

STUDIO LEGALE ASSOCIATO SBARRA BESI

Corso di Porta Vittoria n. 17 – 20122 Milano
TEL. 02. 54.11.81.86 – 02. 54.12.24.11 FAX 02. 54.10.31.89
E-mail: avv sbarra@sbarrabesi.it
E-mail: avvbesi@sbarrabesi.it

AVV. ALBERTO SBARRA

AVV. LIDIA MADDALENA BESI

AVV. ALBERTO BRACCHI
DOTT.SSA ELISA LAZZATI
DOTT. FRANCESCO GROSSO

Milano, 10 aprile 2008

Potere di Controllo del datore di lavoro: nuovi strumenti informatici e tutela della privacy

C.so Venezia, 49 – Palazzo Castiglioni – Sala Turismo

Avv. Alberto Sbarra – Giuslavorista

Il potere di controllo del datore di lavoro sui dipendenti e i limiti imposti dalla normativa vigente, alla luce dei più recenti orientamenti della giurisprudenza nel campo del diritto del lavoro.

Nel contratto di lavoro il datore di lavoro ha il diritto di impartire le disposizioni per l'esecuzione e la disciplina del lavoro ai sensi dell'art. 2104 cod. civ.

In sostanza il datore di lavoro può controllare il dipendente nello svolgimento della sua attività. Egli infatti è creditore della prestazione del lavoratore al quale paga un compenso per il tempo lavoro impiegato.

Con l'entrata in vigore dello statuto dei lavoratori, nel 1970, il legislatore crea delle vere e proprie barriere intorno al luogo di lavoro, contro un eccesso di controllo da parte del titolare dell'azienda o dei suoi incaricati, affinché sia garantita una zona di

riservatezza che ogni persona ha diritto, anche sul posto di lavoro, nonostante vi sia uno strettissimo contatto con il datore di lavoro e, soprattutto, nonostante il lavoratore lavori non a casa sua, ma presso l'imprenditore, utilizzando suoi beni ed attrezzature.

Esaminiamo, dunque, brevemente queste barriere create a favore della riservatezza e libertà del lavoratore per poi arrivare alla questione che più ci interessa, ossia l'utilizzo dei nuovi strumenti informatici.

L'art. 2, comma terzo, Stat. Lav. fa espresso divieto al datore di lavoro di adibire le guardie giurate alla vigilanza sull'attività lavorativa; l'art. 3 prevede che i nominativi e le mansioni del personale addetto alla vigilanza debbono essere comunicati ai lavoratori interessati. E questi sono i controlli esterni all'attività lavorativa.

L'art. 4 Stat. Lav. tutela invece in modo diretto ed interno all'azienda il lavoratore ponendo un divieto ad ogni forma di controllo continuo o comunque ad ogni forma di controllo attuabile in qualsiasi momento dalla direzione aziendale sulla prestazione lavorativa, attraverso l'utilizzo di impianti o di altre apparecchiature per finalità di controllo a distanza dell'attività del lavoratore.

Osserviamo subito che la giurisprudenza ha dato sin dall'inizio dell'entrata in vigore della norma, un'interpretazione estensiva della stessa, ricomprendendo in essa qualsiasi forma di controllo a distanza che sottragga al lavoratore, nello svolgimento delle sue mansioni, ogni margine di spazio o di tempo nel quale possa essere osservato, ascoltato o comunque seguito nei propri movimenti.

Pertanto non soltanto impianti finalizzati a riprendere nel luogo di lavoro immagini o voci, ma anche impianti di registrazione continua delle stesse voci ed immagini. Il divieto attinendo ad “apparecchiature” non si estende al controllo esercitato direttamente dai preposti, dirigenti o dello stesso datore di lavoro.

All’indomani dello Statuto dei Lavoratori, le applicazioni concrete di questa svolta estensiva della giurisprudenza che riteneva applicabile l’art. 4 Stat. Lav. ad ogni forma di controllo continuo sulla prestazione lavorativa, erano state, tutto sommato, limitate: per esempio ai dischi tachigrafici degli autotreni, agli orologi marca tempo, ai sistemi audiovisivi all’interno delle banche, ecc.

Ma l’evoluzione dei sistemi informatici ed il loro utilizzo nello svolgimento della prestazione lavorativa hanno determinato una svolta profonda.

