Riservatezza. Un «disciplinare» in ogni azienda, pubblica e privata, sull'uso di internet e posta elettronica

Computer sorvegliati speciali

Resta il divieto assoluto degli strumenti finalizzati al controllo a distanza

Quando e come il datore di lavoro può controllare l'utilizzo delle e-mail e dell'accesso alla rete Internet da *parte dei* dipendenti? Con il provvedimento generale del 1° marzo scorso, l'autorità garante per la protezione dei dati personali fornisce finalmente le indicazioni, anche pratiche, per una corretta gestione di questi strumenti, rispondendo così alle numerose richieste di chiarimento sull'interpretazione dei limiti posti dalla normativa vigente ai controlli aziendali. Il problema, afferma il Garante, è quello di conciliare l'esigenza di tutela della privacy del lavoratore e il potere/dovere dei datori di lavoro di assicurare la funzionalità e il corretto impiego degli strumenti informatici da parte dei lavoratori nonché l'obbligo datoriale di adottare le misure minime di sicurezza imposte dal Codice per la privacy per garantire la disponibilità e l'integrità dei sistemi informativi e dei dati.

Le premesse

Ogni volta che il datore di lavoro effettua, anche lecitamente, un *controllo sul corretto utilizzo* nel rapporto di lavoro della posta elettronica e della connessione Internet aziendale, pone comunque in essere un trattamento di dati personali del lavoratore. Che, in omaggio al principio di correttezza sancito dal Codice per la privacy, deve essere ispirato a un criterio di trasparenza. Ciò, concretamente, comporta due obblighi:

❶ indicare in modo chiaro ai lavoratori quali siano le corrette modalità di utilizzo degli strumenti informatici aziendali e se, in che misura e con quali modalità, vengano effettuati dei controlli;

❷ fornire idonea e preventiva informativa sulle finalità del trattamento dei dati raccolti nell'ambito dei controlli (articolo 13 del Codice).

Tutti i datori di lavoro devono adottare un regolamento aziendale, o *policy*, o, per dirla con il Garante, un «disciplinare» (si veda la scheda in basso) che dovrà essere portato a conoscenza dei dipendenti con le stesse modalità previste dalla legge per la pubblicità del codice disciplinare (affissione in un luogo accessibile a tutti i dipendenti). Ma ai fini della legittimità dei controlli la policy non basta. Come afferma il Garante, ai fini della tutela della privacy del lavoratore, occorre riferirsi alla normativa introdotta dal Codice del 2003 (Dlgs n.196/2003) e a quella, più stringente, dello Statuto dei lavoratori (legge n. 300/70).

Controlli a distanza

Resta fermo, per il datore, il divieto assoluto di utilizzare strumentazioni hardware e software mirate al controllo a distanza dell'attività lavorativa (lettura e registrazione sistematica dei messaggi di postaelettronica, riproduzione e memorizzazione sistematica delle pagine web visualizzate, lettura e registrazione dei caratteri inseriti tramite la tastiera o, ancora, analisi occulta dei computer portatili affidati in uso). È ammesso, invece, l'utilizzo di sistemi informativi in presenza di determinate esigenze produttive o organizzative o, comunque, per ragioni di sicurezza sul lavoro, che consentano indirettamente o anche solo potenzialmente un controllo a distanza dei lavoratori, a condizione che venga rispettata la procedura richiesta dall'articolo 4 dello Statuto dei lavoratori: un accordo con le rappresentanze sindacali aziendali per l'installazione di tali strumenti o, in mancanza, l'autorizzazione dal servizio ispettivo del lavoro.

Il percorso guidato

Le prescrizioni del Garante con il provvedimento del 1° marzo 2007 riguardano sia i datori di lavoro privati che i datori di lavoro pubblici. Per illustrare i nuovi obblighi nonchè le norme che i datori di lavoro sono chiamati già a rispettare in base a Statuto dei lavoratori e Codice della privacy, nelle due pagine che seguono sono schematizzati gli adempimenti principali delle imprese dal momento dell'assunzione del lavoratore allo svolgimento del rapporto di lavoro, fino alla fase, eventuale, d'adozione di una sanzione disciplinare. L'ultima pagina del Dossier ripercorre le principali pronunce della giurisprudenza e approfondisce i termini dell'uso «personale» consentito al dipendente sulla posta elettronica e su Internet.

