

IL CONTROLLO DELLA MAILBOX AZIENDALE

di Telesio Perfetti¹

Computerlaw.it 2006 – [Alcuni diritti riservati](#)

¹ giurista, esperto in e-privacy e sicurezza informatica. E' Privacy Consultant presso lo Studio Legale F&D (www.studiolegalefd.it), in Roma. E' autore di pubblicazioni scientifiche in materia di diritto delle nuove tecnologie. Collabora attualmente come docente presso il Master universitario di II livello "Diritti della persona e nuove tecnologie" - Università degli Studi di Roma "La Sapienza" - direttore Prof. Stefano Rodotà.

1. CONTROLLI DATORIALI SULLA MAILBOX AZIENDALE E VIOLAZIONE DELLA CORRISPONDENZA

Problema particolarmente spinoso in materia di rispetto della privacy, *rectius* della riservatezza e della dignità del dipendente sul posto di lavoro è se sia legittimo o meno che il datore di lavoro o una persona da lui appositamente delegata e autorizzata (responsabile dell'ufficio, capo-reparto, capo-settore etc.) abbia accesso alla *mailbox* messa a disposizione del prestatore di lavoro per svolgere la propria attività. In effetti, se il datore è legittimato, allora è evidente che il lavoratore vede diminuite le sue garanzie e i suoi diritti. In caso contrario, il datore sarebbe passibile di querela e di conseguente procedimento penale per il delitto di **violazione di corrispondenza** ai sensi dell'art. 616 c.p.²

A tal proposito va segnalata un'interessante sentenza del Tribunale di Torino, Sezione Distaccata di Chivasso, 20/06/2006 (dep. 15 settembre 2006), n. 143, che ha stabilito il seguente principio di diritto: **l'email aziendale appartiene al datore di lavoro e pertanto in relazione al reato di cui all'art. 616 c.p. il fatto non sussiste qualora, anche in presenza di adeguata *policy* aziendale, il datore di lavoro acceda alla casella personalizzata del dipendente**³.

Il caso sottoposto all'attenzione del giudice piemontese non che è uno dei tanti che si possono verificare all'interno di un'azienda. Un dipendente, a cui il datore di lavoro ha assegnato una mailbox per espletare le mansioni lavorative, è assente per ferie o per malattia, ma l'assenza si protrae per diversi giorni. C'è un progetto importante da portare avanti in tempi rapidi ed è necessario dunque accelerare le operazioni e comunicare quanto prima lo stato di avanzamento dei lavori o eventuali impedimenti etc. A tal fine, su delega del datore, il capo-ufficio, essendo a conoscenza del fatto che il dipendente assente si stava occupando di quel progetto e intratteneva i relativi rapporti col cliente interessato, accede alla mailbox aziendale del dipendente stesso. Durante il controllo, il capo-ufficio trova *files* e altra documentazione non consona al lavoro che doveva essere svolto, risultando così lo strumento della mail utilizzato per finalità "private", non istituzionali, i.e. esulanti per l'appunto dall'attività lavorativa⁴. Il datore viene informato del fatto e licenzia in tronco (per giusta causa) il dipendente in questione, ravvisando nel suo comportamento una condotta posta in essere in violazione degli obblighi di fedeltà del lavoratore (v. artt. 2105 e 2106 c.c.). Il dipendente ovviamente non resta a guardare, impugna il licenziamento, altresì sporge querela contro il proprio capo-ufficio, accusandolo di aver violato la segretezza della propria corrispondenza ai sensi dell'art. 616 c.p.

Nel caso specifico, che ora si sta affrontando, l'autorità giudicante, in relazione al reato contestato, pronuncia sentenza di assoluzione con formula piena (*"perché il fatto non sussiste"*), per le ragioni qui di seguito indicate:

- I computers utilizzati dai dipendenti di un'azienda devono ritenersi equiparati a **normali strumenti di lavoro**, forniti loro in dotazione **esclusivamente per lo svolgimento della attività aziendale demandatagli**: suffraga tale assunto la menzione nell'indirizzo di posta elettronica *de quo* dell'identificativo della stessa azienda nonché la **possibilità per il servizio**

² La corrispondenza elettronica – è ormai assodato e risaputo – è stata pienamente equiparata a quella tradizionale o cartacea, grazie all'art. 5 della l. 547/1993, che ha aggiunto, nel corpo dell'art. 616 c.p., il seguente comma: «*Agli effetti delle disposizioni di questa sezione (dei delitti contro l'inviolabilità dei segreti, n.d.r.) per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni forma di comunicazione a distanza*». Pertanto il contenuto di una e-mail può essere letto solo dal legittimo destinatario, essendo essa corrispondenza epistolare a tutti gli effetti, anche penali. Ne consegue che in caso di visione o lettura (ma anche soppressione tramite cancellazione) di essa da parte di estranei si applicherà l'art. 616 c.p. sulla violazione della corrispondenza. La segretezza della corrispondenza ha tra l'altro valore di rango costituzionale (ex art. 15 Cost.) e va garantita e tutelata anche per la posta elettronica. Sulla stessa linea d'onda è anche il Garante Privacy (v. Newsletter del 12-18/07/1999) e nel medesimo senso si è già espressa la I Sez. del T.A.R. del Lazio (v. sent. n. 9425/2001, reperibile all'URL <http://www.fiammella.it/Tar%20Lazio%20riservatezza%20e%20mailing%20list.htm>).

