l'officina dei numeri

lavoro in ... breve
circolare informativa 8/2013 – 7.10.2013
Studio Associato Picchio e Gorretta
Corso Felice Cavallotti 62 – 15121 – Alessandria
tel. 0131262842, fax 0131262581
e-mail: info@picgor.it
sito web: www.picgor.it

CONTROLLO A DISTANZA SUI LAVORATORI: VIDEOSORVEGLIANZA E ALTRE FATTISPECIE

LA PRESENTE TRATTAZIONE HA UNO SCOPO MERAMENTE INFORMATIVO E NON HA PRETESA DI ESAUSTIVITA', PER CUI INVITIAMO A VOLER PRENDERE CONTATTO DIRETTAMENTE CON LO STUDIO QUALORA SI RITENGA DI DOVER AFFRONTARE O INCORRERE UNA DELLE TEMATICHE AFFRONTATE NELLA CIRCOLARE. OGNI FATTISPECIE HA DELLE PARTICOLARITA' E DELLE CARATTERISTICHE PROPRIE, LA CUI VALUTAZIONE DEVE ESSERE EFFETTUATA CASO PER CASO E NON PUO' ESSERE GENERALIZZATA

Il potere disciplinare del datore di lavoro è strettamente connesso agli obblighi di diligenza e fedeltà che gravano in capo al prestatore di lavoro e sono disciplinati dagli art. **2104** e **2105** del Codice Civile. Il lavoratore, nei confronti del proprio datore di lavoro, ha l'obbligo di:

- diligenza nell'adempiere all'obbligazione lavorativa (art. 2104 c.c., comma 1);
- obbedienza alle disposizioni per l'esecuzione e per la disciplina impartite dal datore di lavoro e dai suoi superiori gerarchici (art. 2104 c.c., comma 2);
- fedeltà e non concorrenza nei confronti del datore di lavoro (art. 2105 c.c.).

Ai sensi dell'art **2106** c.c. l'inosservanza dei suddetti obblighi può dar luogo all'applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione. Il procedimento disciplinare è stato normato completamente dall'art 7 della legge 300/1970.
Per poter azionare il potere disciplinare, il datore di lavoro deve venire a conoscenza della infrazioni commesse dai lavoratori e tale conoscenza può avvenire in modo diretto (perché ad esempio presente al momento dell'inosservanza) o indiretto a seguito di informazioni ricevute da altri soggetti o, in casi speciali, **attraverso l'utilizzo di controlli a distanza sui lavoratori**.
Analizzeremo di seguito le tipologie di controllo a distanza più diffuse e le modalità di applicazione degli stessi.

Impianti audiovisivi (videosorveglianza)

Dispone l'art. 4 della legge 300/1970:

1. E` vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.
2. 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, dettando, ove occorra, le modalità per l'uso di tali impianti.
...

Occorre precisare che **il divieto di controllo a distanza sussiste anche nei seguenti casi** (Cass. sent. n. 1490 del 6.3.1986 e sent. n. 9211 del 16.9.1997):

- il sistema di videosorveglianza sia installato e non ancora attivo;
- **uso sporadico delle telecamere**, accompagnato o meno da una informativa fornita ai singoli dipendenti;
- il controllo sia destinato ad essere discontinuo perché esercitato in locali dove i lavoratori possono trovarsi solo saltuariamente.

Inoltre, il riferimento dell'art. 4 cit. al "controllo a distanza" è da intendersi sia in senso **spaziale** (controllo geografico) che **temporale** (differito nel tempo) In sostanza è vietato controllare il lavoratore sia **direttamente** e **contemporaneamente** (utilizzo dei monitor), sia **successivamente** (verifica di registrazioni già effettuate).
Va evidenziato come nel corso degli ultimi anni alcune attività economiche (quali ad esempio ricevitorie, tabaccherie, oreficerie, farmacie, edicole, distributori di carburante etc.) sono divenute attività a forte rischio di rapina a causa delle consistenti giacenze di denaro. In questi casi l'utilizzo di impianti audiovisivi rappresenta sia un fattore deterrente che uno strumento per assicurare le fonti di prova in caso di condotte penalmente rilevanti. In tali ipotesi **si presume la sussistenza dei requisiti** per la presentazione della domanda alla Direzione Territoriale del Lavoro (DTL) e, quindi, non è necessario l'accertamento tecnico preventivo (Ministero del Lavoro, nota prot. n. 7162 del 16.4.2012).
Al di fuori dalla casistica sopra evidenziata, particolare attenzione dovrà invece essere posta sui diversi presupposti legittimanti l'installazione.
Il Ministero del Lavoro, sempre con la nota citata sopra, ha stabilito che, **in calce ai provvedimenti di autorizzazione,** gli Uffici devono riportare i seguenti **elementi condizionanti** a cui il datore di lavoro è tenuto ad attenersi:

