

Privacy e sicurezza nei luoghi di lavoro

a cura di Stefano Gorla

Secondo il Garante risulta necessario trovare un punto d'incontro tra il bisogno di sicurezza e la paura di essere controllati dal proprio datore di lavoro

In generale, il problema della **sicurezza** dei cittadini non pu essere ignorato e pu presentarsi confliggente con quello della **privacy**. Il Garante ha indicato un punto di equilibrio nel bilanciamento fra il bisogno di sicurezza e la paura di essere cos controllati da perdere ogni libert. In sostanza si pu essere disposti a rinunciare ad una parte della propria libert di non essere riconosciuti, ma a condizione che ci corrisponda ad un reale aumento della protezione da parte dello Stato.

Nell'ambito specifico del mondo del lavoro, l'utilizzo delle ICT comporta problemi di privacy sia per le imprese private che per quelle pubbliche. Per esaminare il problema in oggetto e dare delle indicazioni operative sia per quanto attiene alla videosorveglianza che la vigilanza sull'utilizzo di Internet occorre partire dall'**art.114 del Codice per la protezione dei dati personali**.

Il Codice rinvia all'art.4 dello Statuto dei Lavoratori (L.n.300 del 25 maggio 1970) che stabilisce il **divieto del controllo a distanza dei lavoratori**. Pu capitare, tuttavia, che il controllo sia necessario per l'organizzazione della produzione ed allora occorre procedere alla stipula di un accordo sindacale oppure, in sua mancanza, all'ottenimento di un provvedimento della Direzione Provinciale del Lavoro - Servizio Ispettivo.

Coloro che accedono alla zona videosorvegliata, siano essi lavoratori o visitatori, devono essere informati (ex art. 13 del Codice della Privacy) che si trovano o stanno per entrare in un'area controllata e che possono essere oggetto di una eventuale registrazione. Tutte le indicazioni del Garante sono contenute nel Provvedimento generale sulla videosorveglianza del 19 aprile 2004. Per quanto **attiene alla PA** il Garante ha stabilito che un soggetto pubblico pu effettuare attivit di videosorveglianza solo ed esclusivamente per svolgere funzioni istituzionali che deve individuare ed esplicitare con esattezza e di cui sia realmente titolare in base all'ordinamento di riferimento (art. 18, comma 2, del Codice). Diversamente, il trattamento dei dati non lecito, anche se l'ente designa esponenti delle forze dell'ordine in qualit di responsabili del trattamento, oppure utilizza un collegamento telematico in violazione del Codice (art. 19, comma 2, del Codice).

La liceit pertanto determinata dalle funzioni istituzionali e deve essere proporzionata agli scopi che si intendono perseguire (art.11 c.1 lett. d del Codice). Inoltre occorre verificare:

1. che siano realmente insufficienti ed inattuabili altre misure di sicurezza come l'installazione di sistemi di allarme o di protezione agli ingressi;
2. se sia realmente necessario raccogliere immagini dettagliate, stabilendo di conseguenza la dislocazione e la tipologia fissa o mobile degli impianti;
3. limitare la creazione di banche dati quando sufficiente un sistema a circuito chiuso per il controllo di flusso senza registrazione (come ad es.per uno sportello).

In merito alla vigilanza sulle comunicazioni elettroniche e sull'utilizzo di Internet sul posto di

lavoro, il Garante ha chiarito che sia i datori di lavoro pubblici che quelli privati **non possono** controllare la posta elettronica e la navigazione in rete dei dipendenti senza il loro consenso se non in casi eccezionali. Se l'obiettivo dei controlli solo e solamente la gestione della sicurezza della rete aziendale, allora il consenso al trattamento dei dati non richiesto in quanto trattasi di controlli difensivi.

certamente un diritto del datore di lavoro verificare la destinazione delle risorse aziendali ma altrettanto diritto del lavoratore **non subire controlli non trasparenti**. sempre sulla base dell'art. 4 dello Statuto dei lavoratori che possiamo concludere che la lettura e la registrazione sistematica dei messaggi di posta elettronica, al pari del monitoraggio dei siti visitati durante la navigazione in rete da parte del dipendente, sono vietati in quanto forme di controllo a distanza dell'attività lavorativa.

