



Ai Signori Clienti

Rimini, 25/06/2015

Loro indirizzi

Oggetto: Il Potere di Controllo e di Vigilanza

Il potere di controllo e vigilanza è una diretta conseguenza del potere direttivo che il datore di lavoro ha nei confronti del prestatore (art. 2104 c.c.) e nasce dall'esigenza di garantire, all'interno dell'impresa, l'ordinata ed efficiente esecuzione della prestazione lavorativa, il rispetto del regolamento aziendale e la tutela del patrimonio datoriale anche contro eventuali furti o danni.

Tale potere incontra una serie di limiti in *primis* nello Statuto dei lavoratori e poi in vari interventi giurisprudenziali e del garante della Privacy.

Vista la complessità della materia e le numerose tipologie di controlli (controlli diretti, indiretti, tutela patrimonio aziendale, vigilanza attività lavorativa, accertamenti sanitari, visite personali di controllo, controllo a distanza, ecc..) riteniamo sia utile elaborare una prima parte con la distinzione e analisi generale del **controllo sull'attività lavorativa dei dipendenti** e la **vigilanza del patrimonio aziendale** (cd. **Controllo difensivo**), gli accertamenti sanitari e test attitudinali, e una seconda parte concentrata sui cd. "**controlli a distanza**" tramite "**impianti audiovisivi**" e i relativi provvedimenti del garante.

Controllo sull'attività dei dipendenti (contrattuale)

Controlli legittimi

Il controllo dell'adempimento della prestazione lavorativa è un diritto del datore di lavoro che può essere effettuato:

- Direttamente (2104 c.c.);
- Tramite una sua organizzazione gerarchica (2104 c.c.);
- Utilizzando addetti alla vigilanza (art. 3 300/79);

Controlli diretti o tramite organizzazione gerarchica



ROMINA MACRELLI

Consulente Del Lavoro

Ai sensi del c. 2 dell'art. 2104 c.c., il datore di lavoro può controllare direttamente o mediante l'organizzazione che da lui fa capo e che è conosciuta dai dipendenti, l'adempimento delle prestazioni lavorative o il verificarsi di mancanze specifiche dei dipendenti già commesse o in corso di esecuzione (Cass. 8998/2001).

I superiori gerarchici possono anche effettuare controlli occulti (pedinamento di un lavoratore che effettuava spostamenti al fine di verificare la corretta indicazione dei chilometraggi e rimborsi) Cass. n. 7933/98.

Controlli svolti tramite personale di vigilanza

L'art. 3 dello Statuto dei lavoratori prevede che il datore di lavoro possa controllare l'attività lavorativa dei propri dipendenti, utilizzando altro personale esplicitamente addetto a tale attività, previa comunicazione ai lavoratori dei nominativi degli addetti alla vigilanza interna e le mansioni specifiche da questi svolte.

La Cassazione ha più volte ribadito inoltre che l'art. 3 Stat. Lav. non ha modificato l'art. 2104 c.c. e che quindi il controllo demandato a addetti alla vigilanza non esclude il controllo svolto personalmente o tramite una struttura gerarchica (cass. 3960/81 e 1263/82).

Controlli illegittimi

Guardie giurate

L'art. 2 dello Stat. Lav. prevede che, pur potendo il datore di lavoro impiegare guardie particolari giurate per scopi di tutela del patrimonio aziendale, le stesse non possono contestare ai lavoratori azioni o fatti diversi da quelli che attengono alla tutela del patrimonio aziendale, ne possono accedere nei locali dove si svolge l'attività lavorativa durante lo svolgimento della stessa (se non per motivate esigenze di tutela del patrimonio aziendale).

Controlli a distanza

L'art. 4 L. 300/70 prevede che: **“è vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori”** e quindi assolutamente vietato installare impianti audiovisivi o altre apparecchiature aventi la **mera finalità di controllo a distanza dell'attività dei dipendenti** in quanto **“la vigilanza sul lavoro anche se necessaria nell'organizzazione produttiva va infatti mantenuta in una dimensione umana senza l'esagerazione dell'uso di tecnologie che possano renderla continua ed eliminare ogni zona di riservatezza e di autonomia nello svolgimento del lavoro”** (Cass. 4375/2010).