www.ilsole24ore.com/
Le linee guida del Garante

TESTI DI
Aldo Bottini
DOSSIER A CURA DI
Francesca Padula

La difesa

5 giorni
Per giustificarsi
In caso di procedimento disciplinare (contestazione scritta da parte del datore), il lavoratore ha cinque giorni di tempo per fornire giustificazioni

@aziendale
L'alternativa
Il regolamento aziendale può prevedere l'adozione di account condivisi tra più dipendenti (ad esempio, ufficiomarketing@nomeazienda.it) con eventuale eliminazione dell'account personale del dipendente

WP55
I Garanti europei
Il documento adottato il 29 maggio 2002 (noto come WP 55) e al quale il provvedimento del Garante italiano si ispira

Un regolamento per tutti i dipendenti

La tecnologia che evita attività *improprie*

Gli strumenti tecnologici

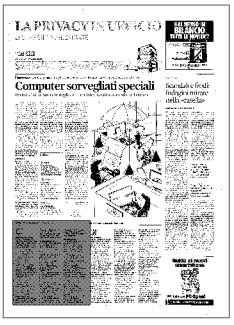
■ Con il provvedimento del 1° marzo 2007 il Garante prescrive, nei confronti dei datori di lavoro che assegnino in dotazione ai propri dipendenti un account di posta elettronica aziendale e un accesso a Internet, l'adozione di misure di tipo tecnologico per prevenire un utilizzo scorretto e, di conseguenza, la necessità di controlli e di sanzioni.
Si tratta, in particolare, di tecnologie finalizzate alla riduzione dei casi di raccolta di dati riferibili al lavoratori o, comunque, di dati identificativi (*Privacy Enhancing Technologies o PETs*). Queste misure rispondono a un principio di necessità del trattamento — sancito dall'articolo 3 del Codice per la protezione dei dati personali — per cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possano essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che consentano di identificare l'interessato solo, appunto, in caso di necessità. Nel provvedimento, queste misure sono distinte a seconda dello strumento informatico utilizzato.

Navigazione in Internet

■ Le misure vengono individuate:
❶ nella selezione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa;
❷ nella configurazione di sistemi o nell'utilizzo di filtri che prevengano determinate operazioni;
❸ nel trattamento di dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni;
❹ nell'eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;
❺ nella graduazione dei controlli. Su quest'ultima misura, il Garante insiste sull'opportunità di procedere, in via preliminare, a controlli su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree, e dunque a un controllo "anonimo" che si concluda con un avviso generalizzato relativo al rilevato utilizzo anomalo degli strumenti aziendali. In assenza di successive anomalie, non sarebbero giustificati controlli su base individuale.

Posta elettronica

■ Rispetto all'utilizzo della posta elettronica, le misure tecnologiche da adottare sono:
a) la messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio: ufficiovendite@nomeazienda.it), eventualmente affiancandoli a quelli individuali;
b) l'eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;
c) la messa a disposizione di apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta contenenti riferimenti utili per contattare altri soggetti dell'organizzazione presso cui opera il lavoratore assente;
d) la nomina da parte del lavoratore di un collega, "fiduciario", autorizzato a controllare le sue e-mail in caso di assenze improvvise o prolungate;
e) l'inserimento nelle e-mail di avvisi circa la natura non personale del messaggio;
f) la graduazione dei controlli.


LA PRIVACY IN UFFICIO
Computer sorvegliati speciali

Un regolamento per tutti i dipendenti

Le informazioni

■ Il provvedimento del Garante contiene importanti indicazioni sul contenuto della *policy* (o procedura aziendale) di cui i datori di lavoro devono dotarsi per verificare il corretto utilizzo della posta elettronica e di Internet da parte dei lavoratori. Con la policy, il datore di lavoro dovrà fornire ai propri dipendenti essenzialmente tre informazioni: quali siano le corrette modalità di utilizzo degli strumenti informatici aziendali, se e come verranno effettuati i controlli, quali sono le sanzioni in caso di utilizzo scorretto. In particolare, si legge nel Provvedimento, nel regolamento dovrà essere indicato:

❶ quali siano i comportamenti «non tollerati» rispetto alla navigazione in Internet (ad esempio, potrebbe non essere consentito il download di software o file musicali oppure la tenuta di file nella rete interna);

❷ in quale misura sia consentito utilizzare anche per ragioni personali i servizi di posta elettronica o di rete;

❸ quali informazioni vengano memorizzate temporaneamente dal sistema (ad esempio, le componenti di file di log eventualmente registrati) ed i soggetti autorizzati ad accedervi (ad esempio, l'amministratore di sistema);

❹ se e quali informazioni siano eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche tramite copie di back up, gestione tecnica di rete o file di log). Il Garante precisa come un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione: a particolari esigenze tecniche o di sicurezza, all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria. In assenza di queste specifiche circostanze, i dati devono essere conservati solo per il tempo strettamente necessario al perseguimento delle finalità per le quali sono raccolti.

