da uno dei soci"*** (accusato poi di concorrenza sleale), ora non più disponibile, e di averne verificato "in rete" la provenienza e la destinazione (le stesse sarebbero ***"partite dal computer aziendale affidato al XY e (...) giunte"*** al predetto ex socio); rilevato che la resistente ha ribadito di aver operato nel rispetto anche del regolamento aziendale secondo il quale gli strumenti aziendali potevano essere sottoposti ***"a verifiche e controlli da parte dell'azienda per verificarne il legittimo utilizzo"***;
VISTE le memorie del 4 novembre, 17 e 20 dicembre 2010 con le quali il ricorrente ha contestato le argomentazioni della controparte e ha sollevato perplessità in ordine alla liceità della raccolta delle informazioni contenute nelle e-mail depositate dall'azienda nel giudizio per il riconoscimento dell'indennità da fine rapporto, ribadendo le proprie richieste;
RILEVATO che il datore di lavoro può riservarsi anche di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (***cfr. provv***. del Garante del 1° marzo 2007 ***"Lavoro: le linee guida del Garante per posta elettronica e internet"*** pubblicate in G. U. n. 58 del 10 marzo 2007 e artt. 2086, 2087 e 2104 cod. civ.);
RITENUTO tuttavia che, nell'esercizio di tale prerogativa, occorre rispettare la libertà e la dignità dei lavoratori, nonché, con specifico riferimento alla disciplina in materia di protezione dei dati personali, i principi di correttezza (secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori), di pertinenza e non eccedenza di cui all'art. 11, comma 1, del Codice; ciò tenuto anche conto che tali controlli, indipendentemente dalla loro liceità, possono determinare il
trattamento di informazioni personali, anche non pertinenti o idonee a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale;
RILEVATO che, nel caso di specie, la società resistente ha dichiarato di limitarsi a conservare il ***notebook*** aziendale che era stato dato in uso al ricorrente e di non aver avuto accesso al suo contenuto e, quindi, ai dati personali che lo riguardano ivi conservati (dichiarazione, questa, della cui veridicità l'autore risponde ai sensi dell'art. 168 del Codice: "Falsità nelle dichiarazioni e notificazioni al Garante"), intendendo solo lasciarlo a disposizione dell'autorità giudiziaria per le eventuali verifiche nell'ambito di procedimenti giudiziari instaurati e instaurandi dalla società;
RILEVATO che, alla luce della documentazione acquisita in atti e delle dichiarazioni rese nel corso del procedimento, risulta comprovato che l'eventuale accesso da parte della società resistente alle ***directory*** indicate dal ricorrente contenute nel notebook in questione comporterebbe il conseguente trattamento di dati personali estranei all'attività lavorativa svolta dallo stesso e ciò in assenza dei presupposti di liceità del trattamento previsti dalla legge (***cfr.*** artt. 23, 24 e 26 del Codice) e in violazione dei principi di pertinenza e non eccedenza delle informazioni personali di cui all'art. 11 del Codice (***cfr.*** al riguardo, i principi richiamati da questa Autorità nel provvedimento del 1° marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e in terne t" in G.U. 10 marzo 2007, n. 58, nonché in ***www.garanteprivacy.it***, doc. ***web***. n. 1387522);
RITENUTO pertanto, alla luce di ciò, di dover dichiarare parzialmente fondato il ricorso e, quale misura necessaria a tutela dei diritti del ricorrente ai sensi dell'art. 150, comma 2, del Codice, di

dover inibire alla resistente di accedere e di trattare i dati personali del ricorrente contenuti nelle ***directory*** dallo stesso indicate nel citato ***"verbale di riconsegna beni e dati"*** ed estranei alla sua attività lavorativa; resta salvo il diritto della resistente di conservare intatto l'***hard disk*** in questione per consentire all'autorità giudiziaria di accedervi laddove necessario, fermo restando quanto disposto dall'art. 160, comma 6, del Codice, con riferimento alle autonome determinazioni da parte della stessa in ordine all'utilizzabilità nell'eventuale procedimento penale dei documenti in esso contenuti;
RITENUTO che sussistono giusti motivi per compensare le spese tra le parti alla luce della peculiarità della vicenda esaminata; VISTA la documentazione in atti;
VISTI gli artt. 145 e s. del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);
VISTE le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1I2000; RELATORE il dott. Giuseppe Chiaravalloti;
TUTTO CIÒ PREMESSO IL GARANTE:
accoglie parzialmente il ricorso e, ai sensi dell'art. 150, comma 2, del Codice, quale misura a tutela dei diritti dell'interessato, inibisce alla società resistente di accedere e trattare le informazioni personali relative al ricorrente contenute nelle ***directory*** dallo stesso indicate nel citato ***"verbale di riconsegna beni e dati"*** ed estranei alla sua attività lavorativa;
dichiara compensate le spese tra le parti. ***Roma, 23 dicembre 2010***

