Il Commerci@lista®

lavoro e previdenza

testata iscritta al Registro Stampa del Tribunale di Biella al n. 576
num. monografico n. 3/2018 an. VII direttore resp. Domenico Calvelli

Vittorio De Luca, Elena Cannone, Giulia Galli
Luciano Vella, Lucio Portaro

I CONTROLLI A DISTANZA NEL RAPPORTO DI LAVORO

Monografie

COMITATO SCIENTIFICO
GRUPPO ODCEC
AREA LAVORO

1. L'art. 4 dello Statuto dei lavoratori

- *L'art. 4 dello Statuto dei lavoratori prima del Jobs Act*

Dopo oltre quarant'anni, le disposizioni dell'art. 4 della legge 20 maggio 1970, n. 300 "*Statuto dei lavoratori"* in materia di controlli a distanza sono state modificate dall'art. 23 del decreto legislativo 14 settembre 2015, n. 151 "*Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunita', in attuazione della legge 10 dicembre 2014, n. 183",* nell'ambito dell'ampio intervento riformatore denominato "*Jobs Act*".

Il lungimirante legislatore del 1970, con l'articolo 4, aveva inteso regolamentare una realtà produttiva nella quale, gli strumenti da cui poteva derivare una possibilità di controllo dell'attività lavorativa erano le apparecchiature "*esterne*" alla prestazione di lavoro, la cui installazione era tuttavia necessaria per soddisfare esigenze specifiche (organizzative, produttive e di sicurezza del lavoro). Al fine di tutelare la dignità del lavoratore, era stato, pertanto, introdotto il divieto assoluto dell'installazione di strumenti aventi come finalità esclusiva quella del controllo dell'attività lavorativa, ammettendo in via eccezionale l'impiego di strumenti e dispositivi per far fronte ad esigenze organizzative e produttive ovvero di sicurezza del lavoro, solo previo ottenimento di una specifica autorizzazione da parte delle rappresentanze sindacali o dell'Ispettorato del lavoro.

Nel corso degli anni sono cominciate, tuttavia, ad emergere difficoltà applicative delle disposizioni di cui sopra, allorquando il controllo a distanza dell'attività lavorativa è divenuto possibile attraverso la consultazione delle informazioni registrate dai dispositivi affidati al lavoratore per lo svolgimento della prestazione lavorativa.

Le nuove tecnologie hanno superato la distinzione concettuale, contenuta nel precedente art. 4, tra strumento delegato al controllo e strumento di lavoro: gli odierni strumenti tecnologici (computer, *smartphone*, *tablet* ect.) costituiscono nell'attuale sistema di organizzazione del lavoro "*normali*" strumenti per rendere la prestazione lavorativa, che consentono al contempo anche un controllo costante e analitico sull'attività del lavoratore[1].

L'evoluzione tecnologica ha, quindi, reso necessario adattare il dettato normativo alla realtà tecnologica delle aziende ed introdurre una distinzione tra due aspetti diversi. Da un lato quello della regolamentazione delle condizioni per l'installazione dell'apparecchiatura dalla quale può derivare il controllo dell'attività; dall'altro, quello della possibilità di monitorare lo strumento per ricavare le informazioni relative allo svolgimento della mansione.

- *L'art. 4 dello Statuto dei lavoratori dopo il Jobs Act*

L'articolo 23, primo comma, del d.lgs. n. 151/2015 detta la nuova disciplina in materia di installazione ed utilizzo di impianti. Come già la precedente disposizione, la norma si applica a tutti i datori di lavoro pubblici e privati di qualsiasi settore merceologico e con qualsiasi numero di dipendenti.

Al riguardo la giurisprudenza è intervenuta negli anni al fine di delimitare in maniera puntuale l'ambito di applicazione delle disposizioni. In particolare, la disciplina non si applica in tutti i casi in cui impianti, sistemi e strumenti dai quali derivi anche la possibilità di controllo dell'attività dei lavoratori siano installati e utilizzati dalle Autorità di Polizia[2]. E' esclusa, altresì, l'applicazione anche nel caso in cui gli impianti e gli strumenti siano utilizzati da agenzie investigative, purché l'incarico affidato dal datore di lavoro riguardi il controllo a distanza dell'attività non lavorativa del dipendente[3].

La norma anche nell'attuale formulazione continua a bilanciare i contrapposti interessi del datore di lavoro, ad esercitare il controllo connesso ai suoi poteri datoriali, e del lavoratore, a preservare una sfera di privatezza intangibile nell'ambito del rapporto.

[1] Cfr. Corte Europea dei diritti dell'uomo, sentenza n. 61496/08 del 12 gennaio 2016
[2] Cfr. Cass. civ., sez. lav., 17 maggio 2013, n. 12091
[3] Cfr. Cass. civ., sez. lav., 12 maggio 2016, n. 9749

La finalità della disposizione non è più quella di impedire ogni forma di controllo sull'adempimento regolare e corretto della prestazione di lavoro, ma di vietare quei controlli che sono posti in essere con forme e con modalità che risultano lesive della dignità dei lavoratori, intesa come manifestazione di riservatezza. Il precedente divieto è stato quindi sostituito da un permesso condizionato.

- *Gli strumenti di controllo*

Va premesso, anzitutto, che l'attuale formulazione dell'articolo 4 identifica due profili della disciplina dei controlli a distanza che vanno considerati separatamente, poiché disciplinano due momenti logicamente distinti.

