[doc. web n. 1812154]

Vietato il trattamento di dati personali del dipendente ricavati da *file* e documenti acquisiti nell'ambito di operazioni di *backup* effettuate sul *server* aziendale - 7 aprile 2011

Registro dei provvedimenti
n. 139 del 7 aprile 2011

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

IN DATA ODIERNA, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Daniele De Paoli, segretario generale;

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

VISTO il provvedimento del 1° marzo 2007, recante le Linee guida per posta elettronica e internet, pubblicato in G.U. 10 marzo 2007, n. 58;

VISTO il reclamo del 6 febbraio 2010 formulato ai sensi degli artt. 142 e ss. del Codice da XY nei confronti di Hi. Tech S.p.A.;

ESAMINATA la documentazione in atti;

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

RELATORE il dott. Giuseppe Chiaravalloti;

PREMESSO

1. Il reclamo.
1.1. XY, dipendente di Hi. Tech S.p.A., in data 8 aprile 2009 ha ricevuto una lettera di contestazione disciplinare con la quale le veniva ascritto, tra l'altro, un indebito utilizzo degli strumenti aziendali volti all'espletamento delle funzioni lavorative. Secondo quanto riferito, tale uso si sarebbe concretizzato nell'impiego del computer –sin dalla data di assunzione dell'interessata e durante l'orario di lavoro– per finalità non riconducibili all'attività istituzionale della società e, più precisamente, per svolgere attività di consulenza a vantaggio di terzi. Di tale attività la società sarebbe venuta a conoscenza nell'ambito di un presunto "controllo" che alcuni esponenti aziendali avrebbero effettuato *"in modo assolutamente occulto e con modalità non dichiarate"* sul computer in uso all'interessata e sui file ivi contenuti, presenti in una cartella che la stessa reclamante aveva qualificato come "personale".
Considerato che tra i file oggetto dell'ipotizzato accesso figurerebbero anche *"prenotazioni alberghiere, foto dei […] bambini e di famiglia ed anche dati sensibili quali referti medici"*, l'istante ha chiesto all'Autorità di disporre il blocco o il divieto del trattamento dei dati personali illecitamente acquisiti dalla società (con contestuale declaratoria di inutilizzabilità degli stessi), prescrivendole, al contempo, di adottare misure opportune o necessarie per conformare le operazioni di trattamento alle disposizioni vigenti.

1.2. Secondo la reclamante, l'accesso al computer e ai file ivi contenuti –in precedenza già oggetto, secondo quanto riferitole da alcuni colleghi, di un altro tentativo di accesso da parte dei medesimi esponenti aziendali– non sarebbe avvenuto "accidentalmente" (come dichiarato dalla società in un pregresso scambio epistolare con l'interessata) nell'ambito di *"ordinarie operazioni di gestione del server"* aziendale (cfr. all. 6 al reclamo), bensì tramite un intervento "diretto" sullo strumento; inoltre, la reclamante ha sostenuto che, in considerazione della natura dichiaratamente "personale" della cartella denominata *"XY_personali"*, contenuta nel disco locale "C" (originariamente "condiviso" di *default*), la stessa avrebbe dovuto essere espunta dalle operazioni di *backup* effettuate periodicamente dalla società. Infine, la XY ha sostenuto che tale intervento sarebbe stato effettuato nonostante il fatto che la società, a dispetto del divieto formalmente imposto ai dipendenti circa un'utilizzazione a fini personali degli strumenti aziendali, avesse comunque sempre manifestato tolleranza nei confronti di tale uso.

