diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

La lettura della casella di posta elettronica da parte del datore di lavoro: Tra pronunce giurisprudenziali e attività regolamentare del garante per la protezione dei dati personali.

Autore: Redazione
In: Diritto civile e commerciale, Diritto del lavoro

Sommario: Introduzione; 1. Le pronunce giurisprudenziali 2. L'attività regolamentare del Garante per la protezione dei dati personali; 3. Linee guida per la redazione del Regolamento aziendale inerente le modalita' di utilizzo della posta elettronica e di internet da parte dei dipendenti della azienda

L'Autore, funzionario AUSL, è Docente Incaricato di: Diritto Privato al Corso di Laurea Specialistica in Scienze Infermieristiche ed **********, e di: Elementi di Diritto Pubblico al Corso di Laurea in Tecnico di Laboratorio Biomedico; presso la Università "G.D'Annunzio" – Facoltà di Medicina e Chirurgia di Chieti-Pescara; a.a. 2006/2007.

Introduzione

L'impiego della posta elettronica[1] costituisce la applicazione più utilizzata in Internet dopo il browser web.

L'utilizzo[2] della posta elettronica all'interno degli uffici, sia pubblici che privati, rappresenta sempre più una necessità al fine di migliorare il rendimento ed agevolare il lavoro del dipendente.

In ambito pubblico, sotto la spinta impressa dal Governo[3] e dal Centro nazionale per l'Informatica nella

Pubblica Amministrazione - CNIPA[4] per facilitare l'impiego della posta elettronica, per tutte le comunicazioni interne alla pubblica amministrazione, in una ottica di cambiamento culturale ed organizzativo della stessa P.A., si è registrato nell'ultimo quinquennio un notevole incremento nell'utilizzo di tali procedure informatiche.

La massiva introduzione di strumenti informatici, alcuni dei quali legati al settore delle tele comunicazioni, costituisce ormai un dato di fatto che però fa sorgere una serie di problematiche di natura legale e/o disciplinare riguardanti il loro corretto utilizzo.

L'impiego della posta elettronica anche per fini extra lavorativi, pur rappresentando quasi una regola non trova giustificazione in nessun disposto normativo, ha fatto sorgere in molti l'erroneo convincimento che rientri nell'ambito delle possibilità attribuite lecitamente al dipendente.

Tale erroneo convincimento ha indotto molti lavoratori a reiterare tale condotta (ci si riferisce all'utilizzo di Internet per inviare la posta elettronica, per partecipare a forum, per chattare, per 'navigare', ecc) senza sapere di violare una norma.

La problematica[5] in oggetto investe molteplici aspetti che vanno dal diritto del datore di lavoro a disporre l'utilizzo di strumentazione informatica da parte dei dipendenti al diritto alla privacy[6] del singolo lavoratore, dal divieto del datore di lavoro a svolgere un controllo a distanza dei lavoratori al dovere del lavoratore di rispettare quanto disciplinato dalle leggi e dalla normativa contrattuale durante lo svolgimento dell'attività lavorativa, fino alla sicurezza nel trattamento dei dati personali.

1. Le pronunce giurisprudenziali

La giurisprudenza, a decorrere dal 2000, ha cominciato ad essere investita da tali problematiche ed ha prodotto una serie di sentenze non sempre tra loro in sintonia. Ci limitiamo, quindi, a illustrare le principali al fine di cercare di individuare un 'filo rosso' che ci consenta di esplicitare i principi giuridici comunemente accolti e riconosciuti.

Diritto & Diritti ISSN 1127-8579

La Corte di Cassazione, con sentenza n. 4746 del 3 aprile 2002[7], ha stabilito la legittimità del controllo delle telefonate effettuate dal dipendente con il telefono aziendale stabilendo che non sia ascrivibile alla fattispecie di cui all'art. 4 della legge 300 (Statuto dei Lavoratori) una condotta disposta dal datore di lavoro finalizzata non ad invadere l'attività lavorativa quanto a tutelare l'Azienda ed il suo patrimonio.

Appare, quindi, possibile estendere tale principio fino a ricomprendervi il controllo della posta elettronica.

Una successiva pronuncia della Suprema Corte,sez. VI, **sentenza n. 30751 del 13 settembre 2002, ha ribadito che l'utilizzo del telefono – ma analogo ragionamento riteniamo possa farsi per la posta elettronica –sul luogo di lavoro integra gli estremi del reato di peculato a meno che tale utilizzo assuma i caratteri della sporadicità o della eccezionalità[8].**

Un impiego reiterato, per fini personali, dell'apparecchiatura, da parte del pubblico ufficiale e dell'incaricato di pubblico servizio provoca un utilizzo indebito delle energie "entrate a fare parte nella sfera di disponibilità della pubblica amministrazione occorrenti per le conversazioni telefoniche."

Il Tribunale di Milano, con ordinanza del 10 maggio 2002, chiamato a pronunciarsi in merito all'accesso della mail box di un dipendente da parte del proprio datore di lavoro, ha stabilito che quest'ultimo non commette reato qualora l'accesso avvenga in assenza del lavoratore, che nella fattispecie era in ferie.

Era accaduto che, in assenza della lavoratrice, il datore di lavoro avesse dato disposizioni di leggere il contenuto della casella di posta elettronica e che a seguito di tale condotta avesse licenziato la dipendente, per violazione dei doveri inerenti al rapporto economico, rea di un utilizzo improprio della strumentazione informatica a lei assegnata per l'espletamento delle proprie mansioni, id est una casella di posta elettronica.

La dipendente, a fronte del proprio licenziamento, aveva lamentato che lo stesso era scaturito – appunto – a seguito della lettura della corrispondenza attraverso la posta elettronica e, quindi, in palese violazione dell'art. 616 del codice penale. Per questi motivi, aveva sporto querela sostenendo che la corrispondenza contenuta nella mail box aziendale è assimilabile alla corrispondenza tradizionale, id est epistolare, telegrafica, telefonica, ecc. e, pertanto, la segretezza della stessa sarebbe garantita dalla Costituzione.

Diritto & Diritti ISSN 1127-8579

L'azienda, da parte sua, aveva giustificato la propria condotta con la necessità di dovere prendere cognizione di eventuali comunicazioni pervenute, durante il periodo di congedo ordinario per ferie della dipendente; atteso che la mancata conoscenza delle stesse avrebbe arrecato danni economici in capo alla azienda.

Il Pubblico Ministero[9] aveva accolto le argomentazioni della azienda, chiedendo l'archiviazione del procedimento, ritenendo che la casella di posta elettronica sia uno strumento di lavoro di proprietà dell'azienda – alla stregua del telefono cellulare, del computer da tavolo, della autovettura aziendale – di cui i dipendenti hanno solo l'uso.