L’attività del lavoratore e le informazioni sull’attività sono un tutt’uno e transitano nel medesimo impianto. Si lavora sulle informazioni che si immettono che si elaborano o che si utilizzano e questo flusso viene governato dentro ad un sistema informatico più o meno complesso. In sintesi, il lavoratore vive in mezzo a dati ed informazioni.

Pertanto l’applicazione dell’informatica ha preso ad invadere capillarmente i luoghi di lavoro ponendo il problema se la norma che abbiamo visto, dettata con riferimento a sistemi di controllo estrinseci ed eventuali rispetto alla prestazione lavorativa (soprattutto impianti televisivi a circuito chiuso), possano applicarsi anche alla strumentazione informatica e telematica laddove questa è o può essere al tempo stesso strumento essenziale della produzione e

sistema di controllo della prestazione.

Orbene, siccome il comma secondo dell'art. 4 prevede la possibilità, previo accordo con le rappresentanze sindacali aziendali, di installare impianti o apparecchiature di controllo che siano richieste da esigenze organizzative e produttive, è evidente il rischio che l'informatizzazione delle imprese, ormai capillare, subisca una sorta di cogestione o addirittura la necessità di un'autorizzazione amministrativa, giacché, sempre in base al predetto secondo comma, può essere l'Ispettorato del lavoro, in difetto di accordo con il sindacato, a dettare le modalità d'uso degli impianti.

A fronte di questa conseguenza palesemente eccessiva alcuni giuristi hanno iniziato a ritenere che l'organizzazione informatico – telematica del lavoro sfugga alla previsione dell'art. 4, in quanto per “apparecchiature” di controllo non possono che essere gli impianti non essenziali rispetto all'esecuzione della prestazione, destinati a rilevare solo ciò che accade nell'ambiente di lavoro (questa è la posizione di Ichino, Pisani e D'Antona).

La giurisprudenza che si è trovata a dover giudicare i controlli sul comportamento del lavoratore in base all'analisi dei sistemi informatici oppure sull'utilizzo del telefono piuttosto che delle e-mail, ha dovuto confrontarsi con la tradizionale interpretazione estensiva dell'art. 4, non fornendo purtroppo, ed è questo il problema, indirizzi univoci a cui fare riferimento.

Tanto più che una norma ad hoc non c'è e, quindi, ci troviamo a dover affrontare il problema dell'utilizzo dei sistemi informatici avendo a che fare con una norma, l'art. 4 Stat. Lav. entrato in vigore addirittura prima del nascere dei predetti sistemi.

Ed allora vediamo come la giurisprudenza si è mossa per trarre delle indicazioni pratiche ed operative che possono servire nell'attività di gestione del personale.

La soluzione sembrava essersi trovata, legittimando i cosiddetti "controlli difensivi" che già da anni la giurisprudenza consente, per esempio attraverso l'utilizzo di agenzie di investigazione che controllano l'attività del lavoratore al fine di stroncare il compimento di atti illeciti: mancata emissione dello scontrino nell'attività di cassa, oppure la simulazione della malattia. Sono tutti controlli esterni allo svolgimento dell'attività lavorativa che a rigore sarebbero vietati, poiché determinano un controllo dell'attività lavorativa con personale esterno.

Però vi è tutta un'ampia giurisprudenza ormai decennale che consente l'utilizzo di soggetti diversi dall'imprenditore al fine di tutelare il suo patrimonio, non ritenendo applicabile gli artt. 2 e 3 dello Statuto. In questi casi la giurisprudenza parla di "controlli difensivi" per distinguerli dai controlli offensivi per indagare sull'attività, o il comportamento privato del lavoratore sicuramente vietati. Sono, quindi, controlli legittimi destinati a difendere il patrimonio aziendale dell'imprenditore.

In riferimento all'art. 4 Stat. Lav. si è andato ad affermare un orientamento giurisprudenziale analogo a quello che si è detto, nel senso della legittimità dell'installazione di impianti per il controllo a distanza mirato non sull'attività lavorativa, ma su possibili attività illecite del lavoratore.

Secondo una nota sentenza della Corte di Cassazione del 2002 (la n. 4746), affinché si possa ritenere operativo il divieto di utilizzo

di apparecchiature per i controlli a distanza dell'attività dei lavoratori previsto dall'art. 4 Stat. Lav. è necessario che il controllo riguardi direttamente o indirettamente l'attività lavorativa, mentre devono ritenersi certamente fuori dall'ambito di applicazione delle norme i controlli diretti ad accertare condotte illecite del lavoratore (c.d. controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate o, appunto, di apparecchi di rilevazione di telefonate ingiustificate.