Il primo nucleo raccoglie le norme destinate a disciplinare la possibilità per il datore di installare strumenti di controllo a distanza, precisando quali sono le condizioni per la legittima installazione dell'apparecchiatura. A questo primo nucleo si aggiungono poi i limiti entro i quali il datore di lavoro può accedere alle informazioni registrate dagli strumenti ed eventualmente utilizzarle, che verrà analizzato in dettaglio di seguito.

Il primo comma del nuovo articolo 4 elenca ora i presupposti che consentono al datore di lavoro l'utilizzo di strumenti dai quali possa derivare anche astrattamente un controllo a distanza dei lavoratori:

(i) esigenze organizzative e produttive;

(ii) sicurezza del lavoro;

(iii) tutela del patrimonio aziendale.

Rispetto al passato, è stata aggiunta l'ipotesi della tutela del patrimonio aziendale, recependo quanto già ammesso dalla giurisprudenza in materia di "*controlli difensivi*"[4]. Il concetto di patrimonio aziendale è, inoltre, di ampiezza tale da ricomprendere tutti i beni aziendali, inclusi quindi anche quelli immateriali (es. marchi e brevetti). Al riguardo si precisa che la giurisprudenza vi ha incluso anche la tutela dell'immagine aziendale da comportamenti illeciti del lavoratore, suscettibili di arrecarvi danno[5].

L'ampio riferimento agli strumenti volti a tutelare il patrimonio aziendale consente di affermare che l'installazione di qualunque tipo di apparecchiatura, che possa essere utilizzata per rilevare dati relativi alla prestazione lavorativa, deve essere adesso sottoposta ad una preventiva autorizzazione. Con la conseguenza, potenzialmente assai restrittiva, che il furto del dipendente potrebbe essere validamente tracciato dal sistema di video sorveglianza e utilizzato ai fini disciplinari, esclusivamente se l'utilizzo di tale impianto è stato autorizzato anche per la tutela del patrimonio aziendale[6].

Il legislatore ha consentito il controllo a distanza non solo mediante gli impianti audiovisivi ma, più in generale, attraverso tutti gli strumenti dai quali derivi anche la possibilità di controllo, ricomprendendo così qualsiasi tipo di tecnologia. In linea di massima, possiamo ipotizzare che vi rientrino:

- telecamere e webcam installate all'interno degli edifici lavorativi e loro eventuali pertinenze (ad esempio aree di parcheggio, garage) per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale che siano in condizione di riprendere l'attività dei lavoratori;
- sistemi di geolocalizzazione (navigazione satellitare e sistemi di antifurto satellitare) installati su veicoli utilizzati da più lavoratori;
- personal computers fissi e portatili e tablets utilizzati senza password da più lavoratori;

[4] In tema di controlli difensivi era sorto un contrasto giurisprudenziale. Secondo un primo orientamento erano ammessi i controlli che riguardavano comportamenti dei lavoratori lesivi del patrimonio e dell'immagine aziendale. Non erano quindi vietati i controlli intesi a rilevare specifiche mancanze e comportamenti estranei alla normale attività lavorativa nonché illeciti (cfr. Cass. civ., sez. lav., 12 ottobre 2015, n.20440). Secondo una diversa tesi i controlli difensivi rientravano invece in ogni caso nell'ambito di applicazione delle disposizioni di cui al precedente articolo 4. L.300/70 (cfr. Cass. civ., sez. lav., 1 ottobre 2012, n. 16622). Sul punto, vedi meglio *infra.*

[5] Cfr. da ultimo Cass. civ., sez. lav., 10 novembre 2017 n. 26682; Cass. civ., sez. lav., 23 febbraio 2012, n. 2722

[6] In materia di cd. Controlli difensivi, in senso contrario, vd. Cass. civ., sez. lav., 8 luglio 2016, n.22662.

- telefoni cellulari (anche del tipo smartphone) utilizzati senza codici personali da più lavoratori;
- centralino telefonico elettronico;
- registratori di cassa elettronici;
- tessere elettroniche (o strumenti assimilabili)
- software per controlli informatici.

- *Procedura sindacale: accordo sindacale*

Quanto alla procedura da espletare per poter utilizzare tali strumenti, il datore di lavoro può alternativamente sottoscrivere un accordo con la rappresentanza sindacale unitaria (RSU) o con le rappresentanze sindacali aziendali (RSA).

Con riferimento all'ipotesi in cui sia costituita in azienda una RSU, varrà la maggioranza prevista espressamente nell'accordo istitutivo delle RSU (cfr. articolo 4 del Testo Unico della Rappresentanza del 10.01.2014).

Più complicato il criterio di validità del contratto collettivo nell'ipotesi in cui in azienda siano costituite delle RSA[7]. Al riguardo il Ministero del lavoro con interpello n. 2975 del 2005 aveva già precisato che è sufficiente la sola maggioranza della RSA, in quanto la regola dell'unanimità potrebbe andare a costituire un vero e proprio diritto di veto.

Una delle principali novità riguarda - sicuramente - la possibilità per le aziende con più unità produttive ubicate in diverse province della stessa regione o in più regioni, di sottoscrivere accordi con le associazioni sindacali territoriali o nazionali comparativamente più rappresentative sul piano nazionale, anziché dover sottoscrivere accordi per ogni singola unità produttiva. E' ipotizzabile, ancorché non espressamente stabilito, che tale meccanismo possa applicarsi anche ai gruppi di imprese, la cui capogruppo stipuli per sé e per altre imprese del gruppo un accordo con le organizzazioni sindacali nazionali.