Il Pubblico Ministero ha colto l'occasione per sollecitare la codificazione dei comportamenti inerenti l'utilizzo delle nuove tecnologie atteso che le stesse sono di sovente regolamentate solo successivamente al loro impiego, dando così la stura a comportamenti non sempre appropriati e coerenti dal punto di vista giuridico[10].

Egli, inoltre, pur riconoscendo come 'personale' l'indirizzo di posta elettronica affidato al lavoratore per lo svolgimento delle proprie mansioni ritiene che 'personalità' dell'indirizzo non sia sinonimo di 'privatezza[11]', in ragione della considerazione che l'indirizzo aziendale è di per sé soggetto all'accesso e alla lettura del personale dell'azienda, previamente, autorizzato.

In merito alla presunta assimilazione del concetto di posta elettronica con quello di posta tradizionale[12] è stato affermato che l'utilizzo illecito di uno strumento di lavoro, quale la mail box aziendale, "non può fare attribuire a chi, questo illecito commette, diritti di sorta".

Il Giudice per le Indagini Preliminari ha stabilito, quindi, non potersi ricondurre, la fattispecie in esame, alla disciplina dell'art. 616 c.p[13]. in quanto l'assegnazione di una casella di posta elettronica al dipendente non comporta da parte di questi l'acquisizione di un diritto di proprietà[14].

La **Corte dei Conti – sezione giurisdizionale Piemonte sentenza n. 1856/2003** chiamata a decidere della condotta trasgressiva posta in essere da un dipendente di un ente comunale, su istanza del Comune datore di lavoro, si è pronunciata in merito al divieto da parte del datore di lavoro di utilizzare impianti audiovisivi per effettuare un controllo a distanza dei lavoratori.

Prima di esporre la decisione assunta, l'organo giudicante ha rimarcato che la materia è disciplinata, in prima battuta, dalla Legge 300/1970 (Statuto dei lavoratori) che all'art. 4 stabilisce "E' vietato l'uso di

Diritto & Diritti ISSN 1127-8579

impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. Gli impianti e le apparecchiature di controllo che siano 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, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna".

La Corte di ***** ha ritenuto infondata la censura avanzata dalla ricorrente in quanto l'operato del Comune – svoltosi per mezzo di software in grado di registrare gli accessi degli utenti collegati in rete - non sembra essere stato invasivo anche perché tali strumenti, rectius software, sono stati impiegati ex post[15].

L'impiego di tali programmi informatici è stato finalizzato, pertanto, non solo per lo svolgimento di una condotta repressiva "di comportamenti illeciti, ma anche per esigenze statistiche e di controllo di spesa".

Il **Tribunale di Perugia con ordinanza 19/5 - 24/5 del 2006** chiamato a giudicare del provvedimento adottato dal Giudice monocratico, con ordinanza del 20.2.06, in merito al licenziamento di un dipendente che aveva fatto ricorso all'utilizzo del personal computer messogli a disposizione della azienda, ha ribadito – in linea con la decisione assunta dal Giudice monocratico – che l'utilizzo, di per sé scorretto del pc aziendale per fini privati, non giustificava il licenziamento in tronco del dipendente.

Nella fattispecie il Tribunale di Perugia ha respinto il ricorso argomentando che "poiché infatti la condotta addebitata allo xx è solamente quella dell'uso (sia pure smodato) del PC per finalità personali, occorre evidenziare che una simile condotta – pur sicuramente illecita – non integra nemmeno giustificato motivo di licenziamento, dal momento che (art. 50 CCNL) 'l'uso di strumenti aziendali per un lavoro (ipotesi senz'altro estensibile all'uso attuato per svago) estraneo all'attività dell'azienda' costituisce illecito disciplinare che legittima unicamente la sospensione dal lavoro e dalla retribuzione".

Il **Tribunale di Torino Sezione distaccata di Chivasso, Sentenza 20 giugno 2006. n. 143** ha stabilito che la e-mail aziendale appartiene al datore di lavoro e che l'accesso da parte di questi al suo contenuto non configura l'ipotesi di reato di cui all'art. 616 c.p., purchè sia preceduto da una specifica policy aziendale.

Nella fattispecie, si era verificato che un dipendente in qualità di **********, aveva preso cognizione della corrispondenza informatica contenuta nella casella di posta elettronica di altra dipendente e diretta ad altro dirigente della società.

Tale ispezione aveva portato al licenziamento della dipendente, per violazione dei doveri inerenti al rapporto di lavoro in quanto, a detta della società, la stessa aveva inviato messaggi di posta elettronica non autorizzati.

La pronuncia acquista una precipua importanza considerato che va a fare luce sulla materia oggetto del presente studio, vale a dire la "questione giuridica relativa ai limiti di tutela della corrispondenza elettronica aziendale e quindi della sostanziale riconducibilità o meno, nella fattispecie, dell'indirizzo di posta elettronica al datore di lavoro benchè personalmente riferito ad un suo dipendente".

Il giudice nel decidere ha preso atto della esistenza di una esplicita policy aziendale[16] relativa all'utilizzo in sicurezza del sistema di information communication technology (******) la quale diffidava dall'utilizzo improprio della dotazione tecnologica aziendale ed appariva essere in sintonia con la disciplina giuridica in materia di trattamento dei dati personali.

Proprio la esplicitazione di un protocollo[17] aziendale in materia di utilizzo della dotazione informatica – pienamente in sintonia con quanto stabilito dal Garante per la protezione dei dati personali - ha consentito al giudice di affermare che la doglianza del lavoratore in merito alla condotta della società, ritenuta invasiva, non ha ragione di apparire.

Viene, inoltre, fatto riferimento all'Allegato B al Codice in materia di protezione dei dati personali per evidenziare come il legislatore abbia disciplinato l'ipotesi in cui il datore di lavoro acceda alle banche dati personali in assenza del lavoratore incaricato[18] del loro trattamento[19], purchè si sia in presenza di "indispensabili ed indifferibili necessità di operatività e di sicurezza del sistema ed attraverso una procedura regolamentata e partecipata."

Così come non è condivisibile la equazione 'personalità dell'indirizzo' = 'privatezza dell'indirizzo' che è, comunque, di proprietà dell'azienda che lo conferisce al dipendente al fine di consentirgli di svolgere meglio il suo lavoro.