Torna al sommario

Provvedimento n. 089 del 2 marzo 2011 Garante della Privacy: avv. Paolo Ricchiuto: *Coordinatore scientifico Sezione Protezione dei Dati Personali*

Con il provvedimento generale 23.11.06 (le cd. Linee Guida Lavoro, ancora reperibili sul sito dell'Autorità - http://www.garanteprivacy.it/garante/doc.jsp?ID=1364099), il Garante aveva, ormai quasi 5 anni orsono, dato vita ad una sorta di vademecum inteso ad agevolare i datori di lavoro nella corretta gestione degli adempimenti privacy nei confronti dei propri dipendenti. Soprattutto in realtà medio-piccole, anche tali principi di base continuano a non esser compiutamente assimilati, e si assiste ancora a condotte datoriali caratterizzate dalla integrale assenza di consapevolezza delle rischiosità connesse (anche in termini di responsabilità penale ed amministrativa). Il provvedimento sotto riportato, adottato a seguito del reclamo di un dipendente nei confronti del proprio datore di lavoro, può costituire una ulteriore fonte di riflessione sia su temi di carattere generale (ad es: la designazione come incaricati o responsabili dei soggetti che trattano i dati), sia su profili più specifici, quali la legittimità della comunicazione ad altri dipendenti (e/o della diffusione) dei dati relativi ad un singolo lavoratore interessato. Nel caso di specie, ad una serie di dipendenti era stato comunicato mediante una apposita missiva il numero di giorni di ferie non godute dai medesimi, così mettendo nella disponibilità di ognuno dei destinatari il dato relativo a tutti gli altri interessati. Il Garante, chiamato a decidere della legittimità di tale condotta, non fa altro sul punto che riprendere un principio già affermato a più riprese, e riprodotto nelle Linee Guida Lavoro, a tenore del quale "*il datore di lavoro, in linea di principio, deve utilizzare forme di comunicazione individualizzata con il lavoratore, adottando le misure più opportune per prevenire un'indebita comunicazione di dati personali, in particolare se sensibili, a soggetti diversi dal destinatario".* Ancora una volta, quindi, va segnalata la opportunità di verificare *de minimis* nelle Linee Guida se esistano punti di riferimento utili, prima di dare corso ad iniziative che impattano sulla riservatezza dei dipendenti: anche la "innocente" pubblicazione nella bacheca aziendale di un computo delle ferie godute, può portare a conseguenze estremamente pesanti se non correttamente gestita !

avv. Paolo Ricchiuto
Centro Assistenza AIDP LAZIO
Coordinatore scientifico
Sezione Protezione dei Dati Personali

Lavoro: garanzie per il trattamento e la comunicazione di dati personali dei dipendenti - 2 marzo 2011

Registro dei provvedimenti n. 089 del 2 marzo 2011

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Daniele De Paoli, segretario generale;

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

VISTO il provvedimento del 23 novembre 2006, avente ad oggetto il trattamento di dati personali dei lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati (doc. *web* n. 1364939); Inoltre, per quel che concerne la comunicazione del 29 ottobre 2009, il centro servizi ha specificato di aver ritenuto *"sufficiente al fine di autorizzare lo stesso CSV alla divulgazione di dati comuni"* relativi all'interessato *"la sottoscrizione dell'informativa da parte [di quest'ultimo] all'atto della stipula del contratto"*.