■ La policy deve anche prevedere:

❺ se e in quale misura verranno effettuati controlli, anche occasionali, in conformità alla legge (e cioè nel rispetto della procedura richiesta dall'articolo 4, comma 2, dello Statuto dei Lavoratori), indicando le ragioni legittime e specifiche per cui verranno effettuati;

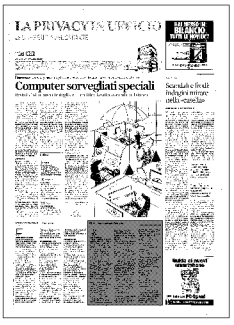
❻ in quali conseguenze, anche di tipo disciplinare, incorra il dipendente che utilizzi indebitamente la posta elettronica o la rete Internet aziendale;

❼ le modalità con cui sarà garantita, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso, con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;

❽ se siano state attivate modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato;

❾ quali particolari misure siano state adottate per la tutela del segreto professionale cui siano eventualmente tenuti i lavoratori;

❿ le prescrizioni interne sulla sicurezza dei dati e dei sistemi (vale a dire le misure di sicurezza adottate dal datore di lavoro in ottemperanza agli obblighi previsti dal Codice per la protezione dei dati personali).


LA PRIVACY IN UFFICIO
Computer sorvegliati speciali

02-APR-2007 Il Sole 24 ORE da pag. 37
Quotidiano Milano Direttore: Ferruccio de Bortoli Lettori Audipress 1242000

ANALISI

Scandali e frodi: indagini mirate nella «casella»

di **Bruno Cova** e **Francesca Petronio***

La vigilanza sui dipendenti (e, in particolare, il controllo delle e-mail aziendali) rappresenta un tema nel quale si intersecano aspetti di diritto del lavoro e di privacy e ulteriori profili di diritto penale. Ma anche uno degli altri grandi temi giuridici di attualità, quello dei controlli interni. Da un lato, infatti, l'imprenditore è tenuto a garantire il diritto alla riservatezza anche sul luogo di lavoro e a rispettare, a tal fine, le prescrizioni imposte dallo Statuto dei lavoratori e dalla disciplina in materia di privacy; dall'altro, e allo stesso tempo, l'imprenditore è chiamato a prevenire il rischio di frodi e illeciti compiuti all'interno dell'azienda e a porre in essere adeguati sistemi di vigilanza e controllo al fine di reprimere gli stessi.

I recenti scandali finanziari che hanno coinvolto alcune tra le maggiori imprese italiane e mondiali hanno scoperchiato un vaso di Pandora, mettendo in luce le falle dei sistemi di controllo interno e inducendo le imprese a un'attenta riflessione sull'importanza dell'adozione di efficaci strumenti di prevenzione e repressione dei *wrongdoings* all'interno dell'azienda. Il problema non è solo teorico e non riguarda solo i casi più famosi assurti ai disonori della cronaca, se si pensa che da una survey pubblicata da PricewaterhouseCoopers nel 2005 emerge che circa il 25% delle aziende italiane ha subito frodi e che quasi la metà delle frodi di cui sono state vittime le imprese italiane è stata commessa da personale interno all'azienda.

Anche per le aziende italiane è diventato quindi di impellente necessità rafforzare il proprio sistema di controlli (sul modello delle imprese statunitensi, che a oggi continuano a dettare le best practice in materia) al fine di prevenire e reprimere la commissione di illeciti che possono depauperare il patrimonio aziendale, esporre l'impresa a un rischio reputazionale o, addirittura, nel caso dei reati previsti dal Dlgs 231/2001, a una concorrente responsabilità. Vale qui la pena di ricordare che proprio il Dlgs 231 richiede espressamente all'impresa di predisporre e implementare *compliance programmes* atti alla prevenzione dei crimini e, nel contempo, di istituire uno specifico organismo («organismo di vigilanza») deputato a vigilare sull'attuazione dei predetti modelli e sulla conformità alle norme della condotta del personale.