Di conseguenza, l'accesso alla posta elettronica aziendale del dipendente non può raffigurare la fattispecie di cui all'art. 616 c.p. in quanto manca l'elemento oggettivo rappresentato "dalla alienità della corrispondenza medesima**[20]**, apparendo infatti corretto ritenere che i messaggi inviati tramite l'e-mail aziendale del lavoratore…rientrino nel normale scambio di corrispondenza che l'impresa intrattiene nello svolgimento della propria attività…"

Diritto & Diritti ISSN 1127-8579

2. L'attività regolamentare del Garante per la protezione dei dati personali

Già nel 1999 tale problema era stato sollevato all'attenzione del Garante che riconobbe in quella occasione che mancava una disciplina compiuta di tale materia e che, comunque, le caselle di posta elettronica così come la posta ordinaria sono sottoposte ad una tutela unitaria. Di conseguenza, in caso di intercettazione della posta elettronica si concreta il reato di violazione di corrispondenza.

Tale situazione cambierà solo allorchè la azienda partecipi, rectius regolamenti, ai dipendenti che l'utilizzo delle caselle di posta aziendale fa venire meno il diritto alla riservatezza[21].

A livello comunitario va citato il Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro, redatto dal Gruppo di lavoro sulla protezione dei dati – Articolo 29[22].

Il Documento citato, tenendo conto delle pronunce adottate dalla Corte europea dei diritti umani[23], nonché della convenzione europea per la protezione dei diritti umani e delle libertà fondamentali[24], dalla Carta dei diritti fondamentali dell'Unione europea[25] attraverso l'art. 11, rubricato con il titolo "Libertà di espressione e d'informazione[26]" e, per finire, della direttiva 95/46/Ce[27], "…offre indirizzi interpretativi ed esempi concreti circa quanto costituisce attività legittima di controllo e circa i limiti accessibili della vigilanza sui dipendenti esercitata dal datore di lavoro".

Risalto è dato alle soluzioni offerte dalla tecnologia[28] in merito alla tracciabilità della navigazione in Internet ed all'utilizzo della posta elettronica, nel convincimento che "prevenire gli abusi debba considerarsi più importante che individuarli".

Nel 2006, il Garante è stato chiamato a pronunciarsi in merito ad un esposto di un lavoratore che aveva contestato la legittimità del datore di lavoro[29] che aveva visionato il contenuto dei siti da lui visitati.

Era accaduto, in buona sostanza, che la 'navigazione' in Internet da parte del lavoratore era stata oggetto di controllo da parte del datore di lavoro il quale anziché limitarsi ad accertare i tempi di connessione e gli accessi aveva preso cognizione anche del contenuto di tali accessi.

Diritto & Diritti ISSN 1127-8579

Così facendo aveva acquisito informazioni su dati di natura sensibile senza avere ricevuto il consenso al trattamento dei dati personali sensibili[30] da parte del dipendente.

Il Garante ha ribadito che il trattamento dei dati sensibili in assenza di consenso[31] dell'interessato[32] è ammesso solo a condizione che sia necessario per fare valere in giudizio un diritto della personalità o un altro diritto costituzionalmente garantito.

Nel caso in oggetto, invece, il diritto che la società intendeva fare valere in giudizio atteneva allo svolgimento del rapporto di lavoro, quindi si veniva a creare una contrapposizione tra il diritto alla riservatezza – del lavoratore – ed un diritto riguardante la sfera lavorativa – della società[33].

Un recente Provvedimento[34] del Garante ha disciplinato l'utilizzo della posta elettronica e della navigazione in Internet, riconoscendo ai lavoratori una tutela esplicita ed imponendo alle aziende una serie di obblighi.

Nella premessa del citato Provvedimento si fa riferimento ad una serie di reclami che hanno indotto il Garante ad intervenire al fine "di prescrivere ai datori di lavoro alcune misure, necessarie o opportune, per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet".

Tra i principi richiamati dal Garante ci sono: a) il principio di necessità per il quale: l'utilizzo dei dati personali, attraverso l'impiego di sistemi informativi e di programmi informatici, deve essere ridotto al minimo tenuto conto delle finalità perseguite[35]; b) il principio di correttezza, per il quale: le caratteristiche essenziali dei trattamenti, siano essi svolti in modalità cartacea od informatica oppure mista: cartacea ed informatica, devono essere partecipate ai lavoratori; c) le finalità alla base del trattamento dei dati personali devono essere: determinate, esplicite e legittime, oltre che pertinenti e non eccedenti[36].

In tema di controlli e di correttezza nel trattamento è fatto espresso riferimento allo Statuto dei lavoratori così come al decreto legge n. 626/94 relativamente all' "uso di attrezzature munite di videoterminali", il quale esclude la possibilità del controllo informatico 'all'insaputa dei lavoratori'**[37]**.

E' vietata la possibilità di utilizzare apparecchiature preordinate al controllo a distanza mentre è

Diritto & Diritti ISSN 1127-8579

consentito al datore di lavoro di "controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro "

Suddetta attività di controllo va svolta nel rispetto della libertà e della dignità dei lavoratori.

E' consentito, ai sensi dell'art. 4 dello Statuto dei Lavoratori[38] e previo accordo con le RSU aziendali e successiva informazione dei lavoratori, un controllo sulla scorta di dati aggregati mirante ad evidenziare il 'minutaggio' dell'utilizzo delle dotazioni informatiche e solo in caso di evidenti anomalie il datore di lavoro inviterà –il Dirigente responsabile ed i dipendenti afferenti alla realtà lavorativa interessata - di attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Qualora la anomalia dovesse ripetersi e riguardare lo stesso ambito lavorativo il datore di lavoro procederà ad effettuare controlli su base individuale.

Una problematica di non poco conto è quella attinente la conservazione dei dati relativi all'acceso ad Internet ed al traffico telematico (log di sistema[39] e del server proxy[40]), rispetto alla quale nel Provvedimento si legge che "I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente… i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria".

Manca, pertanto, una chiara indicazione dei tempi di conservazione di tali dati con la conseguente necessità per l'interprete di dovere effettuare una ricognizione della normativa nazionale e comunitaria sull'argomento alla ricerca di un chiaro riferimento legislativo.

Riteniamo che vada preso in considerazione quanto contenuto nel Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro, redatto dal Gruppo di lavoro sulla protezione dei dati – Articolo 29, il quale al paragrafo 3.1.6 rubricato "Accuratezza e conservazione dei dati" sancisce "I datori di lavoro dovranno precisare un periodo di conservazione dei messaggi di posta elettronica sui loro server centrali in funzione delle esigenze aziendali. Di norma risulterà difficile giustificare un periodo di conservazione superiore ai tre mesi".