- *Procedura amministrativa: Ispettorato nazionale del lavoro*

Con riferimento alla procedura alternativa e sussidiaria del provvedimento di autorizzazione adottato dall'Ispettorato nazionale del lavoro (Inl), è necessario che il datore di lavoro depositi apposita istanza nella quale devono essere specificati i contenuti tecnici e strumentali degli impianti di controllo. L'autorità amministrativa potrà invero dettare indicazioni precettive circa le modalità di utilizzo.

È stata abrogata la possibilità di impugnare mediante ricorso alla competente Direzione generale del Ministero del lavoro le decisioni assunte dall'autorità amministrativa. Il provvedimento di autorizzazione o di diniego è definitivo e quindi inappellabile.

- *Gli strumenti di registrazione delle presenze e gli strumenti di lavoro*

La più rilevante novità introdotta con il d.lgs. 151/2015 è contenuta nel seconda comma del nuovo articolo 4, il quale prevede che l'utilizzo degli strumenti necessari al lavoratore per svolgere la propria prestazione lavorativa, così come le apparecchiature di rilevazione e di registrazione degli accessi e delle presenze al lavoro, non richiedono la sussistenza delle causali (organizzative, produttive, di sicurezza e di tutela del patrimonio aziendale) e non esigono il preventivo accordo sindacale né autorizzazione dell'autorità amministrativa.

L'esclusione dal regime autorizzatorio per tali categorie di strumenti costituisce senza dubbio una delle principali novità della riforma, idonea ad ampliare sensibilmente la libertà del datore di lavoro nell'impiego degli strumenti tecnologici.

Con riferimento agli strumenti di rilevazione degli accessi e delle presenze l'impiego di tali strumenti non appare idoneo a ledere la dignità e la riservatezza del lavoratore, essendo

[7] Sotto la precedente norma la Corte di Cassazione aveva infatti escluso la validità degli accordi sottoscritti con organi di coordinamento delle RSA, precisando che l'individuazione dei soggetti abilitati dall'articolo 4 doveva ritenersi tassativa (cfr. Cass. civ., sez. lav., 16 settembre 1997, n. 9211)

piuttosto finalizzato a riscontrare la presenza del dipendente sul luogo di lavoro[8]. Il datore di lavoro potrà quindi liberamente installare l'apparecchiatura necessaria per rilevare l'accesso e la presenza. Un esempio classico di questo tipo di strumenti è rappresentato da tessere elettroniche (badge) o sistemi di rilevazione biometrici.

Quanto agli strumenti di lavoro, affinché questi possano essere esclusi dall'onere di autorizzazione è necessario che vengano "*utilizzati dal lavoratore*" e che gli stessi siano utilizzati per "*rendere la prestazione lavorativa*".

Il primo requisito comporta che rientrino in tale categoria solo gli strumenti che il lavoratore utilizza direttamente per lo svolgimento della propria attività lavorativa, per cui è richiesta una partecipazione attiva del lavoratore. Inoltre, lo strumento deve costituire un mezzo funzionale alla corretta esecuzione della mansione.

Il Ministero del lavoro, con nota del 18 giugno 2015, ha chiarito che rientrano sicuramente in questa categoria: il computer, la posta elettronica aziendale, l'accesso ad internet. Sono invece esclusi gli eventuali *software* applicativi che vengono installati sul computer che, per esempio, consentano di controllare l'attività del lavoratore con modalità non percepite dall'utente ed in modo del tutto indipendente rispetto alla normale attività dell'utilizzatore. Tali *software* non possono essere qualificati quali strumenti per rendere la prestazione di lavoro, con la conseguenza che l'eventuale installazione è soggetta ad un preventivo accordo aziendale o all'autorizzazione amministrativa[9].

Sul punto è intervenuto anche l'Ispettorato nazionale del lavoro, con il provvedimento n. 2 del 7 novembre 2016, affermando che i sistemi di geolocalizzazione installati sugli strumenti di lavoro rappresentano un elemento aggiuntivo, non utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa ma per rispondere ad esigenze di carattere assicurativo, organizzativo e produttivo o per garantire la sicurezza del lavoro. Motivo per il quale, sempre a parere dell'Inl, "*le relative apparecchiature possono essere installate solo previo accordo stipulato con la rappresentanza sindacale ovvero, in assenza di tale accordo, previa autorizzazione da parte dell'Ispettorato nazionale del lavoro"* con la precisazione che "*solo in casi particolari*", ossia qualora siano installati per consentire la "*concreta ed effettiva attuazione della prestazione lavorativa…ovvero l'installazione sia richiesta da specifiche normative di carattere legislativo e regolamentare…si può ritenere che gli stessi finiscano per "trasformarsi" in veri e propri strumenti di lavoro*".