1. dovrà essere rispettata la disciplina dettata dal Codice in materia di protezione dei dati personali e dai successivi provvedimenti del Garante per la Protezione dei dati personali, in particolare il provvedimento del 8.4.2010;
2. dovrà essere rispettata tutta la normativa in materia di raccolta e conservazione delle immagini;
3. prima della messa in funzione dell'impianto l'azienda dovrà dare apposita informativa scritta al personale dipendente in merito all'attivazione dello stesso, al posizionamento delle telecamere ed alle modalità di funzionamento e dovrà informare i soggetti presenti con appositi cartelli;
4. l'impianto, che dovrà registrare solo le immagini indispensabili, sarà costituito da telecamere orientate verso le aree maggiormente esposte a rischio di furto e danneggiamento (limitando l'angolo delle riprese ed evitando, quando non indispensabili, immagini dettagliate), l'eventuale ripresa di dipendenti avverrà esclusivamente in via incidentale e con criteri di occasionalità;
5. all'impianto non potrà essere apportata alcuna modifica e non potrà essere aggiunta alcuna ulteriore apparecchiatura al sistema, se non in conformità al dettato dell'art. 4 della legge 300/1970 e previa relativa comunicazione alla DTL;
6. le immagini registrate non potranno in nessun caso essere utilizzate per eventuali accertamenti sull'obbligo di diligenza da parte dei lavoratori né per l'adozione di provvedimenti disciplinari (si rimanda ai paragrafi successivi che esplicano la fattispecie anche con esempio);
7. in occasione di ciascun accesso alle immagini (che di norma dovrebbe avvenire solo nelle ipotesi d verificazione di atti criminosi o di eventi dannosi) l'azienda dovrà darne tempestiva informazione ai lavoratori occupati;
8. i lavoratori potranno verificare periodicamente il corretto utilizzo dell'impianto.

Si segnala che **rientra nel divieto** di controllo a distanza sia la **mera attività lavorativa** sia **ogni altra attività svolta in azienda come le pause e gli spostamenti**; mentre **sono legittime**, così come sancito dalla Cass. sent. n. 8998 del 3.7.2001, **le riprese filmate dirette a tutelare il patrimonio al di fuori dell'orario di lavoro e contro possibili atti penalmente illegittimi messi in atto da terzi**, quindi anche dai propri dipendenti che vengono equiparati a terzi quando agiscono al di fuori dell'orario di lavoro. Tuttavia, **tale sistema non può essere attivato durante la prestazione lavorativa**: è questo il caso dei sistemi regolati da temporizzatori che possono essere modificati, per esempio, solo attraverso l'inserimento di una doppia password, di cui una in possesso del datore di lavoro e l'altra del rappresentante dei lavoratori.
Il datore di lavoro una volta espletata la procedura sopra descritta e prima di installare il sistema di telecamere deve:

1. informare i lavoratori della presenza delle telecamere con appositi cartelli di area video sorvegliata;
2. nominare per iscritto i soggetti autorizzati ad accedere nei locali in cui sono conservate le immagini e, se indispensabile, a visionarle.
3. fornire ai lavoratori un'informativa nel rispetto dell'art. 13 del Codice della Privacy
4. posizionare le telecamere verso le zone a rischio, evitando di collocarle in maniera unidirezionale sui lavoratori impegnati nella loro attività;
5. conservare le immagini raccolte solo **per un massimo di 24 ore** dalla rilevazione, salve ulteriori esigenze per festività o chiusura degli uffici e specifiche richieste dell'autorità o della polizia giudiziaria. Solo in alcuni casi, per peculiari **esigenze tecniche** (mezzi di trasporto) o per la **particolare rischiosità** dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ammettersi un tempo più ampio di conservazione dei dati che non può comunque superare la settimana;
6. il sistema deve essere programmato per la cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione.