Da ultimo, il centro servizi ha sostenuto di "aver adottato tutte le misure di sicurezza previste dall'art. 31 del Codice",
manifestando comunque la propria disponibilità ad integrare eventualmente le misure già adottate *"anche attraverso dei momenti formativi sia individuali che collettivi e con delle verifiche interne periodiche per monitorare costantemente la corretta applicazione della normativa"*.
3.1. Il presente reclamo ha ad oggetto il trattamento di dati personali svolto da un centro di servizio con funzioni di sostegno alle organizzazioni di volontariato (art. 15, l. 11 agosto 1991, n. 266) relativamente ai propri dipendenti.
Preliminarmente, si rileva che la richiesta dell'interessato volta ad ottenere la comunicazione in forma intellegibile, da parte del Centro Servizi al Volontariato dei Due Mari, dei dati personali a sé riferiti, ivi compresi quelli relativi *"a ferie, permessi orari retribuiti, banca delle ore da recuperare"*, tenuto conto della sua peculiarità, deve essere proposta con ricorso (art. 141, comma 1, lett. c) del Codice).
Inoltre, deve essere sin d'ora dichiarata inammissibile la richiesta di risarcimento dei danni formulata dal reclamante, non avendo questa Autorità alcuna competenza al riguardo e fermo restando, comunque, che la medesima richiesta potrà essere eventualmente avanzata, se del caso, dinanzi all'autorità giudiziaria.
Nel merito della vicenda, occorre evidenziare quanto segue.
3.2. Le risultanze istruttorie hanno evidenziato che il reclamante è stato previamente informato in ordine al trattamento dei propri dati personali relativi alle attività di gestione del rapporto di lavoro (tra cui sono ragionevolmente annoverabili le operazioni svolte anche per il tramite dei soggetti indicati nella missiva oggetto di contestazione, in quanto afferenti alla *"ricostruzione"* del complessivo quadro quantitativo di ferie, permessi, ecc., spettanti all'interessato); tale circostanza risulta comprovata dalla documentazione prodotta dal centro servizi, attestante l'informativa resa all'istante e la relativa controfirma *"per ricevuta"*.
Vale inoltre rilevare, sul piano generale, che il trattamento dei dati personali, come evidenziato dallo stesso centro servizi, può essere lecitamente svolto dal titolare del trattamento in difetto del consenso dell'interessato qualora il medesimo trattamento sia necessario, come nel caso di specie, per dare esecuzione ad obblighi derivanti da un contratto del quale è parte lo stesso interessato (art. 24, comma 1, lett. b) del Codice).
Alla luce di tali considerazioni –e in ragione del fatto che, dalla documentazione complessivamente prodotta, non emergono, allo stato, elementi idonei a suffragare le dichiarazioni rese dal reclamante–, deve dunque ritenersi non provata, limitatamente ai profili sopra menzionati, la violazione delle disposizioni in materia di protezione dei dati personali lamentate dall'istante.
3.3. Per quanto concerne la liceità del trattamento svolto dal centro servizi per il tramite dei soggetti operanti sui dati personali dei dipendenti, merita rilevare che questa Autorità ha già provveduto, in termini generali, a fornire puntuali indicazioni in ordine al corretto trattamento dei dati personali dei lavoratori nell'ambito delle attività di gestione del rapporto di lavoro privato (*cfr. 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"* del 23 novembre 2006, in particolare il punto 8.2), evidenziando la necessità, per il datore di lavoro, di *"preporre alla custodia dei dati personali dei lavoratori apposito personale, specificamente incaricato del trattamento"* (oltre che adeguatamente formato sotto il profilo della disciplina di protezione dei dati), al fine anche di minimizzare i rischi di accesso non autorizzato ai dati personali dei dipendenti; tali indicazioni costituiscono attuazione dei principi più generali sanciti dal Codice in tema di misure di sicurezza (cfr. artt. 31 e ss. del Codice, nonché allegato "B" allo stesso Codice).
Tanto premesso, nel caso in questione si deve rilevare che lo stesso centro servizi ha ammesso di non aver provveduto a designare formalmente i predetti soggetti quali "incaricati" del trattamento; tale omissione, oltre a comportare la violazione dell'art. 30 del Codice (secondo cui