Ulteriore profilo interpretativo è anche giunto con il Provvedimento n. 138 del 16 marzo 2017 del Garante per la protezione dei dati personali (di seguito "*Garante Privacy*") che, allineandosi proprio alla circolare dell'Ispettorato nazionale del lavoro, ha affermato quanto segue: "*il sistema di localizzazione non è direttamente preordinato all'esecuzione della prestazione lavorativa, con conseguente applicazione dell'art. 4, comma 1"*. E proprio a questo riguardo non può non segnalarsi che, sempre secondo le prescrizioni del Garante Privacy, l'assolvimento dell'onere procedurale di cui all'art. 4 dello Statuto dei lavoratori consente di effettuare il trattamento dei dati di cui si parlerà nel prosieguo, senza il necessario consenso dei lavoratori. Ciò in quanto il trattamento sarebbe finalizzato al perseguimento di un legittimo interesse volto a soddisfare specifiche esigenze (ossia organizzative e produttive; per la sicurezza sul lavoro e per la tutela del patrimonio aziendale). Un aspetto che non è ancora stato oggetto di specifiche valutazione riguarda quegli strumenti di lavoro che il dipendente è autorizzato ad utilizzare nella propria sfera strettamente privato (es. telefono cellulare ad uso promiscuo) e cioè per ragioni del tutto estranee alla propria attività lavorativa. In tale ipotesi, l'utilizzo per fini extralavorativi non consente un tracciamento dei dati né tanto meno un loro utilizzo ai fini del rapporto di lavoro. Si tratterà quindi di individuare dei sistemi tecnologici che siano in grado di rimarcare la distinzione tra la sfera professionale e sfera personale o in alternativa di precluderne l'utilizzo privato.

[8] In precedenza la giurisprudenza si era espressa nel senso di includere anche tali strumenti in quelli richiedenti l'accordo sindacale o l'autorizzazione amministrativa (cfr. Cass. civ., sez. lav., 17 luglio 2007, n. 15892)

[9] Cfr. Cass. civ., sez. lav., 19 settembre 2016, n. 18302; Provvedimento del Garante Privacy n.303 del 13 luglio 2016; Circolare del Ministero del Lavoro n. 4 del 26 luglio 2017

2. Tutela della riservatezza del lavoratore

Il tema della tutela della riservatezza del lavoratore è un nodo nevralgico e centrale nelle disamine giuslavoristiche relative all'art. 4 della legge 300/1970. Non a caso lo stesso titolo I dello Statuto dei lavoratori è intitolato "*Della libertà e dignità del lavoratore*".

Si rammenta, infatti, che il potere di controllo, unitamente al potere disciplinare e al potere direttivo, rientra tra i poteri che il datore di lavoro ha per verificare l'esatto adempimento degli obblighi contrattuali (obbligo di obbedienza, diligenza e fedeltà) da parte del lavoratore.

Tuttavia non si tratta di un potere assoluto, dovendo essere esercitato nel pieno rispetto del diritto del lavoratore alla riservatezza, inteso nella sua accezione sia di diritto alla privacy sia di modalità di tutela della sua libertà di autodeterminazione.

La protezione della dignità e della riservatezza dei lavoratori è diventata nel tempo di primissima importanza in ragione del processo tecnologico e dell'evoluzione che si è registrata nel campo informatico, ove si assiste all'impiego di strumenti (quali posta elettronica ed internet) nonché all'implementazione di sistemi (ad es. quelli di geolocalizzazione) capaci di controllare, anche in maniera capillare, ogni singola attività svolta dal lavoratore nell'ambito della propria prestazione lavorativa, seppur creati ed ideati non certo per tale scopo[10].

Ma anche il diritto del lavoratore alla riservatezza non costituisce un diritto assoluto, in quanto deve essere contemperato con "*altri diritti ed interessi legittimi del datore di lavoro*"[11].

Proprio nell'ottica di delineare un bilanciamento tra tutela del lavoratore e legittime esigenze datoriali è intervenuto il Garante per la protezione dei dati personali (di seguito "*Garante Privacy*"), affermando che il datore di lavoro deve, nell'esercizio della propria attività imprenditoriale, rispettare, in ogni caso, i seguenti principi:

1. principio di necessità, secondo cui i sistemi e i programmi informatici devono essere configurati in modo da ridurre al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice Privacy);
2. principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti svolti devono essere rese note ai lavoratori (art. 11, comma 1, lett. a) del Codice Privacy). In base ad esso, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza (richiamato dallo stesso art. 4 dello Statuto dei lavoratori), gravando appunto sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo, ritenute corrette, degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli;
3. i principi di pertinenza e non eccedenza, per cui i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b) del Codice Privacy). Ciò significa che (i) il datore di lavoro deve trattare i dati nella misura meno invasiva possibile e (ii) le attività di monitoraggio devono essere svolte solo da soggetti preposti.

Lo stesso Regolamento Europeo in materia di protezione dei dati personali 2016/679, entrato in vigore il 25 maggio 2016 e pienamente operativo dal 25 maggio 2018, conferma la necessità di un peculiare bilanciamento idoneo a coniugare i due contrapposti interessi, vale a dire quello del lavoratore e quello del datore di lavoro. Ciò allorquando all'art. 88 legittima gli stati membri all'adozione di norme specifiche rispetto al trattamento dei dati nell'ambito del rapporto di lavoro, a tutela della "*dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati*".

