# Vietato spiare in azienda

## Il Garante della Privacy frena le aziende: vietato spiare la navigazione dei dipendenti. Tra leggi consolidate e nuove tendenze, rimane il caposaldo della tutela della privacy.

Un recente sondaggio ha evidenziato che più di un terzo dei dipendenti italiani viaggia in Rete durante l'orario d'ufficio per scopi personali. Dalle news ai blog, dalle chat allo shopping online, per non parlare della navigazione casuale, le opportunità che offre Internet sono infinite per chi vuole una pausa nella routine delle otto ore di lavoro. Ma quando una società nega espressamente al proprio dipendente la possibilità di navigare in Rete per scopi personali, e il dipendente infrange le regole imposte, può nascere un contenzioso che rischia di portare al licenziamento. Tra le aziende, sono sempre più diffuse le pratiche di monitoraggio sull'uso del computer e di Internet da parte dei dipendenti. Ma spesso sono illegali.

### Vietato spiare

Su questo tema caldo si è espresso il Garante per la privacy, intervenendo in merito a una causa di lavoro intentata da un dipendente licenziato perché scoperto a navigare in Internet durante l'orario di lavoro. La decisione dell'Authority è destinata a far discutere e condizionerà notevolmente le attività di monitoraggio interno delle imprese italiane, compresa la pubblica amministrazione. In sostanza, il datore di lavoro non può verificare analiticamente la navigazione Web del dipendente per ricavare informazioni su quali siti e servizi abbia visitato.

### La vicenda

La controversia vedeva schierati da una parte una società romana e dall'altra un suo dipendente che, pur non essendo autorizzato, si era connesso alla Rete da un computer aziendale. Il datore di lavoro, dopo aver monitorato i dati del computer, aveva accusato il lavoratore di aver visionato siti a contenuto religioso, politico e pornografico. Ne aveva anche fornito l'elenco dettagliato, per dimostrare la violazione del codice regolamentare e della politica aziendale. In seguito al procedimento disciplinare il dipendente è stato poi licenziato. Da qui, l'impugnazione da parte del dipendente del provvedimento e la conseguente causa.

### Eccesso di controllo

Il monitoraggio condotto dall'azienda costituisce un illecito, secondo il Garante: per contestare l'uso indebito del computer aziendale, si legge nel provvedimento dell'Authority, sarebbe stato sufficiente

verificare gli avvenuti accessi a Internet e i tempi di connessione, senza indagare sui contenuti dei siti. Insomma, altri tipi di controlli sarebbero stati più idonei e proporzionati per verificare il comportamento del dipendente. È stato giudicato altrettanto illecito anche il trattamento dei dati relativi allo stato di salute e alla vita sessuale: secondo il codice di tutela della privacy, infatti, questo tipo di trattamento può essere effettuato senza il consenso dell'interessato in casi molto rari, solo se necessario per difendere in giudizio un diritto della personalità o un altro diritto fondamentale. La società in questo caso intendeva invece far valere diritti legati allo svolgimento del rapporto di lavoro.

## I dati sensibili

A portare l'Authority a esprimersi in favore del dipendente è stata la raccolta di dati sensibili: le numerose pagine dei file temporanei e di cookies allegati dalla società alla documentazione a sostegno del licenziamento. Da questi fogli, stampati dalla directory intestata al lavoratore e relativi ad accessi Web avvenuti dalla sua postazione durante l'orario di lavoro, emergevano anche numerose informazioni particolarmente delicate e strettamente personali: la società non poteva raccoglierle senza aver prima informato il lavoratore. Questo aspetto è molto importante, perché le motivazioni del pronunciamento sarebbero da attribuire non solo a un trattamento di dati eccessivo rispetto agli obiettivi prefissati, ma anche a una mancata comunicazione aziendale del monitoraggio del traffico e della Rete interna, effettuata senza l'assenso del dipendente, anzi senza neppure informarlo. Da un punto di vista tecnico-giuridico, l'intercettazione dei dati relativi alla navigazione in Rete dei dipendenti è stato messo allo stesso livello del trattamento di dati sensibili, ovvero a informazioni idonee a rivelare convinzioni religiose, opinioni sindacali, nonché gusti attinenti alla vita sessuale.