È evidente che, in questo contesto, il controllo delle e-mail aziendali del personale coinvolto nella commissione degli illeciti (effettuato tramite una ricerca mirata e l'utilizzo di parole chiave), rappresenta uno dei più validi strumenti di indagine nell'ambito delle investigazioni che le imprese "vittime" di frodi spesso intraprendono (internamente o con l'ausilio di consulenti esterni) al fine di verificare la commissione della condotta illecita, di delinearne i contorni e di prendere i più opportuni provvedimenti al fine di porvi rimedio.

Nel ruolo di consulenti in molteplici investigazioni interne abbiamo, infatti, potuto accertare che spesso l'e-mail viene percepita e utilizzata dal titolare della casella di posta elettronica come un surrogato della comunicazione "orale" e che per questo motivo, proprio le e-mail contengono a volte delle vere *smoking guns*.

Ciò detto, seppure l'esigenza del datore di condurre investigazioni interne al fine di reprimere la commissione di illeciti debba ritenersi senza dubbio meritevole di tutela, ciò non autorizza l'imprenditore (nemmeno in presenza di frodi) a gestire l'azienda come l'Oceania del noto romanzo di Orwell, dovendo l'esigenza di autotutela sempre essere contemperata, nel caso in cui si acceda a dati personali, con il rispetto dei principi di necessità, correttezza, finalità, determinatezza e proporzionalità e, come evidenzia il Garante, delle linee guida dallo stesso dettate.

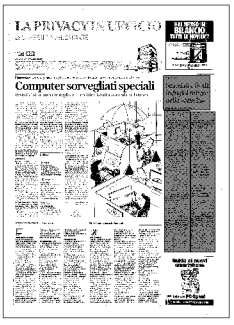
* *Studio Paul, Hastings, Janofsky & Walker (Europe) LLP Milano*

IMPRESE «VITTIME»

Le investigazioni sul personale coinvolto in fatti illeciti passano tramite ricerche ad hoc con parole chiave

La modalità di accesso dev'essere proporzionata e rispettare i principi di necessità, correttezza e finalità

DATI PERSONALI


LA PRIVACY IN UFFICIO
Computer sorvegliati speciali

02-APR-2007 Il Sole 24 ORE da pag. 38
Quotidiano Milano Direttore: Ferruccio de Bortoli Lettori Audipress 1242000

Un «patto» per usare il pc aziendale senza abusi né trappole

Il percorso corretto inizia dal consenso all'assunzione e prevede la massima pubblicità del regolamento ad hoc su posta e internet

La privacy in ufficio

LE LINEE GUIDA DEL GARANTE

La prima informativa. Quali dati personali vanno forniti e quali possono essere trattati

Dall'Authority. L'autorizzazione generale vale fino a giugno 2007 salvo proroga

La «policy». Obbligo del disciplinare interno su comportamenti ammessi e non tollerati

La tecnologia. Si chiama PETs e riduce la raccolta delle informazioni identificative

Necessità produttive. Controlli a distanza se concordati con rappresentanze sindacali

AL MOMENTO DELL'ASSUNZIONE

INFORMATIVA
ex articolo 13, Dlgs 30 giugno 2003, n. 196

Sul trattamento dei dati personali il lavoratore deve essere informato su:

- finalità e modalità del trattamento cui i dati sono destinati
- natura obbligatoria o facoltativa del conferimento dei dati
- conseguenze di un eventuale rifiuto di rispondere
- soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati del trattamento
- eventuale ambito di diffusione dei dati medesimi
- diritti dell'interessato di cui all'articolo 7, Dlgs n. 196/2003
- estremi identificativi del «Titolare» e, se designato, del «Responsabile» del trattamento