"le operazioni di trattamento possono essere effettuate solo da incaricati [ritualmente designati per iscritto] che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite"), ha determinato anche la disapplicazione delle misure di sicurezza che il disciplinare tecnico di cui all'allegato "B" del Codice riconduce alle attività degli incaricati del trattamento, con conseguente violazione degli artt. 33, 35 e 162, comma 2-bis del Codice.
Alla luce di tutto quanto sopra evidenziato, si ritiene di dover prescrivere al Centro Servizi al Volontariato dei Due Mari, ai sensi degli artt. 143, comma 1, lett. b) e 154, comma 1, lett. c) del Codice, di designare quali incaricati del trattamento i soggetti aventi effettivamente titolo a trattare i dati personali dei dipendenti per finalità di gestione del rapporto di lavoro, impartendo loro le relative istruzioni e individuando puntualmente l'ambito di trattamento loro consentito (art. 30 del Codice).
3.4. Per altro verso, deve rilevarsi che le modalità di comunicazione adottate dal centro servizi in occasione della trasmissione della missiva datata 29 ottobre 2009, in quanto effettivamente idonee a rendere i relativi destinatari reciprocamente edotti delle informazioni ivi contenute (concernenti, come detto, il quantitativo di ferie e di ore di permesso da fruire o recuperare), non risultano rispettose delle menzionate Linee guida (*cfr*., in particolare, il punto 5.5., secondo cui il datore di lavoro, in linea di principio, *"deve utilizzare forme di comunicazione individualizzata con il lavoratore, adottando le misure più opportune per prevenire un'indebita comunicazione di dati personali, in particolare se sensibili, a soggetti diversi dal destinatario"*), sicché il correlato trattamento di dati personali relativi anche all'istante non risulta essere avvenuto in conformità alla disciplina in materia di protezione dei dati personali, avuto particolare riguardo ai principi di necessità e di non eccedenza (artt. 3 e 11, comma 1, lett. d), del Codice). Né risulta inficiare tale conclusione la circostanza, pur sostenuta dal centro servizi, che la sottoscrizione dell'informativa resa a suo tempo all'istante avrebbe giustificato tale trattamento, atteso che la stessa non annovera tra i possibili destinatari dei dati i colleghi di ciascun dipendente.
In ragione di tali considerazioni, si ritiene di dover prescrivere al Centro Servizi al Volontariato dei Due Mari, ai sensi degli artt. 143, comma 1, lett. b), e 154, comma 1, lett. c) del Codice, di adottare idonee modalità di comunicazione con i dipendenti, atte a prevenire la conoscenza indebita da parte di terzi di dati personali a loro riferiti.
3.5. Da ultimo, benché non risulti accertata l'avvenuta acquisizione, da parte di terzi, di dati personali dei dipendenti in occasione degli episodi di "abbandono" di documenti segnalati dal reclamante, si ritiene opportuno prescrivere al Centro Servizi al Volontariato dei Due Mari –che ha comunque manifestato ampia disponibilità ad implementare le misure di sicurezza già attuate– di adottare idonee misure organizzative e di sicurezza volte a minimizzare i rischi di accesso indebito ai dati dei lavoratori, garantendo in pari tempo la scrupolosa vigilanza sull'operato degli incaricati e sensibilizzando questi ultimi al rispetto delle istruzioni ricevute, anche in occasione di eventuali iniziative formative e di aggiornamento del personale.
4. Il presente provvedimento lascia impregiudicati eventuali ulteriori profili di responsabilità in capo al centro servizi.

TUTTO CIÒ PREMESSO, IL GARANTE

ai sensi degli artt. 143, comma 1, lett. b) e 154, comma 1, lett. c) del Codice, prescrive al Centro Servizi al Volontariato dei Due Mari di:

a. designare quali incaricati del trattamento i soggetti aventi effettivamente titolo a trattare i dati personali dei dipendenti per finalità di gestione del rapporto di lavoro, impartendo loro le relative istruzioni e individuando puntualmente l'ambito di trattamento loro consentito (art. 30 del Codice);

b. adottare idonee modalità di comunicazione con i dipendenti, atte a prevenire la conoscenza indebita da parte di terzi di dati personali a loro riferiti;

c. adottare idonee misure organizzative e di sicurezza volte a minimizzare i rischi di accesso indebito ai dati dei lavoratori, garantendo in pari tempo la scrupolosa vigilanza sull'operato degli incaricati e sensibilizzando questi ultimi al rispetto delle istruzioni ricevute, anche in occasione di eventuali iniziative formative e di aggiornamento del personale.
Roma, 2 marzo 2011
Torna al sommario