Il Garante conclude il Provvedimento con una prescrizione rivolta ai datori di lavoro affinchè adottino "la misura necessaria a garanzia degli interessati…riguardante l'onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori…, indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati

Diritto & Diritti ISSN 1127-8579

controlli,".

3. Linee guida per la redazione del Regolamento aziendale inerente le modalita' di utilizzo della posta elettronica e di internet da parte dei dipendenti della azienda

Il Regolamento aziendale, inerente le modalità di utilizzo della posta elettronica e di Internet da parte dei dipendenti andrebbe redatto facendo riferimento alla seguente articolazione[41]:

· **"Oggetto e finalità",** al fine di fornire al destinatario del Regolamento una cornice la più esaustiva possibile è opportuno fare riferimento alla normativa disciplinante la materia oggetto del Regolamento: **Legge 20.5.1970, n. 300** "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento"; **Newsletter del 19-25 febbraio 2001 del Garante[42]Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro, adottata dal Gruppo di lavoro sulla protezione dei dati (Articolo 29), in data 29 maggio 2002, oltre che in attuazione del Decreto Legislativo n. 196 del 23 giugno 2003, recante "Codice in materia di protezione dei dati personali"; Provvedimento del Garante per la protezione dei dati personali, del 01 marzo 2007, recante "Lavoro: le linee guida del Garante per posta elettronica e internet"[43]; Documento Programmatico sulla Sicurezza adottato dalla azienda[44].**;

· "**Principi generali**", vanno richiamati ed esplicitati il principio di necessità, il principio di correttezza e quello di finalità. (si rimanda a quanto tratteggiato nel paragrafo 2).

· "**Tutela del lavoratore**", le cui garanzie vanno desunte, in primis, dallo Statuto dei Lavoratori ed, in subordine, dal testo del Codice in materia di protezione die dati personali. Si tenga presente che il regolamento deve avere come elemento fondante la adozione di un principio garantista nei confronti della parte debole rappresentata, appunto,dai lavoratori.

· "**Corretto utilizzo di Internet**", qualora esista va fatto riferimento al regolamento di policy aziendale[45] relativo all'utilizzo della dotazione informatica e, in sua assenza, sono fornite le istruzione alle quali necessita dare attuazione, ad es: utilizzo del pc in sicurezza, divieto di effettuare download,

Diritto & Diritti ISSN 1127-8579

transazioni finanziarie, acquisti on line, abbonamenti privati, partecipazione a Forum e a Chat line non professionali, ecc. E' consigliabile, ad avviso dello scrivente, autorizzare la navigazione in Internet così come l'utilizzo della posta elettronica per fini personali per un periodo massimo che può stimarsi in 10/15 minuti al giorno. In questo modo, responsabilizzandoli, è più facile indirizzare i dipendenti verso comportamenti virtuosi.

· "**Utilizzo di pc portatili**", vanno fornite indicazione nei confronti dei dipendenti assegnatari di pc portatili, relativamente alle loro modalità di utilizzo all'esterno della azienda così come in caso di collegamento alla rete aziendale.

· "**Corretto utilizzo della posta elettronica**", da effettuarsi per motivi inerenti il servizio al quale si è preposti, con divieto di diffondere messaggi non istituzionali. Va disciplinata anche la eventualità in cui sia necessario conoscere i dati contenuti nella casella di posta elettronica ed il dipendente sia assente, per un qualsiasi motivo. La azienda – qualora non sia possibile attivare la funzione autoreply o l'inoltro automatico ad altra casella aziendale di posta elettronica - ha l'onere di individuare un lavoratore che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, abbia la possibilità di verificare il contenuto dei messaggi di posta elettronica ed inoltrare al Titolare o al Responsabile del Trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa[46]. Il documento di policy[47] dovrebbe introdurre una distinzione tra la posta elettronica intesa come comunicazione tra soggetti (ad es: comunicazioni commerciali, newsletter, e-mail personali, spam, messaggi, sic et simpliciter, ecc.) e la posta con finalità istituzionale. Quest'ultima andrebbe integrata col protocollo aziendale per diventare un documento ufficiale e, quindi, un documento da archiviare. Tale modalità di comunicazione rappresenterebbe il secondo canale di ingresso della azienda, c.d. Corporate Portal[48], in aggiunta a quello costituito dalla posta tradizionale.

· "**Controlli disposti dalla Azienda**". E' opportuno specificare che gli eventuali controlli hanno la finalità di garantire la sicurezza[49] nel trattamento dei dati e nell'uso della dotazione informatica e non mirano ad un controllo a distanza nei confronti dei lavoratori. Andrà previsto un primo livello di controlli su dati aggregati, condotto per macro aree aziendali, qualora gli stessi abbiano evidenziato un impiego anomalo degli strumenti informatici ne sarà data comunicazione ai dirigenti interessati e, a caduta ai relativi collaboratori, e se dovessero persistere tali anomalie sarà effettuato un controllo anche su base individuale.

· "**Conservazione dei dati**": in assenza di una espressa indicazione circa la durata dei tempi di conservazione è opportuno fare riferimento a quanto affermato nella Relazione redatta dal gruppo di lavoro sulla Protezione dei dati – Articolo 29 e fissare, quindi,un termine massimo di tre mesi dalla loro produzione.

Diritto & Diritti ISSN 1127-8579

· "**Sanzioni disciplinari**": fa fede quanto stabilito dagli atti interni contenenti il Codice disciplinare oltre a quanto stabilito dallo Statuto dei lavoratori, art. 7. Andrà integrato, di conseguenza, il codice disciplinare con le infrazioni connesse all'utilizzo di Internet e della posta elettronica aziendale, assicurandosi di darne la massima diffusione.

· "**Disposizioni finali**": la diffusione del Regolamento sarà assicurata dal rispetto di quanto stabilito dall'art. 7 della L.n. 300, oltre chè avvalendosi della rete intranet e delle altre modalità ritenute opportune.

· E' consigliabile allegare anche una Legenda esplicativa dei termini impiegati, unitamente al Codice disciplinare interno ed alla Informativa ai sensi del Decreto Legislativo n. 196/03.

Da tenere presente che il Regolamento, andando ad impattare tutti gli ambiti della azienda, va elaborato con il concorso del Responsabile del Servizio Informatico aziendale e del Responsabile della Gestione delle Risorse Umane. Esso prima di essere licenziato e diventare esecutivo va sottoposto al vaglio della RSU aziendale, in quanto gli strumenti hardware e software per il controllo dei dipendenti che utilizzano un sistema di comunicazione elettronica rientrano nella fattispecie di cui all'art. 4 dello Statuto dei Lavoratori, in materia di controllo a distanza[50].