A questo punto la giurisprudenza nel tempo si è nettamente divisa. Da una parte quella che ha applicato pedissequamente questa massima senza però andare a vedere effettivamente se i controlli fossero volti o meno a misurare anche il tempo lavoro o la prestazione del lavoratore e non solo il compimento di atti illeciti ed, invece, quella giurisprudenza, che chiameremo del "caso concreto", che ha ritenuto di misurare quanto il sacrificio e la riservatezza del singolo lavoratore fosse effettivamente giustificato rispetto alla gravità dell'inadempimento o dell'illecito commesso, tenendo soprattutto conto delle modalità in cui venivano acquisiti i dati relativi al comportamento del lavoratore.

Esemplare a questo riguardo la sentenza della Corte d'Appello di Milano del 30 settembre 2005 proprio relativa all'utilizzo di un software denominato "*super scout*" installato per controllare l'accesso dei dipendenti a internet.

In particolare, secondo la Corte d'Appello, tutti quei programmi informatici che consentono un monitoraggio della posta elettronica e degli accessi ad internet che in base alla loro caratteristiche consentano al datore di lavoro di controllare a

distanza, in via continuativa il lavoratore durante la prestazione dell'attività lavorativa, rientrano nell'ambito del divieto previsto dall'art. 4.

Inoltre nel caso in esame non vi era il divieto esplicito dell'utilizzo degli strumenti aziendali non per fini di servizio e neppure vi era la conoscenza da parte del lavoratore del controllo dell'accessibilità ai siti.

A ciò si aggiunga che la conservazione dei dati avveniva per un periodo di oltre due mesi, e, non in ultimo, vi era la mancanza di un meccanismo di scelta dei lavoratori da sottoporre al controllo che, invece, avveniva discrezionalmente da parte del direttore del personale.

A tutto ciò si aggiunge il fatto che la mancanza di regole rigorose o se vogliamo a campione o casuali del personale da controllare metteva a repentaglio anche il diritto alla riservatezza del lavoratore sulle sue opinioni politiche, religiose, sindacali sancito dall'art. 8 dello Statuto, con evidente – secondo la Corte – pericolo di ricatto nei confronti del lavoratore.

Insomma, secondo la sentenza il datore di lavoro non poteva attingere dall'analisi dei programmi informatici dati o elementi sullo svolgimento dell'attività lavorativa svolta, soprattutto se il monitoraggio avveniva in modo estensivo, non a campione, quasi come un occhio vigile e sempre aperto sull'attività del lavoratore, immagazzinando dati per mesi.

Inoltre secondo la Corte l'acquisizione di dati ed informazioni doveva essere proporzionale allo scopo per il quale era stato acquisito al fine del controllo, secondo un orientamento più volte

espresso in sede Europea.

Mi viene da pensare che se l'utilizzo di questo software "super scout" avesse condotto alla scoperta che il dipendente consultava siti pedopornografici, ovvero di terrorismo internazionale forse il trattamento del dato riservato avrebbe comportato l'inapplicabilità dell'art. 4. Infatti nella sentenza della Corte milanese quello che si censura è soprattutto il trattamento di dati riservati senza alcuna trasparenza e correttezza e senza lacuna apparente finalità se non il mero controllo.

Ecco, quindi, l'importanza che i dati acquisiti debbano essere adeguati, pertinenti e non eccedenti rispetto alle finalità che giustificano il monitoraggio, come efficacemente sostenuto dalla sentenza richiamata, che cita sul punto proprio le conclusioni a cui era giunto il Gruppo di Lavoro Europeo del 13 settembre 2001.

Sennonché il criterio della proporzionalità sembra entrare nuovamente in crisi con una recente sentenza della Cassazione dell'anno scorso (sentenza n. 15892 del 17 luglio 2007).

Si trattava del caso di un sistema di rilevazione di entrata e uscita in un garage aziendale che i Giudici di secondo grado ritenevano legittimo proprio perché avente carattere difensivo per individuare abusi di estranei, oppure abusi degli stessi dipendenti sulla frequentazione del posto di lavoro. Invece la Corte di Cassazione ha ritenuto operante ed assoluto il divieto posto dall'art. 4, disattendendo e ritenendo non applicabile il principio sui "controlli difensivi", cassando la sentenza di secondo grado.