CONSENSO DEL LAVORATORE*

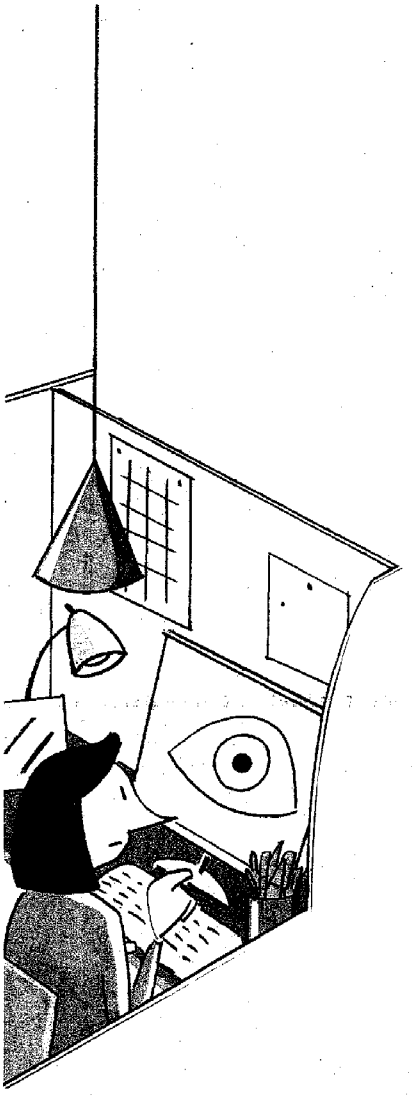
DATI COMUNI

non è richiesto quando:
- il trattamento è necessario per adempiere a un obbligo di legge
- è necessario per eseguire obbligazioni derivanti dal contratto di lavoro
- è necessario per far valere o difendere un diritto in sede giudiziaria

DATI SENSIBILI

non è richiesto quando:
- il trattamento è necessario per far valere o difendere un diritto in sede giudiziaria
- il trattamento è necessario per adempiere a specifici obblighi o compiti previsti dalla legge per la gestione del rapporto di lavoro

(*) in forma scritta se si tratta di dati sensibili



AUTORIZZAZIONE DEL GARANTE

TRATTAMENTO DEI DATI SENSIBILI

- Le disposizioni del Codice della privacy che prevedono un'autorizzazione del Garante sono applicate anche mediante il rilascio di autorizzazioni relative a determinate categorie di titolari o di trattamenti, pubblicate nella Gazzetta Ufficiale della Repubblica italiana

AUTORIZZAZIONE GENERALE

- Autorizzazione Generale del Garante del 21 dicembre 2005, n. 1/2005 al trattamento dei dati sensibili nei rapporti di lavoro (pubbl. in G.U. n. 2 del 3.1.2006-Suppl. Ord. n. 1)
- Efficace a decorrere dal 1° gennaio 2006 fino al 30 giugno 2007, salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.

LE NOVITÀ PER E-MAIL E INTERNET

PROVV. GARANTE 1° MARZO 2007

DISCIPLINARE INTERNO (O POLICY)

CONTENUTO

- comportamenti non tollerati rispetto alla navigazione in Internet (ad. es. download di software o file musicali) oppure alla tenuta di file nella rete interna
- eventuali modalità di utilizzo anche per ragioni personali dei servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle ricorrendo a sistemi di webmail, con indicazione dell'arco temporale di utilizzo (ad esempio, fuori dell'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro)
- informazioni memorizzate temporaneamente (ad es. componenti di file di log eventualmente registrati) e soggetti autorizzati ad accedervi (anche dall'esterno) legittimamente
- informazioni eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di back up, della gestione tecnica della rete o di file di log)
- eventuali modalità di effettuazione di controlli, anche saltuari o occasionali, da parte del datore di lavoro in conformità alla legge, con indicazione delle ragioni legittime - specifiche e non generiche - per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e con precisazione dell'eventuale inoltro, in caso di abusi singoli o reiterati, di preventivi avvisi collettivi o individuali e dell'eventuale svolgimento di controlli nominativi o su singoli dispositivi e postazioni
- conseguenze, anche di tipo disciplinare, dell'utilizzo indebito di posta elettronica e Internet
- soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata) con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti
- eventuali modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato
- misure adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale
- prescrizioni interne sulla sicurezza dei dati e dei sistemi

MISURE DI TIPO TECNOLOGICO (PET'S)

NAVIGAZIONE INTERNET

- individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni
- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni
- eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità *organizzative, produttive e di sicurezza*
- graduazione dei controlli

UTILIZZO DELLA POSTA ELETTRONICA

- messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali
- eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;
- messa a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, di apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le coordinate di altro soggetto o altre utili modalità di contatto dell'istituzione presso la quale opera il lavoratore assente
- consentire che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa - redazione di apposito verbale dell'intervento e informazione al lavoratore interessato alla prima occasione utile
- inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;
- graduazione dei controlli

ARTICOLO 4, STATUTO DEI LAVORATORI

ACCORDO CON RSA O AUTORIZZAZIONE SERVIZIO ISPETTIVO DEL LAVORO

- Per utilizzo di sistemi informativi, che consentano indirettamente un controllo a distanza dell'attività lavorativa, per esigenze produttive, organizzative o comunque di sicurezza del lavoro
- divieto di effettuare trattamenti di dati mediante sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire l'attivita' dei lavoratori