Un aspetto da non sottovalutare è, a parere dello scrivente, quello della formazione del personale su tali tematiche. Disporre di collaboratori consapevoli e responsabilizzati permette di ridurre al minimo il contenzioso legato alla applicazione del regolamento e, quindi, di focalizzare le risorse economiche ed umane dell'azienda su altri settori.

Conclusione

L'impiego da parte del datore di lavoro di programmi - software – finalizzati al monitoraggio delle connessioni che vengono effettuate in ambito aziendale, per la supposta invasività degli stessi, induce ad una serie di riflessioni in merito al rapporto che si viene a creare tra le esigenze del datore di lavoro e la riservatezza del lavoratore.

Diritto & Diritti ISSN 1127-8579

Da una parte c'è la azienda o ente che mira a proteggere la sua rete informatica, attraverso la introduzione di una serie di misure di sicurezza, peraltro esplicitate attraverso il decreto legislativo n. 196/2003 ed in particolare con l'Allegato B al Decreto stesso, dall'altra c'è il lavoratore che utilizzando – per fini privati - la casella di posta elettronica fornitagli dal datore di lavoro, come supporto al suo impiego lavorativo, pretende il rispetto della propria sfera di riservatezza, anch'essa garantita dal decreto sopra menzionato.

L'impiego di software con le caratteristiche sopra indicate se avviene per fini difensivi e, previa regolamentazione e comunicazione ai dipendenti, deve comunque limitarsi ad un controllo inerente non i contenuti della navigazione ma la postazione che ha effettuato il collegamento, l'orario di accesso e la durata.

Un utilizzo di tale software in maniera più invasiva, mirante ad avere cognizione dei siti frequentati e delle pagine aperte, sarebbe contrario al principio di proporzionalità nel trattamento del dato personale, principio cardine di tale disciplina.

Il contemperamento delle due accennate esigenze va risolto tenuto conto che "…è un diritto del datore di lavoro verificare la destinazione della risorsa aziendale (ed Internet è un costo ed una risorsa) ma è altrettanto diritto del lavoratore non subire controlli subdoli ed occulti"[51].

Dott. **********

[1] **Da Wikipedia, "** La **E-****** (abbreviazione di **********, in italiano: **posta elettronica**) è un servizio internet grazie al quale ogni utente può inviare o ricevere dei messaggi. È l'applicazione Internet più conosciuta e più utilizzata attualmente. La sua nascita risale al 1972, quando Ray Tomlinson installò

Diritto & Diritti ISSN 1127-8579

su ARPANET un sistema in grado di scambiare messaggi fra le varie università, ma chi ne ha realmente definito il funzionamento si chiamava, forse non a caso, **********. È la controparte digitale ed elettronica della posta ordinaria e cartacea. A differenza di quest'ultima, il ritardo con cui arriva dal mittente al destinatario è normalmente di pochi secondi/minuti. “ .

[2]Nel 2005 è stata condotta una indagine da parte di una Ditta specializzata in sondaggi, la Internet Monitoring, dalla quale è emerso che circa 22 mila utenti ogni giorno chattano sul luogo di lavoro per un costo presunto a carico delle aziende pari a 500 milioni di euro l’anno.

Da una indagine compiuta da **********, pubblicata ad Aprile 2007, relativamente al costo aziendale annuo per mancata produttività dovuta ad abuso delle risorse informatiche è emerso che ipotizzando un numero di dipendenti, autorizzati ad utilizzare la rete Internet, pari a 100 unità un uso improprio delle risorse aziendali pari a 15 minuti cadauno al giorno comporta per l’azienda un costo medio annuo di oltre 90.000 euro!

[3]**Direttiva 27 novembre 2003, della Presidenza del Consiglio dei Ministri per l’innovazione e le tecnologie, recante “Impiego della posta elettronica nelle pubbliche amministrazioni”**, pubblicata sulla Gazzetta Ufficiale n. 8 del 12 gennaio 2004, ove si legge “Le singole amministrazioni, nell’ambito delle rispettive competenze, ferma restando l’osservanza delle norme in materia della riservatezza dei dati personali e delle norme tecniche di sicurezza informatica, si adopereranno per estendere l’utilizzo della posta elettronica…”.

[4] Il **DPR 11 febbraio 2005, n. 68** (G.U. 28 aprile 2005, n. 97) (PDF) (RTF) disciplina le modalità di utilizzo della Posta Elettronica Certificata (PEC) non solo nei rapporti con la PA, ma anche tra privati cittadini.

[5]**********, Tecnologie aziendali e loro uso privato: che cosa dice il Codice, www.pomante.com, l’Autore analizza l’argomento mettendo in raffronto il codice penale con le direttive del codice in materia di protezione dei dati personali; **********, Il controllo dei lavoratori, www.giuristitelematici.it, l’Autrice passa in rassegna le principali pronunce della giurisprudenza, a decorrere dal 2000, alla luce delle pronunce del Garante; **********, Il controllo della mailbox aziendale, www.filodiritto.com; **********, Lettura della casella di posta elettronica da parte del datore di lavoro: lecito o illecito?; Controllo dei log

Diritto & Diritti ISSN 1127-8579

di connessione e privacy, www.consulentelegaleprivacy.it; **Morgoglione C**., Il Garante per la privacy: la corrispondenza elettronica ha la stessa tutela di quella 'ordinaria; La Repubblica, 13.7.99; ************,** La posta elettronica ed i suoi aspetti nel mondo aziendale, www.Filodiritto.it, l'Autore si sofferma nella lettura critica dell'art. 616 del codice penale alla luce del Decreto legislativo n. 196/03 e delle indicazioni fornite dal "Gruppo europeo per la tutela del trattamento dei dati", senza tralasciare l'apparato di garanzie introdotte dalla legge 300/1970; **Solignani T.,** Le normative per chi usa l'e-mail sul posto di lavoro, in www.distrettopmi.it, sulle leggi ed i provvedimenti che regolano l'utilizzo della posta in azienda; *************,** Internet, posta elettronica e privacy: esigenze di sicurezza e comportamenti a rischio, in www.filodiritto.com; *************,** Chattare sul luogo di lavoro: ipotesi di reato, www.diritto.it, che analizza le ipotesi di reato concretizzabili a carico del lavoratore; ************,** I nuovi obblighi complicano la revisione del documento programmatico di sicurezza, Guida al Diritto, 24 marzo 2007, n. 12; *********,** L'insostenibile riservatezza di un messaggio di posta elettronica, www.Scintilex.it , al quale si rimanda per la trattazione di una querelle sorta negli USA in merito all'accesso alla casella di posta elettronica di un defunto da parte degli eredi.; *************,** Nuove tecnologie: privacy e controlli del datore. Controllo della navigazione in Internet, www.microsoft.com ; ************,** Privacy, doppia bussola per i controlli in ufficio, Il Sole 24 Ore del 3 aprile 2007; ************, ****** F,** La privacy in ufficio. Le linee guida del Garante, in Il Sole 24 Ore di Lunedì 2 aprile 2007; **Cerchi A.,** E-mail con privacy sorvegliata, Il Sole 24 Ore del 6 marzo 2007; ***************,** Per le aziende policy d'obbligo, Il sole 24 Ore, del 06 marzo 2007; ************,** Il sistema di posta elettronica collaborativo ed integrato: tassello strategico del corporate portal, www.iged.it, n. 4, anno 2006, al quale si rimanda per una descrizione del flusso documentale interno alla azienda con particolare riferimento alle problematiche legate alla gestione in sicurezza dei dati ed alla loro archiviazione; **AA.VV.** Lezione 9 sicurezza della posta elettronica, www.isecom.org; *********,**