In generale è **vietato utilizzare le immagini registrate per contestare sanzioni disciplinari al dipendente**, **né ha valore probatorio quanto registrato ai fini della richiesta del risarcimento danni per sottrazione di merci.** In un caso inerente il licenziamento di una barista che le telecamere a circuito chiuso avevano sorpreso a rubare somme custodite nella cassa, la Cassazione ha ribadito l'inammissibilità della prova perché il mezzo di prova era finalizzato a dare dimostrazione di un fatto mediante uno strumento (la telecamera) il cui impiego per finalità di controllo a distanza dell'attività dei lavoratori è espressamente vietato dall'art. 4 della legge 300/1970 (Cass. sent. n. 8250 del 17.6.2000).
Tuttavia, si sta sviluppando un orientamento diverso che ritiene utilizzabili le riprese audiovisive come prova a supporto di un licenziamento per giusta causa, qualora le telecamere siano installate previo accordo con le RSA o autorizzazione della DTL (Cass. sent. n. 6498 del 22.3.2011, cfr. Cass. 4375/2012, 15892/2007).
E' **lecito**, invece, l'utilizzo di videoriprese effettuate con telecamere installate presso una società appaltante per finalità difensive dell'ufficio e della documentazione ivi custodita, per sanzionare dipendenti della società appaltatrice del servizio di sicurezza e vigilanza che vi accedano abusivamente, senza autorizzazione e senza la sussistenza di forza maggiore o necessità di interventi urgenti (Cass. sent. n. 2117 del 28.1.2011).
Si segnala, inoltre, che **qualora l'azienda sia dislocata in più unità produttive sparse in tutto il territorio nazionale, l'accordo per l'installazione delle apparecchiature di controllo va attivato presso tutte le unità produttive** e non è sufficiente un accordo concluso con organi di coordinamento delle RSA di varie unità produttive o con le organizzazioni sindacali territoriali (Cass. sent. n. 9211 del 16.9.1997.
Nel caso in cui non sia possibile raggiungere l'accordo sindacale a livello territoriale e vi sia, quindi, la necessità di ricorrere alla procedura autorizzativa di competenza delle DTL, il Ministero del Lavoro con l'interpello prot. 2975 del 5.12.2005, sancisce che la Direzione generale per l'Attività Ispettiva, al fine di uniformare l'azione degli uffici territoriali, potrà impartire, ove richiesto, eventuali direttive di natura tecnica alle Direzioni territoriali interessate al rilascio delle autorizzazioni.

L'inosservanza delle disposizioni in materia di apparecchi di controllo è punita da **sanzione penale con una ammenda da €uro 154 a €uro 1.549 oppure con l'arresto da 15 giorni a un anno. Nei casi più gravi le pene sono applicate congiuntamente e qualora la pena dell'ammenda sia inefficace, il giudice ha la facoltà di aumentarla fino al quintuplo**. Inoltre, per il mancato rispetto dei provvedimenti in materia di videosorveglianza è prevista, ai sensi dell'art. 162, comma 2-*ter*, D.Lgs 196/2003, **la sanzione amministrativa da €uro 30.000 a €uro 180.000**.

Traffico telefonico

In materia di controllo del telefono aziendale, in linea generale, è **consentito** al datore di lavoro effettuare **l'esame manuale dei tabulati telefonici** ai fini della verifica del traffico telefonico dei propri dipendenti, in quanto tale attività non rientra nell'ambito di applicazione dell'art. 4 della legge 300/1970.
Al contrario, **il contenuto delle conversazioni è costituzionalmente tutelato** e la libertà di segretezza di tale forma di comunicazione può essere limitata solo a seguito di atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge (art. 15 Cost.). E', quindi, **vietato** e punito penalmente (artt. 617 e 617-bis c.p.) **ascoltare o registrare le conversazioni telefoniche**, e l'assenso del lavoratore non esclude la consumazione del reato.
Tuttavia, come chiarito dal Ministero del Lavoro negli interpelli prot. n. 218 del 6.6.2006 e n. 2 del 1.3.2010 se i controlli sono effettuati a campione e non è identificabile il lavoratore né gli altri soggetti coinvolti nella telefonata non vi è reato né si viola la privacy, né, tanto meno, si entra nel campo di applicazione dell'art. 4 cit. in quanto, in tali circostanze, non si tratta di un controllo della prestazione lavorativa bensì di un controllo considerato di tipo difensivo, contabile o qualitativo. Ne è un esempio l'utilizzo di apparecchiature in grado di effettuare registrazioni audio di chiamate in uscita e in entrata in cui le voci di clienti e operatori vengono criptate in fase di registrazione, in modo tale da essere non riconoscibili e non riconducibili all'identità del singolo operatore e cliente (ad es. attività di telemarketing); i primi secondi di conversazione vengono eliminati con conseguente impossibilità di ascoltare il nome dell'operatore; il sistema di monitoraggio non fornisce alcun report di informazioni sul singolo operatore; non vengono tracciati né il nome dell'operatore, né alcun altro dato che possa condurre alla sua identificazione; l'accesso ai dati registrati è rigorosamente tracciabile e limitato ai soggetti autorizzati rispetto alle finalità di monitoraggio. Il Ministero nell'interpello prot. n. 218 del 6.6.2006 chiarisce che è esclusa la possibilità di un controllo dell'attività del lavoratore *"nel caso in cui vi sia un sistema in grado di registrare l'apparecchio chiamato ed il numero della postazione dalla quale è effettuata la chiamata ma comunque sussista una rotazione del personale che usufruisce della postazione stessa, così da impedire una diretta ed inequivocabile correlazione tra l'apparecchio dal quale sono effettuate le chiamate ed il lavoratore*".
Ferma restando la possibilità di disamina manuale dei tabulati e il divieto di ascolto o intromissione nelle conversazioni telefoniche, la Cassazione (sent. n. 4746 del 3.4.2002) ha ritenuto che **l'abuso del telefono aziendale costituisce giustificato motivo di licenziamento indipendentemente dall'entità del danno creato al datore di lavoro.** Aspetto ripreso dalla Cass. sent. n. 10062 del 10.7.2002, secondo cui l**a continua reiterazione di una condotta vietata dal codice disciplinare e oggetto di specifici richiami dall'azienda, fa venire meno la fiducia del datore di lavoro nei confronti del proprio lavoratore**.
A tal proposito, il datore di lavoro, al fine di difendere i propri interessi, può inserire nel codice disciplinare il divieto di effettuare telefonate personali, **salvo casi impellenti**, valutando caso per caso se la telefonata rientra o meno in tali circostanze, e prevedendo anche la possibilità di una sanzione espulsiva in caso di ripetute violazioni. Occorre, però, non tralasciare la questione della privacy del dipendente, **per cui si consiglia di inserire nel codice disciplinare tale divieto facendo contestualmente firmare al lavoratore il consenso a effettuare verifiche sui dati relativi alle telefonate ed informarlo ogni qual volta verrà effettuata tale verifica o se la stessa avverrà sistematicamente**.
E' ammissibile, inoltre, **sanzionare un lavoratore che non abbia vigilato sul telefono assegnatogli creando un danno all'azienda**. Tale situazione si può riscontrare in una sentenza della Cass. sent. n. 15534 del 9.7.2007, nella quale è stata ritenuta **legittima** una **sanzione espulsiva** intimata ad un dipendente accusato di non esser stato responsabile e di non aver vigilato correttamente sul telefono assegnatogli in quanto era emerso che l'**abuso del telefono aziendale** non era attribuibile al dipendente bensì ad **un terzo**, ovvero al figlio.
Al fine di evitare abusi del telefono aziendale il datore di lavoro può ricorrere ad apparecchiature finalizzate ad effettuare un controllo dei costi del servizio telefonico nonché una più corretta e puntuale imputazione contabile di tali costi alle singole unità organizzative. A tal proposito il Ministero del lavoro, con la risposta all'interpello prot. n. 218 del 6.6.2006, ha chiarito che:

- l'**imputazione contabile dei costi telefonici al centro di costo** nel suo complesso, non permette neanche incidentalmente il controllo dell'attività dei lavoratori, per cui tale fattispecie **non rientra nella procedura di cui al comma 2, art. 4, legge 300/1970**;
- qualora l'**imputazione contabile** sia **effettuata nei confronti della singola utenza**, occorre **verificare caso per caso** se tale operazione consenta un controllo indiretto sulla attività lavorativa dei dipendenti (occorre, cioè, **verificare il collegamento tra attività lavorativa e uso dell'apparecchio telefonico,** per cui il controllo è escluso in caso di utenza condivisa da più lavoratori).

Tracciabilità della navigazione in internet

E' **vietato** l'utilizzo di programmi informatici che hanno **la finalità esclusiva di monitorare la prestazione lavorativa**, mentre è **ammesso** l'utilizzo di programmi che hanno altre finalità ma che **incidentalmente permettono** anche il controllo della navigazione, ma solo **previo accordo** con le RSA o, in mancanza, autorizzazione della DTL competente (art. 4, comma 2, legge 300/70).
In questo contesto acquistano fondamentale importanza le **"Linee Guida per posta elettronica ed internet nel rapporto di lavoro"** del Garante della Privacy del 1.3.2007 (v. allegato), le quali, ai fini del principio di correttezza e trasparenza dei dati relativo all'utilizzo delle tecnologie informatiche, **escludono** la possibilità di **controllo informatico all'insaputa dei lavoratori** interessati.
I lavoratori hanno, infatti, **il diritto di essere informati preventivamente ed in modo chiaro, sui trattamenti di dati che possono riguardarli.** Ne consegue che il datore di lavoro **ha l'obbligo di informare i lavoratori**, ai sensi dell'art. 13 del Codice della Privacy, **degli eventuali controlli effettuati**, indicando le principali caratteristiche dei trattamenti, nonché il soggetto o l'unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i propri diritti.
Il datore di lavoro dovrà indicare in modo chiaro e particolareggiato, il corretto utilizzo degli strumenti messi a disposizione dei lavoratori e se, in che misura e con quali modalità vengano effettuati controlli. Come suggerito dallo stesso Garante, può risultare opportuno l'adozione di un **disciplinare interno** da redigere in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente e da sottoporre ad aggiornamento periodico. Nella *policy* interna, a seconda dei casi, il Garante suggerisce di specificare:

- quali comportamenti siano o meno tollerati rispetto alla "navigazione" in Internet (ad es., il *download* di *software* o di *file* musicali), oppure alla tenuta di file nella rete interna;
- in quale misura è consentito utilizzare anche per ragioni personali servizi di rete, anche solo da determinate postazioni di lavoro, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- quali informazioni sono memorizzate temporaneamente (ad es., le componenti di *file* di *log* eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di *back up*, della gestione tecnica della rete o di *file* di *log*);
- se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime, specifiche e non generiche, per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la rete Internet sia utilizzata indebitamente;
- se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato;
- quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato
- l'eventuale segreto professionale cui siano tenute specifiche figure professionali;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi.

E', quindi, **vietato il trattamento dei dati effettuati mediante sistemi hardware e software preordinati al controllo a distanza**, **grazie ai quali sia possibile ricostruire, talvolta anche minuziosamente, l'attività dei lavoratori**; è il caso ad esempio di programmi volti:

- alla riproduzione e memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- alla lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- all'analisi occulta di computer affidati in uso(ad esempio desktop remoti)

Il datore di lavoro deve promuovere ogni opportuna misura, organizzativa e tecnologica, volta a a ridurre l'utilizzo improprio della navigazione che possono così prevenire controlli successivi sul lavoratore. Il Garante suggerisce in merito l'adozione di una o più delle seguenti misure:

- individuazione di categorie di siti correlati o meno alla prestazione lavorativa (*white list* e *black list*);
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni – reputate inconferenti con l'attività lavorativa - quali l'*upload* o l'accesso a determinati siti (inseriti in una *black list*) e/o il *download* di *file* o *software* aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai *file* di *log* riferiti al traffico *web*, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

Si segnala che i sistemi vanno **programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati relativi agli accessi ad internet e al traffico telematico**, la cui conservazione non sia necessaria.

Uso della posta elettronica

Occorre innanzitutto segnalare che **non integra il reato di cui all'art. 616 c.p.** (violazione, sottrazione e soppressione di corrispondenza) **la lettura della e-mail aziendale del dipendente da parte del datore di lavoro quando è previsto che il datore di lavoro stesso o un superiore gerarchico del lavoratore debba essere messo a conoscenza della password del dipendente per l'accesso alla sua casella**. Infatti, in tal caso, la corrispondenza elettronica può dirsi "chiusa" solo nei confronti dei soggetti che non siano legittimati all'accesso dei sistemi informatici di invio o ricezione dei singoli messaggi (Cass. sent. n. 47096/2007).
Come nel caso della navigazione esistono due tipi di programmi informatici per la posta elettronica: **quelli che hanno il fine di monitorare la posta elettronica e quelli che la monitorano solo incidentalmente**. **La prima tipologia di programmi è assolutamente vietata** ai sensi dell'art. 4, comma 1, legge 300/1970, perché volti al mero controllo a distanza dell'attività dei lavoratori, mentre **la seconda tipologia di programmi è ammessa**, previo rispetto della procedura ex art. 4, comma 2, l.cit., ossia accordo con le RSA o, in mancanza, autorizzazione della DTL competente.
Anche in questo caso è importante il rinvio alle **"Linee Guida per posta elettronica ed internet nel rapporto di lavoro"** del Garante della Privacy del 1.3.2007, le quali prevedono, appunto, che il trattamento dei dati relativo all'utilizzo di tecnologie informatiche debba esser ispirato al principio di correttezza e trasparenza e quindi va **esclusa la possibilità di controllo informatico all'insaputa dei lavoratori** interessati.
I lavoratori hanno, infatti, **il diritto di essere informati preventivamente ed in modo chiaro, sui trattamenti di dati che possono riguardarli** ed il datore di lavoro **ha**, pertanto, **l'obbligo di informare i lavoratori** ai sensi dell'art. 13 del Codice della Privacy **degli eventuali controlli effettuati**, indicando le principali caratteristiche dei trattamenti, nonché il soggetto o l'unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i propri diritti.
Il datore di lavoro dovrà, inoltre, indicare in modo chiaro particolareggiato, l'utilizzo corretto degli strumenti messi a disposizione dei lavoratori e se, in che misura e con quali modalità vengano effettuati controlli. Anche in questo caso il Garante suggerisce l'adozione di un **disciplinare interno** da redigere in modo chiaro e senza

formule generiche, da pubblicizzare adeguatamente, da sottoporre ad aggiornamento periodico, specificando quanto segue:

- se e in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica, anche solo da determinate caselle oppure ricorrendo a sistemi di *webmail*, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime per cui verrebbero effettuati e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica sia utilizzata indebitamente;
- **le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso** (specie se programmata), **con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti**.