A tale riguardo, la reclamante ha precisato che la società non avrebbe adottato alcuna specifica *policy* volta a disciplinare, in forma chiara e puntuale, l'utilizzo degli strumenti elettronici affidati in dotazione ai dipendenti, ma si sarebbe limitata a redigere un regolamento interno contenente alcune "norme di comportamento" da osservare ai fini del "corretto e regolare svolgimento dell'attività" lavorativa. L'omessa adozione di tale *policy*, a detta dell'istante, avrebbe determinato un trattamento illecito dei suoi dati, perché acquisiti, oltre che in violazione dell'art. 11, comma 1, lett. a) e b) del Codice, anche in difetto delle indicazioni impartite da questa Autorità con le Linee guida per posta elettronica e internet (Provv. 1° marzo 2007, doc. *web* n. 1387522) che, tra l'altro, prevedono l'onere, a carico dei titolari dei trattamenti, di disciplinare e rendere note agli interessati anche le modalità di eventuali controlli posti in essere per verificare l'utilizzo degli strumenti aziendali.

Tale trattamento, inoltre, sarebbe avvenuto in assenza di preventiva informativa all'interessata e in difetto del relativo consenso (anche scritto, in relazione ai propri dati sensibili), con conseguente violazione degli artt. 13, 23, 24 e 26 del Codice.

Infine, la reclamante ha lamentato che le credenziali di accesso al computer affidatole in dotazione, *"fino alla prima metà di febbraio 2009"*, non sarebbero state conformi alle prescrizioni di cui all'allegato "B" al Codice, con relativa violazione anche delle misure minime di sicurezza di cui agli artt. 31 e ss. dello stesso Codice.

1.3. A sostegno delle proprie deduzioni, la reclamante ha prodotto copia:

a) di una comunicazione inviata dalla società, nella quale si afferma che *"i files rinvenuti sul computer utilizzato dalla [reclamante] (trattasi di documenti di monitoraggio, proposte di rinnovo contrattuale, mansionari sulla privacy, documenti programmatici sulla sicurezza, fatture, ecc.) sono indubitabilmente da attribuirsi alla [stessa]"* (*cfr.* nota del 26 aprile 2009: all. 3 al reclamo);

b) del riscontro inviato all'interessata in relazione a un'istanza di accesso formulata ai sensi dell'art. 7 del Codice, dal quale risulta che tra i dati personali detenuti dalla società figurano *"numerose lettere e documenti estranei alla […] attività lavorativa [della società], ma […] elaborati [dall'istante] durante l'orario di lavoro […]. Tali documenti –comprovanti lo svolgimento da parte [della reclamante] di un'attività di consulenza […] nei confronti di clienti operanti in diversi settori merceologici del tutto estranei alla […] società– possono essere così riassunti: - proposte di rinnovo di contratto di consulenza […]; - documenti di monitoraggio personalizzati […]; - documenti programmatici di sicurezza personalizzati […]; - corrispondenza […] intrattenuta con i clienti […] ignoti [alla società]"* (*cfr.* nota del 28 dicembre 2009, all. 6 al reclamo). *"Per quanto attiene questi dati"*, prosegue tale ultima nota, *"essi sono stati rilevati nei server aziendali nell'ambito delle ordinarie operazioni di gestione del server"*;

c) del regolamento interno (datato 9 giugno 2008) relativo alle *"norme di comportamento"* da osservare ai fini del *"corretto e regolare svolgimento dell'attività"* lavorativa. Tale regolamento, per quanto concerne l'utilizzo degli strumenti aziendali, prevede il divieto di utilizzo *"per scopi e motivi personali di tutta l'attrezzatura e strumentazione aziendale, quale a titolo esemplificativo e non esaustivo: telefono, personal computer, collegamento a internet compreso qualsiasi utilizzo della posta elettronica"*.

2. Le osservazioni della società.
2.1. Con comunicazioni del 3 marzo 2010 e del 30 aprile 2010, la società ha fatto pervenire le proprie osservazioni, rappresentando preliminarmente che l'acquisizione dei documenti citati dalla reclamante sarebbe avvenuto "accidentalmente" –e non in forma occulta come sostenuto da quest'ultima– *"al momento di eliminare i backup [..] relativi al 2008"*; peraltro, la società si sarebbe limitata a trattare i soli dati contenuti in documenti relativi all'attività di consulenza svolta dall'interessata a vantaggio di terzi, senza accedere ad *"altri files inerenti documenti personali"* a lei riconducibili (*cfr.* nota del 3 marzo 2010).

