VideoLavoro del 17 maggio 2018

La privacy nei rapporti di lavoro con particolare riferimento al controllo a distanza dei lavoratori.

Andrea Rapacciuolo –Area Coordinamento Vigilanza
Ispettorato Interregionale del Lavoro di Milano
nonché Direttore del Dipartimento di Scienze Giuridiche del Centro Ricerche e Studi dei Laghi

Il controllo a distanza

L'intento dell'art. 4 è quello di trovare il <u>punto di equilibrio</u> tra diritti costituzionali contrapposti

Diritti inviolabili dell'uomo (art. 2 della Costituzione)

Libertà di iniziativa economica (art. 41 della Costituzione)

Se infatti è assolutamente legittimo che il datore di lavoro impieghi, nello svolgimento dell'attività lavorativa, gli strumenti che ritiene più opportuni e che gli offrono maggiori possibilità di profitto, è anche vero che questo non può andare a discapito dei diritti personali inviolabili dei lavoratori *in primis* i diritti posti a tutela della dignità del lavoratore e della riservatezza.

2

Vecchio Art. 4

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."

Art. 4 vigente

1: "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 di [illegible] ambiti di [illegible]avoro, del

Viene meno il "DIVIETO" e così "*impianti audiovisivi ed altre apparecchiature etc. etc.* possono essere impiegati esclusivamente"

Il controllo a distanza intenzionale e finalizzato al monitoraggio continuo e indiscriminato del lavoratore è proibito quale principio di civiltà: anche nella nuova formulazione dell'art. 4 della Legge n.300/1970, introdotta con il Jobs Act il principio cardine resta quello secondo cui una forma di controllo sui lavoratori è lecita solo se nasce incidentalmente dall'uso di uno strumento che non è destinato alla funzione di controllo (la Cassazione la definisce **possibilità "indiretta" e "preterintenzionale" di controllo a distanza dell'attività dei lavoratori**).

Con salvezza di quanto si dirà in seguito sul tema dei c.d. controlli difensivi.

Vecchio Art. 4

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.”

Art. 4 vigente

1: “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

Apertura della visione normativa: è possibile l’installazione di impianti di controllo a distanza dei lavoratori non più per sole esigenze organizzative e produttive, o per la sicurezza sul lavoro, ma anche per la tutela del patrimonio aziendale

In particolare sul «patrimonio aziendale»

Nell'ipotesi in cui la richiesta di installazione riguardi dispositivi operanti in presenza del personale aziendale, la generica motivazione di "tutela del patrimonio" va necessariamente declinata per non vanificare le finalità poste alla base della disciplina normativa.

In tali fattispecie, come ricorda il garante della privacy, i principi di legittimità e determinatezza del fine perseguito, nonché della sua proporzionalità, correttezza e non eccedenza, impongono una gradualità nell'ampiezza e tipologia del monitoraggio, che rende assolutamente residuali i controlli più invasivi, legittimandoli solo a fronte della rilevazione di specifiche anomalie e comunque all'esito dell'esperimento di misure preventive meno limitative dei diritti dei lavoratori.

In particolare sul «patrimonio aziendale»

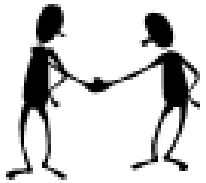
Del resto, anche secondo la Corte di Cassazione, la sussistenza dei presupposti legittimanti la tutela del patrimonio aziendale mediante le visite personali di controllo, va valutata in relazione ai mezzi tecnici e legali alternativi attuabili, all'intrinseca qualità delle cose da tutelare, alla possibilità per il datore di lavoro di prevenire ammanchi attraverso l'adozione di misure alternative (Cass. sent. n. 84/5902).

Inoltre, tra gli elementi che devono essere tenuti presenti nella comparazione dei contrapposti interessi, non possono non rientrare anche quelli relativi all'intrinseco valore e alla agevole asportabilità dei beni costituenti il patrimonio aziendale.

In particolare sul «patrimonio aziendale»

Da ultimo la circolare n.5 ha altresì chiarito che tale problematica non si pone per le richieste che riguardano dispositivi collegati ad impianti di antifurto che tutelano il patrimonio aziendale in quanto tali dispositivi, entrando in funzione soltanto quando in azienda non sono presenti lavoratori, non consentono alcuna forma di controllo incidentale degli stessi e pertanto possono essere autorizzati secondo le modalità usuali di cui agli strumenti di controllo come illustrato dall'Ispettorato Nazionale del Lavoro con la nota n. 299 del 28 novembre 2017.

Prima possibilità: <u>previo</u> (cioè <u>prima dell'installazione</u>) <u>accordo</u> con le RSA/RSU



Seconda possibilità: in <u>mancanza di accordo con le RSA/RSU</u> o <u>in assenza di RSA/RSU</u>, previa AUTORIZZAZONE dell'ITL

1: "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 **<u>previo</u>** 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 **<u>previa</u>** autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali."

Prima possibilità: accordo sindacale

L’accordo va sottoscritto con:

- **RSA/RSU**
- **Associazioni sindacali comparativamente più rappresentative sul piano nazionale per imprese plurilocalizzate («*nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni*»).**

Prima possibilità: accordo sindacale

- ***Tassatività dei soggetti legittimati a negoziare*:** le RSA, non possono essere sostituite da altri organismi sindacali, ad es. soggetti territoriali o nazionali, organi di coordinamento delle RSA (in tal senso nota Min. Lav. 26 gennaio 1979 e nota Min. Lav. 19 giugno 1989; Cassazione 16 settembre 1997, n. 9211).

- L'accordo deve essere raggiunto con le RSA ***di ogni unità produttiva*** ove l'apparecchiatura verrà installata (Interpello Min. Lav. 5 dicembre 2005).

- L'accordo deve essere raggiunto con ***la sola maggioranza*** delle RSA esistenti in azienda (Interpello Min. Lav. 5 dicembre 2005).