In caso di utilizzo da parte del datore di lavoro di programmi che consentono un **controllo indiretto** dell'attività dei lavoratori, potrebbe risultare opportuno adottare una serie di accorgimenti per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza e minimizzare l'uso dei dati riferibili ai lavoratori. Per questo è consigliabile che:

- il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad es.: info@ente.it, ufficiovendite@ente.it, etc.), eventualmente affiancandoli a quelli individuali (ad es., m.rossi@ente.it, mario.rossi@società.it);
- il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore;
- il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. É opportuno anche prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati;
- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore la verifica del contenuto dei messaggi ed inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa;
- i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla *policy* datoriale;
- i sistemi vanno programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati relativi al traffico telematico, la cui conservazione non sia necessaria.

Può risultare utile menzionare il caso di un lavoratore al quale è stata estratta e visionata la corrispondenza dal suo account di posta elettronica aziendale contenente anche informazioni personali. Il Garante della Privacy analizzando il caso ha ritenuto che la raccolta dei dati effettuata dall'azienda nel caso di specie non era legittima in quanto **non era stata adottata una policy interna e non era stato indicato in nessun modo al lavoratore le caratteristiche del trattamento dei dati e l'eventualità che potessero esservi controlli sugli strumenti di comunicazione elettronica, compreso l'account di posta elettronica.** Inoltre, poiché era stato possibile per l'azienda recuperare, esaminando la cronologia, le mail del dipendente, per il Garante nel caso di specie **si deve ritenere la sussistenza di un vero e proprio controllo a distanza dell'attività lavorativa** rientrante nel campo di applicazione dell'art. 4 legge 300/1970, senza che l'azienda sia ricorsa alle procedure di accordo con le RSA o, in mancanza, autorizzazione preventiva della DTL (Garante della Privacy, provv. 2.4.2008).

Controllo del computer aziendale (PC, tablet, portatile, ecc.)

Il datore di lavoro non può controllare il contenuto del PC di un dipendente senza averlo prima informato di questa possibilità e senza il pieno rispetto della libertà e della dignità del lavoratore. Questa è quanto emerge dalla decisione del Garante della privacy dinnanzi ad un ricorso [doc. web n. 2149222] presentato da un dipendente che era stato licenziato senza preavviso dalla propria azienda. Dai riscontri è, infatti, emerso che una serie di documenti, sulla base dei quali il datore di lavoro aveva fondato la sua decisione, erano contenuti in una cartella personale del PC portatile assegnato al lavoratore e, contrariamente a quando affermato dall'impresa, non risulta che l'uomo fosse stato informato sui limiti di utilizzo del bene aziendale, né sulla possibilità che potessero essere avviate così penetranti operazioni di analisi e verifica sulle informazioni contenute nel PC stesso.

Il Garante ha ribadito che **il datore di lavoro può effettuare controlli mirati al fine di verificare l'effettivo e corretto adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro ma tale attività può essere svolta solo nel rispetto della libertà e della dignità dei lavoratori e della normativa sulla protezione dei dati personali che prevede, tra l'altro che alla persona interessata debba essere sempre fornita un'idonea informativa sul possibile trattamento dei suoi dati connesso all'attività di verifica e controllo.**

Un caso simile è stato trattato dalla Cassazione nella sentenza n. 18443/2013, nel quale la Corte ha respinto il ricorso di un'azienda che a seguito di un controllo approfondito del PC e della navigazione aveva riscontrato che un proprio dipendente durante l'orario di lavoro e dalla sua postazione si collegava abitualmente alla rete internet nonostante l'attività non fosse prevista per le mansioni cui era adibito a svolgere. Secondo la Cassazione, il computer del dipendente non può essere **perquisito** dal datore di lavoro per contestare una violazione disciplinare, in quanto il PC contiene i cd. **dati sensibili** la cui presa visione viola la riservatezza del lavoratore e oltrepassa la proporzionalità che deve rispettata tra infrazione e **tutela della privacy** della persona. L'azienda nel caso specifico avrebbe dovuto procedere alle contestazioni disciplinari limitandosi alla sola circostanza che il dipendente si collegava ad internet senza che ciò fosse previsto, e nemmeno indispensabile, per le sue mansioni.

Dello stesso parere è anche il Garante della privacy (interpellato dal dipendente) il quale evidenzia che il metodo utilizzato per il controllo, ossia accesso diretto al PC e copia di tutte le cartelle personali, era andato ben oltre il consentito, in quanto il trattamento aveva oltrepassato i limiti di pertinenza e di "***non eccedenza rispetto alle finalità per le quali sono raccolti o successivamente trattati***", come previsto dall'art. 11 del D.Lgs 196/2003. Il Garante aggiunge, inoltre, che il dipendente non era stato informato dell'eventualità di tali controlli e del tipo di trattamento che sarebbe stato effettuato.