È necessario chiarire che nonostante l'art. 4 Stat. Lav. parli di “impianti audiovisivi”, la norma si riferisce a **diverse apparecchiature aventi finalità di controllo a distanza**.

Vigilanza del patrimonio aziendale, Controllo Difensivo (extra-contrattuale)

Il controllo difensivo è un controllo volto alla **tutela del patrimonio aziendale** o all'accertamento di **comportamenti illeciti** dei lavoratori che esulino dalla normale attività lavorativa anche se posti in essere durante lo svolgimento della stessa (furti, danneggiamenti ecc.).

Guardie giurate e investigatori privati



ROMINA MACRELLI

Consulente Del Lavoro

Il datore di lavoro può impiegare le guardie particolari giurate soltanto per scopi di tutela del patrimonio aziendale. L'accesso al luogo di lavoro delle stesse è ammesso sia per specifiche e motivate esigenze attinenti ai compiti di tutela del patrimonio aziendale, che al di fuori dell'orario di lavoro.

Nel caso di comportamenti illeciti dei lavoratori che esulino dalla normale attività il datore di lavoro può utilizzare le guardie giurate e investigatori privati per l'accertamento di tali illeciti anche tramite controlli occulti. Alcuni esempi:

- Cass. 829/1992 in materia di utilizzo di agenzia investigativa per verificare appropriazioni di denaro fingendosi clienti;
- Cass. 9836/1995 in materia di utilizzo di un istituto di vigilanza sull'incasso del prezzo e rilascio dello scontrino fiscale da parte di un dipendente;
- Cass. 26991/2009 in materia di controlli svolti da guardie giurate per accertare che un lavoratore omettesse la consegna dello scontrino fiscale ai clienti;
- Cass. 12489 del 2011 in materia di controlli occulti tramite agenzie investigative con la quale si dichiara che basta il sospetto o la mera ipotesi degli illeciti in corso di esecuzione.

Nel caso di inosservanza da parte di una guardia giurata delle disposizioni previste dall'art. 2 L. 300/70, è prevista la sospensione dallo stesso dal servizio, la revoca della licenza nei casi più gravi e il datore di lavoro che viola l'art. 2 è punito con ammenda o con l'arresto da 15 giorni a un anno.

Ispezioni personali

L'art. 6 della L. 300/70 pone un divieto per il datore di lavoro di effettuare, direttamente o tramite terzi, perquisizioni personali del lavoratore, **salvo che siano giustificate** da indispensabili esigenze di **tutela del patrimonio aziendale**, in relazione alla **qualità degli strumenti di lavoro** o delle **materie prime** o dei **prodotti**.

Le perquisizioni così definite possono essere effettuate a condizione che:

- Vengano svolte all'**uscita** dei luoghi di lavoro;
- siano salvaguardate la dignità e la riservatezza del lavoratore;
- avvengano con l'applicazione di **sistemi di selezione automatica** riferiti alla **collettività** o a **gruppi di lavoratori**;
- le modalità vengano concordate dal datore di lavoro con le **rappresentanze sindacali aziendali** oppure, in mancanza, con la **commissione interna**. In difetto di accordo provvede **l'ispettorato del lavoro**.

Secondo la giurisprudenza le visite personali di controllo devono costituire **l'ultima spiaggia**, dopo aver quindi valutato tutte le alternative tecnicamente e legalmente attuabili (cass. 5902/1984). Se quindi fosse possibile e sufficiente prevenire a furti, danneggiamenti o ammanchi tramite adeguate registrazioni dei movimenti delle merci, **l'utilizzo dell'ispezione personale sarebbe illegittima**.

Le visite personali di controllo **non possono essere tali da valicare** i limiti della **riservatezza personale** e del **riserbo dell'intimità dell'individuo** e quindi non possono arrivare a forme di ingerenza nell'intimità fisica o di degradazione psicologica.



ROMINA MACRELLI

Consulente Del Lavoro

Il lavoratore che **si rifiuti** di sottoporsi o si sottragga ingiustamente ad una richiesta di controllo personale legittima è **passibile di una sanzione disciplinare ai sensi dell'art. 7 Stat.Lav.**

Il datore di lavoro che esegua una visita personale illegittima risponde ai sensi dell'art. 38 dello Stat. Lav. (ammenda da 154 a 1.549) nonché del reato di violenza privata se sottopone forzatamente il lavoratore ad un controllo personale senza il necessario consenso dello stesso (**anche nel caso di ispezione legittima ma con rifiuto da parte del lavoratore**).