## Un freno ai controlli

Il provvedimento dell'Authority sulla privacy pone un brusco freno alle pratiche interne alle aziende: spiare l'utilizzo dei computer e la navigazione in Rete da parte dei lavoratori mette a rischio la libertà e la segretezza delle comunicazioni e le garanzie previste dallo Statuto dei lavoratori. Il semplice rilevamento dei siti visitati, infatti, può rendere noti dati delicatissimi della persona: convinzioni religiose, opinioni politiche, appartenenza a partiti, sindacati o associazioni, stato di salute, indicazioni sulla vita sessuale e altri, che potrebbero poi essere utilizzati per discriminare il soggetto interessato. La sentenza ribadisce e tutela un principio sacrosanto: il diritto da parte del navigatore della Rete di poter frequentare il Web nella massima libertà e riservatezza, contro ogni tentativo di controllo della navigazione personale.

## La trasformazione del lavoro

D'altra parte bisogna riconoscere come lo statuto dei lavoratori sia uno strumento che non è in grado di rispondere ai nuovi problemi che le tecnologie hanno portato nel mondo del lavoro. Le questioni che ormai da qualche anno sono dibattute sull'uso di Internet dalle postazioni di lavoro, domani si rifletteranno anche nell'uso dei cellulari di nuova generazione e nella disponibilità della Tv mobile. Quello che è certo è il grande cambiamento avvenuto nelle modalità di lavoro dei dipendenti. E il problema più serio non è tanto quello della navigazione esterna, quanto quello della navigazione interna all'azienda. Infatti, ormai tutte le aziende dotate di Intranet possiedono aree particolarmente sensibili nelle quali non è opportuno che tutti i dipendenti possano entrare e modificare dati.

## Le risposte a disposizione

A queste sfide, in parte, una risposta può essere data da alcuni strumenti come i firewall, che opportunamente configurati impediscono, in modo del tutto legale, l'accesso ad alcune aree interne e ad alcuni siti esterni. Ma la risposta vera avviene in un cambio di mentalità totale delle aziende, sia tra i vertici sia tra i lavoratori. Il valore del lavoro è spostato dal concetto di orario al concetto di produttività. In questo senso, la navigazione su Internet non è un problema, se non pregiudica la produttività. Questo approccio, però, prevede un cambio di mentalità che può avvenire soltanto con un approccio culturale diverso al lavoro, con la formazione continua, con l'affermarsi di una politica aziendale incentrata sulla collaborazione e la crescita interna

---

Come detto prima , basta l'intenzione di spiare, per mettersi dalla arte del torto. il lavoratore dovrebbe essere avvisato. però l'appiglio che usano "i capi" è che il computer è dell'azienda, ti viene dato per lavorare e il lavoro c'è sopra appartiene per l'azienda. io sono stato (non posso dire dove, ma tratta telefonia) a lavorare in un posto, dove veniva monitorato all'occorrenza anche il traffico internet.

in un altra azienda, il ns capo aveva tutte le nostre password, tranne quella della messaggistica (appunto per questioni di privacy) e quindi libero accesso ai nostri pc, e ad una collega fu notificato un richiamo verbale perchè si portava gli mp3 e li sentiva sul pc (infrazione delle più elementari norme di sicurezza informatica). tenendo conto che era un lavoro su turni e si lavorava in due per volta, i casi sono 2: il collega ha fatto la spia (probabile ma inverosimile, dati i legami che si creano tra turnisti), il capo ha dato un'occhiata per chissà quale motivo al pc col profilo della persona interessata (non avevamo pc "personali", ma si faceva a chi arrivava prima) e ha beccato i temporanei.