E' appena il caso di ricordare che il comma 3 dell'art. 4 dello Statuto dei Lavoratori, nella sua nuova formulazione, prevede che le informazioni "*raccolte ai sensi dei commi 1 e 2*" sono

[10] Cfr. L. Perina, *L'evoluzione della giurisprudenza e dei provvedimenti del garante in materia di protezione dei dati personali dei lavoratori subordinati*, in *Riv. it. dir. lav.*, 2010, II, p. 306

[11] Cfr. Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro del 29 maggio 2002 - WP 55

utilizzabili a tutti i fini connessi al rapporto di lavoro (ivi compresi, quindi, quelli disciplinari), a condizione che:

- sia stata data adeguata informazione al lavoratore circa le modalità d'uso degli strumenti stessi e di effettuazione dei controlli e
- siano state rispettate le disposizioni di cui al Codice Privacy.

L'espresso richiamo al Codice Privacy obbliga così il datore di lavoro a dover rispettare quanto in esso disposto nonché le indicazioni che si traggono dai provvedimenti adottati, di volta in volta, dal Garante Privacy in materia.

- *Le linee guida del Garante Privacy sull'utilizzo di Internet e posta elettronica*

L'utilizzazione della posta elettronica e di internet ha da sempre determinato dubbi circa la corretta ingerenza del datore di lavoro sui flussi informativi relativi ai dati personali dei dipendenti da questi ricavabili. Infatti, non di rado, nell'ambito dell'organizzazione aziendale, le informazioni di carattere personale del dipendente passano attraverso i canali di comunicazione funzionali all'esercizio della prestazione lavorativa, come nel caso della posta elettronica.

Con riferimento alla posta elettronica, lo stesso Garante Privacy ha osservato che la raccolta sistematica e massiva delle comunicazioni in transito sugli account aziendali dei dipendenti e la loro memorizzazione per un lungo periodo è un'attività in contrasto con la disciplina di settore in materia di controlli a distanza di cui all'art. 4 dello Statuto dei lavoratori[12]. Come se non bastasse, il contenuto dei messaggi di posta elettronica, i dati esteriori delle comunicazioni e i *file* allegati, costituiscono forme di corrispondenza assistite da garanzie di segretezza "*protette*" costituzionalmente e dalle norme penali a tutela dell'inviolabilità dei segreti (si pensi ad es. agli artt. 2 e 15 Cost. o all'art. 616, 4° comma, c.p.).

In questo contesto una indubbia rilevanza è rivestita, quindi, dalle "*Linee guida*" in materia Internet e Posta elettronica emanate dal Garante Privacy con la deliberazione n. 13 del 1 marzo 2007, pienamente attuali. Basti al riguardo considerare che il Ministero del lavoro e delle politiche sociali, nel comunicato del 18 giugno 2015 sul "*nuovo*" art. 4 dello Statuto dei lavoratori, ha affermato che esso "*è in linea con le indicazioni che il Garante ha fornito negli ultimi anni e, in particolare, con le linee guida del 2007 sull'utilizzo della posta elettronica e di internet*".

Nello specifico, il Garante Privacy, nelle sue linee guida del 2007, ha stabilito che grava sul datore di lavoro l'onere di informare i dipendenti, in modo chiaro e dettagliato circa le modalità di utilizzo degli strumenti informatici, ivi inclusa la posta elettronica, messi a disposizioni dei lavoratori nello svolgimento della loro attività lavorativa, nonché se, in che misura, e con quali modalità vengono effettuati controlli.

Il summenzionato onere informativo, secondo il Garante Privacy, deve essere assolto tramite l'adozione di una policy aziendale (i) in cui siano chiaramente indicate, senza l'utilizzo di formulazioni generiche, le regole per l'utilizzo dei sistemi informatici, (ii) che venga pubblicizzata adeguatamente e (iii) che sia soggetta ad aggiornamenti periodici. Al suo interno, continua il Garante Privacy, debbono essere indicati:

- i comportamenti non tollerati rispetto alla navigazione in Internet;
- in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete;
- quali informazioni vengono memorizzate temporaneamente e chi vi può accedere legittimamente;
- se e quali informazioni verranno conservate per un periodo più lungo;
- se e, in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, indicando le ragioni legittime in cui verrebbero effettuati e le relative modalità;

[12] Cfr Provvedimento del Garante Privacy n. 547 del 22 dicembre 2016

- le conseguenze, anche di tipo disciplinare, che il datore di lavoro si riserva di trarre qualora si accorga che la posta elettronica e la rete internet siano stati utilizzati indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la prosecuzione dell'attività lavorativa in caso di sua assenza, specie se programmata;
- se sono consentite modalità d'uso personale dei mezzi, con pagamento o fatturazione a carico dell'interessato;
- quali misure sono adottate per realtà lavorative nelle quali debba essere rispettato il segreto professionale cui siano tenute specifiche figure professionali;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi.

In ogni caso, specifica il Garante Privacy, il datore di lavoro è tenuto a rilasciare idonea informativa agli interessati, ai sensi dell'art. 13 del Codice privacy, circa il corretto utilizzo dei mezzi e gli eventuali controlli effettuati sugli stessi, inoltre il trattamento effettuato mediante sistemi *hardware* e *software* non deve essere preordinato al controllo a distanza, poiché sarebbe possibile ricostruire l'attività dei lavoratori.