In merito alla definizione di **visita "personale"** la giurisprudenza è discordante nell'estensione di tale definizione anche sugli effetti personali del lavoratore (borse, valigette ecc.). Un primo orientamento ritiene che l'ispezione sulle **"cose" non rientri nella sfera delle tutele dell'art. 6** in questione mentre il secondo ritiene che in tale definizione debbano **rientrare necessariamente anche gli effetti personali** (portafogli, borse, ecc.).

Accertamenti Sanitari

L'art. 5 della L. 300/70 prevede che il datore di lavoro non possa effettuare controlli diretti sulla idoneità ed infermità per malattia ed infortunio dei propri dipendenti. Per il controllo delle assenze per malattia il datore deve infatti servirsi dei servizi ispettivi degli istituti previdenziali competenti mentre per il controllo dell'idoneità fisica deve servirsi degli enti pubblici ed istituti specializzati di diritto pubblico.

Il datore di lavoro può inoltre servirsi di terzi per verificare circostanze di fatto atte a dimostrare l'insussistenza della malattia o all'accertamento dello svolgimento di un'altra attività lavorativa (Cass. 6236/2001).

Ai sensi del D.Lgs. 81/08 nei casi in cui è obbligatoria la sorveglianza sanitaria, il datore di lavoro è obbligato a fare la visita preassuntiva e ha la facoltà di farla effettuare al suo medico competente o dai dipartimenti medici di prevenzione della ASL.

Test Attitudinali

La sottoposizione dei dipendenti a test attitudinali deve ritenersi legittima, alla luce dell'art. 8 dello Statuto dei lavoratori, nella misura in cui sia realizzata con modalità leali e trasparenti, e sia strettamente finalizzata ad una valutazione dell'attitudine professionale del lavoratore, tenuto conto del tipo di mansioni dedotte in contratto. La funzione dell'art. 8 deve essere, infatti, ridefinita in chiave di protezione della sfera privata dell'individuo nei confronti delle istanze che, pur a prescindere da discriminazioni in senso proprio, tendono a realizzare un integrale coinvolgimento della persona nella vita aziendale. Integra, pertanto, **una violazione di detta norma** la sottoposizione di gruppi di dipendenti ad un test attitudinale, **comportante la risposta a numerose domande concernenti aspetti privatissimi della loro personalità**, ed in qualche caso **miranti anche a coglierne la propensione conflittuale o, invece, collaborativa**. Nel caso di specie, in particolare sono state numerose le domande giudicate prive di un particolare collegamento con le mansioni assegnate ai dipendenti, e quindi lette come indebito tentativo di individuazione della personalità degli stessi (Pretura di Pisa 30/03/1999).

I test attitudinali sottoposti ai lavoratori sul posto di lavoro devono assicurare precise **garanzie** per la **tutela della riservatezza** degli stessi e la **non discriminazione** in base alle loro **opinioni politiche e sindacali** (Garante Privacy 1998).

Secondo il Garante i test attitudinali:

- devono essere **accompagnati da un'adeguata informativa sullo scopo** in base al quale si raccolgono i dati;



- devono **precisare se la risposta è obbligatoria o facoltativa** nonché le **conseguenze della mancata risposta**;
- devono contenere l'**indicazione degli soggetti esterni**, come società specializzate o esperti, che eventualmente **collaborino alla messa a punto dei test e alla successiva elaborazione delle risposte**, e che possono quindi avere accesso ai dati; nel caso in cui si avvalgano di tali soggetti esterni, l'ente pubblico o l'impresa privata dovranno rispettare le disposizioni della legge sulla privacy, le quali permettono queste forme di collaborazione solo in presenza di un atto scritto che designi i soggetti esterni responsabili o incaricati del trattamento;
- i **dati richiesti** devono essere **pertinenti alle finalità** per le quali sono raccolti;
- nel formulare i test si deve tenere conto della **libertà** riconosciuta al **lavoratore** nella Legge 300/1970 **di non manifestare le proprie opinioni politico-sindacali**;
- quando è necessario o opportuno raccogliere valutazioni sulla gestione dell'ente o dell'impresa, i **dati** devono essere **richiesti in forma anonima**.