- La procedura ***non può essere sostituita né dal consenso unanime*** dei prestatori di lavoro (Pretura Milano 23 luglio 1991) ***né dalla conoscenza dei lavoratori dell'esistenza dell'impianto*** (Cassazione sent. n. 9211/1997) né dall'uso pacifico e non contestato dell'impianto stesso.

Seconda possibilità: autorizzazione ITL

L'autorizzazione va richiesta **preventivamente** a:

- **Ispettorato Territoriale del Lavoro** (ITL)
- **Ispettorato Nazionale del Lavoro** (INL) per imprese plurilocalizzate («*nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Ispettorati territoriali del lavoro*»).

Seconda possibilità: autorizzazione ITL

Per integrare la illiceità e la responsabilità penale del datore di lavoro, è sufficiente che le apparecchiature installate in azienda consentano la possibilità di operare il controllo. La Cassazione la definisce "mera potenzialità" del controllo consentito dalla installazione di un impianto audiovisivo o altra apparecchiatura, indipendentemente dall'effettiva attivazione dello stesso da parte del datore di lavoro (Cass. 12-11-2013 n. 4331; Cass. 17-07-2007 n. 15892).

Può accadere che il controllo non sia mai effettuato o che sia impossibile perché l'impianto non è funzionante o è finto. E' irrilevante che il controllo ci sia o meno: tutto ciò che conta ai fini della violazione della norma di legge è che il controllo sia possibile.

Seconda possibilità: autorizzazione ITL

L'istanza volta ad ottenere l'autorizzazione amministrativa all'installazione va presentata utilizzando la «nuova» specifica modulistica ministeriale indirizzo https://www.ispettorato.gov.it/it-it/strumenti-e-servizi/Modulistica/Pagine/Home-Modulistica.asp.

Le autorizzazioni dell'Ispettorato del Lavoro sono definitive vale a dire che non è più ammesso ricorso in via gerarchica (al Ministro del Lavoro): ma contro il diniego comunque esperibile rimedio del ricorso straordinario al Presidente della Repubblica oppure ricorso in via giurisdizionale al TAR, in ogni caso solo per vizi di legittimità e non di merito.

Seconda possibilità: autorizzazione ITL

Secondo la recentissima circolare INL n.5/2018, l'oggetto dell'attività valutativa va concentrata sulla effettiva sussistenza delle ragioni legittimanti l'adozione del provvedimento, comma 1 dell'art. 4, tenendo presente in particolare la specifica finalità per la quale viene richiesta l'autorizzazione e cioè le ragioni organizzative e produttive, quelle di sicurezza sul lavoro e quelle di tutela del patrimonio aziendale. Conseguentemente, le eventuali condizioni poste all'utilizzo delle varie strumentazioni utilizzate devono essere necessariamente correlate alla specifica finalità individuata nell'istanza senza, però, particolari ulteriori limitazioni di carattere tecnico che talvolta finiscono per vanificare l'efficacia dello stesso strumento di controllo. L'eventuale ripresa dei lavoratori, di norma, dovrebbe avvenire in via incidentale e se se sussistono le ragioni giustificatrici del controllo (ad esempio tutela della "sicurezza del lavoro" o del "patrimonio aziendale") è possibile inquadrare direttamente l'operatore senza introdurre condizioni quali, per esempio, "l'angolo di ripresa" della telecamera oppure "l'oscuramento del volto del lavoratore".

Seconda possibilità: autorizzazione ITL

Parimenti, sempre in tema di videosorveglianza, la circolare indica chiaramente che non è fondamentale specificare il posizionamento predeterminato e l'esatto numero delle telecamere da installare fermo restando, comunque, che le riprese effettuate devono necessariamente essere coerenti e strettamente connesse con le ragioni legittimanti il controllo e dichiarate nell'istanza, ragioni la cui effettiva sussistenza va sempre verificata in sede di eventuale accertamento ispettivo. Ciò in quanto lo stato dei luoghi e il posizionamento delle merci o degli impianti produttivi è spesso oggetto di continue modificazioni nel corso del tempo (si pensi ad esempio alla rotazione delle merci nelle strutture della grande distribuzione) e pertanto rendono scarsamente utile una analitica istruttoria basata su planimetrie che nel corso del breve periodo non sono assolutamente rappresentative del contesto lavorativo.

Seconda possibilità: autorizzazione ITL

Del resto, un provvedimento autorizzativo basato sulle esibizione di una documentazione che "fotografa" lo stato dei luoghi in un determinato momento storico rischierebbe di perdere efficacia nel momento stesso in cui tale "stato" venga modificato per varie esigenze, con la conseguente necessità di un aggiornamento periodico dello specifico provvedimento autorizzativo, pur in presenza delle medesime ragioni legittimanti l'installazione degli strumenti di controllo.

In vero la circolare precisa che il provvedimento autorizzativo viene rilasciato sulla base delle specifiche ragioni dichiarate dall'istante in sede di richiesta. L'attività di controllo, pertanto, è legittima se strettamente funzionale alla tutela dell'interesse dichiarato, interesse che non può essere modificato nel corso del tempo nemmeno se vengano invocate le altre ragioni legittimanti il controllo stesso ma non dichiarate nell'istanza di autorizzazione.

Seconda possibilità: autorizzazione ITL

Quanto invece al "perimetro" spaziale di applicazione della disciplina in esame, l'orientamento giurisprudenziale tende ad identificare come luoghi soggetti alla normativa in questione anche quelli esterni dove venga svolta attività lavorativa in modo saltuario o occasionale (ad es. zone di carico e scarico merci). La Corte di Cassazione penale (sent. n. 1490/1986) afferma infatti che l'installazione di una telecamera diretta verso il luogo di lavoro dei propri dipendenti o su spazi dove essi hanno accesso anche occasionalmente, deve essere preventivamente autorizzata da uno specifico accordo con le organizzazioni sindacali ovvero da un provvedimento dell'Ispettorato del lavoro.
Sarebbero invece da escludere dall'applicazione della norma quelle zone esterne estranee alle pertinenze della ditta, come ad es. il suolo pubblico, anche se antistante alle zone di ingresso all'azienda, nelle quali non è prestata attività lavorativa.