ESEMPIO

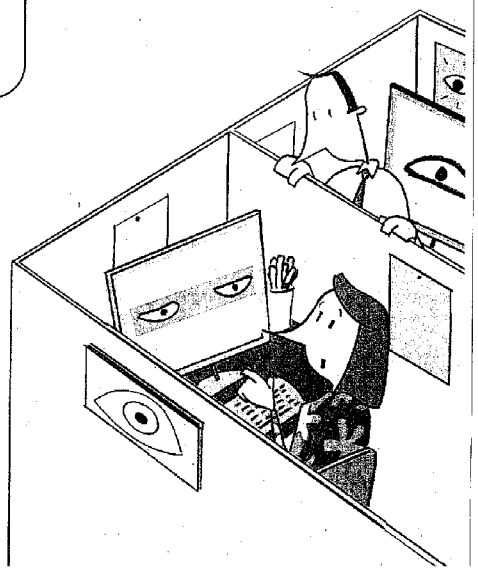
- lettura e registrazione sistematica delle e-mail, al di là di quanto necessario per il servizio o riproduzione e memorizzazione sistematica delle pagine web visitate dal lavoratore

PROCEDIMENTI DISCIPLINARI

ARTICOLO 7, STATUTO DEI LAVORATORI

- Integrazione del codice disciplinare con infrazioni connesse all'utilizzo di Internet e dell'e-mail aziendale e relative sanzioni applicabili
- Affissione del codice disciplinare (così integrato) in un luogo accessibile a tutti
- Contestazione per iscritto dell'eventuale addebito disciplinare che deve essere specifica e tempestiva
- Le giustificazioni del lavoratore destinatario devono essere fornite entro un termine di cinque giorni dalla ricezione della contestazione disciplinare in forma verbale o scritta. Il lavoratore può farsi assistere da un rappresentante sindacale
- Irrogazione di una sanzione proporzionata all'infrazione: biasimo scritto, multa, sospensione dal servizio e dalla retribuzione, fino al licenziamento
- In ogni caso, onere del datore di lavoro di attendere detto termine di cinque giorni dalla ricezione, da parte del lavoratore, della contestazione prima di irrogare l'eventuale sanzione

- Utilizzo dei dati personali di tipo sensibile del lavoratore (ad esempio convinzioni religiose, opinioni politiche, stato di salute e vita sessuale) solo se indispensabili ai fini della specificità della contestazione
- Autorizzazione del Garante n.1/2005 al trattamento dei dati sensibili nei rapporti di lavoro. Si tratta di un'autorizzazione che riguarda in generale tutti i datori di lavoro privati, e che è valida fino al 30 giugno 2007 salvo proroghe



02-APR-2007 Il Sole 24 ORE da pag. 40
Quotidiano Milano Direttore: Ferruccio de Bortoli Lettori Audipress 1242000

Ammessa la caccia agli illeciti

Controlli «difensivi» secondo le decisioni della giurisprudenza

La privacy in ufficio

LE LINEE GUIDA DEL GARANTE

Le verifiche. Possono essere giustificate da un concreto pericolo per il patrimonio

Tutela dell'azienda. Le condotte scorrette mettono a rischio i rapporti con l'esterno

Le linee guida del Garante sull'uso della posta elettronica e della rete Internet aziendale incideranno, probabilmente in senso restrittivo, sull'interpretazione dell'articolo 4 dello Statuto dei lavoratori fino a oggi fornita dalla giurisprudenza italiana.

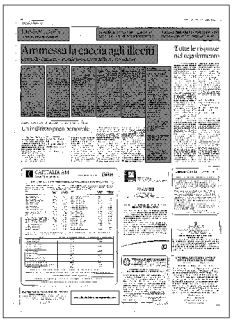
PROGRAMMI INFORMATICI
Il monitoraggio a distanza di posta e internet è equivalente a quello sui contatti telefonici

La norma dello Statuto stabilisce un divieto assoluto per i datori di lavoro di utilizzare impianti audiovisivi e altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. La stessa norma consente, invece, l'installazione di impianti e apparecchiature giustificata da ragioni organizzative o produttive o di sicurezza del lavoro — anche se ne derivi la possibilità di un controllo a distanza dell'attività del lavoratore — a condizione, però, che sia concordata con le rappresentanze sindacali aziendali o, in mancanza, sia autorizzata dal servizio ispettivo del lavoro.