Confermata la corresponsabilità di un datore di lavoro per il sito personale di un dipendente, www.apogeonline.com, L'Autrice prende in esame una pronuncia della Corte di appello di Aix en ******** che ha confermato la sentenza di primo grado che aveva condannato una impresa e un suo dipendente che aveva realizzato, dal posto di lavoro, un sito personale a contenuto diffamatorio; **********,** Legittimo il controllo dell'e-mail (e del telefono) aziendale del dipendente www.infogiur.com; ********** L**., L'utilizzo della strumentazione informatica da parte del dipendente pubblico, www.consulentelegaleprivacy.it

[6] Sulla materia inerente il trattamento dei dati personali sia consentito rimandare a ************, ******** breve al D.Lgs.vo n. 196/2003. Codice in materia di protezione dei dati personali,** su www.dirittosuweb.com; ottobre 2005 e su www.diritto.it/articoli/dir_privacy/diritto_privacy.html; (2005); **Il trattamento dei dati sensibili a livello di azienda: aspetti normativi e di sicurezza** ", su www.diritto.it/articoli_materiali/privacy/diritto_privacy.html; (2005); **Introduzione al Decreto Legislativo n. 196 del 2003 (Codice in materia di protezione dei dati personali) con particolare riferimento alle misure di sicurezza**, su www.filodiritto.com/diritto/privato/informaticagiuridica/introduzioneprivacymisuresicurezzamodesti.htm; (

2005)

[7] “Ai fini dell’operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell’attività dei lavoratori…, è necessario che il controllo riguardi (direttamente o indirettamente) l’attività lavorativa, mentre devono ritenersi certamente fuori dell’ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (c.d. controlli difensivi) quali, ad esempio, i sistemi di controllo dell’accesso ad aree riservate, o, appunto, gli apparecchi di rilevazione di telefonate ingiustificate”.

[8]Un punto dolens di tale pronuncia consiste nella mancata esplicitazione/quantificazione da parte della Cassazione di cosa debba intendersi per uso “sporadico o episodico”.

[9] “…le caselle di posta elettronica recanti quali estensioni nell’indirizzo e-mail @ (…).it, seppur contraddistinte da diversi ‘username’ di identificazione e password di accesso, sono da ritenersi equiparate ai normali strumenti di lavoro della società e quindi soltanto in uso ai singoli dipendenti per lo svolgimento dell’attività aziendale agli stessi demandata; considerando quindi che la titolarità di detti spazi di posta elettronica debba ritenersi riconducibile esclusivamente alla società…”

[10]Il Pubblico Ministero ha individuato una serie di aree tematiche, relativamente all’utilizzo della posta elettronica, che necessitano di una apposita regolamentazione “a) utilizzo anche per fine privato dell’indirizzo di posta elettronica da parte del lavoratore con eventuale esposizione dello stesso sulla carta da visita intestata a proprio nome; b) possesso di un indirizzo ‘generalista’ per cui la posta ivi indirizzata può avere come destinatario un qualunque altro dipendente con conseguente incertezza sulla ‘consegna’; c) mancata individuazione del mittente (in possesso di un indirizzo in codice o con sigla) che non provvede a sottoscrivere il messaggio ovvero che non si preoccupa di farsi riconoscere rendendosi di fatto anonimo”.

[11] “Personalità dell’indirizzo non significa necessariamente privatezza del medesimo, dal momento che, salve le ipotesi in cui la qualifica del lavoratore lo consenta o addirittura lo imponga…l’indirizzo aziendale, proprio perché tale, può sempre essere nella disponibilità di accesso e lettura da parte di persone diverse dall’utilizzatore consuetudinario…”

[12]"Né si può ritenere che l'assimilazione della posta elettronica alla posta tradizionale,con consequenziale affermazione 'generalizzata' del principio di segretezza, si verifichi nel momento in cui il lavoratore utilizzi lo strumento per fini privati (ossia extralavorativi), atteso che giammai un uso illecito (o, al massimo, semplicemente tollerato ma non certo favorito) di uno strumento di lavoro può far attribuire a chi, questo illecito commette, diritti di sorta."

[13]**Art. 616 c.p. Violazione, sottrazione e soppressione di corrispondenza**
Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prendere o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, e' punito, se il fatto non e' preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da lire sessantamila a un milione.
Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, e' punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un piu' grave reato, con la reclusione fino a tre anni.
Il delitto e' punibile a querela della persona offesa.
Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza (1).
(1) Comma cosi' sostituito dall'art. 5, L. 23 dicembre 1993, n. 547.

[14] Qualora per assurdo "...si volesse ritenere che con la loro condotta la C. e il R. nelle loro rispettive qualità, entrando nella casella di posta elettronica in uso alla lavoratrice abbiano commesso nei confronti della stessa un'illecita intromissione in una sfera personale privata, nondimeno la configurabilità del reato di cui all'art. 616 c.p. verrebbe ugualmente esclusa sotto il profilo soggettivo attesa la totale mancanza di dolo nella loro condotta".

[15]**Corte dei Conti – sezione giurisdizionale Piemonte sentenza n. 1856/2003** "...l'Ufficio Requirente di questa Corte, ravvisata l'esistenza di profili di responsabilità a carico del Dirigente in parola per il danno patrimoniale cagionato all'Amministrazione, consistente nel mancato svolgimento della prestazione lavorativa durante le citate ore di connessione...Il Collegio...non ravvisa nell'operato del Comune (omissis) alcun comportamento invasivo preordinato al controllo rendiconto dell'attività del proprio dipendente, ma semplicemente l'impiego, con verifiche svolte ex post, di un tipo di software in uso

Diritto & Diritti ISSN 1127-8579

a molte Pubbliche Amministrazioni in grado di registrare i dati inerenti agli accessi degli utenti collegati alla rete, non solo per finalità di repressione di comportamenti illeciti, ma anche per esigenze statistiche e di controllo della spesa."