Seconda possibilità: autorizzazione ITL

A proposito di autorizzazione la circolare n.5 precisa che, ove sussistano le ragioni giustificatrici del provvedimento, è autorizzabile da postazione remota sia la visione delle immagini "in tempo reale" che registrate. Tuttavia, l'accesso da postazione remota alle immagini "in tempo reale" deve essere autorizzato solo in casi eccezionali debitamente motivati. L'accesso alle immagini registrate, sia da remoto che "in loco", deve essere necessariamente tracciato anche tramite apposite funzionalità che consentano la conservazione dei "log di accesso" per un congruo periodo, non inferiore a sei mesi; pertanto non va più posta più come condizione, nell'ambito del provvedimento autorizzativo, l'utilizzo del sistema della "doppia chiave fisica o logica".

SANZIONI

Il nuovo testo dell'art. 4 non ha modificato sostanzialmente il sistema sanzionatorio previsto dal combinato disposto degli articoli 171 e 172, D.Lgs. n. 196/2003 e dall'art. 38, legge n. 300/1970

ART. 38. - Disposizioni penali.

«Le violazioni degli articoli 2,4,5,6 e 15, primo comma lettera a), sono punite, salvo che il fatto non costituisca più grave reato, con l'ammenda da lire 300.000 **(€ 154)** a lire 3.000.000 **(€1.549)** o con l'arresto da 15 giorni ad un anno. Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente. Quando, per le condizioni economiche del reo, l'ammenda stabilita nel primo comma può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo. Nei casi previsti dal secondo comma, l'autorità giudiziaria ordina la pubblicazione della sentenza penale di condanna nei modi stabiliti dall'articolo 36 del Codice penale.

In caso di accertata installazione di impianti di controllo a distanza senza specifico accordo con le organizzazioni sindacali o in mancanza dell'autorizzazione, l'ispettore deve impartire una prescrizione allo scopo di eliminare gli effetti della contravvenzione accertata mediante l'immediata cessazione della condotta illecita e la rimozione materiale degli impianti, fissando un termine per la regolarizzazione non eccedente quello tecnicamente necessario: "trattandosi di apparecchiature per la cui rimozione è necessario l'intervento di personale specializzato, si evidenzia che il tempo da assegnare dovrà essere congrue".

Nei casi in cui, nel periodo di tempo assegnato dall'ispettore si raggiunga l'accordo sindacale oppure venga rilasciata l'autorizzazione prevista dalla Legge, a fronte del venire meno dei presupposti oggettivi dell'illecito e, quindi, dell'avvenuto ripristino della legalità violata, l'ispettore può ammettere il datore di lavoro a pagare in sede amministrativa, nel termine di 30 giorni, una somma pari a 387,25 euro, vale a dire al quarto del massimo dell'ammenda stabilita per la contravvenzione (art. 21, d.lgs. n. 758/1994)

Il 2° comma dell'articolo 38, punisce tale reato nei casi di maggiore gravità con l'arresto congiunto all'ammenda, rendendo, in tal caso impraticabile, per l'ispettore che accerti la condotta illecita, il ricorso all'istituto della prescrizione obbligatoria.

Si rimette all'ispettore il potere-dovere di individuare i casi di maggiore gravità e quindi di applicare o meno l'istituto della prescrizione.

A tal riguardo sembra potersi affermare che l'inciso di cui all'art. 38, 2° comma, "nei casi più gravi" faccia riferimento ad indici che rendono la condotta illecita del datore di lavoro, così come descritta dall'art. 4, della Legge n. 300/1970, maggiormente riprovevole.
Tali indici, peraltro, sono elencati dall'art. 133 c.p. che, con riferimento alla determinazione concreta della pena da parte del giudice, fa riferimento alle modalità esecutive dell'azione (mezzi, oggetto, tempo e luogo), alla gravità del pericolo/danno cagionato alla persona offesa dal reato, nonché all'intensità del dolo o al grado della colpa.

Nell'intento, pertanto, di esemplificare (ovviamente in maniera non esaustiva data l'innumerevole casistica riscontrabile in concreto) le violazioni della normativa in parola che sono caratterizzati da maggiore gravità (e che non consentono, pertanto, l'applicazione dell'istituto della "prescrizione obbligatoria") si possono citare alcune significative ipotesi (non proprio di scuola, atteso che si sono verificate i questi anni).

1) L’installazione di telecamere fisse che inquadrano esclusivamente luoghi adibiti al godimento della pausa (area break, macchinette erogatrici di bevande e alimenti) ovvero alla consumazione del pasto da parte degli stessi.

2) L’assenza eclatante di esigenze organizzative, produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale che rendano necessaria l’installazione di strumenti di controllo a distanza.

3) L’installazione degli impianti a totale insaputa del lavoratore. Non v’è dubbio, difatti, che la condotta del datore sia maggiormente idonea a mettere in pericolo la riservatezza del lavoratore così come più volte affermato anche dalla Suprema Corte.

4) Da ultimo, alla luce dell’art. 162-bis c.p., sono da ritenersi ostative all’applicazione del provvedimento di prescrizione obbligatoria le ipotesi in cui il contravventore si dimostri specificatamente recidivo alla violazione degli obblighi in materia ovvero contravventore abituale o professionale, in quanto queste ipotesi rilevano come indici di una maggiore pericolosità sociale del reo.

I controlli difensivi.

Cosa si intende per controlli difensivi ?

In un primo momento, genericamente intesi come controlli diretti ad accertare comportamenti illeciti, estranei al rapporto di lavoro, posti in essere dai dipendenti (Cass. 4746/2002); successivamente, l'interpretazione giurisprudenziale ha specificato che il controllo sul comportamento illecito si deve riferire alla tutela di beni ed interessi (es. tutela del patrimonio o dell'immagine aziendale) diversi dalla corretta esecuzione dell'obbligazione contrattuale del lavoratore (Cass.15892/2007; Cass. 2722/2012)

Ulteriori precisazioni in giurisprudenza hanno riguardato:

- rilevanza penale dei comportamenti illeciti (Cass. 4375/2010);
- controlli ammessi non solo per l'avvenuta perpetrazione di illeciti e l'esigenza di verificarne il contenuto, ma anche in ragione del solo sospetto o della mera ipotesi che illeciti siano in corso di esecuzione (Cass. 4984/2014): si tratta comunque di una legittimazione di un controllo *ex post*.