Secondo la Suprema Corte l'apparecchiatura o l'impianto utilizzato non controllava solo le modalità di svolgimento del

rapporto, verificando eventuali illeciti, ma anche il *quantum* della prestazione e l'orario di lavoro risolvendosi in un accertamento circa la quantità di lavoro svolto che rientrava nella fattispecie prevista dall'art. 4.

Ed allora proviamo a tirare le prime conclusioni.

Vi è l'assoluta necessità che l'azienda predisponga un'insieme di regole che disciplinino l'utilizzo di internet e della posta elettronica, dettandone gli scopi e le finalità ed informando soprattutto i lavoratori del controllo e delle regole che presiedono all'utilizzo dei predetti strumenti informatici.

Ciò è assolutamente necessario se solo consideriamo che secondo l'allegato VII al D.Lgs. n. 626/94 nell'utilizzo di videoterminali, *"nessun dispositivo di controllo quantitativo o qualitativo può essere utilizzato all'insaputa dei lavoratori"*.

Inoltre i controlli in azienda possono essere espletati in due modi o mediante l'acquisizione preventiva degli elementi concreti di sospetto sull'utilizzo eccessivo o comunque illecito di internet o di altri strumenti utilizzati come il telefono, senza attivare in modo estensivo il controllo a tutti i dipendenti; oppure effettuando controlli a campione, tenendo conto anche del tipo di lavoro svolto dal lavoratore. Va evitato, quindi, di tenere aperto un occhio "segreto" in modo continuativo sull'attività lavorativa del dipendente, con possibilità di accesso a dati riservati o privati di soggetti anche diversi, senza alcuna relazione con la difesa degli interessi aziendali (per esempio dati acquisiti in modo estensivo dal direttore del Personale o dall'A.D. ecc). Bisogna invece muoversi assumendo elementi di fatto che possano poi supportare il "controllo

difensivo”.

Soggiungiamo che il controllo potrebbe essere giustificato con il tipo di lavoro svolto e su questo non ci potrebbero essere obiezioni. Pensiamo al controllo delle telefonate per contenere i costi o per imputare i costi a determinati venditori o centri di costo. Se in questa occasione si riscontra un utilizzo distorto del mezzo (per esempio collegamenti continui anomali) non si potrà sostenere un controllo a distanza.

Oppure pensiamo alla necessità dichiarata e conosciuta a tutti i dipendenti di effettuare controlli per evitare intrusioni esterne a seguito dell'utilizzo di internet.

Non meno importante è la questione relativa al controllo delle e-mail in azienda.

Occorre innanzitutto sottolineare che i controlli ai quali il prestatore di lavoro sia assoggettato con il contratto di lavoro devono essere tenuti ben distinti da quelli che il datore di lavoro può invece compiere al di fuori del rapporto contrattuale in forza del quale esistono ben precisi limiti e vincoli costituzionali.

Infatti al di là del divieto di indagini stabilite dallo Statuto dei Lavoratori esiste una sfera di riservatezza che è comunque garantita al lavoratore in quanto cittadino, anche se temporaneamente operativo in azienda. Il lavoratore ha diritto sul posto di lavoro a riservare per sé degli spazi privati ben precisi: la corrispondenza, le comunicazioni, il proprio bagaglio, la propria borsa, la propria autovettura, l'armadietto dello spogliatoio, il cassetto della scrivania, ecc.

Questa essendo la regola, vi sono problemi di applicazioni per

ragioni tecniche in riferimento al caso in cui il lavoratore utilizza un telefono aziendale, il collegamento ad internet o il sistema di posta elettronica in modo promiscuo, per esigenze d'ufficio e per esigenze personali.

Il datore di lavoro può, entro limiti di ragionevolezza vietare l'uso promiscuo dell'apparecchiature aziendali di comunicazione (salva la possibilità per esempio di consultare l'orario dei treni in internet, o la telefonata privata).

Quando l'uso promiscuo delle apparecchiature aziendali sia vietato deve a mio avviso considerarsi legittima, per esempio, per le conversazioni telefoniche la registrazione dei numeri via via chiamati da ciascun apparecchio, nonché la durata di ciascuna conversazione, anche perché questo costituisce una forma di controllo correlata all'esigenza aziendale di contenimento della spesa per il servizio telefonico.

