Federico GRILLO PASQUARELLI
Consigliere Sezione Lavoro Corte d'Appello di Torino
Relazione 18.10.2013

I controlli a distanza sui lavoratori in azienda

L'art. 4 dello Statuto dei Lavoratori, le tipologie dei controlli e l'evoluzione della giurisprudenza

Premessa

I poteri di controllo del datore di lavoro sulla prestazione del lavoratore subordinato sono definiti e limitati nel nostro ordinamento da un complesso sistema di fonti normative. Per limitarci all'essenziale, dobbiamo citare il codice civile, la Costituzione, lo Statuto dei Lavoratori e il Codice della Privacy.
In base all'art. 2104 c.c. "il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione" ed il datore di lavoro ha il potere di impartire "le disposizioni per l'esecuzione e per la disciplina del lavoro"; conseguentemente, l'imprenditore ha il potere di verificare, direttamente o mediante i propri collaboratori, l'esatto adempimento della prestazione lavorativa, controllando che il lavoratore usi la diligenza richiesta dalla natura della prestazione ed osservi le disposizioni impartitegli.
Il codice civile, peraltro, non conteneva alcuna norma specifica – al di là dell'art. 2087 c.c., che in generale impone all'imprenditore di adottare tutte le misure "necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro" – volta a tutelare i diritti fondamentali dei lavoratori.
È solo con la Costituzione che hanno trovato riconoscimento i "diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità" (art. 2) e che si è affermata la necessità di tutelare la persona del lavoratore anche all'interno dell'organizzazione imprenditoriale in cui è inserito, e dunque sul luogo di lavoro; è ancora la Costituzione che, dopo avere riconosciuto la libertà dell'iniziativa economica privata, afferma che essa "non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana" (art. 41).
La – felice – sintesi di queste opzioni e del loro possibile contrasto si è avuta con lo Statuto dei Lavoratori, nel quale sono dettati un complesso di garanzie a tutela della libertà, dignità e riservatezza del lavoratore ed una serie di limiti all'ingerenza del datore di lavoro nella sfera personale dei propri dipendenti: a mero titolo esemplificativo, si possono citare l'art. 1 (libertà di manifestazione del pensiero nei luoghi di lavoro), gli artt. 2 e 3 (che disciplinano l'utilizzo delle guardie giurate per scopi di tutela del patrimonio aziendale e l'impiego del personale di vigilanza per il controllo dell'attività lavorativa), l'art. 4 (che regola l'utilizzo di impianti audiovisivi e di altre apparecchiature per il controllo a distanza dell'attività dei lavoratori), gli

artt. 5 e 6 (che disciplinano gli accertamenti sanitari sui lavoratori e le visite personali di controllo).
In tempi più recenti, con l'avvento delle tecnologie informatiche, hanno assunto una particolare rilevanza la raccolta e l'utilizzo dei dati personali dei lavoratori, che sono stati oggetto di disciplina prima nella Legge sulla Privacy (L. 675/1996) e poi, più compiutamente, nel Codice della Privacy (D.Lgs. 196/2003).

L'art. 4 dello Statuto dei Lavoratori

"È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (1° comma):

- "impianti audiovisivi": tutti i sistemi che consentono al datore di lavoro di acquisire, mediante la trasmissione o la registrazione di immagini e/o di suoni, una diretta conoscenza dell'attività svolta dai propri dipendenti (es. telecamere a circuito chiuso, dotate o no di microfoni);
- "altre apparecchiature": ogni altro dispositivo tecnologico che possa essere utilizzato per finalità di controllo a distanza dell'attività dei lavoratori, anche se incorporato negli strumenti di lavoro (es. *software* installati nel centralino telefonico, nel personal computer, nel *server*, che consentano il monitoraggio delle telefonate, della posta elettronica, degli accessi Internet);
- "controllo a distanza": ogni possibilità di sorveglianza, attuabile dalla direzione aziendale, sull'attività dei lavoratori, sia in senso fisico-spaziale (in qualsiasi luogo in cui possano trovarsi i lavoratori, sia all'interno che all'esterno dell'azienda) sia in senso temporale (in modalità continua o discontinua, ed in qualsiasi momento, anche mediante la possibilità di registrare immagini e di visionarle successivamente);
- "attività dei lavoratori": la norma non parla di "attività lavorativa" (come l'art. 3), quindi si riferisce non solo all'adempimento della prestazione lavorativa in senso stretto, ma ad ogni comportamento tenuto dal lavoratore in azienda (es. durante le pause, gli spostamenti all'interno dello stabilimento, ecc.), sul presupposto che le attività non riconducibili alla collaborazione dovuta dal lavoratore subordinato (ex art. 2094 c.c.) sono irrilevanti per l'imprenditore e, quindi, precluse alla sua conoscenza, a tutela non solo della dignità del lavoratore ma anche della sua sfera di riservatezza.