Decreto Sviluppo, Decreto Salva-Italia e modifiche al Codice Privacy: Roma, 23.01.2012 **avv. Paolo Ricchiuto**

Non c'è dubbio: l'intervento sul Codice Privacy operato nel dicembre u.s. dal Governo Monti mediante il decreto Salva-Italia ha una portata eccezionale.
Prima di lanciarsi in proclami sulla completa liberazione dagli oneri burocratici (operazione nella quale si sono improvvidamente lanciati nell'immediato diversi organi di stampa), è necessario però comprendere la natura delle novità ed il loro effettivo ambito applicativo: ne emergerà che, quantomeno ai fini della gestione dei rapporti di lavoro, i cambiamenti più rilevanti sono in realtà quelli che erano stati messi in campo in precedenza, mediante il cd. decreto Sviluppo, passati inspiegabilmente quasi sotto silenzio.
Proviamo allora a mettere un po' di ordine, concentrando l'attenzione sui temi di interesse per l'HR:
§ - Decreto Sviluppo:
con il d.l. 70/11 (convertito in L.106/11) il precedente Governo aveva operato alcune modifiche molto importanti per la semplificazione degli adempimenti relativi al rapporto con il personale.
In particolare:
- nella norma relativa alla informativa (art. 13) era stato inserito il comma 5 bis, in base al quale "*l'informativa non è dovuta in caso di ricezione di curricula spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Al momento del primo contatto successivo all'invio del curriculum, il titolare è tenuto a fornire all'interessato, anche oralmente, una informativa breve contenente almeno gli elementi di cui al comma 1, lettere a), d) ed f*"

A compendio di tale principio, era stata inserita una nuova disposizione nelle norme relative al consenso per il trattamento di dati comuni (art. 24) e sensibili (art. 26), di tal che tra i cd. casi di esclusione, sono ora contemplati (rispettivamente, all'art. 24 comma 1 i-bis ed all'art. 26 comma 3 b-bis) i trattamenti posti in essere dal titolare del trattamento/datore di lavoro con riguardo ai "*dati contenuti nei curricula, nei casi di cui all'articolo 13, comma 5-bis*".
Il complesso di queste disposizioni, risolve quindi definitivamente l'annoso problema della gestione degli adempimenti privacy in relazione ai CV inviati dai candidati all'assunzione, ai quali oggi, sulla base di una norma (e non più in virtù di mere interpretazioni) non è più necessario dare né una informativa (se non al primo successivo contatto) e dai quali non è necessario acquisire un consenso;
- con riferimento al Documento Programmatico sulla sicurezza (vero e proprio incubo per i più, da gestire ed aggiornare ogni 31 marzo), le precedenti semplificazioni (introdotte con il d.l. 112/08 convertito in L. 133/08) avevano garantito la possibilità di sostituire la redazione del DPS con una mera autocertificazione per i titolari del trattamento/datori di lavoro che trattano come unici dati sensibili quelli costituiti "dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi" e quelli relativi alla "adesione ad organizzazioni sindacali o a carattere sindacale (art. 34 comma 1-bis). Opportunamente, il Decreto Sviluppo ha esteso tale area, modificando la lettera della norma come segue: "*titolari che trattano come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori, anche se extracomunitari, compresi quelli relativi al coniuge e ai parenti":* l'inserimento esplicito di un

riferimento ai dati giudiziari, e l'allargamento a tutti i dati sensibili (non solo quelli sanitari e sindacali) dei dipendenti e collaboratori di ogni genere e natura, delinea più chiaramente l'area dei soggetti che possono usufruire dell'autocertificazione;

- le stesse innovazioni del Legislatore del 2008 prevedevano poi un ulteriore regime speciale che abilitava a fruire di misure di sicurezza semplificate (poi identificate nel provvedimento reso dal Garante il 27.11.08 - http://www.garanteprivacy.it/garante/doc.jsp?ID=1571218)

per coloro che rientravano nella categoria di cui al punto precedente, ed in più per coloro che effettuano esclusivamente trattamenti "*per correnti finalità amministrative e contabili, in particolare preso piccole e medie imprese, liberi professionisti ed artigiani*." (art. 34 comma 1 bis)

La norma non chiariva, però, cosa potesse intendersi con la obliqua nozione di "finalità amministrative e contabili", lasciando una sinistra aura di incertezza tale, nei casi limite, da neutralizzare la efficacia innovativa della disposizione.