³ La massima e il testo integrale della decisione possono essere lette all'URL <http://www.penale.it/page.asp?mode=1&IDPag=381>.

⁴ Si pensi alle ipotesi in cui il lavoratore utilizzi la mail aziendale per intrattenere rapporti epistolari telematici con l'amante o con persone ai lui legate da vincoli di parentela o di amicizia ovvero per effettuare ordinazioni di beni o prodotti acquistabili online etc. Per quel che concerne il caso affrontato dal Tribunale *de quo*, a quanto è dato sapere, il "Key Account Manager" (il responsabile della gestione e del controllo degli accessi logici ai sistemi informatici aziendali, nonché custode delle password e degli altri codici identificativi e di autenticazione informatica), scopri che il lavoratore (successivamente licenziato) aveva inviato messaggi di posta elettronica non autorizzati, contenenti dati ed informazioni riservate di carattere strategico aziendale relativi alla politica commerciale e ai prezzi del proprio settore, a persona non più coinvolta nell'area di sua competenza.

informatico della società stessa di accedere a qualsiasi computer, grazie alla *security-policy* espressamente approvata, resa nota a tutto il personale e conseguentemente adottata⁵.

- **Personalità dell'indirizzo non significa "privatezza"** del medesimo poiché l'indirizzo aziendale – al di là dell'uso di intestazioni apparentemente personali del lavoratore quale principale utilizzatore – proprio in quanto tale, per sua intrinseca natura, può sempre essere *«nella disponibilità di accesso e lettura da parte di soggetti diversi, sempre appartenenti all'azienda, rispetto al suo consuetudinario utilizzatore»* al fine, per esempio, di consentire la regolare continuità della attività aziendale nelle frequenti ipotesi di sostituzioni di colleghi per ferie, malattia oppure gravidanza. Pertanto, *«così come non può configurarsi un diritto del lavoratore ad accedere in via esclusiva al computer aziendale, parimenti non appare astrattamente prospettabile un suo diritto all'utilizzo esclusivo e riservato di una casella di posta elettronica aziendale»*.
- Orbene la mailbox del lavoratore è sì personale, ma non "privata" (i.e. riservata) e il dipendente si espone al rischio che anche altri della medesima azienda – unica titolare del predetto indirizzo – possano lecitamente accedere alla casella in suo uso non esclusivo e leggerne i relativi messaggi in entrata ed in uscita ivi contenuti. E ciò è reso possibile tramite l'uso della "password", la cui conoscenza sia stata in precedenza (legittimamente) acquisita da un collega ovvero dal responsabile dell'ufficio. Finalità di tale chiave d'accesso al sistema infatti non risulta essere (solo) quella di proteggere la segretezza dei dati personali custoditi negli strumenti posti a disposizione del singolo lavoratore, ma (altresi) quella di **impedire che ai suddetti strumenti possano accedere anche persone estranee alla società**⁶.
- Se le affermazioni precedenti sono vere, ne deriva che, in caso di accesso da parte di colleghi o capi-ufficio alla posta elettronica aziendale del dipendente, **non sembra ravvisabile** un elemento essenziale della fattispecie delittuosa di cui all'art. 616 c.p. rappresentato, sotto il profilo oggettivo, dalla **alienità** della corrispondenza medesima, apparendo infatti corretto ritenere che *«i messaggi inviati tramite l'e-mail aziendale del lavoratore (anche se nell'estensione dell'indirizzo compare il nome dello stesso dipendente) rientrano nel normale scambio di corrispondenza che l'impresa intrattiene nello svolgimento della propria attività organizzativa e produttiva e, pertanto, devono ritenersi relativi a quest'ultima, materialmente immedesimata nelle persone che sono preposte alle singole funzioni: le attrezzature, comprese quelle informatiche,*

⁵ In motivazione può infatti leggersi: *«...nel protocollo aziendale relativo alla "Information System Security", pubblicizzato nel 2000, si precisa, tra l'altro, come: "... La strumentazione informatica e quanto con essa creato è di proprietà aziendale in quanto mezzo di lavoro. È 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... Tutti i sistemi... che procurano ed elaborano informazioni e le informazioni stesse sono patrimonio del Gruppo" che si riserva il diritto di ispezionare, esaminare e monitorare in qualsiasi momento e senza avviso alcuno il proprio sistema di comunicazioni elettroniche, ivi compresi i messaggi creati, ricevuti o spediti dal sistema aziendale»*.