In ogni caso, la società ha sostenuto che i dati acquisiti (non riguardanti *"argomenti di natura sensibile"*) potevano essere lecitamente trattati in difetto del consenso dell'interessata, perché volti a far valere o difendere un diritto in sede giudiziaria (art. 24, comma 1, lett. f), del Codice).Sotto distinto profilo, la società ha poi precisato che il computer affidato alla reclamante, come quelli in dotazione al restante personale, sarebbe stato privo *"di capacità di archiviazione autonoma"*, in quanto dotato di un *"sistema operativo scaricato da un apposito server e condiviso da tutti i pc […]"*; più precisamente, *"i pc destinati al personale non [sarebbero dotati] di un sistema operativo locale"* ma *"si connett[erebbero] direttamente ai server aziendali per tutte le funzioni di elaborazione e di registrazione dei dati"*, con la conseguenza che gli stessi conterrebbero *"solo una copia (cache) locale dei file [direttamente] residenti sul server"*. La società ha quindi ribadito che *"nessun accesso è mai stato effettuato sul computer in uso alla [reclamante]"* e che *"tutti i files in questione sono stati reperiti su backup archiviati sui server"*.

Inoltre, *"tutto il personale era [stato] informato, attraverso un regolamento aziendale, che era fatto assoluto divieto di usare gli strumenti di lavoro aziendale per uso personale"*; lo stesso personale era consapevole *"che i dati ven[iva]no registrati sul server e [che] pertanto, per motivi di lavoro, [potevano] essere acceduti anche da altri utenti"*; ciò anche alla luce del fatto che *"a norma di regolamento [gli stessi] non po[teva]no contenere per nessun motivo dati personali"* (*cfr.* nota inviata il 30 aprile 2010).

Diversamente da quanto asserito dalla reclamante, la società ha dichiarato di conservare "in busta chiusa sigillata" le credenziali di accesso al computer già in uso alla stessa, credenziali ritenute conformi *"alle prescrizioni minime di cui all'allegato B del Codice"* (*cfr.* nota inviata il 30 aprile 2010).

Con specifico riferimento alle procedure e alle operazioni di controllo effettuate sui computer in dotazione al personale, è stato poi affermato che *"vengono effettuati dei controlli saltuari previa comunicazione al personale tramite e-mail"* da parte di personale appositamente autorizzato (*"responsabile della sicurezza informatica, eventualmente mediante l'ausilio tecnico degli amministratori di sistema"*).

Infine, per quanto concerne le *"policy di rotazione dei backup in uso"*, la società ha dichiarato che *"ogni giorno viene effettuato backup notturno dei dati interni, che vengono archiviati a intervalli mensili e cancellati dopo i termini previsti dalla normativa vigente"*.

2.2. Tra i documenti prodotti dalla società a suffragio delle proprie dichiarazioni figurano alcuni allegati dai quali risulta, in particolare, che le password utilizzate da un incaricato negli anni 2006 e 2007 (con scadenza, rispettivamente, 31 dicembre 2006 e 30 giugno 2007) erano costituite da parole composte, rispettivamente, da n. 7 e n. 5 caratteri (all. 7 e 8).

Inoltre, è stata prodotta copia di un regolamento aziendale (datato 27 novembre 2009 ed efficace dal 1° dicembre 2009), distinto da quello consegnato a suo tempo anche alla reclamante, recante istruzioni sul corretto utilizzo degli strumenti

informatici affidati in dotazione ai dipendenti (all. 14).

Da ultimo, è stata acquisita una comunicazione intercorsa tra la società e un legale (datata 7 aprile 2009), dalla quale si evince che i file relativi alla reclamante sarebbero stati oggetto di reperimento *"nel backup di un […] server aziendale"* e che il correlato trattamento non presupporrebbe il consenso dell'interessata *"anche in considerazione del fatto che i dati rinvenuti non sono di natura sensibile"* (all. 11).