GPS - I sistemi Global Positioning System

I GPS o localizzatori satellitari permettono un controllo del cd. personale viaggiante ovvero di tutte quelle figure che, per svolgere la propria prestazione lavorativa, si spostano sul territorio nazionale ed estero, in quanto consente anche di controllare gli spostamenti dei dipendenti, le eventuali pause, i tempi di percorrenza, etc.

Tali sistemi come tutti i sistemi di controllo a distanza possono essere adottati e quindi installati sui veicoli dei dipendenti solo in presenza di esigenze organizzative e/o di sicurezza del veicolo e del conducente e previo accordo con le RSA o in mancanza autorizzazione della DTL.

In via di massima, se viene richiesta l'autorizzazione all'installazione alle DTL queste la rilasciano purché sia concessa all'**autista** la possibilità di **azionare o staccare il rilevamento satellitare, volontariamente**. In caso di **controllo a tempo** viene, invece, richiesto che quando il sistema registri la posizione del mezzo, l'autista sia informato con **l'accensione di una spia posta sul cruscotto** o comunque con **mezzi idonei al fine**.

Badge

Il badge è un mezzo utilizzato per **controllare l'orario di entrata e di uscita** dal luogo di lavoro dei dipendenti e **l'ingresso in aree riservate**.
Il Garante per la Privacy ha ritenuto che sia **lecito** l'utilizzo del badge **per la sola verifica del rispetto dell'orario di lavoro** in quanto non viola le norme sul controllo della prestazione lavorativa. Tuttavia le rilevazioni effettuate mediante "badge" magnetico e conservate in un archivio informatico **costituiscono dati personali e possono essere oggetto di una richiesta di accesso da parte dell'interessato**. Inoltre, trattandosi di un trattamento di dati personali **è necessario informare il soggetto a cui si riferiscono i dati e rispettare tutte le altre norme del Codice della Privacy**.
È, pertanto, **legittimo** rilevare le presenze dei propri dipendenti mediante l'utilizzo di badge in quanto tale modalità di rilevazione non rappresenta una modalità di controllo a distanza dei lavoratori, né consente un controllo durante l'attività lavorativa, vietata dall-'art. 4, legge 300/1970, bensì trattasi di un controllo diretto a verificare l'adempimento dei rapporto di lavoratore.

Visite personali di controllo

Ai sensi dell'art. 6 delle legge 300/1970, le visite personali di controllo sul lavoratore **sono vietate a meno che non siano indispensabili ai fini della tutela del patrimonio aziendale**, in relazione alla qualità degli strumenti di lavoro o delle materie prime o dei prodotti, e sempre a condizione che:

- siano eseguite all'uscita dei luoghi di lavoro;
- siano salvaguardate la dignità e riservatezza del lavoratore;
- avvengano con l'applicazione di sistemi di selezione automatica riferiti alla collettività o a gruppi di lavoratori.

Le ipotesi in cui possono essere disposte le visite personali, nonché le relative modalità devono essere concordate dal datore di lavoro con le RSA, e in difetto di accordo, su istanza del datore di lavoro, provvede la Direzione Territoriale del Lavoro.
Secondo la Cassazione (sent. n. 5902 del 19.11.1984) occorre valutare la reale indispensabilità delle visite, in quanto **le visite personali di controllo devono costituire l'ultima opzione del datore di lavoro**, dopo che lo stesso abbia valutato tutti gli alternativi mezzi di controllo tecnicamente e legalmente attuabili.
Sempre la Cassazione, nella sentenza n. 5902 del 19.11.1984 sancisce che le visite personali di controllo, anche nel caso in cui siano assolutamente indispensabili ai fini della tutela del patrimonio aziendale, **non possono essere tali da oltrepassare i limiti della riservatezza personale, del riserbo e dell'intimità dell'individuo**, il cui superamento è consentito solo agli organi pubblici nell'osservanza delle garanzie di legge ed in relazione ad imprescindibili esigenze di sicurezza. Quindi, **sono vietate le visite personali di controllo che, pur nell'adozione di determinate cautele oggettive, si risolvono in un'ingerenza nell'intimità fisica del soggetto**, come forme di perquisizione o ispezione tali da poter creare nel dipendente un senso di particolare disagio ed anche di degradazione psicologica. Qualora le visite personali di controllo **superino** i suddetti **limiti**, il **lavoratore può rifiutarsi** e in tal caso sono da ritenersi illegittime anche eventuali applicazioni di sanzioni disciplinari da parte del datore di lavoro. Anche la Corte Costituzionale si è espressa in merito, con sent. n. 99 del 25.6.1980, affermando la conformità dell'art. 6 della legge 300/1970 al principio di libertà personale di cui all'art. 13 Cost. ed ha precisato che **le modalità di esercizio del controllo** devono essere dirette a **salvaguardare la tranquillità e serenità dell'ambiente di lavoro** ed a proteggere sia i beni del patrimonio, sia quelli personali degli stessi lavoratori custoditi nei luoghi di lavoro.
Qualora il datore di lavoro, svolte le prassi sopra esposte (accordo con le RSA o in difetto autorizzazione della DTL), decida di effettuare una visita personale di controllo, si ritiene che sia **necessario il consenso del lavoratore da sottoporre ad "ispezione"**, pena la violazione della libertà personale del prestatore di lavoro, costituzionalmente protetta. Tuttavia, nei casi in cui la visita di controllo sia consentita e legittima, il **mancato consenso del lavoratore può giustificare la comminazione di una sanzione sul piano disciplinare** nei suoi confronti, sempre che la possibilità d'irrogare le sanzioni sia **prevista dall'accordo tra datore di lavoro e RSA o, quanto meno, non risulti vietata dallo stesso**, il cui contenuto va interpretato secondo i canoni ermeneutici di cui agli art. 1362 e ss. c.c. (Cass. sent. n. 5902 del 19.11.1984).
Se il datore di lavoro **effettuasse la visita personale in assenza di consenso,** commetterebbe il **reato di violenza privata** (art. 610 c.p.).