Tra l'altro il giudicante, in riferimento alla policy, aggiunge che essa risulta conforme a quanto affermato in materia di riservatezza delle e-mail sin dal Giugno 1999 dal Garante Privacy, 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 già dettato il principio in base al quale 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"*. Pertanto, il lavoratore secondo quanto indicato dal Garante nel parere del 16 Giugno 1999 e soprattutto secondo l'interpretazione autentica dello stesso fornita all'epoca dal segretario generale dell'Autorità Giovanni Buttarelli poteva invocare il diritto alla riservatezza fino a quando il datore di lavoro non avesse chiarito formalmente, mettendolo nero su bianco, che tutti i testi in entrata e in uscita da qualsiasi account interno all'azienda potevano essere resi pubblici in qualsiasi momento.

⁶ Nella stessa ottica, osserva il giudice piemontese, sempre il Garante Privacy, nella Newsletter del 19-25 febbraio 2001, ha riconosciuto il diritto del datore di lavoro di accedere alla posta elettronica rilevando come, conformemente al D.P.R. n. 318/1999 (oggi sostituito dall'Allegato B al D.Lgs. 196/2003, contenente il *"Disciplinare tecnico in materia di misure minime di sicurezza"*): *«Al dipendente deve essere consentito di procedere autonomamente alla sostituzione della parola chiave... previa comunicazione ai soggetti preposti alla custodia delle password. La prescritta comunicazione della sostituzione delle chiavi al personale preposto alla custodia deve essere effettuata con modalità tali... da renderla in casi particolari accessibile da parte dell'azienda... per interventi consentiti dalla legge, come nel caso di assenza o di impedimento del dipendente... 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»*. Lo stesso protocollo aziendale relativo alla "Information System Security", al quale prima si è accennato, prevede che *«... Ogni computer e postazione di lavoro deve essere protetta da password. Il dipendente ha altresì l'obbligo di comunicare la nuova password adottata, e ad ogni sua variazione, in busta chiusa firmata e datata di suo pugno, al suo diretto superiore gerarchico. Questi in caso di emergenza e/o di assenza del lavoratore, avrà diritto di accedere al suo computer ed ai suoi contenuti per esigenze di carattere lavorativo, utilizzando la password comunicata»* e anche di ciò il Tribunale dà conto in motivazione.

devono allora reputarsi direttamente correlate alla funzione del soggetto che nel frangente rappresenta l'impresa e, solo in via mediata, assegnate alla singola persona comunque fungibile nel rapporto col mezzo medesimo».

- Peraltro, a parere del Tribunale, non è accettabile l'assimilazione della posta elettronica a quella tradizionale, con relativa invocazione di un principio generale di segretezza, nelle ipotesi in cui il lavoratore utilizzi lo strumento per fini privati, ossia extralavorativi, posto che **«giammai un uso illecito di uno strumento di lavoro può consentire di attribuire alcun diritto a colui che tale illecito commette».**
- Il giudicante poi cita, a suffragio delle proprie asserzioni, quella dottrina che riconduce la fattispecie dell'accesso alla mailbox aziendale da parte del datore di lavoro alla **causa di giustificazione di cui all'art. 51 c.p.** (scriminante dell'esercizio di un diritto). Dunque, il datore di lavoro, nel prendere conoscenza delle e-mail contenute nella casella di posta elettronica aziendale, non farebbe altro che esercitare una sua legittima facoltà: *«... il capo di un ufficio, al quale ufficio siano dirette corrispondenze d'ogni specie, ha il potere-dovere di aprirle o farle aprire, se chiuse, e di prendere cognizione del loro contenuto, anche se «riservate» e indirizzate, presso l'ufficio medesimo, a singoli impiegati»* (Manzini, *“Trattato di Diritto Penale Italiano”*).
- Infine, conclude il Tribunale, anche ammesso (per assurdo, stanti le ragioni sopra viste) che il dirigente, che ha effettuato l'accesso alla mailbox, possa aver commesso nei confronti del dipendente una illecita intromissione in una sfera personale privata, nondimeno la configurabilità del reato di cui all'art. 616 c.p. dovrebbe egualmente essere esclusa sotto il profilo soggettivo alla luce della **totale mancanza di dolo** nel suo comportamento.
- In conclusione, l'accesso alla casella di posta elettronica operato dal dirigente risulta essere avvenuto **per motivi assolutamente connessi allo svolgimento della attività aziendale**, oltre che in assenza del dipendente, *«in una situazione nella quale non vi era altro modo per accedere a quelle necessarie informazioni e comunicazioni che diversamente se non ricevute ovvero recepite con ritardo avrebbero potuto verosimilmente arrecare un evidente pregiudizio economico e non solo alla società».*