Il primo comma dell'art. 4 vieta in modo assoluto i c.d. controlli intenzionali, o diretti, ossia preordinati a sorvegliare il lavoratore durante lo svolgimento della prestazione, e dunque vieta l'installazione di impianti e apparecchiature aventi come scopo proprio quello del controllo a distanza dell'attività dei lavoratori; la fattispecie non è caratterizzata da un particolare elemento psicologico (dolo specifico), ma presuppone il verificarsi di circostanze oggettive, ossia l'idoneità degli impianti a consentire il controllo a distanza dei lavoratori.

Il divieto colpisce non solo l'esecuzione del controllo ma la semplice potenzialità del controllo. È quindi vietata la stessa installazione di sistemi tecnologici adottati allo scopo di controllare i lavoratori, anche se non ancora messi in funzione; il divieto non è escluso dal fatto che i lavoratori siano stati messi a conoscenza delle apparecchiature e dunque siano stati preavvisati della possibilità di controllo; è vietato anche il controllo destinato ad essere discontinuo, perché esercitato in locali dove i lavoratori si recano saltuariamente; è vietata l'installazione di telecamere nei bagni, negli spogliatoi, nel locale mensa, e in generale in tutti i luoghi destinati esclusivamente alle necessità personali dei lavoratori, o non destinati all'attività lavorativa.

* * * * *

"Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro (ora Direzione Territoriale del Lavoro, *n.d.e.*), dettando, ove occorra, le modalità per l'uso di tali impianti" (2° comma).

Il secondo comma dell'art. 4 consente, a determinate condizioni, i c.d. controlli preterintenzionali, o indiretti: sistemi di videosorveglianza adottati dall'imprenditore per esigenze organizzative, produttive o di sicurezza del lavoro dai quali derivi, come conseguenza accidentale, non specificamente voluta, la possibilità di controllo a distanza dell'attività dei lavoratori. Anche questa fattispecie si caratterizza esclusivamente per la presenza di elementi oggettivi, che attengono alle modalità di funzionamento degli strumenti tecnologici, indipendentemente dalla volontà del datore di lavoro. La procedura autorizzatoria di cui all'art. 4, 2° comma, è necessaria tutte le volte in cui i controlli vengono a consentire in via di normalità, inevitabilmente, il controllo anche delle attività dei lavoratori (v. Cass. 22.3.2011 n. 6498)

Per poter installare apparecchiature che consentono il controllo indiretto, il datore di lavoro deve raggiungere un accordo preventivo con le rappresentanze sindacali aziendali: ciò comporta che il rifiuto di trattare con le r.s.a. ed il ricorso diretto alla D.T.L. costituisce violazione della procedura prevista dall'art. 4, 2° comma, e configura, quindi, condotta antisindacale.

Qualora siano presenti più r.s.a. in azienda, l'accordo deve essere raggiunto con tutte (in questo senso, v. App. Torino n. 91/2012). Il Ministero del Lavoro, nel 2005, ha affermato che sarebbe legittimo il comportamento del datore di lavoro che abbia predisposto l'installazione di alcune telecamere "previo accordo con la sola maggioranza delle r.s.a.", in quanto la necessaria adesione di tutte le r.s.a. finirebbe per attribuire un vero e proprio diritto di veto anche alle rappresentanze più esigue; la tesi è infondata perché, oltre ad essere antiletterale (la norma richiede l'accordo "con