inoltre, presso l'azienda in questione, facemmo un corso proprio sulla privacy, tenuto da consulenti esterni, e fu fatto proprio il caso di un capo che intrufolava il naso nel pc del dipendente. ci fu detto che non si trattava di violazione della privacy, per tutto ciò che concerneva il lavoro e l'azienda, a meno chè non ficcasse il naso nella posta o in cose personali, che però sul pc aziendale, non dovrebbero nemmeno esistere.

loro te la rigirano sull'interesse aziendale, e lì ci fai poco. è loro dovere vedere e controllare se si lavora. per cui bisogna vedere se possono attuare alcuni tipi di misure di controllo. tutto qui. non sto difendendo simili atteggiamenti, sia chiaro. si lavora male, se si sa che ti spiano e, naturalmente, è una cosa disdicevole...

Vorrei solo spendere 2 parole sul dicorso Privacy:

1) Se il Titolare del Trattamento NON richiede espressamente e per iscritto il consenso al dipendente, NON può controllare il contenuto del Pc aziendale.
Ovviamente il dipendente non ha modo di opporsi se vuole utiliizare il Pc aziendale = lavorare....

**Il Titolare deve far firmare almeno 2 moduli:**

**- Autorizzazione al trattamento dei dati sensibili del Dipendente ( ad esempio la busta paga contiene dati sensibili... )**

**- Incarico al trattamento**

**2) I file di Log sono un argomento discusso da sempre...**
**Non vi è una regola generale che ne imponga l'utilizzo ma nemmeno che lo vieti...**
**Il problema fondamentale non è tanto la loro compilazione, quanto il loro utilizzo per fini diversi...**

**3) Il Custode delle Password ( che deve sempre essere espressamente nominato dal Titolare del Trattamento... ) NON deve conoscere le password per l'accesso al Pc del dipendente.**
**La Normativa prevede esplicitamente ( allegato B al disciplinare tecnico per il trattamento con strumenti elettronici... ) la consegna delle Password di accesso in busta chiusa, l'obbligatorietà del cambiamento della medesima al primo accesso, oltre ai requisiti minimi di sicurezza ( minimo 8 caratteri etc. etc. )**

**4) La privacy NON è riferita SOLO ai dati trattati in azienda, ma anche in difesa del dipendente, e + in generale, alla garanzia di privacy di tutti gli individui...**

Mha....secondo me la causa in tribunale sarebbe interessante di certo... perchè da un lato il dipendente potrebbe parlare di "violazione della privacy", dall'altro lato il capo potrebbe parlare di "contromisure nei confronti di eventuali illeciti aziendali" o roba simile..... Certo, la privacy in un posto che non è di tua proprietà, con mezzi che non appartengono a te.....dato che non è una toilette o una camera da letto...., .....non può fare niente il dipendente, se non soltanto chiedere spiegazioni al suo capo, dopo aver accertato che sia vero....se possibile, eludere lo spionaggio in modo informatico..... ma è il capo che comanda, e in questo caso ha tutto il diritto di evitare che i pc aziendali vengano usati in modo improprio..... tutto IMHO.

---

quello è il meno, viola lo statuto dei lavoratori che vieta il controllo a distanza dei dipendenti.

Se non sbaglio **Citrix Metaframe 1.8** lo faceva, in modo del tutto trasparente. Contromisure: nessuna, ma se riesci a dimostrare che il tuo capo "ti spia" senza il tuo consenso puoi fargli passare delle grane molto amare. P.S: non crosspostare P.P.S.: con XP centra una mazza

Vero, ma il monitoraggio dei dipendenti deve essere noto, in azienda. Se non lo è si incorre in una violazione della privacy. In sostanza: in azienda non si può navigare a scopo privato e/o ci possono essere controlli sull'attività lavorativa solo se ciò viene espressamente comunicato dal datore di lavoro. vedi qui:

http://www.shinynews.it/diritto/0306-vietato-spiare.shtml