In ogni caso in dottrina i controlli difensivi sono stati ritenuti legittimi se effettuati con impianti il cui utilizzo è proporzionalmente orientato a scongiurare il rischio concreto di comportamenti del lavoratore di rilevanza penale posti in essere in occasione dello svolgimento della prestazione lavorativa.

Il concetto fondamentale di proporzionalità si declina con riferimento a due condizioni:

- controllo finalizzato solo al riscontro di uno stato di fatto in caso di sospetto concreto;

- solo per il tempo strettamente necessario.

In argomento ricordiamo la sentenza Cass. 27 maggio 2015 n. 10955 in cui si asserisce la legittimità di un controllo difensivo occulto, se diretto a tutelare beni del patrimonio aziendale ovvero ad accertare comportamenti illeciti dei lavoratori, purché ciò avvenga con modalità non eccessivamente invasive e rispettose della libertà, dignità e riservatezza e canoni di buona fede e correttezza.

La Corte ha giudicato legittimo un controllo difensivo attuato con la creazione di un falso profilo Facebook da parte del responsabile del personale della società datrice di lavoro, attraverso cui mettersi in contatto con un lavoratore, per dimostrare l'esistenza di conversazioni tramite il *social network* durante l'orario di lavoro e nel luogo di lavoro.

Secondo la Corte quindi è necessario rispettare un principio imprescindibile: adeguato bilanciamento tra gli interessi in ballo, quello del lavoratore alla tutela della riservatezza e dignità e quello del datore di lavoro al controllo e alla difesa della propria organizzazione produttiva.

In tal senso la creazione di un falso profilo su Facebook è una mera modalità di accertamento dell'illecito commesso dal lavoratore (mera occasione o sollecitazione cui il lavoratore ha aderito) e non crea «sproporzione» nell'esercizio dei reciproci diritti delle parti.

Vediamo come il tema dei controlli difensivi viene visto a livello sovraordinato europeo.

Per prima ricordiamo la sentenza Barbulescu vs Romania del 5 settembre 2017 della Corte Europea dei Diritti dell'Uomo, Grande Camera di Strasburgo, ruolo n.61496/08.

La CEDU (Corte Europea dei Diritti dell'Uomo) di Strasburgo, ribaltando una precedente sentenza, si è espressa sul caso riguardante il licenziamento per motivi disciplinari di un ingegnere, il Sig. Bogdan Mihai Barbulescu, accusato dall'azienda romena per la quale lavorava di aver utilizzato sul posto di lavoro internet, telefono e fotocopiatrice per fini personali.

Il caso risale al 2007: l'1 agosto di quell'anno l'ingegnere, allora 27enne, era stato licenziato dall'azienda per la quale era impiegato dal 2004 per aver infranto il codice interno che vietava l'utilizzo di strumenti di lavoro a fini personali.

La Corte Europea afferma che è stato violato l'articolo 8 della Convenzione europea dei diritti dell'uomo ovvero il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza. La Corte conclude che le autorità nazionali che si erano espresse sul caso "non hanno protetto in maniera corretta il diritto di Barbulescu" e non hanno gestito "in modo equilibrato gli interessi in gioco". In particolare, i tribunali nazionali non hanno da un lato verificato se il dipendente fosse stato avvertito in anticipo della possibilità che le proprie comunicazioni potessero essere sorvegliate e, dall'altro, non hanno tenuto conto che Barbulescu non era stato informato della natura e della durata di questa sorveglianza e del grado di intrusione nella sua vita privata.

Ed ora analizziamo la più recente sentenza López Ribalda vs Spagna (ricorso 1874/13) del 9 gennaio 2018 nella quale la Corte Europea dei Diritti dell'Uomo ha ritenuto sussistente una violazione dell'art. 8 della CEDU – che sancisce il diritto al rispetto della vita privata – nel caso della videosorveglianza occulta di dipendenti posta in essere da una catena di supermercati spagnola, a fronte di sospetti, poi confermati, di furto.

Secondo la Corte, in base alla normativa sui dati personali (vigente in Spagna e aderente al nuovo GDPR) i ricorrenti avrebbero dovuto essere informati del fatto che fossero soggetti alla videosorveglianza, quanto meno in maniera generale. Al contrario, i dipendenti erano all'oscuro della presenza di alcune delle telecamere. Pertanto, la Corte ha ritenuto che i Tribunali spagnoli, che avevano accolto come prove i materiali video ottenuti illecitamente, non avessero adeguatamente bilanciato il diritto al rispetto della vita privata dei dipendenti con il diritto di proprietà privata del datore di lavoro.

Ma secondo la CEDU la Spagna non ha violato l'articolo 6 ed il procedimento di licenziamento è stato considerato equo: quando i filmati non sono decisivi e sono accompagnati da ulteriori elementi probatori, il loro utilizzo come prova nel processo è legittimo. I video non erano le uniche prove su cui si era basato licenziamento, ma vi erano ulteriori elementi probatori, come le discrepanze tra gli incassi e le rimanenze di magazzino a fine giornata o la stessa ammissione di colpevolezza dei dipendenti davanti alle registrazioni video che palesavano i loro furti. Inoltre i ricorrenti avevano avuto modo di partecipare al contraddittorio e confutare l'autenticità delle riprese.