le rappresentanze sindacali aziendali"), è smentita dalla possibilità del datore di lavoro, in difetto di accordo con tutte le r.s.a., di rivolgersi alla D.T.L., il che significa che non esiste alcun potere di veto in capo alle r.s.a..
L'accordo con le r.s.a. sull'installazione degli impianti si configura come un contratto collettivo aziendale con efficacia *erga omnes*, la cui validità non è limitata ai soli lavoratori iscritti alle OO.SS. che lo hanno sottoscritto, ma si estende a tutti i dipendenti dell'imprenditore.
Scopo della norma è quello di sottoporre ad un controllo sindacale la sussistenza delle esigenze oggettive richieste dalla legge e di affidare all'accordo collettivo ogni decisione sulle modalità di funzionamento degli impianti.
In mancanza di accordo con tutte le r.s.a. (anzi, dopo avere esperito senza successo un serio tentativo di accordo), il datore di lavoro non può provvedere all'installazione degli impianti, ma deve chiedere un provvedimento autorizzatorio alla D.T.L., la quale potrà esercitare poteri istruttori, con accessi e ispezioni sul luogo di lavoro. La pronuncia della D.T.L. è volta sia a verificare che le apparecchiature che si vogliono installare rispondano ad "esigenze organizzative e produttive o di sicurezza del lavoro", sia a prescrivere le modalità del loro utilizzo.
Contro il provvedimento della D.T.L. il datore di lavoro, le r.s.a. e i sindacati dei lavoratori di cui all'art. 19 "possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale (ora, Ministro del lavoro e delle politiche sociali, *n.d.e.*)" (4° comma); contro il provvedimento del Ministro è ammesso ricorso al giudice amministrativo (TAR e Consiglio di Stato).
I singoli lavoratori non sono legittimati a proporre il ricorso amministrativo al Ministro, ma possono sempre ricorrere al giudice ordinario, sia contro l'accordo raggiunto dal datore di lavoro con le r.s.a., sia contro i provvedimenti della D.T.L. o del Ministro, qualora li ritengano illegittimi per assenza delle "esigenze organizzative e produttive o di sicurezza del lavoro" che giustificano l'installazione degli apparecchi.

* * * * *

Accanto ai controlli intenzionali, vietati (1° comma), e ai controlli preterintenzionali, consentiti a determinate condizioni (2° comma), la giurisprudenza ha elaborato una terza tipologia di controlli, i c.d. controlli difensivi, che sarebbero rivolti "esclusivamente" ad accertare comportamenti illeciti dei lavoratori, in quanto le norme dello Statuto a tutela della libertà e dignità del lavoratore non escluderebbero il potere dell'imprenditore di controllare "non già l'uso, da parte dei dipendenti, della diligenza richiesta nell'adempimento delle obbligazioni contrattuali, bensì il corretto adempimento delle prestazioni lavorative al fine di accertare mancanze specifiche dei dipendenti già commesse o in corso di esecuzione" (Cass. 14.7.2001 n. 9576, Cass. 2.3.2002 n. 3039, Cass.12.6.2002 n. 8388, Cass. 10.7.2009 n. 16196, tutte peraltro in fattispecie di controlli mediante clienti o dipendenti appositamente inviati dal datore di lavoro, o mediante investigatori privati, non, dunque, mediante apparecchiature di controllo a distanza).