Nel 2007, l'Associazione Direttori Risorse Umane (GIDP/HRDA - Gruppo Intersettoriale Direttori del Personale - Human Resources Director Association) ha condotto un'indagine da cui sono emersi dati interessanti. Circa la metà delle aziende rispondenti (il 56,4%) ha dichiarato di non effettuare controlli, mentre il 41% invece lo fa e rileva che Internet utilizzato dal 56,4% dei dipendenti per scopi personali. Le misure precauzionali adottate riguardano solo il 39,7% dei casi. Le risposte dei sindacati interni all'azienda sono state poco collaborative: ha approvato i provvedimenti cautelativi solo il 23%, mentre ben il 75,7% non ha risposto.

Il Garante, con il Provvedimento generale del **1 marzo 2007**, ha raccomandato il coinvolgimento delle rappresentanze dei lavoratori per l'adozione di un disciplinare interno. Al datore di lavoro viene assegnato il compito di adottare ogni misura in grado di prevenire il rischio di utilizzi impropri di Internet, in modo che vengano ridotti all'indispensabile i controlli successivi sui lavoratori. In questo senso necessario considerare queste utili indicazioni pratiche (<http://www.garanteprivacy.it/garante/doc.jsp?ID=1387978>):

- individuare preventivamente i siti correlati con la prestazione di lavoro;
- utilizzare filtri per prevenire determinate operazioni, come l'accesso a siti compresi nelle black list o il download di file multimediali;
- utilizzare indirizzi di posta elettronica a livello di ufficio al fine di rendere trasparente la natura non privatistica della corrispondenza;
- prevedere, in caso di assenza di un lavoratore, messaggi di posta automatica con le coordinate dei colleghi a cui rivolgersi;
- mettere in grado il dipendente di delegare un suo collega fiduciario alla verifica del contenuto delle mail a lui indirizzate in caso di assenza prolungata o imprevista e per improrogabili necessit dell'attività lavorativa.

Se le misure preventive non sono sufficienti ad impedire comportamenti anomali, il datore di lavoro pu procedere gradualmente ad altri controlli con verifiche non dirette sul singolo lavoratore, ma a livello di ufficio per individuare l'area a cui attribuire comportamenti non conformi. Solo con il persistere delle anomalie sar possibile procedere a controlli di tipo individuale.

L'argomento in questione oggi di estrema attualit e si inquadra nell'ambito pi generale della sicurezza, coinvolgendo non solo i rapporti aziendali ma l'intera societ democratica chiamata a rispondere alla minaccia terroristica senza ricorrere a provvedimenti di emergenza che prevedano la sospensione dei diritti civili. Negli Usa, controllare i dipendenti con le ICT consentito dal **Patriot**

Act, un insieme di misure varate all'indomani degli attentati dell'11 settembre 2001, che includono anche la possibilità di leggere tutte le email inviate dall'ufficio, ma anche le conversazioni private effettuate da casa.

La soluzione totalitaristica offerta dall'**Ufficio di propaganda di Goebbels** consisteva in questa regola: *Se non hai nulla da nascondere, non hai niente da temere*. Si tratta della codificazione della regola del sospetto che trova risposta in quanto affermato dal Prof. Stefano Rodotà nel 2001 durante il dibattito acceso dopo l'11 settembre: "L'uomo di vetro" una metafora totalitaria, perché su di essa si basa poi la pretesa dello Stato di conoscere tutto, anche gli aspetti più intimi della vita dei cittadini, trasformando automaticamente in "sospetto" chi chieda salvaguardia della vita privata.

Versione originale: <http://www.pubblicaamministrazione.net/leggi-e-norme/articoli/789/privacy-e-sicurezza-nei-luoghi-di-lavoro.html>

Copyright 2007 HTML.it | La vendita, il noleggio, il prestito e la diffusione del contenuto di questa pagina sono vietate, tranne nei limiti specificati nella pagina <http://www.pubblicaamministrazione.net/note-legali.html>.