La soluzione migliore proposta in dottrina allora è quella che distingue tra:

- controlli a difesa del patrimonio aziendale (beni materiali e immateriale di cui l'imprenditore ha proprietà/godimento) che riguardano la generalità dei dipendenti nel normale svolgimento dell'attività lavorativa e rientrano oggi nell'alveo dell'art. 4;
- controlli difensivi in senso stretto (mirati ad accertare condotte illecite di cui si presume, in base ad indizi concreti, siano autori singoli dipendenti, in occasione dello svolgimento dell'attività lavorativa) che non rientrano nell'alveo dell'art. 4 ma che devono essere attuati mediante strumenti tecnologici idonei che evitino un controllo eccessivamente invadente massivo e persecutorio (ad es. software che identifica autore di reati informatici).

Art. 4 comma 2

Strumenti di controllo rispetto ai quali il lavoratore è SOGGETTO PASSIVO

1: "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, etc. etc.

Strumenti di controllo rispetto ai quali il lavoratore è SOGGETTO ATTIVO

2: "La disposizione di cui al comma 1 non si applica **agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa** e agli strumenti di registrazione degli accessi e delle presenze.

Strumenti di controllo rispetto ai quali il lavoratore è soggetto passivo

Impianti di videosorveglianza




Sistemi di geo-localizzazione e tracciamento, cosiddetto GPS


Strumenti di controllo rispetto ai quali il lavoratore è parte attiva = sono intrinsecamente parte dei mezzi che il lavoratore utilizza per l'esecuzione della prestazione, compreso gli strumenti di registrazione degli accessi e delle presenze

- **Hardware** (smartphone, PC, telefoni)


- **Software** (sistemi operativi, posta elettronica)
- **Rete informatica**

- **Accessi aree riservate** (lettori biometrici)
- **Badge**

La vera problematica è rappresentata dalla corretta individuazione degli strumenti che sono **utilizzati dal lavoratore per rendere la prestazione lavorativa**. Trattandosi di eccezione ad una regola, la nozione sembra imporre una lettura restrittiva ed in base al testo della disposizione si potrà affermare che rientrano nell'esclusione solamente gli strumenti "**serventi**" vale a dire **quelli necessari imprescindibilmente al lavoratore per rendere la prestazione**.

Lo stesso bene può essere sia strumento di controllo sia strumento di lavoro: ad esempio impianti di geolocalizzazione sono strumenti di controllo se lasciano traccia dei movimenti del lavoratore ma sono strumenti di lavoro se il lavoratore li usa per ricevere indicazione del luogo in cui deve intervenire o per dare conferma dell'avvenuta presa in carico del servizio o per individuare percorso più rapido o per registrare la chiusura di un'operazione.

Esempi pratici:

- tecnico che effettua interventi di manutenzione sul territorio muovendosi con l'auto aziendale;
- venditore;
- rappresentante farmaceutico.

Un altro caso problematico: hardware + software = PC

Ma come considero il PC ai fini dell'applicazione dell'art. 4 ?

Prevale la teoria dell'unitarietà dello strumento (più ragionevole) = se il PC deve essere inteso come *unicum*, nessun problema nella qualificazione come strumento di controllo/di lavoro

oppure

prevale la teoria della divisione hardware/software = hardware sarà strumento di lavoro, ma di ciascun software dovrò valutare se in concreto è strumento di lavoro o di controllo ?

In argomento il Garante ritiene che sono ricompresi solo servizi, software o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza, come ad esempio il servizio di posta elettronica offerto ai dipendenti e gli altri servizi della rete aziendale, fra cui anche il collegamento a siti internet. Ma integrano il concetto di strumenti di lavoro anche i sistemi e le misure che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore, come ad esempio i sistemi di *logging* per il corretto esercizio del servizio di posta elettronica, con conservazione dei soli dati esteriori, contenuti nella cosiddetta "*envelope*" del messaggio, per una breve durata non superiore comunque ai sette giorni; sistemi di filtraggio anti-virus che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui server per l'erogazione dei servizi di rete; sistemi di inibizione automatica della consultazione di contenuti in rete inconferenti rispetto alle competenze istituzionali, senza registrazione dei tentativi di accesso.

Altri strumenti pure utili al conseguimento di una elevata sicurezza della rete aziendale, invece, non possono normalmente consentire controlli sull'attività lavorativa, non comportando un trattamento di dati personali dei dipendenti, e di conseguenza non sono assoggettati alla disciplina di cui all'art. 4 dello Statuto dei lavoratori. Ad esempio: sistemi di protezione perimetrale – firewall – in funzione antintrusione e sistemi di prevenzione e rilevamento di intrusioni – IPS/IDS – agenti su base statistica o con il ricorso a sorgenti informative esterne.

Sul concetto di strumento di lavoro si esprime l'INL nella circolare n.2/2016, relativa al GPS ma valida per ogni altra casistica consimile: in tutti i casi in cui si possa affermare che si tratta di strumenti **imprescindibilmente necessari** al lavoratore per rendere la prestazione lavorativa solo allora non è necessaria la procedura di cui al comma 1. **Solo quando la prestazione lavorativa non può assolutamente essere resa senza lo strumento fornito dal datore di lavoro** allora può ritenersi escluso l'obbligo di accordo sindacale preventivo o, in assenza, dell'autorizzazione della autorità pubblica. Ed i GPS sono stati esclusi da questo novero e non sono stati considerati quindi strumenti di lavoro bensì strumenti di controllo.

47

Tra gli interventi in materia di GPS ricordiamo il provvedimento del Garante del 16 marzo 2017, pubblicato con il numero 138 del registro provvedimenti, nel quale si è soffermato sui sistemi di geolocalizzazione installati sui veicoli aziendali decidendo in merito alla richiesta di verifica preliminare presentata da una Società che offre servizi idrici e assistenza in caso di problemi alla rete. La premessa del Garante è che la Società deve provvedere ad integrare l'accordo già stipulato con la rappresentanza sindacale ovvero, in assenza di accordo, a richiedere l'autorizzazione all'ITL competente.