Inizialmente, si è ritenuto che i controlli difensivi, anche se svolti mediante apparecchiature di controllo a distanza, fossero fuori dal campo di applicazione dell'art. 4 e, dunque, sempre leciti: Cass. 3.4.2002 n. 4746 ha affermato che "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 i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate o gli apparecchi di rilevazione di telefonate ingiustificate".
Non si capisce, tuttavia, come si possa distinguere il controllo (vietato) "sull'uso della diligenza richiesta nell'adempimento delle obbligazioni contrattuali" dal controllo (consentito) sul "corretto adempimento delle prestazioni lavorative", volto ad accertare eventuali condotte illecite del lavoratore che sarebbero tenute, necessariamente, durante lo svolgimento dell'attività lavorativa e sul luogo di lavoro; anche dal punto di vista tecnologico, non si capisce come sia possibile predisporre un sistema di videosorveglianza esclusivamente al fine di accertare comportamenti illeciti dei lavoratori senza che ciò comporti, allo stesso tempo, un controllo a distanza sull'esatto adempimento della prestazione lavorativa.
Inoltre, ammettere la categoria dei controlli difensivi significa affidare la verifica circa la legittimità del controllo ad una valutazione da effettuare, necessariamente, *ex post*: soltanto nel momento in cui si accerta la commissione di un illecito da parte del lavoratore, l'esercizio del potere di controllo diventa legittimo; e se non si accerta nessun illecito? Si verifica così un vero cortocircuito logico: anziché fornire una regola che il datore di lavoro deve osservare nel momento in cui decide di controllare il lavoratore, si formula la regola in modo da fare riferimento ad elementi di cui il datore di lavoro viene a conoscenza solo dopo avere effettuato il controllo.
La giurisprudenza più recente della S.C., Sez. Lavoro, quindi, ha ricondotto anche i controlli difensivi nel campo di applicazione dell'art. 4, affermando che "le garanzie procedurali imposte dall'art. 4, 2° comma, della legge n. 300 del 1970 per l'installazione di impianti ed apparecchiature di controllo richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, trovano applicazione anche ai controlli c.d. difensivi, ovverosia a 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 dei beni estranei al rapporto stesso, dovendo escludersi che l'insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti possa assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore" (Cass. 17.7.2007 n. 15892, Cass. 23.2.2010 n. 4375, Cass. 23.2.2012 n. 2722, Cass. 1°.10.2012 n. 16622; la giurisprudenza penale della S.C., invece, resta ancora saldamente ancorata all'idea che le norme dello Statuto dei Lavoratori non vietano i controlli difensivi del patrimonio aziendale

nemmeno se esercitati mediante impianti di controllo a distanza: v. Cass. pen. 12.7.2011 n. 34842, Cass. pen. 18.3.2010 n. 20722).
I controlli difensivi restano certamente consentiti nell'ambito degli artt. 2 e 3 St. Lav., cioè quando sono esercitati a mezzo di guardie giurate per la tutela del patrimonio aziendale o dal personale di vigilanza; le norme dello Statuto dei Lavoratori non escludono nemmeno il potere dell'imprenditore di controllare direttamente o mediante la propria organizzazione gerarchica l'adempimento delle prestazioni lavorative e quindi di accertare mancanze specifiche dei dipendenti già commesse od in corso di esecuzione indipendentemente dalle modalità di controllo, che può avvenire anche occultamente, purché ad opera di persone (altri dipendenti, clienti, investigatori privati, ecc.) e non di impianti audiovisivi ed altre apparecchiature di controllo (v. Cass. 18.11.2010 n. 23303, Cass. 10.7.2009 n. 16196, Cass. 12.6.2002 n. 8388, Cass. 2.3.2002 n. 3039, Cass. 14.7.2001 n. 9576).
Si può convenire, infine, che non rientrano nel campo di applicazione dell'art. 4 gli impianti di videosorveglianza installati all'esterno dei locali aziendali, ai fini di tutela del patrimonio aziendale contro atti illeciti compiuti dai terzi, o anche quelli installati all'interno dell'azienda ma destinati ad operare esclusivamente al di fuori dell'orario di lavoro (v. Cass. 3.7.2001 n. 8998: "sono pertanto legittimi … gli accertamenti operati dall'imprenditore attraverso riproduzioni filmate dirette a tutelare il proprio patrimonio aziendale, al di fuori dell'orario di lavoro e contro possibili atti penalmente illegittimi messi in atto da terzi e quindi anche dai propri dipendenti, i quali a questi non possono non essere in tutto equiparati allorquando agiscano al di fuori dell'orario di lavoro").
Il divieto previsto dall'art. 4, infine, si riferisce alle sole installazioni poste in essere dal datore di lavoro: quest'ultimo, al fine di dimostrare l'illecito posto in essere da propri dipendenti, può utilizzare le risultanze di registrazioni video operate fuori dall'azienda da un soggetto terzo, del tutto estraneo all'impresa e ai lavoratori dipendenti della stessa, per esclusive finalità difensive del proprio ufficio e della documentazione in esso custodita (v. Cass. 28.1.2011 n. 2117: nella specie, i lavoratori, addetti a mansioni di sorveglianza dei locali di un'impresa committente di tale servizio, erano abusivamente entrati nell'ufficio di un dirigente di tale impresa ed avevano rovistato nei cassetti e negli armadi, e tale condotta era stata ripresa dall'impianto di videoregistrazione ivi installato; il datore di lavoro, presa contezza dell'accaduto, aveva licenziato i lavoratori utilizzando, a sostegno della propria decisione, il filmato; la S.C. ha confermato la sentenza n. 652/2007 della Corte d'Appello di Torino che aveva ritenuto ammissibile la produzione in giudizio della registrazione; nello stesso senso v. Cass. 4.4.2012 n. 5371, che ha confermato il licenziamento di un dipendente di un istituto di vigilanza che operava all'interno della guardiola di un Ospedale; l'Ospedale, rilevato un numero e una durata eccessivi di telefonate effettuate dalla guardiola, aveva acquisito i tabulati telefonici e li aveva consegnati all'istituto di vigilanza).
Riguardo a queste ultime ipotesi, tuttavia, si potrebbe obiettare che i lavoratori che operano nei locali di un committente del loro datore di lavoro sono, irrazionalmente, meno tutelati: per il solo fatto che gli impianti audiovisivi sono stati installati da un