Il Decreto Sviluppo ha colmato questa crepa, prevedendo espressamente (nel nuovo art. 34 comma 1-ter) che "*ai fini dell'applicazione delle disposizioni in materia di protezione dei dati personali, i trattamenti effettuati per finalità amministrativo-contabili sono quelli connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro".*

L'ampiezza e la migliore identificazione dell'area di riferimento, allarga il novero dei soggetti coinvolti e soprattutto rende più certa la utilizzabilità delle misure semplificate;

- al di là di ulteriori residuali modifiche (che non possono essere commentate in questa sede), l'altro profilo centrale del Decreto Sviluppo afferiva all'ambito di applicazione di tutte le disposizioni contenute nel Codice Privacy: intervenendo direttamente sull'art. 5, ed inserendo il comma 3 bis, si era infatti stabilito che "*Il trattamento dei dati personali relativi a persone giuridiche, imprese, enti o associazioni effettuato nell'ambito di rapporti intercorrenti esclusivamente tra i medesimi soggetti per le finalità amministrativo - contabili, come definite all'articolo 34, comma 1-ter, non è soggetto all'applicazione del presente codice.*" La conseguenza era che ogni impresa, limitatamente ai soli dati relativi ad altre imprese trattati per le sole finalità connesse alla propria normale funzionalità, poteva considerarsi esentata da ogni onere derivante dall'applicazione del Codice. Attenzione però: questa disposizione, per come formulata, lasciava intatti tutti gli oneri, in relazione al trattamento dei dati relativi a persone fisiche, ivi compresi dipendenti e collaboratori. Di tal che, quand'anche si potesse fruire della esenzione per una certa area dell'attività connessa al rapporto con le altre realtà imprenditoriali, rimanevano fermi, per quanto qui interessa, tutti i vincoli relativi al rapporto con il personale.

§ - Decreto Salva-Italia

Il d.l. 201/11 (poi convertito con la legge 22 dicembre 2011 n. 214) si è posto, come è noto, l'obiettivo di salvare il Paese dalla altrimenti inevitabile deriva (da qui la sua scenografica denominazione). All'interno del decreto, nel capo III intitolato "*misure per lo sviluppo industriale*" è contenuta la norma dell'art. 40, rubricata "*riduzione degli adempimenti amministrativi per le imprese*". Il comma 2 si apre quindi con la seguente petizione di principio: " *per la riduzione degli oneri in materia di privacy sono apportate le seguenti modifiche*".

Il contesto nel quale si collocano le innovazioni è quindi molto chiaro: secondo il Legislatore, tra le varie iniziative necessarie a "salvare l'Italia" ed a garantire lo "sviluppo industriale" , vi è la "riduzione degli oneri" imposti dal Codice Privacy.

E' in questa prospettiva che vanno letti, allora, gli apparentemente minimali, ma per certi aspetti rivoluzionari, interventi operati. Eccoli: andando ancora più a monte di quanto non aveva fatto il

Decreto Sviluppo (la cui giovanissima disposizione inserita all'art. 5 comma 3 viene infatti abrogata), il Decreto Salva Italia modifica la nozione stessa di "dato personale" (art. 4 comma 1 lett. b) e quella di "interessato" (art. 4 comma 1 lett. i), eliminando ogni riferimento a "persona giuridica, ente o associazione". Si realizza dunque un ritorno ancora più netto ai concetti di base contenuti nella Direttiva 95/46/CE che era tutta tarata esclusivamente sui trattamenti di dati inerenti le persone fisiche, e che solo in sede di recepimento nel nostro Paese (prima con la L. 675/96, poi con il Codice Privacy) aveva visto estendersi l'area applicativa anche alle persone giuridiche.

Ne deriva che, oggi, chiunque (impresa o meno) tratti dati che si riferiscono a soggetti che non siano persone fisiche, può considerarsi esentato, relativamente a quei trattamenti, da qualsiasi adempimento privacy.

Esiste quindi una larghissima (quasi sconfinata) fetta di adempimenti che di fatto tramonta, liberando le imprese da oneri certamente pesanti in termini organizzativi ed economici.

Tutto ciò significa che la privacy in azienda può considerarsi morta e defunta?