I Controlli a Distanza

Il c. 1 dell'art. 4 della Stat. Lav. stabilisce un **divieto assoluto di installare impianti audiovisivi o altre apparecchiature aventi la mera finalità del controllo a distanza dell'attività dei dipendenti**, demandando esclusivamente alla dimensione "umana" tali controlli.

Ai sensi dell'art. 4 dello Stat. Lav., sono considerati **controlli a distanza** tutti i controlli effettuati con **impianti audiovisivi e con altre apparecchiature** e la distanza deve essere intesa sia come spaziale che temporale e per cui è vietato un controllo sia a distanza di tipo geografica che una distanza differita nel tempo.

La dottrina e la giurisprudenza ritengono l'art. 4 come una **norma aperta** nel senso che le prescrizioni contenute sono generiche e capaci di adattarsi ai diversi sistemi di controllo a distanza, anche a quelli che verranno in futuro.

Non rientrano nel divieto i sistemi di videosorveglianza che **entrano in funzione al di fuori dell'orario di lavoro**, come deterrente per i furti, purchè il sistema non possa essere attivato durante la prestazione lavorativa (sistemi regolati da temporizzatori che possono essere modificati solo attraverso l'inserimento di una doppia chiave o password di cui una in possesso del datore di lavoro e l'altra del rappresentante dei lavoratori) (Cass. 8998/2001).

Non rientrano nel divieto, e sono legittimamente producibili in giudizio quali prove, le **videoriprese effettuate (anche se in maniera occulta)** al fine di porre in essere i cd. controlli difensivi ossia quelli rivolti non al mero controllo dei lavoratori ma alla tutela del patrimonio aziendale.

Con sentenza n. 3122 del 17/02/2015 è stato inoltre affermato che *"in tema di controllo a distanza dei lavoratori, il divieto previsto dall'art. 4 dello statuto dei lavoratori di installazione di impianti audiovisivi od altre apparecchiature per il controllo a distanza dell'attività dei lavoratori, riferendosi alle sole installazioni poste in essere dal datore di lavoro, non preclude a questo, al fine di dimostrare l'illecito posto in essere da propri dipendenti, di 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, con la conseguenza che tali risultanze sono legittimamente utilizzabili nel processo dal datore di lavoro"* (conforme Cass. 2117/2011).



ROMINA MACRELLI

Consulente Del Lavoro

Sono assolutamente vietati i controlli occulti ovvero quelli effettuati celando i sistemi di videosorveglianza. Il Garante per la Privacy (provvedimento 164 del 2013) ha dichiarato illecito un sistema di videosorveglianza installato in una sede di una società, all'insaputa dei lavoratori, senza accordo sindacale né autorizzazione DTL, formato da apparati di ripresa nascosti all'interno di rilevatori di fumo ed all'interno di segnali luminosi delle uscite di emergenza e collegati ad un registratore digitale.

Il divieto **non è escluso** né dalla circostanza che le apparecchiature di videosorveglianza siano state installate ma **non siano ancora funzionanti**, né dell'eventuale **preavviso dato ai lavoratori**, i quali, quindi, siano stati avvertiti del controllo suddetto, né dal fatto che tale **controllo sia destinato a essere discontinuo** perché esercitato in locali dove i lavoratori possono trovarsi solo saltuariamente (Cass. 1490/86 e Cass. 921/97).

Controllo Preterintenzionale

Fermo restando il divieto di controllo sulla prestazione lavorativa, l'installazione di impianti audiovisivi o di altri sistemi di controllo può essere ammessa, ai sensi del c. 2 e 3, nel caso di **controllo preterintenzionale** (non voluto ma incidentale).

Tale controllo è possibile solo se:

- dovuto ad **esigenze organizzative e produttive** o per **motivi di sicurezza del lavoro**;
- a condizione che ci sia un preventivo **accordo con le RSA**;
- in mancanza delle RSA, a seguito di **autorizzazione all'installazione da parte della Direzione Territoriale del Lavoro**.