Il datore di lavoro, a parere del Garante Privacy, è tenuto ad adottare ogni opportuna misura volta a prevenire il rischio di utilizzi inopportuni dei dati personali e che consenta di:

- procedere ad una attenta valutazione, prima di installare apparecchiature suscettibili di realizzare un controllo a distanza, dell'impatto sui diritti dei lavoratori;
- individuare preventivamente i lavoratori a cui è accordato l'utilizzo della posta elettronica e l'accesso a internet;
- determinare quale ubicazione è riservata alla postazione di lavoro per ridurre al minimo il rischio di un loro impiego abusivo.

In tal senso, secondo il Garante Privacy, il datore di lavoro è tenuto a implementare all'interno della sua azienda una serie di misure tecnologiche che siano tese con riferimento:

- alla navigazione in internet, a minimizzare l'uso di dati identificativi, risultando quantomeno opportuno:
  a. pre-determinare categorie di siti considerati correlati o meno con la prestazione lavorativa;
  b. trattare i dati in forma anonima o in modo tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni;
  c. limitare la conservazione di dati nel tempo al solo perseguimento di finalità organizzative, produttive e di sicurezza;
- all'utilizzo della posta elettronica a:
  a. rendere disponibili indirizzi di posta elettronica condivisi tra più lavoratovi, affiancandoli a quelli individuali;
  b. valutare la possibilità di attribuire al lavoratore un diverso indirizzo di posta elettronica destinato ad uso privato;
  c. mettere a disposizione di ciascun lavoratore apposite funzionalità di sistema che consentano di inviare automaticamente messaggi di risposta contenente le coordinate di un altro soggetto, in caso di assenza dell'interessato;
  d. prevedere, nel caso in cui un lavoratore si assenti e si debba conoscere il contenuto dei messaggi di posta elettronica, la possibilità che l'interessato venga messo in grado di delegare ad un altro lavoratore il controllo delle proprie mail, ritenute rilevanti per lo svolgimento dell'attività lavorativa;
  e. suggerire la pre-impostazione di messaggi di posta elettronica contenenti un avvertimento ai destinatari, nei quali venga dichiarata l'eventuale natura non personale dei messaggi stessi.

- *Il Provvedimento Generale del Garante Privacy sulla videosorveglianza*

L'installazione e l'utilizzo degli impianti di videosorveglianza, oltre a consentire potenzialmente un controllo sull'attività lavoratori, comportano un trattamento di dati personali e, quindi, richiedono anch'essi il rispetto della normativa in materia di privacy.

Il Garante Privacy con il Provvedimento generale dell'8 aprile 2010 ha affermato che:

- gli interessati (alias, i dipendenti) devono essere sempre informati che stanno per accedere ad una zona videosorvegliata. A tal fine il Garante Privacy ha indicato un modello semplificato di informativa (c.d. cartello) che (i) deve essere reso visibile prima di accedere all'area oggetto delle riprese e (ii) rinvii poi a un testo completo contenente tutti gli elementi di cui all'art. 13 del Codice Privacy;
- le telecamere debbono essere posizionate verso le "zone a rischio" cercando, nei limiti del possibile, di non collocarle in maniera unidirezionale verso i lavoratori in attività;
- le immagini debbono essere conservate per un periodo temporale limitato, massimo 24 ore (a decorrere dalla rilevazione). In casi specifici è consentita una conservazione temporale delle immagini più ampia, ma per un termine che non può eccedere la settimana, salvo eventuale richiesta preliminare ex art 17, comma 2, del Codice Privacy (ndr adempimento abrogato dal Regolamento Europeo sul trattamento dei dati che diverrà operativo dal 25 maggio 2018), da presentarsi al Garante Privacy qualora si intenda conservare i dati per una durata superiore;
- l'accesso ai dati sia consentito ai soli incaricati dell'azienda che, in ragione delle mansioni svolte, possono legittimamente prenderne conoscenza, procedendo, ai sensi dell'art. 30 del Codice Privacy, alla loro nomina come "Incaricati del trattamento";
- sia nominato "Responsabile esterno del trattamento", ai sensi dell'art. 29 del Codice Privacy, il terzo che eventualmente si trova a trattare i dati personali raccolti.

Non solo. I dati raccolti nel rispetto delle prerogative di cui sopra devono essere protetti con idonee e preventive misure di sicurezza, riducendo i rischi di distruzione, di perdita o di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.

Tra le misure indicate dal Garante Privacy si può evidenziare la necessità:

- di configurare diversi livelli di visibilità e trattamento di immagini, in presenza di differenti competenze specificamente attribuite ai singoli operatori;
- di limitare la possibilità per gli abilitati di visionare le immagini registrate laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate;
- che, qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi siano protetti contro i rischi di accesso abusivo.

- *La posizione del Garante sui sistemi di geolocalizzazione dei lavoratori*

Con frequenza, ormai, vengono installati dal datore di lavoro sui dispositivi elettronici (quali *smartphone* e *tablet*) e/o sui veicoli concessi in dotazione ai dipendenti, sistemi di localizzazione e comunicazione (anche in tempo reale) della relativa posizione lavorativa.

I dati così raccolti costituiscono, però, anche informazioni personali riferibili al lavoratore assegnatario e, pertanto, richiedono, al pari di quanto abbiamo visto per i sistemi di videosorveglianza, il rispetto della normativa in materia di privacy.