terzo (il committente), i dipendenti dell'appaltatore possono essere liberamente controllati, e le risultanze di questi controlli possono essere utilizzate dall'appaltatore contro i suoi dipendenti, a fini disciplinari o risarcitori, e possono anche essere prodotti in giudizio. In tal modo, questi lavoratori hanno un trattamento diverso e meno garantista sia rispetto ai dipendenti del committente (nei confronti dei quali le riprese non sarebbero utilizzabili) sia rispetto ai loro colleghi che operano presso l'appaltatore (nei confronti dei quali quest'ultimo non potrebbe procurarsi né utilizzare informazioni acquisite mediante controlli a distanza ...).

* * * * *

La violazione dell'art. 4 è sanzionata penalmente dall'art. 38 St. Lav. (ora, più precisamente, dal combinato disposto degli artt. 114 e 171 Codice Privacy e dell'art. 38 St. Lav.) con l'ammenda da 154,94 a 1.549,40 euro o con l'arresto da 15 giorni a 1 anno; nei casi più gravi l'arresto e l'ammenda sono applicati congiuntamente.
La violazione dell'art. 4 rende illegittima l'attività di controllo svolta dal datore di lavoro e, quindi, comporta che la documentazione così acquisita è inutilizzabile sia a fini disciplinari sia a fini probatori in un'eventuale azione di risarcimento danni.
La violazione della procedura prevista dall'art. 4, 2° comma (rifiuto di trattare con le r.s.a o con alcune di esse; installazione degli impianti pur in mancanza di accordo con tutte le r.s.a.) costituisce comportamento antisindacale, di cui le OO.SS. possono chiedere la repressione con il procedimento previsto dall'art. 28 St. Lav.

Casistica

Telecamere a circuito chiuso in una struttura sanitaria, destinate al controllo degli ospiti non sempre autosufficienti, che rende possibile il controllo a distanza dell'attività dei dipendenti
CONSENTITO PREVIO ACCORDO CON R.S.A.
Cass. pen. 22.10.2002 n. 42217

Telecamera a circuito chiuso installata in un esercizio commerciale – fotogramma che documenta la sottrazione, da parte di un dipendente, di somme custodite nella cassa – produzione del documento in giudizio di risarcimento danni
INAMMISSIBILE
Cass. 16.7.2000 n. 8250: "l'uso di una telecamera a circuito chiuso, finalizzata a controllare a distanza l'attività dei dipendenti, è illegittimo ai sensi dell'art. 4, 1° comma; ne consegue, sul piano processuale, che non può attribuirsi alcun valore probatorio al fotogramma illegittimamente conseguito"

Telecamere a circuito chiuso, in grado di controllare a distanza l'attività dei lavoratori, la cui attivazione, in mancanza di accordo con le r.s.a., era stata preventivamente autorizzata per iscritto da tutti i dipendenti.
CONSENTITO
Cass. pen. 17.4.2012 n. 22611
SBAGLIATO !! il consenso di tutti i lavoratori non può sostituire l'accordo con le r.s.a., che hanno una propria soggettività giuridica e sono portatrici di un interesse collettivo ulteriore e diverso rispetto alla somma degli interessi individuali dei lavoratori