Accordo con le RSA

Nel caso di presenza di RSA il datore di lavoro deve cercare **in primis** l'accordo con le stesse e solo successivamente è possibile richiedere l'autorizzazione alla DTL, **la mancata consultazione preventiva delle RSA integra la condotta antisindacale ai sensi dell'art. 28 Stat.Lav.**

Qualora il datore di lavoro abbia **diverse unità produttive**, l'accordo deve essere **ricercato presso tutte le unità produttive**; non è infatti ritenuto sufficiente un accordo concluso con organi di coordinamento delle RSA di varie unità produttive o con le organizzazioni sindacali territoriali (Cass. 9211/97).

Il Ministero del Lavoro ha ritenuto **non sufficiente** l'accordo raggiunto con **le RSA della direzione generale** di un istituto bancario anche qualora l'impianto tecnologico presenti caratteristiche costruttive e di funzionamento standardizzate e del tutto identiche su tutto il territorio nazionale ed ha confermato che **la procedura per l'installazione** delle varie apparecchiature di controllo **va avviata presso tutte le unità produttive sparse sul territorio nazionale** (risposta interpello prot. 2975/2005).

Autorizzazione della DTL

Nel caso in cui non fossero presenti le RSA o non si riesca a raggiungere con le stesse un accordo, il datore di lavoro può inoltrare apposita richiesta alla Direzione Territoriale del Lavoro competente. Anche in questo caso la richiesta e **la relativa autorizzazione devono essere preventive all'installazione**.



ROMINA MACRELLI

Consulente Del Lavoro

Alla domanda dovrà essere allegata una planimetria dei locali con l'indicazione del numero ed il posizionamento delle telecamere e delle postazioni fisse di lavoro, nonché l'indicazione delle caratteristiche tecniche.

La DTL eseguirà un **preventivo accertamento** di tipo tecnico dello stato dei luoghi volto sia a **verificare le esigenze organizzative e produttive e di sicurezza che giustifichino l'installazione**, sia che le **telecamere non riprendano postazioni fisse di lavoro**.

Per alcune attività economiche in cui manchino comunque le RSA e a forte rischio di rapina (tabaccherie, ricevitorie, oreficerie, farmacie, edicole, distributori di carburante ecc.), poiché il sistema di videosorveglianza rappresenta un deterrente ed una prova in caso di condotte penalmente rilevanti, **si presume la sussistenza dei requisiti per la presentazione della domanda e quindi non sarà necessario l'accertamento tecnico preventivo** (Ministero del Lav. nota 7162/2002).

Per il Ministero del Lavoro (nota prot. 7162/2012) il datore di lavoro è tenuto ad attenersi alle seguenti condizioni:

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 dell'8 aprile 2010;
2. dovrà rispettare tutta la normativa in materia di raccolta e conservazione delle immagini;
3. prima della messa in funzione dell'impianto dovrà dare apposita informativa scritta al personale dipendente in merito all'attivazione, al posizionamento delle telecamere ed alle modalità di funzionamento e dovrà informare i clienti 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, 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 da installare, se non in conformità al dettato art. 4 L. 300/70 e previa 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;
7. in occasione di ciascun accesso alle immagini (che di norma dovrebbe avvenire solo nelle ipotesi di verifica 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.

Provvedimento del Garante del 08/04/2010

- è necessario che sussistano principi di liceità, necessità e proporzionalità per l'installazione dei sistemi di videosorveglianza;
- sussiste l'obbligo di apporre cartelli di area videosorvegliata per informare coloro che accedono nei luoghi di lavoro;



ROMINA MACRELLI

Consulente Del Lavoro

- la conservazione delle immagini deve essere limitata a 24 ore, salvo festivi o chiusura degli esercizi commerciali o nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Solo per alcuni casi, per peculiari esigenze tecniche o per particolare rischiosità dell'attività svolta dal titolare del trattamento può ammettersi un tempo più ampio che non può comunque superare la settimana;
- il sistema deve essere programmato per la cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione;
- è confermato il divieto di installazione di apparecchiature preordinate al controllo a distanza dell'attività lavorativa;
- non devono essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa;
- quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro, se può derivare la possibilità di controllo a distanza dei dipendenti va rispettato quanto previsto dai commi 2 e 3 art. 4 legge 300/1970;
- è necessario fornire ai lavoratori una informativa nel rispetto dell'art. 13 del codice della privacy;
- il datore di lavoro deve nominare per iscritto i soggetti autorizzati ad accedere ai locali in cui sono conservate le immagini e, se indispensabile, a visionarle.