[16]"…nel protocollo aziendale relativo alla 'Information System Security'…si precisa ..'La strumentazione informatica e quanto con essa creato è di proprietà aziendale in quanto mezzo di lavoro. E' pertanto fatto divieto di utilizzo del mezzo informatico e delle trasmissioni interne ed esterne con esso effettuate per fini ed interessi non strettamente coincidenti con quelli della Società e con i compiti ai singoli dipendenti affidati…"

[17]"Tale guida sui sistemi informatici adottata dalla società xxx appare, pertanto,…in sintonia con quanto affermato in materia di riservatezza delle e-mail …dal garante…che nel sostenere che le caselle di posta elettronica sono equiparate e quindi vanno tutelate come i normali recapiti per la corrispondenza su carta, aveva anticipato il principio secondo cui chi utilizzava indirizzi e-mail presso i server del proprio datore di lavoro poteva rivendicare il diritto alla segretezza dei contenuti spediti o ricevuti 'fino a prova contraria'".

[18]**Incaricati** "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile"; art. 4, c.1, lett. h) D.Lgs. n. 196/03

[19]**Trattamento "** qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati**;"** art. 4, c. 1, lett. a), D.lgs. n. 196/03

[20]Di pari avviso una ordinanza del **Tribunale di Vasto del 24.6.02** ove si legge "il delitto di violazione della corrispondenza…di necessità implica la materialità del fatto della presa di cognizione di corrispondenza (anche informatica) all'agente non diretta, evenienza questa che può in concreto escludersi nella fattispecie in cognizione…e che ad ogni modo va correlata alla proprietà dei beni in uso al lavoratore ed alla loro stessa destinazione funzionale, alle ragioni dunque del loro affidamento al singolo lavoratore (ragioni quelle che allora non escludono in ipotesi la liceità del concorrente impiego da parte di

altri dipendenti della medesima postazione di lavoro aziendale)".

[21]L'allora Segretario generale dell'Autorità garante della tutela dei dati personali, dott. ********** ha affermato che "Stabilendo con certezza, attraverso regole comunicate ai dipendenti senza possibilità di equivoci, se si dà loro – o meno – la libertà di utilizzare l'indirizzo dell'ufficio in maniera riservata, oppure no. Entrambe le possibilità sono legittime: ma se la società o l'ente non spiega qual è la regola, si intende che il lavoratore ha tutto il diritto a vedere tutelata la privacy."

[22]Il gruppo di lavoro ex art 29 è un gruppo consultivo composto da rappresentanti delle autorità competenti per la protezione dei dati nei diversi Stati membri.

[23]In riferimento al caso **Halford contro Regno Unito,** la Corte ha stabilito che l'intercettazione delle chiamate telefoniche svolte dai dipendenti sul posto di lavoro costituisce una violazione della convenzione.

[24]**Art 8** "1. Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza. 2. Non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto se non laddove sia contemplata dalla legge in quanto provvedimento che, in una società democratica, risulti necessario per la sicurezza nazionale, l'ordine pubblico…la protezione dei diritti e delle libertà altrui."

Art. 10 "1. Ogni persona ha diritto alla libertà di espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni od idee senza ingerenza alcuna… 2: L'esercizio di queste libertà, comportando doveri e responsabilità, può essere sottoposto a determinate formalità, condizioni, restrizioni o sanzioni disposte dalla legge…"

[25]Tale Carta richiama i principi stabiliti dalla Corte europea e lo fa ampliando il concetto di 'segretezza delle comunicazioni' alle comunicazioni elettroniche. Altri articoli di rilievo per la nostra trattazione sono: l'art. 8 "Protezione dei dati di carattere personale" e l'art. 42 "Diritto di accesso ai documenti". Sulla stessa linea è il Codice di condotta in tema di protezione dei dati personali dei lavoratori stilato dall'Ufficio internazionale del lavoro.

[26]"1. Ogni individuo ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. 2. (omissis)".

[27]**Direttiva 95/46/CE** del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati, recita "che gli Stati membri assicurino la tutela dei diritti e delle libertà delle persone fisiche e particolarmente del diritto alla vita privata, per quanto riguarda il trattamento dei dati personali, al fine di garantire il libero flusso dei dati personali nella Comunità." Nella elaborazione del Documento ha avuto rilievo anche la **Direttiva 97/66/CE** , del 15 dicembre 1997, relativa alla elaborazione dei dati personali ed alla tutela della vita privata nel settore delle telecomunicazioni.

[28] Proprio per la valenza riconosciuta al progresso tecnologico che è prevista una revisione dell'attuale documento negli anni 2002-2003.

[29]**Comunicato stampa – 14 febbraio 2006** "Non è ammesso spiare l'uso dei computer e la navigazione in rete da parte dei lavoratori. Sono in gioco la libertà e la segretezza delle comunicazioni e le garanzie previste dallo Statuto dei lavoratori. Occorre inoltre tenere presente che il semplice rilevamento dei siti visitati può rilevare dati delicatissimi della persona: convinzioni religiose, opinioni politiche, appartenenza ai partiti, sindacati o associazioni, stato di salute, indicazioni sulla vita sessuale".

[30]**Dati sensibili** " i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale". Art. 4, c.1, lett. d) D.Lgs. n. 196/03

[31] Il consenso è una manifestazione di volontà espressa dal soggetto definito 'interessato' al fine di autorizzare il trattamento dei propri dati personali.

Diritto & Diritti ISSN 1127-8579

[32]**Interessato** "la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali". Art. 4, c.1, lett. i) D.Lgs. n. 196/03

[33] **Comunicato stampa – 14 febbraio 2006** " Illecito anche il trattamento dei dati relativi allo stato di salute e alla vita sessuale. Secondo il Codice della privacy infatti tale tipo di trattamento può essere effettuato senza consenso solo se necessario per difendere in giudizio un diritto della personalità o un altro diritto fondamentale. La società in questo caso intendeva far valere diritti legati allo svolgimento del rapporto di lavoro."

[34]**Garante per la protezione dei dati personali – Provvedimento 1° marzo 2007, "Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte di lavoratori".** Pubblicato sulla Gazzetta Ufficiale n. 58 del 10 marzo 2007

[35]Bisogna tendere ad un livello di intrusione 'minimo' nella sfera privata delle persone, privilegiando metodi tradizionali di vigilanza prima di ricorrere ad un controllo elettronico delle comunicazioni.