3. Ulteriori osservazioni della reclamante.
Con successiva nota del 22 giugno 2010, la reclamante, nel confermare la propria versione dei fatti, ha evidenziato alcune contraddizioni in cui sarebbe incorsa la controparte, sottolineando, tra l'altro, che:

a) gli interventi "per esigenze di manutenzione del sistema informatico aziendale" avrebbero dovuto essere effettuati "in modo tale da escludere l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati ai dipendenti", sicché la cartella "espressamente qualificata come personale" dall'istante "avrebbe dovuto essere esclusa dalle copie di backup";

b) a prescindere dalla liceità o meno del trattamento effettuato, la società avrebbe comunque dovuto rendere all'interessata "una preventiva ed esplicita informativa" in ordine alle tipologie e modalità del controllo effettuabile relativamente all'utilizzo degli strumenti informatici, invero mai rilasciata nemmeno al restante personale.

Alla luce di tali ulteriori considerazioni, la reclamante, nel richiamarsi alle conclusioni già formulate nel reclamo, ha chiesto l'accoglimento delle proprie richieste.

4. Profili di illiceità del trattamento.
4.1. Le risultanze istruttorie hanno preliminarmente confermato che la società ha effettivamente trattato dati personali riferiti all'istante desunti da file e documenti concernenti la sua presunta attività di consulenza svolta a vantaggio di terzi; ciò emerge sia dalle dichiarazioni rese dalla società (cfr. nota del 3 marzo 2010, p. 2, e nota inviata il 30 aprile 2010, p. 3) che dalla documentazione acquisita agli atti (cfr. all. 6 al reclamo).

Per contro, non risulta invece provato che tale trattamento abbia interessato anche dati sensibili riferiti all'interessata, stanti le dichiarazioni rese sul punto dalla società (ai sensi e per gli effetti di cui all'art. 168 del Codice, con conseguente assunzione di responsabilità anche penale) e il contenuto del materiale prodotto da quest'ultima (cfr. punti 2.1. e 2.2.).
Circoscritto così il campo di indagine al solo trattamento (dei dati comuni) correlato alla presunta attività di consulenza che la reclamante avrebbe effettuato a vantaggio di terzi, occorre esaminare le modalità con le quali sono stati concretamente acquisiti i dati personali a lei riferiti.

4.2. In proposito, vale anzitutto rilevare che, sulla base degli elementi prodotti, non risulta con certezza che la società abbia concretamente acquisito file e documenti riferiti all'interessata attraverso un intervento "diretto" sul computer affidatole in dotazione.

In primo luogo un accesso diretto non può ritenersi dimostrato dalla semplice affermazione, da parte della sola reclamante, dell'esistenza, in tal senso, di alcune "voci di corridoio" in ambito lavorativo.

Inoltre, la stessa Hi.Tech S.p.A. ha prodotto una nota datata 7 aprile 2009, inviatale per chiarimenti dal proprio legale, da cui risulta espressamente che l'accertamento sulle effettive modalità di utilizzazione del computer aziendale assegnato in uso alla reclamante era dipeso dall'avvenuto "reperimento dei files nel back up del […] server aziendale"; tale specifica circostanza non può ritenersi contraddetta dalla successiva nota del 26 aprile 2009, sottoscritta da altro legale ed inviata al difensore della reclamante, nella quale si fa soltanto un generico riferimento ai *"files rinvenuti sul computer utilizzato"* dalla XY.

Ciò nonostante, si deve rilevare che il trattamento operato dalla società in relazione ai dati personali dell'interessata non sia comunque lecito per le ragioni che seguono.

4.3. In primo luogo, sul piano sistematico, occorre evidenziare che questa Autorità, pur avendo rammentato più volte che il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro da parte dei dipendenti (artt. 2086, 2087 e 2104 cod. civ.) (*cfr.,* da ultimo, *Provv*. 10 giugno 2010, doc. *web* n. 1736780; *Provv*. 24 febbraio 2010, doc. *web* n. 1712856; *Provv*. 23 dicembre 2010, doc. *web* n. 1786116), ha comunque chiarito che, nell'esercizio di tale prerogativa, debbono essere salvaguardati la libertà e la dignità dei lavoratori, nonché i principi fissati dall'art. 11 del Codice sul trattamento dei dati personali, che impongono, tra l'altro, di rendere note ai lavoratori le caratteristiche essenziali dei trattamenti, soprattutto se effettuati per finalità di controllo (*cfr.* p. 5.2 e 6.1 delle citate *Linee guida*).