Utilizzo delle immagini registrate per sanzionare il dipendente

È in generale vietato l'utilizzo di immagini registrate per la contestazione di sanzioni disciplinari né ha valore probatorio quanto registrato ai fini della richiesta del risarcimento danni per sottrazione di merci.

Con sentenza di Cassazione 8250/2000 è stata dichiarata l'inammissibilità della prova perché il mezzo di prova era finalizzato a dare dimostrazione di un fatto mediante uno strumento il cui impiego per finalità di controllo a distanza è espressamente vietato dall'art. 4 dello Stat. Lav.

Esistono però più recenti ma non ancora consolidati orientamenti che ritengono che qualora le telecamere siano installate previo accordo con RSA o autorizzazione DTL che le stesse siano legittimamente utilizzabili (Cass. 6498/2011).

Da segnalare inoltre che schema di decreto legislativo recante disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di lavoro e pari opportunità, nel modificare l'art. 4 prevede che sono utilizzabili a tutti i fini connessi al rapporto di lavoro (provvedimenti disciplinari ecc..) le informazioni raccolte nel rispetto dell'art. 4 e a condizione che ne sia data adeguata informazione.

Alcune ipotesi in cui è stata riconosciuta la violazione del divieto di controllo a distanza tramite telecamere e nelle quali il comportamento aziendale è stato invece ritenuto conforme:



ROMINA MACRELLI

Consulente Del Lavoro

Ipotesi	Violazione	fonte
In funzione solo fuori orario di lavoro	No, controllo difensivo	CAss. 8998/2001
Orientate sul badge	Si, le riprese non devono essere effettuate per verificare l'osservanza dell'orario di lavoro e la correttezza dell'esecuzione della prestazione lavorativa	Prov. Garante Privacy
Su veicoli adibiti al servizio di linea per trasporto di persone o veicoli addetti al servizio di noleggio con conducente	Si, se riprendono in modo continuativo la prestazione di guida e le immagini vengono utilizzate per controlli sull'attività lavorativa	Prov. Garante Privacy
In luoghi riservati esclusivamente ai lavoratori (bagni, spogliatoi, docce)	Si	Faq Min. Lav. 2010 Prov. Garante Privacy
Orientate verso addetto alla cassa	No, anche occulta, in presenza di fondato sospetto di condotta illecita	Cass. Pen. 20722/2010
Orientate verso addetto alla cassa	Si, se la finalità è quella di controllare l'attività di lavoro senza fondati sospetti	Cass. 4375/2010
In aree in cui i lavoratori possano essere saltuariamente	Si	Garante Privacy
Installate in modo occulto all'insaputa dei lavoratori	Si	Garante Privacy

Ulteriori Forme di Controlli a Distanza

Controllo di Internet, posta elettronica e computer

Ai sensi dell'art. 4 della L. 300/70 è vietato installare sui computer aziendali software finalizzati alla registrazione e al controllo della attività del lavoratore. Devono invece essere oggetto di accordo con le RSA o autorizzazione DTL i programmi con altre finalità ma che incidentalmente permettano il controllo..

Anche per le e-mail aziendali sussiste l'illegittimità di installazione o utilizzo di programmi informatici che abbiano il fine di monitorare la posta e quelli che la monitorano in via incidentale necessitano dell'accordo RSA o autorizzazione DTL. La Cassazione con sentenza n. 47096 del 2007 ha escluso però che la lettura delle e-mail aziendali da parte del datore di lavoro integri il reato di cui all'art. 616 c.p. in quanto la stessa può dirsi "chiusa" solo



ROMINA MACRELLI

Consulente Del Lavoro

nei confronti dei soggetti che non siano legittimati all'accesso. Se quindi l'email è protetta da password si ritiene che la stessa sia legittimamente visualizzabile da tutti coloro che possiedono la chiave di accesso o dal datore di lavoro o superiore che deve essere messo a conoscenza della password.