Per quanto concerne la posta elettronica, quando non sia consentito il suo uso da parte del lavoratore per scopi personali, l'imprenditore o altro suo incaricato può accedere liberamente ai messaggi trasmessi o ricevuti da ciascuna postazione.

Se il dipendente è assente per malattia o per ferie è logico che il datore di lavoro possa accedere alla sua casella di posta elettronica al fine di evadere ordini, comunicazioni con i clienti, ecc.

Attenzione quando invece l'uso promiscuo sia consentito.

In questo caso il datore di lavoro corre il serio rischio di leggere messaggi di posta elettronica privati; quindi se concede l'uso promiscuo deve poi rispettare rigorosamente l'inaccessibilità dei messaggi privati che è oltretutto penalmente sanzionata. Infatti la

posta elettronica è parificata a quella cartacea e la sua consultazione costituisce reato (art. 616, 617, 617-bis, 617-ter cod. pen.).

Ecco quindi l'assoluta necessità di regolamentare sia le chiamate telefoniche che l'accesso ai sistemi di posta elettronica.

Da un punto di vista pratico è forse consigliabile regolamentare l'utilizzo della posta elettronica aziendale solo per usi attinenti alla sfera di lavoro, mentre può essere consentito di consultare il proprio indirizzo di posta elettronica utilizzando un sito qualsiasi (yahoo, virgilio o altri).

Può anche capitare che il lavoratore nonostante il divieto di ricevere posta elettronica personale ne riceva comunque di nascosto o all'insaputa del datore di lavoro e nel contempo si assenti per malattia o infortunio.

E' buona norma che sia il gestore del sistema informatico, ovvero il soggetto autorizzato ai sensi dell'art. 30 della Legge sulla privacy, ad accedere, conoscendone la password, al computer del lavoratore in modo che l'eventuale accidentale consultazione di posta elettronica personale possa essere effettuata da soggetto neutrale.

Accenno ora brevemente alla delibera n. 13 del 1 marzo 2007 del Garante per la protezione di dati personali che si propone di dettare delle regole generali che disciplinano l'esercizio dei poteri di trattamento dei dati personali da parte del datore di lavoro effettuato per verificare il corretto utilizzo della posta elettronica e di internet all'interno del rapporto di lavoro.

La delibera è interessante laddove ritiene pienamente operante, come del resto già indicato dal codice sulla privacy, l'art. 4

Stat. Lav., esponendo alcune interessanti riflessioni.

Innanzitutto è consentito effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili se ricorrono gli estremi del legittimo esercizio di un diritto in sede giudiziaria (art. 24 del Codice sulla privacy).

Inoltre nella delibera si identifica come illecito l'impiego di apparecchiature (hardware e software) la cui finalità esclusiva sia il mero controllo del lavoratore, lasciando intendere che il controllo per altre finalità di carattere "difensivo" sia consentito.

Interessante poi è il passaggio nel provvedimento in esame in cui si riferisce che il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto o altre condotte personali poste in essere nel luogo di lavoro. Anche in questo caso lasciando spazio al controllo finalizzato ad accertare inadempimenti contrattuali del lavoratore.

Infine è oltremodo interessante il passaggio nella delibera in cui si fa l'accento alla possibilità che i dati trattati illecitamente non siano utilizzabili, a parte nell'ipotesi di accertamento di eventuali responsabilità civili e penali.

In base a questi elementi mi pare che il Garante, in definitiva, ritenga ammissibile quel bilanciamento di interessi che consenta al datore di lavoro di difendere la propria azienda da comportamenti scorretti o addirittura illeciti del lavoratore.

Quindi si può concludere rilevando come in assenza di una disciplina di dettaglio di carattere normativo vi sia la costante ricerca di un bilanciamento di interessi tra il rispetto della riservatezza e dignità del lavoratore e le preoccupazioni di tutelare l'azienda da

parte dell'imprenditore.

Questa è una ricerca faticosa ma credo che gli strumenti per gli imprenditori per tutelarsi vi siano, purché si proceda con estrema prudenza ed in presenza di effettive violazioni di legge o di contratto da parte del lavoratore da far accertare, come legittimo diritto, in sede giudiziaria.

Avv. Alberto Sbarra