Per quanto concerne la possibilità o meno di effettuare verifiche sugli effetti personali del lavoratore, quali ad esempio borse e valigette, la giurisprudenza ha orientamenti contrastanti:

1) **il primo orientamento**, basandosi sulla definizione di "visita personale", ritiene che l'art. 6 della legge 300/1970 si riferisca **solo** alle **verifiche corporali sul lavoratore** (ex plurimis: Cass. sent. n. 1461 del 10.2.1988) così che l'ispezione sulle cose non rientri nella sfera di applicazione delle norme in esame in quanto le "cose" delle persone non sono la "persona del lavoratore";
2) il **secondo orientamento** è esattamente opposto e, rifacendosi alla sentenza della Cass. sent. n. 5902 del 19.11.1984, ritiene che il diritto alla riservatezza può definirsi correttamente come la giusta pretesa di impedire intrusioni altrui all'interno della propria sfera privata, intendendosi con tale ultima espressione l'insieme degli spazi di cui la persona ha un godimento esclusivo. Sicché, la nozione di persona va ben oltre la mera identificazione dell'elemento corporeo e il **termine "personale" indica tutto quanto risulta nella diretta disponibilità del lavoratore**. In conclusione, seconda questa interpretazione, **l'art. 6 dello Statuto dei Lavoratori si estende anche a quegli effetti personali** (come portafogli, borsette, borselli) che possono essere considerati come **diretta pertinenza della persona**, ed appartenenti al normale utilizzo di accessori dell'abbigliamento, sulla base delle ordinarie abitudini o mode.

Appartiene al primo orientamento la sentenza della Cassazione (1461 del 10.2.1988), che ha annullato la pronuncia del giudice del merito che aveva giudicato illegittimo il licenziamento intimato ad un lavoratore per essersi illecitamente appropriato di beni dell'azienda, sulla base del fatto che le modalità con cui il datore di lavoro era venuto a conoscenza del fatto, ossia ispezione eseguita sulla borsa personale del lavoratore, violassero l'art. 6 della legge 300/1970. Nella sentenza, la Corte ha statuito che le visite personali di controllo sul lavoratore riguardano unicamente le ispezioni corporali, ma non anche quelle sulle cose del lavoratore, atteso che la norma citata (da interpretarsi letteralmente) prevede solo la "visita personale" che nell'ordinamento processuale sia civile (artt. 118 e 258 c.p.c.) che penale (art. 309 c.p.p.) è tenuta distinta dall'ispezione di cose e luoghi.

La **violazione dell'art. 6 della legge 300/1970, è punita** ai sensi dell'art. 38 l.cit., **salvo che il fatto non costituisca più grave reato**, **con l'ammenda da euro 154 ad euro 1549 o l'arresto da 15 giorni ad un anno.** Quando, per le condizioni economiche del reo, l'ammenda può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo. Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente e l'autorità giudiziaria ordina la pubblicazione della sentenza penale di condanna nei modi stabiliti dall'articolo 36 c.p.
All'ipotesi base è applicabile la prescrizione obbligatoria ex art. 15 del D.Lgs. n. 124/2004, per cui al datore di lavoro viene prescritta la cessazione della condotta illecita e, in caso di esito positivo, lo stesso viene ammesso al pagamento di una sanzione pari ad €uro 387,25.