Le Linee Guida del Garante del 2007

Il Garante ha emanato nel 2007 le "Linee Guida per la posta elettronica e internet" che richiedono che il trattamento dei dati relativo all'utilizzo delle tecnologie informatiche debba essere ispirato al principio di trasparenza con assoluta esclusione di controlli informatici all'insaputa dell'interessato.

Visto che grava sul datore di lavoro l'onere di indicare chiaramente e in modo particolareggiato quali siano le modalità ritenute corrette di utilizzo degli strumenti messi a disposizione, può risultare opportuno adottare un disciplinare interno, pubblicizzato e reso noto ai dipendenti, da sottoporre ad aggiornamento periodico (policy interna). Nella policy deve essere specificato:

- se determinati comportamenti non sono 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 posta elettronica o di rete, anche solo da determinate postazioni di lavoro o 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);
- 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 posta elettronica e la rete Internet sono utilizzate 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;
- 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 (art. 34 del Codice, nonché Allegato B), in particolare regole 4, 9, 10)

Oltre alla policy interna, il garante ricorda che **rimane un dovere del datore di lavoro informare comunque gli interessati ai sensi dell'art. 13 del Codice della Privacy.**

Le linee guida evidenziano poi la necessità che il controllo del datore di lavoro **debba rispettare la dignità dei lavoratori**, in particolare per ciò che attiene al divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori". Il trattamento dei dati derivanti da tali finalità è illecito, a prescindere dall'illiceità dell'installazione **e anche quando i singoli lavoratori ne siano consapevoli.**



ROMINA MACRELLI

Consulente Del Lavoro

Secondo il garante, dal punto di vista organizzativo è quindi opportuno che:

- si valuti attentamente l'impatto sui diritti dei lavoratori (prima dell'installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell'eventuale trattamento);
- si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e l'accesso a Internet; (13)
- si determini quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo.

Il datore di lavoro ha inoltre l'onere di adottare tutte le misure tecnologiche volte a minimizzare l'uso di dati identificativi (c.d. *privacy enhancing technologies*–PETs). Le misure possono essere differenziate a seconda della tecnologia impiegata (ad es., posta elettronica o navigazione in Internet).

a) Internet: la navigazione web

Il datore di lavoro, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (art. 8 l. n. 300/1970; artt. 26 e 113 del Codice; Prov. 2 febbraio 2006, cit.).

In particolare, il datore di lavoro può adottare una o più delle seguenti misure opportune, tenendo conto delle peculiarità proprie di ciascuna organizzazione produttiva e dei diversi profili professionali:

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevenivano determinate operazioni –reputate inconferenti con l'attività lavorativa– quali l'upload o l'accesso a determinati siti (inseriti in una sorta di *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.

b) Posta elettronica

Il contenuto dei messaggi di posta elettronica –come pure i dati esteriori delle comunicazioni e i file allegati– riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale). (14)

Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.

La mancata esplicitazione di una policy al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione.

Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore (posta "in entrata") o di quelli inviati da quest'ultimo (posta "in uscita").

È quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare le esigenze di ordinato



svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza.

In questo quadro è opportuno che:

- il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami@società.com, urp@ente.it, etc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente.it, rossi@società.com, mario.rossi@società.it);
- il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore; (15)
- 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. È parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. (16) 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 (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- 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 predetta policy datoriale.

Le Novità del “Jobs Act”

La bozza dello Schema di decreto legislativo recante disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di lavoro e pari opportunità, prevede la modifica dell'art. 4 della L. 300/70 e più precisamente:

“ART. 23 (Modifiche all'articolo 4 della legge 20 maggio 1970, n. 300 e all'articolo 7] del decreto legislativo 30 giugno 2003, n. 196) 1.

L'articolo 4 della legge 20 maggio 1970, n. 300 è sostituito dal seguente: «ART. 4. Impianti audiovisivi e strumenti di controllo. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso d'impresa con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali. La disposizione di cui al primo comma non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. Le informazioni raccolte ai sensi del primo e del secondo comma sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata



ROMINA MACRELLI

Consulente Del Lavoro

informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196».