All’esito dell’istruttoria basata sulla documentazione presentata, il Garante ha affermato la liceità dei sistemi di localizzazione geografica sui veicoli aziendali una volta accertato che gli stessi rispondono a varie (lecite) esigenze quali l’ottimizzazione della gestione delle richieste di intervento/emergenze, l’innalzamento delle condizioni di sicurezza sul lavoro dei dipendenti, la corretta manutenzione dei veicoli, la tutela del patrimonio aziendale, il calcolo del tempo di lavoro effettivo ed anche la gestione di eventuali incidenti stradali o di sanzioni subite per violazioni del codice della strada.

Quindi l'Autorità ha riconosciuto il legittimo interesse della Società a rilevare la posizione dei propri mezzi per le molteplici finalità indicate ma solo nel pieno rispetto della privacy dai lavoratori: il legittimo interesse della impresa dovrà quindi contemperarsi con il rispetto delle regole poste a tutela della riservatezza e della dignità personale dei lavoratori. In particolare si dovrà attentamente procedere a:

- **fornire adeguata informazione preventiva** ai singoli lavoratori circa l'uso degli strumenti e le modalità di effettuazione dei controlli;
- **definite le modalità di raccolta elaborazione e conservazione** dei dati (di geolocalizzazione e personali) differenziando le tutele in base alla specifica finalità perseguita;
- **adottare idonee e specifiche misure di sicurezza**, consentendo in particolare l'accesso ai dati trattati al solo personale incaricato, definendo per i dati di geolocalizzazione appositi profili autorizzativi individuali per singolo utente;
- **utilizzare tutte le informazioni nel rispetto delle previsioni contenute nel D.L.gs n.196/2003** e **nei provvedimenti successivi del Garante**.

In ogni caso, è principio affermato dalla giurisprudenza penale che l'attività di indagine volta a seguire i movimenti di un soggetto e a localizzarlo, controllando a distanza la sua presenza in un dato luogo ed in un determinato momento attraverso il sistema di rilevamento satellitare (GPS), costituisce una forma di pedinamento eseguita con strumenti tecnologici, non assimilabile ad attività di intercettazione prevista dall'art. 266 e seguenti c.p.c. (Cass. pen. 13 febbraio 2013 n.21644), ma piuttosto ad un'attività di investigazione atipica (Cass. pen. 27 novembre 2012 n.48279), i cui risultati sono senz'altro utilizzabili in sede di formazione del convincimento del giudice (cfr. sul libero apprezzamento delle prove atipiche, Cass. 5 marzo 2010 n.5440).

Su questo delicatissimo argomento (cosa possa definirsi strumento di lavoro e cosa no) si è espresso diverse altre volte l'INL in questi anni.

1. Con la circolare n.4/2017 l'INL ha fornito indicazioni assai importanti con riferimento al settore dei *call center*. E' stato così considerato «strumento che serve al lavoratore per rendere la prestazione» il c.d. CRM (*Customer Relationship Management*) che consente la gestione dell'anagrafica e di tutti i dati «contrattuali» del cliente. **Ma attenzione a verificare che il CRM sia tale e non nasconda invece uno strumento vietato di controllo della prestazione (provvedimento Garante n.139 dell'8 marzo 2018)**. Trattasi di *software* che consente il monitoraggio dell'attività telefonica dell'operatore: si ritiene che i suddetti *software* siano del tutto «illeciti e non autorizzabili» in quanto consentono un <u>controllo prolungato costante indiscriminato ed invasivo</u>.

52

2. Con la nota n.8931 dell'11/10/2017 l'INL ha fornito successive indicazioni con riferimento al settore delle officine meccaniche. E stata così considerata «strumento che serve al lavoratore per rendere la prestazione» l'apparecchiatura di video-registrazione del c.d. protocollo MCTC-NET2 che prevede la registrazione video delle operazioni di revisione obbligatoria degli autoveicoli in funzione antielusiva della normativa di settore.

3. Con la nota n. 1899 dello scorso 12/2/2018 l'IIL di Milano ha fornito indicazioni con riferimento al settore aereo. E stata così considerata «strumento che serve imprescindibilmente per rendere la prestazione» l'apparecchiatura di video-registrazione sugli aeromobili in funzione anti-terrorismo prevista dalla normativa speciale europea.

4. Con la circolare INL n.5/2018 viene specificamente ribadito che il riconoscimento biometrico, installato sulle macchine con lo scopo di impedire l'utilizzo della macchina a soggetti non autorizzati, necessario per avviare il funzionamento della stessa, può essere considerato uno strumento indispensabile a "…rendere la prestazione lavorativa…" e pertanto si potrà prescindere, ai sensi del comma 2 dell'art. 4, sia dall'accordo con le rappresentanze sindacali sia dal procedimento amministrativo di carattere autorizzativo.

Un altro caso interessante: app, smartphone e dispositivi di geolocalizzazione per finalità di rilevazione delle presenze.

Caso «Manpower», 8 settembre 2016, doc web n. 549752

Istanza di verifica preliminare: due società appartenenti a un gruppo che si occupa di ricerca, selezione e somministrazione di lavoro a tempo determinato hanno presentato al Garante una istanza di verifica preliminare per chiedere di poter installare sugli smartphone dei propri dipendenti (non smartphone aziendali ma privati cd. BYOD) una app in grado di effettuare una timbratura virtuale per i casi di lavoro fuori sede.

Finalità del trattamento dichiarate dall'azienda: snellire le procedure relative alla gestione amministrativa del personale, di volta in volta collocato presso altre ditte o semplificare e rendere più efficiente la rilevazione della presenza dei dipendenti che lavorano per lo più all'esterno della sede aziendale.

Le prescrizioni del Garante:

1. Chi non intende scaricare la app potrà continuare a entrare e uscire dal posto di lavoro impiegando i sistemi tradizionali in uso.
2. La società dovrà implementare la "privacy by design", applicando il principio di necessità e anche alla luce dei possibili errori nell'accuratezza dei sistemi di localizzazione. In particolare, verificata la associazione tra le coordinate geografiche della sede di lavoro e la posizione del lavoratore, il sistema potrà conservare il solo dato relativo alla sede di lavoro, oltre a data e orario della "timbratura" virtuale, cancellando il dato relativo alla posizione del lavoratore.
3. Sullo schermo del telefonino dovrà essere sempre ben visibile un'icona che indichi che la funzione di localizzazione è attiva.