Un fatto simile è già successo in precedenza ed è stato sottoposto all'attenzione di un giudice di Milano (un G.I.P. per la precisione), il quale emanò un'ordinanza di archiviazione divenuta ormai celebre per essere stata la prima decisione in materia di controllo della mailbox aziendale da parte del datore di lavoro. Nel provvedimento, risalente al 10 Maggio 2002⁷, così può leggersi: *«La mailbox aziendale – pur se “personale” (perché assegnata al singolo dipendente che ha un proprio “username” e una propria “password” per accedervi) – deve...essere intesa come semplice “strumento di lavoro”, e nulla più».* Insomma, quando la casella di posta elettronica è messa a disposizione del dipendente da parte del datore di lavoro, perde la sua qualità di strumento di comunicazione segreto o quanto meno riservato e allo stesso modo perdono tale carattere anche i contenuti dei messaggi inviati o ricevuti. Si tratta pertanto di uno strumento di lavoro, che il datore mette a disposizione dei propri dipendenti esclusivamente perché questi ultimi possano svolgere al meglio le loro attività. Ergo il datore avrà sempre libero accesso alla loro mailbox aziendale, in quanto strumento di lavoro che pur sempre resta nella piena disponibilità del datore stesso⁸.

⁷ Il testo integrale è consultabile all'URL <http://www.ictex.net/index.php/2002/05/10/gip-milano-ord-10-maggio-2002/>.

⁸ In senso parzialmente difforme (con riferimento specifico ai colleghi o equiordinati, ma non al datore di lavoro), v. Giudice di Pace di Bari, 7 Giugno 2005 (la sentenza è citata in un interessante articolo a cura di M.Gobbato e S.Tagliabue, dal titolo *“Il controllo dei lavoratori: stato dell'arte alla luce delle pronunce del Grante e della recente”*, reperibile all'URL <http://www.giuristitelematici.it/modules/bdnews/article.php?storyid=692>). In tal caso il giudice ha sanzionato, per violazione della riservatezza della corrispondenza informatica, ai sensi dell'art. 616 c.p., una giornalista colpevole di aver letto il contenuto delle e-mail di un proprio collega durante la sua assenza considerando che *«la posta elettronica dei colleghi in quanto personale, ancorché inserita nel computer aziendale attribuito dall'editore e utilizzato per fini di lavoro, debba considerarsi inaccessibile ancorché non utilmente protetta nel sistema informatico, come dovrebbe essere; a meno che non vi sia l'autorizzazione dell'interessato, che è il solo a sapere se la casella contiene o meno informazioni riservate».*

2. IL DIFFICILE EQUILIBRIO TRA ESIGENZE DI SICUREZZA DEL PATRIMONIO AZIENDALE E TUTELA DELLA PRIVACY DEI DIPENDENTI

È indubbio, anche alla luce della sentenza analizzata nel paragrafo precedente, che al fine di realizzare una efficace e legittima security-policy all'interno di una struttura aziendale o di un'organizzazione, è necessario formalizzare le scelte e gli obiettivi da perseguire, ossia fissarne i principi e i criteri in un documento scritto, la cui conoscenza va diffusa tra il personale interessato. Ciò è indispensabile per conformarsi alla normativa della legge 300/1970, cd. "*Statuto dei lavoratori*", che vieta i controlli occulti e lesivi della dignità e riservatezza del lavoratore, consentendoli invece solo a determinate condizioni e garanzie (in particolare cfr. gli artt. 2, 3, 4 e 6 dello SdL). È dunque il principio di "*trasparenza*" che necessariamente permea di sé le attività di controllo, poste in essere dal datore di lavoro onde assicurare la sicurezza e l'efficienza degli impianti, nonché l'integrità degli strumenti e del patrimonio aziendali.

Un documento siffatto dovrebbe avere un contenuto chiaro, facilmente comprensibile, non equivoco e il più possibile dettagliato per non creare fraintendimenti e per non lasciare nulla al caso. In particolare:

- Vanno anzitutto adempiuti gli indispensabili obblighi inerenti alla normativa in materia di trattamento e protezione dei dati personali dei lavoratori prevista dal D.Lgs. 196/2003, cd. "*Codice della Privacy*" (di seguito, Codice), soprattutto per quel che concerne informativa (art. 13 del Codice), esercizio dei diritti e pronto riscontro al medesimo (art. 7 e s. del Codice), raccolta del consenso (art. 23 e s. del Codice) e adozione delle misure di sicurezza (art. 31 e s. del Codice).
- I vertici aziendali dovranno predisporre un piano adeguato di formazione/informazione/sensibilizzazione dei dipendenti e dei diretti superiori gerarchici degli stessi per quel che pertiene il rispetto almeno dei principi previste dalle normative che, più in generale, si riferiscono alla sicurezza del patrimonio informatico e informativo della struttura, con specifica attenzione:
 - alla legislazione in materia di "*computer-crimes*" (vedasi soprattutto la legge 547/1993);
 - alla normativa in materia di protezione dei dati personali (in particolare, il Codice della Privacy)
 - al rispetto degli obblighi stabiliti dalla legge in tema di sicurezza del lavoro (es. legge 626/1994) e di tutela della dignità e dei diritti fondamentali del lavoratore sul posto di lavoro (es. SdL);
 - alla normativa sulla responsabilità amministrativa delle persone giuridiche in caso di reato commesso dai dipendenti (vedasi D.Lgs. 231/2001 e successive modifiche);
 - alla tutela giuridica del "*digital copyright*" e delle "*banche-dati*" (l. 633/1994 e successive modifiche) e alla normativa in materia di "*file sharing*" (l. 128/2004, cd. "*Legge Urbani*");
 - alla disciplina della concorrenza (es. art. 2125 c.c.);
 - agli obblighi di fedeltà del dipendente (es. artt. 2105 e 2106 c.c.);
 - alla tutela delle informazioni segrete (es. art. 623 c.p. ovvero art. 6-bis del R.D. 1127/1939).