Assolutamente no: essendo i dipendenti e collaboratori persone fisiche (ed essendosi riprodotto, seppure per una diversa via, il doppio binario già delineato dal Decreto Sviluppo) non esiste il minimo dubbio sul fatto che tutto l'impianto degli adempimenti (informativa, consenso, diritti di accesso, misure di sicurezza, DPS etc.etc.) non sia nemmeno sfiorato dalle ultime innovazioni semplificatrici, e resti, relativamente al trattamento di questa tipologia di dati, perfettamente integro.

*

Questo è, sinteticamente, il quadro. Rivoluzionario, sì; per certi aspetti, magari anche "salvifico", ma in ogni caso ancora incombente per chi opera nella gestione delle risorse umane.

Resta da verificare se ulteriori novità rilevanti per il nostro settore saranno contenute nell'annunciata nuova lenzuolata di semplificazioni contenute nel decreto legge di prossima emanazione (che conterrebbe, secondo alcune anticipazioni tutte da verificare, addirittura la eliminazione per tutti dell'obbligo di redigere il DPS).

12.02.2012 ULTIMA ORA

Con il decreto legge sulle semplificazioni (d.l. 09.02.12 n. 5 pubblicato in pari data sulla G.U.)), il Governo Monti supera sé stesso e, dando concretezza alle voci di corridoio che erano circolate, elimina tout court dal panorama degli adempimenti privacy la redazione e l'aggiornamento annuale del Documento Programmatico sulla sicurezza.

Molto eloquente (e per certi versi irritante, se si guarda a quanto accaduto finora) il comunicato stampa reperibile sul sito del Governo,dove si legge: " eliminato l'obbligo di predisporre e aggiornare il documento programmatico sulla sicurezza (DPS) che, oltre a non essere previsto tra le misure di sicurezza richieste dalla Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, rappresenta un adempimento meramente superfluo".

(http://www.governo.it/Governo/ConsiglioMinistri/dettaglio.asp?d=66448&pg=1%2C2173%2C4209%2C6511%2C8757%2C10950%2C12987%2C15310%2C17599%2C19895%2C21901%2C24277%2C26284%2C27392&pg_c=6).

Pur rimanendo ferme tutte le misure minime di sicurezza previste dal Codice Privacy, aziende e professionisti sono liberati quindi dall'obbligo che il Governo dei tecnici ritiene "superfluo" (e l'abrogazione dell'art. 34 comma 1-bis del Codice, consente di evitare ogni approfondimento sui soggetti che erano abilitati all'autocertificazione, anch'essa ovviamente superata dall'integrale eliminazione dell'adempimento).

Attenzione:come detto, restano obbligatorie tutte le altre misure di sicurezza previste dal Codice Privacy: ci sarà quindi da valutare, caso per caso, se sia realmente opportuno gettare nel cestino il DPS, ovvero se (come per le realtà più rilevanti sembra decisamente consigliabile) utilizzare quella traccia per dare evidenza dell'avvenuta adozione di tutte le misure ancora in vigore.

Semplificazioni in materia di dati personali

Art. 45

1. Al decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) all'articolo 21 dopo il comma 1 e' inserito il seguente:

«1-bis. Il trattamento dei dati giudiziari e' altresi' consentito quando e' effettuato in attuazione di protocolli d'intesa per la prevenzione e il contrasto dei fenomeni di criminalita' organizzata stipulati con il Ministero dell'interno o con i suoi uffici periferici di cui all'articolo 15, comma 2, del decreto legislativo 30 luglio 1999, n. 300, che specificano la tipologia dei dati trattati e delle operazioni eseguibili.»;

b) all'articolo 27, comma 1, e' aggiunto, in fine, il seguente periodo: "Si applica quanto previsto dall'articolo 21, comma 1-bis.";

c) all'articolo 34 e' soppressa la lettera g) del comma 1 ed e' abrogato il comma 1-bis;

d) nel disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B sono soppressi i paragrafi da 19 a 19.8 e 26.

Torna al sommario

Videosorveglianza: è sufficiente il consenso di tutti i dipendenti **avv. Paolo Ricchiuto:** *Coordinatore scientifico Sezione Protezione dei Dati Personali*

La Cassazione penale torna sul tema della videosorveglianza, con una pronuncia che, se compresa a fondo nelle sue linee argomentative, potrebbe assurgere a nuovo punto di riferimento in materia di controlli a distanza.