La modifica apporta in sostanza le seguenti novità:

- nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, l'accordo può essere stipulato con le associazioni sindacali comparativamente più rappresentative sul piano nazionale o con il Ministero del lavoro e delle politiche sociali;
- le disposizioni di cui all'art. 4 non si applicano agli strumenti utilizzati dal lavoratore **per rendere la prestazione lavorativa** e agli strumenti di registrazione degli accessi e delle presenze;
- Le informazioni raccolte ai sensi del primo e secondo comma sono utilizzabili a tutti i fini connessi al rapporto a condizione che sia data adeguata informazione.

Il Ministero del Lavoro ha poi pubblicato un comunicato stampa per meglio chiarire la portata delle novità:

La norma sugli impianti audiovisivi e gli altri strumenti di controllo contenuta nello schema di decreto legislativo in tema di semplificazioni, adegua la normativa contenuta nell'art.4 dello Statuto dei lavoratori – risalente al 1970 – alle innovazioni tecnologiche nel frattempo intervenute.

*La norma **non “liberalizza”**, dunque, i controlli ma si limita a fare chiarezza circa il concetto di “strumenti di controllo a distanza” ed i limiti di utilizzabilità dei dati raccolti attraverso questi strumenti, **in linea con le indicazioni che il Garante della Privacy ha fornito negli ultimi anni e, in particolare, con le linee guida del 2007 sull'utilizzo della posta elettronica e di internet.***

Come già la norma originaria dello Statuto, anche questa nuova disposizione prevede che gli strumenti di controllo a distanza, dai quali derivi anche la possibilità di controllo dei lavoratori, possono essere installati:

- ***esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale;***
- ***ed esclusivamente previo accordo sindacale o, in assenza, previa autorizzazione della Direzione Territoriale del Lavoro o del Ministero.***

*La modifica all'articolo 4 dello Statuto chiarisce, poi, **che non possono essere considerati “strumenti di controllo a distanza” gli strumenti che vengono assegnati al lavoratore “per rendere la prestazione lavorativa” (una volta si sarebbero chiamati gli “attrezzi di lavoro”), come pc, tablet e cellulari.***

In tal modo, viene fugato ogni dubbio – per quanto teorico- circa la necessità del previo accordo sindacale anche per la consegna di tali strumenti.

*L'espressione “per rendere la prestazione lavorativa” **comporta che l'accordo o l'autorizzazione non servono se, e nella misura in cui, lo strumento viene considerato quale mezzo che “serve” al lavoratore per adempiere la prestazione: ciò significa che, nel momento in cui tale strumento viene modificato (ad esempio, con l'aggiunta di appositi software di localizzazione o filtraggio) per controllare il lavoratore, si fuoriesce dall'ambito della disposizione: in tal caso, infatti, da strumento che “serve” al lavoratore per rendere la prestazione il pc, il tablet o il cellulare divengono strumenti che servono al datore per controllarne la prestazione. Con la***



ROMINA MACRELLI

Consulente Del Lavoro

conseguenza che queste “modifiche” possono avvenire solo alle condizioni ricordate sopra: la ricorrenza di particolari esigenze, l'accordo sindacale o l'autorizzazione.

Perciò, è bene ribadirlo, **non si autorizza nessun controllo a distanza**; piuttosto, si chiariscono solo le modalità per l'utilizzo degli strumenti tecnologici impiegati per la prestazione lavorativa ed i limiti di utilizzabilità dei dati raccolti con questi strumenti.

Il nuovo articolo 4, peraltro, rafforza e tutela ancor meglio rispetto al passato la posizione del lavoratore, imponendo:

- che al lavoratore venga data adeguata informazione circa l'esistenza e le modalità d'uso delle apparecchiature di controllo (anche quelle, dunque, installate con l'accordo sindacale o l'autorizzazione della DTL o del Ministero);
- e, per quanto più specificamente riguarda gli strumenti di lavoro, che venga data al lavoratore adeguata informazione circa le modalità di effettuazione dei controlli, che, comunque, non potranno mai avvenire in contrasto con quanto previsto dal Codice privacy. Qualora il lavoratore non sia adeguatamente informato dell'esistenza e delle modalità d'uso delle apparecchiature di controllo e delle modalità di effettuazione dei controlli dal nuovo articolo 4 discende che i dati raccolti non sono utilizzabili a nessun fine, nemmeno a fini disciplinari.

Restando a Vostra disposizione per ulteriori eventuali chiarimenti cogliamo l'occasione per porgere cordiali saluti.



Romina Macrelli