Per il Garante non c'è dubbio che i sistemi hardware e software idonei al controllo, anche solo potenziale e discontinuo, dell'attività lavorativa rientrino tout court tra le apparecchiature cui si riferisce lo Statuto dei lavoratori. In questo modo l'Autorità s'allinea alle più recenti sentenze della giurisprudenza di merito secondo cui «i programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi ad Internet sono necessariamente apparecchiature di controllo nel momento in cui, in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e in via continuativa durante la prestazione, l'attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento». Perciò «qualora il datore di lavoro (...) effettui il controllo dei collegamenti e dei siti Internet in via continuativa mediante strumenti informatici centralizzati non accessibili al lavoratore e conservi la registrazione dei dati per un certo periodo, si debba ritenere l'applicabilità dell'articolo 4 statuto dei lavoratori» (Corte d'appello di Milano, sezione lavoro, 30 settembre 2005, n. 668). Non ricadono, invece, nel campo d'applicazione di questa stessa norma i controlli cosiddetti «difensivi», cioè diretti ad accertare condotte illecite dei lavoratori. Sono, invero, numerose le pronunce di merito in tal senso (da ultimo, una sentenza del Tribunale di Teramo 12 maggio 2006; un'ordinanza del Tribunale di Perugia del 2 febbraio 2006), tutte aderenti al noto principio affermato dalla Suprema Corte, secondo cui «devono ritenersi certamente fuori dall'ambito di operatività della norma sopra citata (articolo 4, statuto dei lavoratori) i controlli diretti ad accertare condotte illecite del lavoratore (...) quali, ad esempio, (...) gli apparecchi di rilevazione di telefonate ingiustificate» (Cassazione 3 aprile 2002, n. 4746).

Il controllo difensivo è l'unica eccezione alla regola della procedimentalizzazione dei controlli sull'attività lavorativa, e come tutte le eccezioni, ha un campo d'applicazione ristretto. Perché il controllo difensivo sia giustificato occorre, infatti, che sussista un concreto pericolo di pregiudizio al patrimonio aziendale o, ancora meglio, come precisato da una recente sentenza del Tribunale del lavoro di Milano, l'esigenza di «evitare condotte illecite da parte dei prestatori di lavoro che potrebbero esporre la società (...) a denunce anche da parte degli utenti, con la conseguente necessità per l'azienda di avere a disposizione materiale probatorio utile per contrastare o accertare eventuali addebiti (...)» (così Tribunale Milano, 5 luglio 2006).

È obbligatorio segnalare che, in altre sentenze riferite a fattispecie del tutto analoghe, lo stesso ufficio giudiziario si è pronunciato in maniera completamente opposta, ritenendo l'applicabilità dell'articolo 4, comma 2, dello Statuto dei lavoratori ed escludendo, per contro, la sussistenza di un controllo «difensivo».



Le sentenze

■ Corte d'Appello di Milano Sez. Lav, 30/9/2005, n. 668

«I programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi a Internet sono necessariamente apparecchiature di controllo nel momento in cui, in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e in via continuativa durante la prestazione, l'attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento. Qualora il datore di lavoro (...) effettui il controllo dei collegamenti e dei siti Internet in via continuativa mediante strumenti informatici centralizzati non accessibili al lavoratore e conservi la registrazione dei dati per un certo periodo, si debba ritenere l'applicabilità dell'articolo 4 Statuto dei lavoratori»

■ Tribunale di Torino, Sezione distaccata di Chivasso, sentenza 5 settembre 2006

«Anche se nell'estensione dell'indirizzo di posta elettronica compare il nome del dipendente che procede all'invio, i messaggi inviati attraverso l'e-mail aziendale rientrano nel normale scambio di corrispondenza che l'impresa intrattiene»

In caso di accesso. La e-mail non è equiparata alla corrispondenza privata

Un indirizzo poco personale

SENZA EFFETTI PENALI
Il titolare è il principale utilizzatore, ma è ammesso l'uso da parte di colleghi: in questo caso non si configura un reato

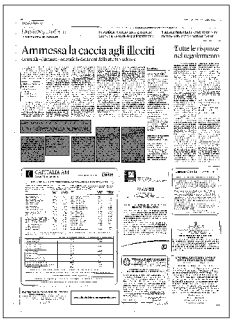
Nel quadro degli obblighi e dei limiti connessi all'utilizzo della posta elettronica aziendale, merita un cenno a parte la questione della sussistenza o meno, in caso di controllo occulto dell'account dei dipendenti da parte del datore di lavoro, di una violazione della norma penale in tema di segretezza della corrispondenza (articolo 616 Codice penale). In proposito, la giurisprudenza penale tende a escludere la configurabilità del reato sulla base della considerazione che il dipendente non è titolare di un diritto all'utilizzo esclusivo della posta elettronica aziendale.