A dispetto del rigore esegetico consacrato nei noti provvedimenti del Garante per la protezione dei personali ed in alcune pronunce della sezione lavoro, i Supremi Giudici, nel dichiarare la insussistenza del reato connesso alla installazione di un sistema di videosorveglianza non accompagnato dall'accordo sindacale né dalla autorizzazione dell'Ispettorato del Lavoro, affermano un principio rivoluzionario.

Nella sentenza n. 22611/12, trova infatti spazio una lettura "sostanzialistica" dei principi affermati dall'art. 4 L. 300/70 che, scevra dall'imperante, spesso acefalo, formalismo, sembra cogliere il vero spirito della norma.

La fattispecie è quella di una installazione (peraltro con 2 delle 4 telecamere puntate direttamente su postazioni di lavoro) effettuata dal datore di lavoro sulla base del consenso espresso individualmente da tutti i lavoratori, e non corredata da accordo con le RSA (né da autorizzazione dell'Ispettorato).

Il Giudice di prima istanza, verificata la violazione formale dell'art. 4, e non annettendo alcun rilievo giuridico ai consensi individuali anche se prestati da tutti i dipendenti, aveva ritenuto perfezionato il reato.

La Cassazione, riformando integralmente detta pronuncia statuisce quanto segue:

"L'inquadramento del fatto in esame non può che avvenire prendendo come parametro di riferimento la fattispecie normativa. Sotto questo aspetto, deve ricordarsi, perciò, che l'art. 4 L. 300/70, nel secondo comma, precisa che impianti di controllo in ambito lavorativo possono essere installati soltanto «previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste con la commissione interna».

Ciò posto, non può essere ignorato il dato obiettivo - ed indiscusso - che, nel caso che occupa, era stato acquisito l'assenso di tutti i dipendenti attraverso la sottoscrizione da pare loro di un documento esplicito.

Orbene, se è vero che non si trattava né di autorizzazione della RSU né di quella di una "commissione interna", logica vuole che il più contenga il meno sì che non può essere negata validità ad un consenso chiaro ed espresso proveniente dalla totalità dei lavoratori e non soltanto da una loro rappresentanza. Del resto, non risultando esservi disposizioni di alcun tipo che disciplinino l'acquisizione del consenso, un diverso opinare, in un caso come quello in esame, avrebbe un taglio di un formalismo estremo tale da contrastare con la logica.

Ed infatti, l'interpretazione della norma deve sempre avvenire avendo presente la finalità che essa intende perseguire.

Se è vero - come è innegabile - che la disposizione di cui all'art. 4 intende tutelare i lavoratori contro -"forme subdole di controllo della loro attività da parte del datore di lavoro e che tale rischio viene escluso in presenza di un consenso di organismi di categoria rappresentativi (RSU o commisione interna), a fortiori, tale consenso deve essere considerato validamente prestato quando promani proprio da tutti i dipendenti.

Senza mezzi termini , quindi, la bocciatura della posizione formalistica: "*il giudice di merito* ha *dato della norma una interpretazione eccessivamente formale e meccanicistica limitandosi a*

constatare l'assenza del consenso delle RSU o di una commissione interna ed affermando, pertanto, l'equazione che ciò dava automaticamente luogo alla infrazione contestata. In tal modo, però, egli ha ignorato il dato obiettivo (peraltro di provenienza non sospetta, visto che sono stati gli stessi ispettori del lavoro a riportarlo) che l'odierna ricorrente aveva acquisito il consenso di tutti i dipendenti.
Cosi facendo, la decisione impugnata è censurabile per non avere interpretato correttamente la norma sotto il profilo oggettivo ed analoga censura può essere mossa anche sotto il profilo psichico una volta che si consideri che la piena consapevolezza dei lavoratori è risultata provata, non solo dal documento da loro sottoscritto, ma anche dal fatto che, come riferito dal teste A., «la B., aveva fatto comunque installare dei cartelli che segnalavano la presenza del sistema ai video sorveglianza".
L'accidentato percorso di risistemazione dell'art.4 e dei relativi risvolti a livello privacy si arricchisce quindi di un nuovo punto di prospettiva, che non potrà essere ignorato.
Nemmeno dal Garante.

Torna al sommario