Tutto dovrà avvenire in un clima di collaborazione tra vertici e personale, per garantire trasparenza nei controlli che il datore può predisporre a tutela del patrimonio aziendale, onde prevenire illeciti, e per trovare in tal modo il giusto equilibrio tra le esigenze di privacy del dipendente (rispetto della di lui riservatezza e dignità sul posto di lavoro) e la necessità di assicurare integrità, efficienza, operatività e competitività dell'organizzazione.

Il documento potrà certo prevedere parti che autorizzano capi-ufficio, capi-reparto etc. a effettuare controlli sui dipendenti anche per quel che concerne i contenuti delle mail inviate e ricevute sul posto di lavoro. Orbene, tralasciando, per il momento, tutta la problematica relativa ai controlli datoriali (guardie particolari giurate, personale di vigilanza, videosorveglianza, visite personali di

controllo, controlli sui PC aziendali tramite firewall o proxyfirewall o IDS o IPS, predisposizione di filtri di navigazione etc.), si può tentare di tracciare i "limina" del controllo legittimo sulla mailbox aziendale concessa in dotazione al dipendente. Di seguito le direttrici:

- ❖ Trattandosi di una forma di "controllo elettronico", che potrebbe risultare particolarmente invasivo e talora "occulto", è indispensabile osservare i principi del Codice della Privacy, nonché i dettami del Gruppo dei Garanti europei (cd. **Gruppo di lavoro ex Articolo 29 della direttiva 95/46/CE**) raccolti nel **"Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro"**, adottato il 29/05/2002 e i cui principi sono applicabili a ogni forma di controllo sui computer aziendali. In particolare, il controllo deve essere:
 - **necessario** o meglio indispensabile al perseguimento dei fini per i quali esso è previsto e tale da **ridurre al minimo** l'uso di dati identificativi del dipendente (v. anche art. 3 del Codice)
 - **trasparente** e quindi non occulto. A tal proposito, lo si ribadisce, deve anzitutto essere fornita al lavoratore un'**informativa** preventiva, completa e adeguata ai sensi dell'art. 13 del Codice, che indichi modalità e finalità del controllo e la persona alla quale ci si può rivolgere per esercitare i propri diritti. Indi va raccolto il consenso libero, specifico, espresso e documentato per iscritto⁹ e bisogna comunque adempiere agli altri obblighi previsti *ex lege* o stabiliti dai provvedimenti generali emanati dall'Autorità Garante per la protezione dei dati personali (Garante Privacy)
 - **proporzionato** e dunque pertinente e non eccedente rispetto alle finalità perseguite (v. art. 11, co. 1, lett. d) del Codice). La proporzionalità va riferita in particolare:
 - alla tipologia di dati trattati dal dipendente e alle operazioni effettuate
 - alla tipologia di dati monitorati (ci si dovrebbe per es. limitare ai cd. "*dati di traffico*", senza controllare i contenuti, ma nel caso di una mail spesso ciò potrebbe risultare non sufficiente¹⁰)
 - agli strumenti utilizzati per il monitoraggio e per il tracciamento
 - alle finalità perseguite dal datore/titolare, che devono comunque essere legittime, determinate e trasparenti (art. 11, co.1, lett. b) del Codice): il datore non si può avvalere del personale addetto al controllo o degli strumenti all'uopo predisposti per controllare a distanza l'attività lavorativa, bensì per verificare il corretto uso da parte del dipendente dei mezzi informatici posti a sua disposizione esclusivamente per finalità professionali¹¹
 - alla durata dei tempi di conservazione (art. 11, co.1, lett.e) del Codice)
 - **sicuro** in un duplice significato:
 - non deve porre a rischio l'integrità psico-fisica del dipendente (per es. non deve essere ossessivo o deliberatamente mirato)

⁹ In relazione alla videosorveglianza, ma pur sempre con possibilità di analogia rispetto al controllo elettronico, il Garante ha stabilito, con provvedimento del 29/04/2004 (in particolare v. paragrafo 6.2), che un'ideale alternativa all'esplicito consenso va ravvisata nell'istituto del bilanciamento di interessi (art. 24, comma 1, lett. g), del Codice). Ed in effetti la rilevazione delle immagini può avvenire senza consenso, qualora, con le modalità stabilite nello stesso provvedimento, sia effettuata "*nell'intento di perseguire un legittimo interesse del titolare o di un terzo attraverso mezzi di prova o perseguendo fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, o finalità di prevenzione di incendi o di sicurezza del lavoro*".