In relazione ai trattamenti effettuati mediante tali sistemi nell'ambito dell'esecuzione di un rapporto di lavoro, il Garante Privacy ha, con proprie decisioni, osservato che:

- la loro installazione deve corrispondere ad uno scopo lecito e funzionale al raggiungimento di un determinato risultato, come ad esempio: (a) ottimizzare la gestione e il coordinamento degli interventi effettuati dai dipendenti sul campo, incrementando la tempestività di fronte alle richieste dei clienti; (b) rafforzare le condizioni di sicurezza del lavoro; (c) soddisfare le esigenze organizzative e produttive;
- deve essere rilasciata ai dipendenti interessati una apposita informativa, comprensiva di tutti gli elementi di cui all'art. 13 Codice Privacy;
- debbono essere adottate tutte le misure di sicurezza idonee a preservare l'integrità dei dati trattati e prevenire l'accesso agli stessi da parte di soggetti non autorizzati;

- debbono essere nominati quali incaricati interni coloro che, in ragione delle mansioni svolte all'interno dell'azienda, trattino dati di localizzazione e quali responsabili esterni i fornitori dei servizi di localizzazione dei veicoli o dei dispositivi di comunicazione nonché di trasmissione della loro posizione.

Con riferimento ai dispositivi elettronici, il Garante Privacy ha precisato, altresì, che[13]:

- il trattamento dei dati personali, in termini di condizioni di liceità del trattamento e rispetto dei principi privacy, può essere effettuato solo a condizione che il datore di lavoro rispetti le indicazioni e le raccomandazioni di cui al provvedimento del 1 marzo 2007 (illustrato nel paragrafo precedente);
- il sistema sia configurato in modo tale che sullo schermo del dispositivo compaia sempre, ben visibile, un'icona che indichi ai dipendenti quando la funzione di localizzazione è attiva;
- vengano implementate tutte le misure volte a garantire che le informazioni visibili o utilizzabili sull'eventuale applicazione siano solo quelle di geolocalizzazione, impedendo l'accesso ad altri dati, quali ad esempio, sms, posta elettronica, traffico telefonico;
- vengano adottate le cautele necessarie per far sì che la rilevazione dei dati di geolocalizzazione non sia continuativa.

Per quanto riguarda l'utilizzo di strumenti di localizzazione installati su veicoli aziendali, degno di nota è il Provvedimento del Garante Privacy del 4 ottobre 2011 (ripreso anche dal provvedimento n. 247 del 24 maggio 2017), nel quale lo stesso ha prescritto in capo al datore di lavoro le seguenti misure:

- nel rispetto del principio di necessità, che la posizione del veicolo non sia di regola monitorata continuativamente ma solo quando ciò si renda necessario per il conseguimento delle finalità legittimamente perseguite;
- nel rispetto dei principi di pertinenza e non eccedenza, che i tempi di conservazione delle diverse tipologie di dati personali eventualmente trattati siano commisurati tenendo conto di ciascuna delle finalità in concreto perseguite.

3. Il regime sanzionatorio in caso di violazione dell'art. 4 dello Statuto dei lavoratori

Tutto quanto sopra evidenziato, occorre delineare il regime sanzionatorio predisposto dal legislatore al fine di reprimere le condotte di parte datoriale che, nei fatti, si dimostrino in palese contrasto con le disposizioni di cui all'art. 4 dello Statuto dei lavoratori.

Anzitutto, la violazione dell'art. 4 della legge 300/1970 è punita - ai sensi dell'art. 171 del Codice Privacy, così come modificato ad opera del d.lgs. 151/2015 - con le sanzioni ex art 38 dello Statuto dei lavoratori, una ammenda da 154 euro a 1.549 euro ovvero l'arresto da 15 giorni a 1 anno e, nei casi più gravi, le due sanzioni dell'arresto e dell'ammenda sono applicate congiuntamente.

Ad ogni modo, la suddetta violazione dell'art. 4 della legge 300/1970 non integra solo una fattispecie di reato ma anche di condotta antisindacale da parte del datore di lavoro, censurabile con la procedura ex art. 28 dello Statuto dei lavoratori, la cui finalità è, appunto, quella di garantire l'effettività, oltre che del principio di libertà sindacale, dei diritti previsti dallo Statuto dei lavoratori. Al riguardo si ricorda che legittimato attivo all'avvio della procedura in questione è il sindacato e non il lavoratore. Su ricorso del sindacato, dunque, il tribunale territorialmente competente, nei due giorni successivi alla richiesta, convocate le parti e assunte sommarie informazioni, qualora ritenga sussistente la violazione, ordina, con decreto, al datore di lavoro la cessazione del comportamento illegittimo nonché che si adoperi al fine di eliminarne gli effetti. Il datore di lavoro che non ottemperi al decreto, o alla sentenza pronunciata nel giudizio di opposizione, è punito ai sensi dell'art. 650 c.p. con l'ammenda fino a 206 euro o l'arresto fino a tre mesi.

[13] cfr Provvedimenti del Garante Privacy n. 401 e n. 448 rispettivamente dell'11 settembre 2014 e del 9 ottobre 2014

Al riguardo si aggiunga che ai sensi dell'art. 11, comma 2, del Codice Privacy, i dati trattati in violazione di quanto disposto dall'art. 4 in esame sono inutilizzabili e che l'omessa o inidonea informativa di cui all'art. 13 del Codice Privacy è punita, ex art. 161 del Codice Privacy, con una sanzione amministrativa, che va da un minimo di euro 6.000,00 ad un massimo di euro 36.000,00.