Tessera magnetica (*badge*) e tornelli che consentono la registrazione dell'identità dei lavoratori e degli orari di entrata e di uscita - Congegno di sicurezza attivato da un *badge* per l'accesso delle auto dei dipendenti all'autorimessa aziendale, che registra l'identità di chi passa e l'orario di passaggio
CONSENTITI PREVIO ACCORDO CON R.S.A.
Cass. 17.7.2007 n. 15892: "il controllo sull'orario di lavoro, risolvendosi in un accertamento circa la quantità di lavoro svolto, si inquadra, per ciò stesso, in una tipologia di accertamento pienamente rientrante nella fattispecie prevista dal secondo comma dell'art. 4" (nello stesso senso Trib. Napoli 29.9.2010; *contra*, Trib. Napoli 23.9.2010, entrambe in *RIDL* 2011, II, 31; il secondo provvedimento sembra accontentarsi del fatto che le modalità concrete di operatività del *badge* non realizzavano "un'esagerata ed esasperata ingerenza da parte dell'azienda nella riservatezza ed autonomia dei dipendenti", cioè pare escludere che il *badge* sia vietato ex art. 4, 1° comma, ma non si pone il problema dell'applicabilità del 2° comma)

Centralino telefonico, con un *software* (Bluè s 2002) che consente la registrazione e la trascrizione automatica su tabulati dei dati (numero interno chiamante, numero esterno chiamato, data, ora e durata della telefonata) relativi alle telefonate in uscita effettuate dai lavoratori
CONSENTITO PREVIO ACCORDO CON R.S.A.
Cass. 1°.10.2012 n. 16622: "i controlli difensivi posti in essere con il sistema informatico Bluè s 2002, ricadono nell'ambito della L. n. 300 del 1970, art. 4, comma 2, e, fermo il rispetto delle garanzie procedurali previste, non possono impingere la sfera della prestazione lavorativa dei singoli lavoratori; qualora interferenze con quest'ultima vi siano, e non siano stati adottati dal datore di lavoro sistemi di filtraggio delle telefonate per non consentire, in ragione della previsione dell'art. 4, comma 1, di risalire all'identità del lavoratore, i relativi dati non possono essere utilizzati per provare l'inadempimento contrattuale del lavoratore medesimo".

Software (Super Scout) installato per protezione della rete aziendale da aggressioni esterne (virus, *spam*, *hackers*), che consente il monitoraggio della posta elettronica e degli accessi ad Internet dei dipendenti, conservandoli in memoria per due mesi
CONSENTITO PREVIO ACCORDO CON R.S.A.

Cass. 23.2.2010 n. 4375: “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, sotto il profilo del rispetto delle direttive aziendali)”.
Un utilizzo sicuramente lecito, e più efficace, dei *software* di controllo della navigazione in Internet è sicuramente l’uso preventivo, cioè l’installazione di *software* che bloccano l’accesso a determinate categorie di siti (*chat*, *social networks*, gioco, gioco d’azzardo, porno) o il *download* di determinati tipi di *files* (musicali, video, ecc.); in questo modo si riduce al minimo la possibilità che il dipendente operi in contrapposizione alle regole della professionalità, dell’onestà e della correttezza che deve tenere in azienda, senza bisogno di controllarlo quotidianamente

Controllo effettuato da un istituto bancario sulla posta elettronica del dipendente, diretto ad accertare *ex post* una condotta attuata in violazione degli obblighi fondamentali di fedeltà e riservatezza: il dipendente era accusato di avere divulgato, mediante la posta elettronica aziendale, notizie riservate concernenti un cliente, e di avere posto in essere, grazie a tali informazioni, operazioni finanziarie da cui aveva tratto vantaggio
CONSENTITO
Cass. 23.2.2012 n. 2722: “tale fattispecie è estranea al campo di applicazione dell’art. 4 dello statuto dei lavoratori. Nel caso di specie, infatti, il datore di lavoro ha posto in essere una attività di controllo sulle strutture informatiche aziendali che prescindeva dalla pura e semplice sorveglianza sull’esecuzione della prestazione lavorativa degli addetti ed era, invece, diretta ad accertare la perpetrazione di eventuali comportamenti illeciti (poi effettivamente riscontrati) dagli stessi posti in essere”.

