



DATORE SPIONE

<http://blog.libero.it/lav/uglcreditoinforma@libero.it>
a cura dell'avv. Rosario Francese

Cassazione Lavoro: il datore di lavoro non può spiare la posta elettronica e gli accessi ad internet aziendale da parte lavoratore (Corte di Cassazione - Sezione Lavoro, Sentenza 23 febbraio 2010, n.4375: Controllo a distanza dei lavoratori con programmi informatici).



Roma 14.03.2010 – la Cassazione Lavoro ha chiarito quali sono i limiti del controllo da parte Aziendale alla postazione p.c. del dipendente.

I programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi ad internet dei dipendenti sono necessariamente apparecchiature di controllo da assoggettare alle condizioni di cui all'articolo 4 dello Statuto dei lavoratori. Lo ha affermato la Cassazione, confermando la sentenza di secondo e di primo grado.

Nel caso di specie, risalente a fatti verificatisi nel 2002, una lavoratrice era stata licenziata a causa dell'utilizzo di internet non giustificato da esigenze d'ufficio, rilevato da un programma di controllo informatico denominato Super Scout. Tribunale e Corte d'appello avevano giudicato illegittimo il licenziamento in quanto i fatti contestati (accesso ad internet) erano stati rilevati e registrati dal suddetto programma in violazione dell'articolo 4 comma 2 dello Statuto dei lavoratori, con la conseguente inutilizzabilità dei dati acquisiti, ritenendo in ogni caso violate le regole di proporzionalità e gradualità delle sanzioni disciplinari.

La Cassazione ha richiamato il proprio orientamento secondo cui "ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 legge n. 300 del 1970, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma sopra citata i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aule riservate o gli apparecchi di rilevazione di telefonate ingiustificate (v. Cass. 3-4-2002 n. 4746). Il detto articolo 4, infatti, sancisce, al suo primo comma, il divieto di utilizzazione di mezzi di controllo a distanza sul presupposto -

espressamente precisato nella Relazione ministeriale - che la vigilanza sul lavoro, ancorché necessaria nell'organizzazione produttiva, vada mantenuta in una dimensione "umana", e cioè non esasperata dall'uso di tecnologie che possono rendere la vigilanza stessa continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro.

Lo stesso articolo, tuttavia, al secondo comma, prevede che esigenze organizzative, produttive ovvero di sicurezza del lavoro possano richiedere l'eventuale installazione di impianti ed apparecchiature di controllo, dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori. In tal caso è prevista una garanzia procedurale a vari livelli, essendo l'installazione condizionata all'accordo con le rappresentanze sindacali aziendali, ovvero, in difetto, all'autorizzazione dell'Ispettorato del lavoro.

In tal modo, come è stato evidenziato da Cass. 17-7-2007 n. 15892, *"il legislatore ha inteso contemperare l'esigenza di tutela del diritto dei lavoratori a non essere controllati a distanza e quello del datore di lavoro, o, se si vuole, della stessa collettività, relativamente alla organizzazione, produzione e sicurezza del lavoro, individuando una precisa procedura esecutiva e gli stessi soggetti ad essa partecipi"*.

Con la stessa sentenza, è stato però precisato che la *"insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore"*, per cui tale esigenza *"non consente di estrarre dalla fattispecie astratta i casi dei c.d. controlli difensivi ossia di quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso"*. In tale ipotesi si tratta, infatti, comunque di un controllo c.d. "preterintenzionale" che rientra nella previsione del divieto di cui al secondo comma dell'art. 4 citato.

In definitiva, *"i programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi 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 (se non altro, nel nostro caso, sotto il profilo del rispetto delle direttive aziendali)"*.

"Ciò è evidente laddove nella lettera di licenziamento i fatti accertati mediante il programma Super Scout sono utilizzati per contestare alla lavoratrice la violazione dell'obbligo di diligenza sub specie di aver utilizzato tempo lavorativo per scopi personali (e non si motiva invece su una particolare pericolosità dell'attività di collegamento in rete rispetto all'esigenza di protezione del patrimonio aziendale)".

LA REDAZIONE È STATA CURATA DALL'AVV. ROSARIO FRANCESE

Troverai tutti i numeri precedenti di UglCreditoInforma all'indirizzo internet <http://blog.libero.it/lav/> .

Utilizza il suddetto **blog** e l'indirizzo **e-mail** uglcreditoinforma@libero.it per richiedere la trattazione di specifici argomenti, per inviare documenti utili alla redazione di nuovi numeri e per comunicare i tuoi commenti e suggerimenti.

Grazie per il vostro costante supporto.