Ovviamente il consenso potrà non essere necessario qualora il trattamento dei dati del dipendente avvenga in una delle ipotesi esimenti espressamente previste dall'art. 24 del Codice, come in quelle di cui alle lett. d (esercizio di attività economiche) o f (indagini difensive).

¹⁰ Effettivamente, tramite i dati di traffico, conservati nel cd. "*registro di log*", è possibile identificare la macchina (*workstation*) dalla quale parte il messaggio (potendosi così risalire al nome del dipendente che in quel momento utilizzava la mail), la macchina alla quale è stato spedito (potendosi così verificare se il destinatario è "legittimo" o meno, per es. se rientra tra la lista dei clienti, fornitori etc. oppure no), orario dell'inoltro e della ricezione. D'altro canto, per il caso in cui il dipendente sia assente e sia necessario ai fini della continuità nel business accedere a documenti archiviati nella mailbox, allora non si potrà prescindere anche dal controllo dei contenuti, in quanto materialmente impossibile evitarli e ciò quand'anche il dipendente avesse fatto in modo di gestire la posta per cartelle separate, come pure è tecnicamente fattibile, distinguendo tra posta privata e posta istituzionale.

¹¹ Più in generale gli strumenti di controllo elettronico devono poter migliorare la sicurezza all'interno di edifici o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi, oppure avere lo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del titolare del trattamento o di terzi sulla base di immagini utili in caso di fatti illeciti. V. anche il provvedimento generale sulla videosorveglianza cit. (in esso, al paragrafo 4.1., si afferma tra l'altro che il divieto di controllo a distanza vale anche in caso di erogazione di servizi per via telematica mediante c.d. "*web contact center*".

- i dati raccolti devono essere adeguatamente conservati e protetti da alterazioni, falsificazioni, modifiche non consentite etc. (principio di integrità dei dati ex art. 31 e s. del Codice)

- ❖ Sempre per rispetto ai principi di necessità e proporzionalità, è preferibile effettuare preliminarmente una **selezione del personale** che possa accedere a Internet e che sia fornito di una mailbox aziendale, in entrambi i casi per esclusive finalità lavorative o istituzionali. In tal modo si eviterebbero controlli troppo allargati e penetranti sui dipendenti stessi.
- ❖ Sarebbe opportuno raggiungere un'intesa coi rappresentanti dei lavoratori ai sensi dell'art. 4 SdL¹² (articolo previsto specificamente per la video-sorveglianza, ma estensibile analogicamente anche ai controlli elettronici, ivi inclusi quelli sulla mailbox dei dipendenti), vera e propria "valvola di sicurezza" e casco protettivo per il datore di lavoro, che così potrebbe concordare con le r.s.a. o r.s.u ovvero con la c.i. tipologia, modalità e finalità dei controlli, personale specificamente addetto e autorizzato ai medesimi¹³, tempi minimi e massimi di conservazione dei dati raccolti e monitorati. In tal senso il controllo risulterebbe trasparente, lecito, necessario, proporzionato e teleologicamente giustificato. È possibile anche allegare il documento contenente la policy all'accordo, una volta che sia stato raggiunto e, comunque, è sempre indispensabile (i lettori scuseranno l'insistenza) **fornire ai lavoratori l'informativa sul trattamento dei loro dati a fini di controllo anche a prescindere dall'accordo**, laddove fosse ritenuto non necessario dagli organi apicali (salvo poi contestazione ed eventuale sollevazione della *quaestio* davanti al giudice) o non fosse stato richiesto dai lavoratori stessi.

¹² Si riporta per comodità il testo integrale della disposizione:

«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».

È appena il caso di ricordare che l'art. 114 del Codice della Privacy fa salvo proprio quanto previsto dall'art. 4 SdL in tema di controllo a distanza del lavoratore e inoltre l'art. 171 del Codice prevede che la violazione dell'art. 114 cit. venga punita con le sanzioni di cui all'art. 38 dello SdL.

Sull'importanza del rispetto dell'art. 4 SdL al fine di rendere legittimo il controllo datoriale sui PC aziendali per finalità di sicurezza (nel caso di specie, trattavasi di registro di log, in cui erano stati archiviati i dati relativi alla navigazione in rete dei lavoratori), v. Tribunale di Perugia, 19 Maggio 2006, riportata nell'articolo a cura di M.Gobbato e S.Tagliabue cit. Con la stessa sentenza il giudice ha peraltro stabilito come il licenziamento fosse da ritenersi sanzione disciplinare eccessiva a seguito della verifica di un comportamento scorretto del dipendente per l'abuso di internet sul luogo di lavoro, posto che tale atteggiamento non è stato in grado di determinare un calo di rendimento del lavoratore o un danno diretto al suo datore di lavoro. Sempre in riferimento ad eventuali eccessi, sulla possibilità e tollerabilità di un "uso minimo extralavorativo" della mail da parte del dipendente si era espressa l'ordinanza del G.I.P. di Milano cit. senza che tuttavia ne sia mutata la natura di mezzo di comunicazione con colleghi e clienti. In sostanza, il dipendente può anche utilizzare la casella di posta elettronica per comunicazioni personali, a condizione che si tratti di un uso, appunto, "minimo" e non tale da cambiare la natura dello strumento o influire sul corretto adempimento delle sue mansioni. In tal senso v. anche T.Solignani, in *"Leggi e provvedimenti che regolano l'utilizzo della posta in azienda"*, consultabile all'URL http://www.distrettopmi.it/01NET/HP/0,1254,5_ART_62975,00.html.