4. L'applicazione dovrà essere configurata in modo tale da impedire il trattamento, anche accidentale, di altri dati contenuti nel dispositivo di proprietà del lavoratore (ad esempio, dati relativi al traffico telefonico, agli sms, alla posta elettronica, alla navigazione in Internet o altre informazioni presenti sul dispositivo).

5. Prima dell'avvio del nuovo sistema di accertamento delle presenze, le società dovranno effettuare la notificazione al Garante, indicando i tipi di trattamenti e le operazioni che intende compiere, e fornire ai dipendenti un'informativa comprensiva di tutti gli elementi (tipologia dei dati, finalità e modalità del trattamento, tempi di conservazione, natura facoltativa del conferimento, soggetti che possono venire a conoscenza dei dati in qualità di responsabili o incaricati del trattamento).

6. Le società dovranno, infine, adottare tutte le misure di sicurezza previste dalla normativa per preservare l'integrità dei dati e l'accesso a persone non autorizzate.

L'ACQUISIZIONE ED IL TRATTAMENTO DELLE INFORMAZIONI

La vera novità introdotta dal Jobs Act è rappresentata dal comma 3 del nuovo art. 4, secondo cui le informazioni raccolte attraverso gli strumenti di controllo di cui ai primi due commi **sono utilizzabili a tutti i fini connessi al rapporto di lavoro a patto che siano rispettate due condizioni indispensabili:**

1. **sia stata fornita adeguata preventiva informazione ai lavoratori circa l'uso degli strumenti e le modalità di effettuazione dei controlli,**
2. **le informazioni siano utilizzate nel pieno rispetto delle previsioni contenute nel D. L.gs n. 196/2003**.

Così, diventa centrale in questo sistema, il più tipico strumento di regolamentazione ed informazione preventiva cioè la c.d. *policy*: utilizzando come riferimento le prescrizioni ad oggi in vigore del Garante per la privacy, il datore di lavoro dovrà indicare se, in quale misura e con quali modalità il datore di lavoro si riserva di effettuare controlli e le conseguenze di tipo disciplinare.

La legge condiziona il trattamento dei dati al solo obbligo di informativa: non richiede espressamente consenso del lavoratore, ma solo atto unilaterale del datore di lavoro. E' necessaria informativa preventiva per qualsiasi trattamento dei dati raccolti dove per «trattamento» il GDRPR intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione

Principi applicabili al trattamento di dati personali (art. 5 GDPR)

I dati personali devono essere:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato,
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità,
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati,
- esatti e, se necessario, aggiornati,
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati,
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Informativa

L’informativa diventa sempre di più uno strumento di trasparenza riguardo al trattamento dei dati personali e all’esercizio dei diritti.

Gli interessati dovranno sapere se e perché saranno trattati i loro dati personali e con quali garanzie; cosi come dovranno sapere che hanno il diritto di revocare il consenso a determinati trattamenti, come quelli a fini di marketing diretto.

Il Regolamento sancisce a carico dei Titolari del trattamento obblighi di informativa prevedendo numerose informazioni aggiuntive da fornire agli interessati.

L’informativa va resa per iscritto o con altri mezzi, anche elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Informativa

Il Titolare del trattamento deve inserire obbligatoriamente nell'informativa privacy anche le seguenti informazioni aggiuntive sul trattamento:

1. **i dati di contatto del titolare, del responsabile del trattamento e del responsabile della protezione dei dati personali (ove applicabile);**
2. **la finalità e la base giuridica del trattamento;**
3. **qualora il trattamento si basi sulla necessità di perseguire un legittimo interesse del titolare del trattamento o di terzi, la specificazione di quali siano i legittimi interessi perseguiti dal titolare del trattamento o da terzi;**
4. **gli eventuali destinatari dei dati personali;**
5. **l'intenzione di trasferire dati personali a un paese terzo o a un'organizzazione internazionale;**
6. **il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;**
7. **l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;**

Informativa

8. **l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;**
9. **il diritto di proporre reclamo al Garante privacy;**
10. **se la comunicazione di dati personali è un obbligo o un requisito necessario per la conclusione di un contratto e se l'interessato ha l'obbligo di fornirli nonché le conseguenze della mancata comunicazione di tali dati;**
11. **l'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;**
12. **informare l'interessato, prima del trattamento, se si intende trattare i dati personali per una finalità diversa da quella per cui essi sono stati raccolti.**

Informativa

Se i dati non sono stati ottenuti presso l'interessato, il Titolare del trattamento fornisce all'interessato anche le seguenti informazioni:

1. **la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;**
2. **le categorie di dati personali oggetto del trattamento;**
3. **fornire le informazioni all'interessato entro un mese dall'ottenimento dei dati o alla prima comunicazione se destinati alla comunicazione con l'interessato, oppure non oltre la prima comunicazione se è prevista la comunicazione ad altro destinatario.**

Informativa

L’informativa rappresenta quindi la base del trattamento dei dati e deve sempre essere fornita all’interessato.

Un’informativa corretta e completa è un presupposto fondamentale per la validità del consenso.

Può esistere un’informativa senza consenso ma non si può avere un consenso che non sia preceduto da idonea informativa.

Consenso

Il Regolamento fonda sul consenso dell'interessato la principale precondizione (salvo le deroghe) di liceità del trattamento, in quanto è vietato trattare i c.d. dati sensibili (oggi indicati semplicemente come «categorie particolari di dati personali») a meno che l'interessato non abbia prestato il proprio consenso.

Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale.
Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle.

Consenso

Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità; qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste.

Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.

Il titolare del trattamento deve poter dimostrare che l'interessato ha prestato il consenso al trattamento dei propri dati personali. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro, pena l'invalidità del consenso prestato.

L'interessato ha poi il diritto di revocare il proprio consenso (e tale informazione è uno dei nuovi elementi obbligatori dell'informativa privacy) in qualsiasi momento (anche se la revoca non pregiudica la liceità del trattamento fino a quel momento effettuato), con modalità di esecuzione della revoca del consenso facili come la sua prestazione originaria.