Peraltro, il lavoratore interessato o l'autorità competente potrebbero promuovere, qualora ritenessero che il trattamento dei dati non sia stato conforme alle disposizioni illustrate, un'azione volta al risarcimento del danno ex art. 2050 del codice civile[14] (vedasi art. 15 del Codice Privacy), la cui quantificazione è rimessa alla valutazione equitativa dell'autorità giudiziaria.

In conclusione, è necessario evidenziare che il Regolamento Europeo n. 2016/679 ha notevolmente inasprito le conseguenze sanzionatorie previste in caso di violazione delle disposizioni relative alla privacy e dunque anche di quelle sottese all'art. 4 della legge 300/1970, che potrebbero esporre il datore di lavoro a conseguenze sanzionatorie pari a 20.000.000,00 di euro o fino al 4% del fatturato annuo mondiale dallo stesso prodotto, se superiore rispetto all'importo di cui sopra.

Non bisogna, poi, dimenticare che il Regolamento Europeo lascia liberi gli stati membri di stabilire ulteriori norme relative ad altre sanzioni (cfr art. 84).

14 L'art. 2050 cod. civ. dispone che "*chiunque cagiona danno ad altri nello svolgimento di una attività pericolosa, per sua natura o per la natura dei mezzi adoperati è tenuto al risarcimento, se non prova di aver adottato tutte le misure idonee ad evitare il danno*"

Il Commerci@lista® *lavoro e previdenza*

Rivista a diffusione nazionale di diritto, economia ed organizzazione del lavoro
in collaborazione con il ***Comitato scientifico Gruppo Odcec Area lavoro***

Piazza Vittorio Veneto - Biella
Testata iscritta al Registro Stampa del Tribunale di Biella al n. 576
ISSN 2531-5250

---

comitatoredazione@gruppoarealavoro.it

SELLA2BUSINESS

L'offerta digitale completa per il tuo business

SCEGLI I MODULI E COMPONI LA TUA OFFERTA

Offerta modulare rivolta a Liberi Professionisti, Artigiani, Commercianti e PMI che hanno l'esigenza di valide soluzioni digitali abbinate a conti correnti a canoni contenuti e prefissati, che consentano di quantificarne agevolmente il relativo costo e che si adattino alle loro peculiarità operative (prevalenza online, prevalenza tradizionale).

La promozione, valida fino al 31 dicembre 2017, prevede:

STARTER KIT

Possibilità di scegliere il conto corrente tra conto Aziend@web e conto Small Business. Aziend@Web è il conto perfetto per gestire la tua impresa soprattutto online; mentre Small Business unisce la comodità dell'online alla praticità di una Succursale di riferimento. Grazie ai servizi Internet Banking e Remote Banking si potrà operare in piena autonomia con tutte le banche. L'offerta di base è completata da una carta di debito o una carta di credito.

CASH

Disponibilità di tutte le soluzioni necessarie per la gestione degli incassi; e-commerce per ricevere pagamenti online e POS con funzionalità contactless.

ECONOMIA DIGITALE

Tutte le potenzialità del digitale per supportare ogni tipologia di business. Fatturazione elettronica e conservazione sostitutiva per gestire nel modo più moderno la fatturazione verso la Pubblica Amministrazione. Supporto di SellaLab quale polo d'innovazione ed acceleratore d'impresa per aiutare i giovani talenti a far crescere i progetti e supportare le aziende nel processo di trasformazione digitale.

FUNDING

Vasta gamma di opzioni per soddisfare le esigenze di credito, finanziamenti e mutui, anche con forme di credito innovative e agevolate per coprire tutte le esigenze. In particolare:

Finanziamenti a medio termine destinati a qualsiasi tipo di investimento, abbinabili alle garanzie concesse da:

- Fondo di Garanzia del MISE per le PMI - L. 662/96 - gestito dal Mediocredito Centrale
- INNOVFIN, rilasciata dal Fondo Europeo per gli Investimenti (FEI)
- SACE, Società Assicuratrice Crediti verso Estero facente parte del Gruppo Cassa Depositi e Prestiti
- ISMEA, Istituto di Servizi per il Mercato Agricolo Alimentare che si rivolge al mondo dell'agricoltura.

Finanziamenti a breve termine destinati a:

- Formazione di scorte di materie prime o prodotti finiti
- Pagamento tredicesime/quattordicesime ai propri dipendenti
- Dotazione impianti e attrezzature per aziende agricole
- Conduzione per acquisto mezzi produttivi per aziende agricole

ALLA CONQUISTA DEL WEB

Grazie alla sinergia con SellaLab e i suoi partner, si ha accesso a professionisti e soluzioni per portare il business online e far crescere le aziende. Si possono confrontare e scegliere tra diverse web agency con i nostri esperti che seguono i clienti nella realizzazione del sito internet ed e-commerce.

PER I GRANDI PROGETTI

Una gamma completa di soluzioni per essere al fianco delle aziende nel loro percorso di internazionalizzazione. Attraverso la finanza di impresa offriamo una serie di servizi specialistici dagli elevati standard qualitativi volti a soddisfare tutte le esigenze finanziarie.

La competenza dei nostri specialisti, unita alla qualità dei servizi e dei prodotti offerti e alla tradizionale capacità di essere vicino al Cliente, ci rendono il partner ideale per pianificare e realizzare sia operazioni di business ordinarie sia di finanza straordinaria.

BANCA SELLA

sella.it