¹³ Tale personale va designato per iscritto ai sensi dell'art. 30 del Codice della Privacy, considerando che l'attività di controllo costituisce comunque trattamento di dati personali (del dipendente, nella fattispecie) e pertanto ogni singolo "controllore" acquisirà la qualifica di "incaricato del trattamento". Deve trattarsi di un numero molto ristretto di soggetti (principio di proporzionalità), a fortiori quando ci si avvale di una collaborazione esterna. Anzi in tal caso, trattandosi di trattamento externalizzato, cd. in *"outsourcing"*, è necessario rispettare le disposizioni dell'Allegato B, in particolare:

- la Regola 19.7, che stabilisce che nel D.P.S. va effettuata la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- la Regola 25, che prescrive invece l'obbligo per il titolare, che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, di farsi rilasciare dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

In riferimento ai cd. “*custodi delle password*” o “*Key Access Manager*”, già il giudice piemontese, nella sentenza sopra analizzata, ha chiarito che tali figure sono pienamente legittime e come tali hanno il pieno diritto di accedere alla mailbox aziendale, una volta approvata, resa manifesta al personale e adottata la security policy (presente o meno l'accordo ex art. 4 Sdl).

Inoltre, il Punto o Regola 10 dell'Allegato B al D.Lgs. 196/2003 (e ciò non sfugge al giudice piemontese) recita come segue:

« Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante 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 tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.»

La disposizione merita un breve commento. Il Titolare deve **dettare per iscritto** apposite istruzioni (o modalità operative) per le ipotesi di impedimento o di assenza (per qualsivoglia motivo e di qualsiasi durata, non necessariamente prolungata, come si vedrà) dell'incaricato, affinché le copie delle credenziali (generate preventivamente proprio per tali evenienze) siano custodite in modo tale da garantirne la segretezza e da individuare (sempre preventivamente) i soggetti incaricati della custodia e autorizzati a operare il trattamento di dati. Essi a loro volta provvederanno ad informare (*ex post* e cioè ad intervento effettuato) l'incaricato assente o impedito. Tale misura va presa nei casi in cui l'accesso al sistema sia possibile esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione (è proprio il caso della password). Naturalmente tramite le istruzioni scritte, di cui sopra, dovrà essere garantito l'accesso sia ai dati (es. per singoli files, come quelli archiviati nella mailbox...) sia agli strumenti (es. per il funzionamento della macchina come le PW per il *boot* o *bios* etc.). L'impedimento e l'assenza dell'incaricato rilevano, è vero, come presupposti per l'attuazione della regola di cui al Punto 10, ma va altresì valutata la **assoluta necessità (indispensabilità) e tempestività (indifferibilità) dell'intervento in relazione a esigenze operative e di sicurezza**. Quanto alle esigenze di sicurezza, nulla quaestio, in quanto un intervento potrebbe essere assolutamente richiesto in caso di pericoli o minacce alla riservatezza, integrità o disponibilità dei dati di uno o più interessati (per necessità, dunque, di tutelarne i diritti) ovvero al funzionamento dei sistemi. Quanto invece alle esigenze operative, l'espressione va intesa *strictu sensu*, onde evitare di giustificare un qualsivoglia intervento, anche quando non assolutamente necessario. Ed allora non v'è dubbio che, nell'individuare tali esigenze, bisognerà bilanciare interessi contrapposti quali:

- la **libertà d'iniziativa economica** del Titolare (art. 41 Cost.);
- i **limiti a tale diritto costituzionalmente garantito** (art. 41, co.2 Cost., con particolare riferimento alla libertà e alla dignità umana).

Proprio tale bilanciamento dovrebbe essere oggetto dell'accordo tra datore di lavoro/Titolare e associazioni sindacali rappresentative dei lavoratori sulla base del modello di concertazione previsto ex art. 4 SdL.

Dalle considerazioni suddette può tra l'altro inferirsi che la valenza temporale dell'impedimento o dell'assenza (la disposizione che si sta analizzando prevede che essa sia "prolungata") non è decisiva al fine di predisporre le misure richieste dal Punto 10, poiché anche nel caso di un'assenza di breve durata possono verificarsi circostanze gravi tali da rendere assolutamente necessario e tempestivo l'intervento (avendo presenti le esigenze di cui sopra, quelle sì veramente determinanti).