Lavoratore adibito a registrazione di pratiche amministrative con sistema informatico, con procedura standardizzata – controllo *ex post* da parte del datore di lavoro sui tabulati del computer, da cui risulta una quantità di prestazione notevolmente inferiore a quella degli altri colleghi (per numero di pratiche registrate e tempi di registrazione di ogni singola pratica) e licenziamento per scarso rendimento
LEGITTIMO
App. Torino n. 497/2010: “ciò che l’art. 4 vieta *tout court*, o subordina all’accordo con le r.s.a., è il controllo a distanza dell’attività dei lavoratori e non certo il controllo della produttività degli stessi … quello che l’azienda ha accertato in concreto attraverso i dati del computer è, in sostanza, solamente la produttività individuale di ogni singolo lavoratore, controllo sulla cui legittimità non è consentito dubitare”.

Impianto di localizzazione satellitare GPS su automezzi aziendali, che consente di verificare gli spostamenti del lavoratore e, indirettamente, di accertare se sta lavorando o no
CONSENTITO PREVIO ACCORDO CON R.S.A
Garante Privacy, 4.10.2011 n. 370

BIBLIOGRAFIA

Olivelli F. – *Il difficile bilanciamento tra la tutela della privacy e le esigenze di controllo del datore di lavoro, ADL* 2013, II, 372

Finucci F. – *Ancora sulla legittimità dei controlli a distanza ex art. 4 L. n. 300/1970 diretti a verificare condotte dei dipendenti lesive di beni estranei al rapporto di lavoro, Giur. It.* 2013, p. 402

Rausei P. – *Controllo a distanza: autorizzazione rapida e non sempre necessaria, Dir. & Pratica del Lav.* 2013, p. 339

Visconti A. – *Privacy e lavoro: datore e dipendenti devono imparare a convivere, Altalex* 22.04.2013

Barraco E e Sitzia A. – *Un de profundis per i controlli a distanza del datore di lavoro?, Lav. nella Giur.* 2013, p. 383

Spinelli G. – *La legittimità dei controlli datoriali c.d. difensivi: certezze apparenti in una categoria dubbia, RIDL* 2013, II, p. 113

De Luca Tamajo R. e Mazzotta O. – *Commentario breve alle leggi sul lavoro*, CEDAM, 2013

Frontini G. – *Sulla ritenuta sufficienza dell'accordo dei lavoratori in materia di videosorveglianza, RGLPS* 2012, p. 721

Golisano G. – *Controllo della posta elettronica e accertamento ex post degli abusi del dipendente, RGLPS* 2012, p. 740

Malizia M. – *Orientamenti giurisprudenziali sul potere/dovere di controllo del datore di lavoro, ADL* 2012, p. 1071

Burroni D. e Frosini A. - *La videosorveglianza nel rapporto di lavoro privato*, in AA.VV., *Videosorveglianza e Privacy*, Experta, 2011, p. 69 e ss.

Fusco F. – *Il pomo della discordia: il badge come strumento di controllo a distanza?, RIDL* 2011, II, p. 31

Bellavista A. – *La Cassazione e i controlli a distanza sui lavoratori, RGLPS,* 2010, p. 462

Galardi R. – *Il controllo sugli accessi ad Internet al vaglio della Cassazione, RIDL* 2010, II, p. 564

Ravelli F. – *Controlli informatici e tutela della privacy: alla ricerca di un difficile punto di equilibrio, RCDL* 2010, P. 317

Zoli C. – *Il controllo a distanza del datore di lavoro: l'art. 4 L. n. 300/1970 tra attualità ed esigenze di riforma, RIDL* 2009, I, p. 485

Caruso A.R. - *Videosorveglianza e autorizzazione all'installazione da parte della DPL territoriale*, *Altalex* 01.07.2009

Vallauri M.L. – *È davvero incontenibile la forza espansiva dell'art. 4 dello Statuto dei Lavoratori?*, *RIDL* 2008, II, p. 718

Amoroso G., Di Cerbo V. e Maresca A. – *Statuto dei Lavoratori e disciplina dei licenziamenti*, Giuffrè, 2006