Nel caso di specie, dalle risultanze istruttorie è emerso che la società ha trattato dati personali riferiti alla reclamante acquisendoli in occasione di una verifica effettuata sui propri sistemi informativi; tale attività, però, risulta compiuta senza che fosse stata fornita ai dipendenti –e quindi neanche all'odierna reclamante- un'idonea e preventiva informativa sul punto (art. 13 del Codice), non potendo a tal fine ritenersi sufficienti le scarne indicazioni contenute nel regolamento del 9 giugno 2008, unico documento avente contenuto informativo posto a conoscenza dell'interessata (l'altro regolamento richiamato dalla società, infatti, risulta predisposto ed entrato in vigore in data successiva al licenziamento della predetta). Difatti, benché il regolamento del giugno 2008 rechi un riferimento all'obbligo di utilizzare gli strumenti elettronici affidati ai lavoratori per esclusive finalità professionali, esso non riporta alcuna indicazione circa la possibilità per la società di acquisire e conservare dati personali dei dipendenti anche per effetto di copie di backup (cfr. punto 3.2 delle Linee guida del 1° marzo 2007, *cit*.; *cfr*. altresì *Provv*. 2 febbraio 2006, doc. *web* n. 1229854), né sull'eventualità di trattare tali dati in vista di possibili

controlli (anche occasionali), le cui modalità di effettuazione, peraltro, non risultano neanche adombrate.

Ne consegue che il trattamento operato dalla società, alla luce dei principi di correttezza e finalità posti dal Codice (art. 11, comma 1, lett. a) e b)) e richiamati nelle citate Linee guida, non può essere reputato conforme a legge.

Inoltre, il trattamento risulta essere anche eccedente rispetto alla finalità perseguita (art. 11, comma 1, lett. d) del Codice).

Infatti, fermo restando il diritto della società di verificare l'eventuale violazione, da parte della reclamante, degli obblighi cui la stessa era tenuta in qualità di prestatrice di lavoro (stante anche l'esplicito divieto contenuto nel regolamento del 9 giugno 2008 di utilizzare per motivi personali "tutta l'attrezzatura e strumentazione aziendale"), non può non rilevarsi che ai fini di tale accertamento, anziché prendere conoscenza degli specifici contenuti nella directory denominata "XY_personali" (circostanza, questa, non smentita dalla società), sarebbe stato sufficiente constatare l'esistenza della "cartella" stessa, la quale, già in ragione della sua denominazione, lasciava intuire la presenza di informazioni di carattere privato (cfr., in proposito, anche *Provv*. 10 giugno 2010, doc. *web* n. 1736780 e *Provv*. 18 maggio 2006, doc. *web* n. 1299082).

Tutto ciò premesso, stante l'acclarata violazione dei princìpi di correttezza, finalità e proporzionalità del trattamento (art. 11, comma 1, lett. a), b) e d) del Codice), si ritiene di dover disporre nei confronti di Hi. Tech S.p.A. il divieto dell'ulteriore trattamento dei dati personali riferiti all'interessata e ritratti dai file e documenti acquisiti in occasione delle operazioni di backup effettuate sul server aziendale.

4.4. Per quanto concerne, invece, la tipologia di *password* di accesso al computer utilizzate in epoca meno recente per accedere al sistema informatico della società (quantomeno fino al primo semestre del 2007), esse non risultano conformi alle disposizioni contenute nell'allegato "B" al Codice; tale circostanza emerge dallo stesso materiale prodotto dalla società, ove si fa riferimento all'impiego di parole chiave inferiori agli otto caratteri e, comunque, non pari al numero massimo di caratteri consentito dallo strumento (reg. 5 del menzionato allegato "B").