Così si è espresso ad esempio il Tribunale di Torino, sezione distaccata di Chivasso, nella sentenza del 15 settembre 2006, secondo cui «le attrezzature lavorative e, tra queste, quelle informatiche, devono considerarsi direttamente correlate alla funzione del soggetto che rappresenta l'impresa e, solo in via mediata, devono reputarsi assegnate al singolo dipendente, comunque fungibile nel rapporto con lo strumento aziendale.

L'indirizzo di posta elettronica aziendale, al di là dell'uso solo apparentemente personale da parte del dipendente quale principale utilizzatore aziendale, può sempre essere a disposizione di soggetti diversi, appartenenti alla sua stessa impresa. Anche se nell'estensione dell'indirizzo di posta elettronica compare il nome del dipendente che procede all'invio, i messaggi inviati attraverso l'email aziendale rientrano nel normale scambio di corrispondenza che l'impresa intrattiene».

Pertanto, conclude il giudice penale di Chivasso «in caso di accesso alla casella di posta elettronica aziendale del dipendente da parte dell'impresa, non può ravvisarsi una violazione dell'articolo 616 Codice penale».

Questa pronuncia conosce un noto precedente in un'ordinanza di archiviazione del Gip di Milano del 15 maggio 2002.



Tutte le risposte nel regolamento

Come vanno utilizzati gli strumenti elettronici aziendali? La *policy* (o regolamento) aziendale sull'uso di Internet e della posta elettronica che d'ora innanzi dovrà accompagnare l'assegnazione di questi strumenti al dipendente fornirà a quest'ultimo tutte le risposte.

Dipenderà dalla scelta del datore di lavoro se i lavoratori potranno utilizzare la propria e-mail o l'accesso alla rete Internet aziendale anche per ragioni personali. L'uso personale potrà quindi essere consentito oppure escluso, anche — ma non necessariamente — tramite l'adozione di account condivisi tra più dipendenti (ad esempio: ufficiomarketing@nomeazienda.it) e la conseguente eliminazione dell'account con nome e cognome del dipendente. Quel che è certo è che una possibilità di accesso, limitato e ragionevole, a Internet e alla posta elettronica sui luoghi di lavoro difficilmente potrà essere vietata in assoluto. Ciò è quanto indica il Gruppo dei Garanti europei con il «Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro» adottato il 29 maggio 2002 (noto come WP55) e al quale il provvedimento del Garante italiano s'ispira. Con particolare riferimento al diritto-dovere delle aziende di controllare se gli strumenti aziendali vengano utilizzati in conformità alle direttive datoriali, occorre tener conto, secondo i Garanti europei, che «la tutela della vita privata comprende in certa misura anche il diritto a stabilire e sviluppare relazioni con altri esseri umani. Il fatto che tali relazioni interessino in larga misura l'ambiente di lavoro pone alcuni limiti alle legittime esigenze del datore di lavoro in fatto di provvedimenti di vigilanza». In ogni caso, indipendentemente dall'esclusione o meno dell'uso personale dell'e-mail aziendale (o dell'accesso a Internet) — e salvo i limiti di tolleranza appena visti — i controlli datoriali dovranno sempre essere contenuti entro i confini stabiliti da quelle norme dello Statuto dei lavoratori, che costituiscono, secondo un'opinione condivisa, la prima vera legge in tema di privacy introdotta nell'ordinamento italiano. Ci si riferisce non solo e non tanto ai limiti previsti dall'articolo 4 dello Statuto dei lavoratori, ma anche e soprattutto al divieto di indagini sulle opinioni e su ogni altra informazione che non attenga alla valutazione delle capacità lavorative del dipendente sancito dall'articolo 8 dello Statuto dei lavoratori. Questa norma, che è espressamente richiamata dal Codice della privacy (articolo 113, Dlgs. n. 196/2003) — e che è penalmente sanzionata — vieta comunque al datore di lavoro di utilizzare strumentazioni di controllo, anche se installate lecitamente, per raccogliere dati personali dei lavoratori di natura sensibile la cui conoscenza non abbia rilevanza ai fini della valutazione dell'attitudine professionale dello stesso.

LA SCELTA DEL DATORE
In ogni disciplinare interno dovranno essere specificati i comportamenti consentiti e quelli che rischiano sanzioni


Ammessa la caccia agli illeciti