Consenso

Si presume che il consenso non sia stato liberamente espresso

- **se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o**
- **se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione.**

Nel Regolamento non esiste più una specifica definizione

- **di dati personali "sensibili" o**
- **di dati personali "giudiziari"**

però la definizione è ricavabile dagli articoli generali dedicati a queste categorie di informazioni.
L'art. 9, infatti, individua in generale le "*categorie particolari di dati personali*" nelle informazioni "che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona fisica".
L'art. 10, invece, disciplina poi il trattamento dei "*dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza*".

I dati sono conservati per periodi indefiniti, molto lunghi, o spesso "per sempre".

Il titolare del trattamento deve richiedere il consenso per il trattamento di questi dati e, per assicurare che i dati personali non siano conservati più a lungo del necessario, deve stabilire un termine per la cancellazione o per la verifica periodica.

I tempi di conservazione dei dati personali devono:

1. **essere commisurati e non eccedenti rispetto alle finalità**
2. **tenere conto di eventuali prescrizioni di legge.**

IL MONITORAGGIO DEGLI ACCESSI AD INTERNET

L'utilizzo della rete internet è ormai uno strumento essenziale per lo svolgimento dell'attività lavorativa per una vastissima platea di lavoratori

I datori di lavoro hanno quindi l'esigenza di a) impedire che i lavoratori non si dedichino, nell'utilizzo del personal computer aziendale connesso alla rete internet, ad attività diverse rispetto a quelle contrattualmente previste; b) preservare da costi indebiti e rischi il patrimonio aziendale (es: collegamento a siti a pagamento, intrusione di virus, salvataggio sui server aziendali di contenuti illecitamente prelevati dalla rete internet, ecc.)

I lavoratori rimangono quindi esposti alla possibilità che il datore di lavoro, monitorando gli accessi ad Internet: a) rilevi l'attività lavorativa sotto il profilo della tempistica, della quantità e dei contenuti; b) invada la sfera di riservatezza monitorando anche i contenuti dei siti visitati, potendo quindi risalire a convinzioni politiche, sindacali, religiose del dipendente, ecc.

In questo ambito quindi si verifica uno dei maggiori momenti di tensione tra le contrapposte esigenze (datoriali e dei lavoratori) di cui si è accennato nelle premesse.

Il Garante della Privacy (con largo anticipo rispetto alla novella legislativa che ha riguardato l'art. 4, co. 3 dello Statuto dei Lavoratori) ha emanato, con delibera n. 13 di data 1.3.2007, le Linee Guida per posta elettronica e internet.

Il dato di partenza da cui muove il Garante sono i principi generali in materia di trattamento dei dati personali contenuti nel Codice della Privacy, vale a dire:

- principio di necessità: gli strumenti informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali in relazione alle finalità perseguite;
- principio di correttezza: le caratteristiche essenziali dei trattamenti – considerando oltretutto l'invasività e il carattere a volte occulto dei controlli tecnologici – devono essere rese note ai lavoratori;
- principio di pertinenza e non eccedenza: la raccolta ed il trattamento dei dati devono essere pertinenti rispetto alle finalità perseguite (che a loro volta devono essere lecite) e il meno invasivi possibile;
- principio di trasparenza: il datore di lavoro deve indicare chiaramente ed in modo particolareggiato quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengono effettuati i controlli

Il Garante della Privacy indica pertanto ai datori di lavoro l'opportunità di dotarsi di un disciplinare interno (nella prassi nominato "policy aziendale"), cui dare adeguata pubblicità, in cui specificare, ad esempio:

- quali comportamenti rispetto alla navigazione in rete non sono tollerati;

- se e in quale misura è consentito utilizzare per ragioni personali i servizi di posta elettronica o di rete, indicandone le relative modalità;

- se e quali informazioni sono eventualmente conservate nel tempo e chi sono i soggetti che vi possono accedere;

- se e in quale misura il datore di lavoro si riserva di effettuare controlli, e con quali modalità;

- quali conseguenze (risarcitorie, disciplinari ecc.) il datore di lavoro si riserva di trarre in caso di indebito utilizzo di internet e della posta elettronica;

- le soluzioni prefigurate per garantire la continuità dell'attività lavorativa in caso di assenza dal lavoratore.

Le misure specificamente dedicate alla navigazione in internet nelle linee guida sono le seguenti:

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazioni 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 sorta di black list) e/o il download di file aventi particolari caratteristiche (dimensionali e di tipologia di dato)
- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad esempio, con riguardo ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- l'eventuale conservazione dei dati per il tempo strettamente necessario al perseguimento di finalità organizzativa, produttive e di sicurezza, fatta salva la possibilità di prolungare i tempi di conservazione in relazione a casi eccezionali, quali: a) particolari esigenze tecniche e di sicurezza; b) indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria; c) obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria

Nella vigenza del “vecchio” art. 4 dello Statuto dei Lavoratori, si riteneva che, per ragioni di prudenza, i datori di lavoro avrebbero dovuto rispettare, oltre alle norme in materia di privacy, anche la procedura codeterminativa di cui alla predetta norma, garantendosi per questa via la piena utilizzabilità processuale dei risultati dei controlli compiuti sugli accessi ad Internet.

Con l’avvento del “nuovo” art. 4, invece, si ritiene che, limitatamente ai casi in cui il computer dotato di connessione ad internet costituisca uno strumento essenziale per l’esecuzione dell’attività lavorativa, non sia più necessario seguire la procedura codeterminativa. Ciò fermo restando che, ai sensi del terzo comma dell’art. 4, il datore di lavoro deve provvedere a consegnare al lavoratore la completa informativa circa la modalità di utilizzo di tali strumenti e la sottoposizione dei lavoratori ai relativi controlli.

Arrivederci al prossimo incontro

Videolavoro
14 giugno 2018

La gestione dei prestO.

Novità del periodo per l'area lavoro.