[36]Ciò si traduce nella conseguenza che se i dati, rectius la elaborazione dei dati, mira a garantire la sicurezza del sistema, gli stessi dati non potranno essere successivamente utilizzati per controllare il comportamento dei dipendenti.

[37] Sull'argomento sia consentito rimandare a ************, Il decreto legislativo n. 626 del 19 settembre 1994 e il sistema di responsabilità all'interno delle Aziende Sanitarie, alla luce delle recenti pronunce della Corte di Cassazione.** (2005) su www.iureconsult.com/areatema/diritto_sanitario/responsabilità_aziende_sanitarie/index.htm; settembre 2005); **Lettura breve del decreto legislativo n. 626/1994 con riferimento all'istituto della delega di funzioni in materia di tutela delle condizioni di lavoro**; su **www.diritto.it**; (settembre 2006);

[38] **Art. 4 Impianti audiovisivi. "**È vietato l'uso di impianti audiovisivi e di altre apparecchiature per

finalità di controllo a distanza dell'attività dei lavoratori. Gli impianti e le apparecchiature di controllo che siano 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, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, 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. Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti. Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale."

[39] Da **Wikipedia**: "**Log** in inglese significa tronco di legno; (omissis). Il **logbook** (1800) era il registro di navigazione, presente in ogni nave, su cui veniva segnata, ad intervalli regolari la velocità, il tempo, la forza del vento, oltre a eventi significativi che accadevano durante la navigazione. Con il significato di giornale di bordo, o semplicemente giornale, su cui vengono registrati gli eventi in ordine cronologico il termine è stato importato nell'informatica (1963) per indicare: la **registrazione cronologica** delle operazioni man mano che vengono eseguite; il **file** su cui tali registrazioni sono memorizzate.

[40] Da Wikipedia, "NavigazionecercaUn proxy è un programma che si interpone tra un client ed un server, inoltrando le richieste e le risposte dall'uno all'altro. Il client si collega al proxy invece che al server, e gli invia delle richieste. Il proxy a sua volta si collega al server e inoltra la richiesta del client, riceve la risposta e la inoltra al client."

[41]Va da sé che le seguenti linee guida, contenute in questo paragrafo, non hanno la pretesa della esaustività in quanto non è ipotizzabile pensare ad un testo regolamentare che vada bene per ciascuna situazione: azienda, ente pubblico, studio professionale, ecc. Da parte dell'Autore c'è solo il proposito di condividere alcuni spunti con chi, studioso o operatore, deve confrontarsi con tale obbligo normativo.

Diritto & Diritti ISSN 1127-8579

[42] Ha riconosciuto il diritto del datore di lavoro di accedere alla posta elettronica rilevando come " al dipendente deve essere consentito di procedere autonomamente alla sostituzione della parola chiave…previa comunicazione della sostituzione delle chiavi ai soggetti preposti alla custodia delle password…tali modalità consentono di proteggere i dati personali dalla possibile intrusione da parte di soggetti non legittimati all'accesso, permettendo contestualmente al titolare del trattamento di accedere in caso di necessità e di urgenza alle informazioni contenute nella memoria del computer per utilizzi consentiti dalla legge".

[43] Si tenga presente anche il Comunicato stampa del Garante per la protezione dei dati personali del 5 marzo 2007 sulle "linee guida del garante per posta elettronica e internet. Le regole aziendali, il doppio indirizzo e-mail, il fiduciario, i siti non accessibili."

[44] Ai sensi del punto 19 dell'Allegato B, "entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni…"

[45] Riteniamo che una corretta policy aziendale debba, per prima cosa, stabilire i principi generali che regolano l'uso della dotazione informatica, lo scopo della posta elettronica e della navigazione in Internet, le regole di utilizzo e il regolamento del personale. Successivamente debba tendere a contenere il numero di caselle di posta elettronica che andrebbero assegnate in base all'organigramma aziendale e sulla scorta di una effettiva necessità lavorativa. In questo modo verrebbe favorita una più efficace politica di sicurezza, a sua volta supportata da uno stringente Documento Programmatico per la Sicurezza. Andrebbe posta attenzione anche ad un aspetto della security policy spesso trascurato, mi riferisco al software per la gestione dei profili di autorizzazione, per la gestione delle vulnerabilità e degli eventi di sicurezza.

[46]E' quanto stabilisce l'art. 10 dell'Allegato B al Codice in materia di protezione dei dati personali "Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante l'uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema…." In tale caso va individuato il custode delle copie delle credenziali.

Diritto & Diritti ISSN 1127-8579

[47]Tra gli adempimenti a carico dell'Amministratore di sistema ci sono: tenere aggiornato il software per la posta elettronica; installare un apposito antivirus in grado di filtrare la posta in entrata ed in uscita; filtrare lo spamming; dare istruzioni ai dipendenti affinchè non aprano messaggi provenienti da sconosciuti e non trasmettano mai dati personali sensibili a meno che non vanga fatto ricorso all'invio criptato, ecc.

[48]Una tale architettura informatica consentirebbe una gestione relativa all'accesso alle informazioni in grado di affrontare con successo una serie di problematiche ad esso connesso. Ci si riferisce: alla archiviazione dei dati (quali?, per quanto tempo?m con quali modalità?); alla sicurezza del trattamento dei dati (quali misure adottare per evitare access illegittimi dall'interno e/o dall'esterno?, come garantire il superamento di eventi dannosi, tipo il disaster recovery?, ecc.); alla profilazione dei soggetti autorizzati a trattare i dati, ecc.

[49] L'impiego sempre più diffuso della posta elettronica ha prodotto, tra le altre cose, un cambiamento nella gestione dei dati personali presenti in azienda e la creazione di archivi elettronici che hanno finito con l'affiancare quelli cartacei. Attraverso la casella di posta elettronica sono veicolate informazioni anche di natura ufficiale che è necessario archiviare ed è in questo momento che si profila un problema legato alla sicurezza e, quindi, al corretto utilizzo dei dati personali che – per la quasi totalità delle aziende – costituiscono il vero valore aggiunto. Perdere informazioni equivale a perdere dati e, quindi, avere difficoltà a competere.

[50] Va sottolineato che la mancata adozione di una policy di sicurezza aziendale da parte della azienda rende inutilizzabili i dati raccolti dal datore di lavoro tramite i controlli, anche se questi hanno evidenziato gravi inadempimenti.

[51] ************,** Controllo dei log di connessione e privacy, www.consulentelegaleprivacy.it

Diritto & Diritti ISSN 1127-8579

Diritto & Diritti ISSN 1127-8579