In conclusione sono dunque leciti interventi da parte del datore di lavoro (titolare del trattamento) sia sui dati che sugli strumenti elettronici in presenza di *"indispensabili ed indifferibili necessità di operatività e di sicurezza del sistema"*, tra le quali si fa rientrare, a mo' d'esempio, l'accesso alla casella di posta elettronica aziendale di un dipendente assente per malattia purché il singolo utente-lavoratore sia debitamente informato in via preventiva della suddetta procedura.

3. DALL'USO "CORRETTO" ALL'USO "SICURO" DELLA MAILBOX AZIENDALE

Quanto sopra detto, attiene all'uso corretto, leale e fedele della mailbox aziendale da parte del dipendente. Altro problema è invece l'uso "sicuro" della medesima, considerando che l'uso della mail spesso reca seco minacce non da poco per l'intergrità e il funzionamento del sistema informatico utilizzato e per i dati e le informazioni in esso trattati e conservati.

Così, in riferimento a specifici rischi connessi all'uso della posta elettronica, anche al fine di agevolare le attività dei dipendenti (es. scarico e lettura delle mail e degli allegati, archiviazione, risposta, inoltro, eliminazione etc.), all'interno del documento contenente la security-policy aziendale, sarebbe opportuno prevedere (e, di conseguenza, adottare) le seguenti misure:

- tra gli interventi formativi da prevedere e inserire nel contenuto del D.P.S. (cfr. la Regola 19.6 dell'Allegato B), andrebbero programmati, previsti ed effettuati anche quelli per il personale addetto all'uso della mail aziendale, per renderlo edotto dei rischi correlati all'uso dell'e-mail, delle contromisure da attuare, delle relative responsabilità (civili e penali) e degli aspetti più rilevanti della normativa in tema di *"data protection"*;
- tra le contromisure più efficaci da prevedersi nella policy (e anche nel D.P.S.) si possono indicare, a titolo esemplificativo, le seguenti:
 - non "aprire" (i.e., mandare in esecuzione) gli *"attachment"* o allegati alle mail ricevute da persone sconosciute o che presentino un oggetto sospetto o in lingua straniera ovvero accattivante, intrigante o provocatorio;
 - anche nel caso in cui una mail contenente l'allegato provenga da persona nota, nel dubbio chiedere sempre conferma telefonica a chi invia il messaggio¹⁴;
 - non cliccare sui *link* presenti nel corpo della mail, dal momento che basta questa semplice operazione (senza la necessità di aprire allegati) per attivare codici maligni di nuova concezione, siano essi *trojan, dialer, bot, backdoor, rootkit* etc.;
 - limitare l'uso di *client* di posta elettronica come *Outlook Express*, dal momento che un malware può diffondersi anche senza allegato, semplicemente sfruttando il supporto *"HTML"* che viene usato proprio da questi software di gestione della posta elettronica¹⁵;
 - predisporre software o dispositivi in grado di effettuare lo *"screening"* preventivo (i.e. prima che vengano aperti o mandati in esecuzione) degli allegati di posta elettronica; talora a tali scopi potrebbe essere sufficiente anche un *firewall* ben configurato ovvero uno *"screening router"*, che blocchino la ricezione (e l'invio) di allegati dall'estensione sospetta (es. *.exe, .com, .dll, .asx, .wms, .wmz* etc.);
 - fare molta attenzione ai falsi allarmi e ai messaggi che avvisano di procedure urgenti da seguire per cambiare la propria password: potrebbe trattarsi di *"phishing"* o di altri tentativi di attacchi fraudolenti o truffaldini tipici della *"social engineering"*¹⁶;

¹⁴Anche in tali casi la prudenza non è mai troppa, dal momento che molti *backer* o *virus-writer* o *phisher* sono talmente abili da falsificare l'indirizzo di provenienza (tecnica di *"spoofing"*, da *to spoof*, ingannare).

Senza obliare poi che una mail può essere inviata in automatico (e all'insaputa del legittimo utilizzatore) da un computer che sia stato precedentemente infettato da un worm o da un trojan. Infatti molti di questi malware sono in grado di raccogliere gli indirizzi e-mail presenti nella rubrica dei client di posta (es. Outlook, Eudora etc.) o nel *"WAB"* (*Windows Address Book*) per poi autospedirsi in allegato, talora realizzando veri e propri attacchi di *mass-mailing* e *mail-bombing*.

¹⁵ Infatti tramite il linguaggio HTML basta anche solo leggere, anzi visionare, la pagina infettata di una mail ricevuta perché il proprio PC ne venga contagiato. Se è proprio necessario usare il client di posta, allora è buona norma eliminare l'anteprima, nella quale per l'appunto appare la posta scaricata in automatico.

¹⁶ In tali casi dunque è indispensabile chiedere sempre conferma dell'esistenza e della veridicità dell'avviso all'amministratore di rete o di sistema.

- non inoltrare falsi allarmi, *"hoax"* e *"catene di Sant'Antonio"*;
- predisporre "filtri" anti-spamming.

Spesso in soccorso della persona, laddove non arriva la sicurezza informatica, arriva il buonsenso!