Al contrario, non risulta provato che la società utilizzi ancora attualmente parole chiave inferiori agli otto caratteri; ciò si desume non solo dal regolamento adottato dalla società il 27 novembre 2009 (ove si afferma che la parola chiave utilizzata "deve essere composta da almeno otto caratteri") ma, a contrariis, dalle stesse affermazioni della reclamante che, avendo sostenuto la non conformità delle credenziali di accesso "fino alla prima metà di febbraio 2009", ha lasciato intendere che successivamente sia intervenuta una "regolarizzazione" delle stesse.

Ne consegue che, allo stato, rispetto a tale profilo, non sussistono i presupposti per adottare specifiche prescrizioni nei confronti della società.

4.5. Da ultimo, va rilevato che la società, nell'adottare successivamente al licenziamento della reclamante una più dettagliata policy aziendale sul corretto utilizzo degli strumenti affidati in dotazione ai dipendenti (cfr. regolamento del 27 novembre 2009, all. 14 alla nota inviata il 30 aprile 2010), ha individuato termini e modalità di accesso agli strumenti aziendali non sempre conformi alle indicazioni suggerite da questa Autorità con le richiamate Linee guida del 1° marzo 2007.

In particolare, da un esame di detto regolamento emerge che per ragioni di sicurezza e di salvaguardia del sistema, oltre che per motivi tecnici e manutentivi, il personale "sistemistico" potrà avere accesso *"in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché effettuare verifiche "sui siti internet acceduti dagli utenti […]"*; inoltre, *"tutti i dati contenuti"* nelle caselle di posta elettronica aziendale potranno *"essere acceduti da personale della […] azienda per motivi inerenti all'organizzazione del lavoro"*, ivi compresi il *"superiore gerarchico dell'utente"* o altra *"persona individuata dall'azienda"* per *"ogni ipotesi in cui [ciò] si renda necessario"*, mentre gli eventuali controlli relativi alla navigazione *web* da parte dei dipendenti *"potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta"*.

In ragione di tali disposizioni, riservati comunque eventuali approfondimenti in relazione ai trattamenti di dati personali dei dipendenti ad esse correlati, ai sensi degli artt. 143, comma 1, lett. b) e 154, comma 1, lett. c) del Codice, si ritiene di dover prescrivere a Hi. Tech S.p.A. di conformare il contenuto del regolamento adottato il 27 novembre 2009 per disciplinare le modalità di utilizzo degli strumenti elettronici aziendali alle istruzioni fornite da questa Autorità con le già citate *Linee guida per posta elettronica e internet* del 1° marzo 2007 e con il provvedimento del 27 novembre 2008, recante *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"* (doc. web n. 1577499).

TUTTO CIÒ PREMESSO, IL GARANTE

accertata l'illiceità del trattamento svolto:

a) ai sensi degli artt. 143, comma 1, lett. c) e 154, comma 1, lett. d) del Codice, dispone nei confronti di Hi. Tech S.p.A., perché in contrasto con i princìpi di correttezza e finalità (artt. 11, comma 1, lett. a), e 13 del Codice) e proporzionalità (art. 11, comma 1, lett. d) del Codice), il divieto dell'ulteriore trattamento dei dati personali riferiti all'interessata e ritratti dai *file* e documenti acquisiti nell'ambito delle operazioni di *backup* effettuate sul *server* aziendale;

b) ai sensi dell'art. 143, comma 1, lett. b) e 154, comma 1, lett. c) del Codice, prescrive a Hi. Tech S.p.A. di conformare il contenuto del regolamento adottato il 27 novembre 2009 per disciplinare le modalità di utilizzo degli strumenti elettronici aziendali alle istruzioni fornite da questa Autorità con le Linee guida del 1° marzo 2007 (posta elettronica e internet) e con il

provvedimento del 27 novembre 2008 (amministratori di sistema).

Roma, 7 aprile 2011

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

Il SEGRETARIO GENERALE
De Paoli