AVV. ENRICO U. M. CAFIERO

FORO DI MILANO

GIUSLAVORISTA

Corso di Porta Romana, n. 74
20122 – Milano
Via Cesare Battisti, 112
73100 - Lecce

Controlli a distanza: utilizzabilità dei dati raccolti

- INDICE -

22. Provvedimento del 30 luglio 2015, n. 456;

23. Violazione dell'art. 4 dello Statuto dei Lavoratori:

a) inutilizzabilità del dato acquisito dal datore di lavoro attraverso gli accertamenti svolti sul lavoratore;

b) responsabilità penale

24. La legittimità degli accertamenti operati dal datore di lavoro tramite agenzia investigativa al fine di verificare la non idoneità della malattia a determinare uno stato di incapacità lavorativa

25. Policy aziendali:

a) Utilizzo internet e posta elettronica;

b) Riservatezza;

c) Dress code.

1. L'articolo 4 dello Statuto dei Lavoratori ante riforma

2. 1° Comma: divieto di controlli c.d. intenzionali

Art. 4, Statuto dei Lavoratori
versione previgente

1° Comma

«E' vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori».

Divieto di controlli c.d. intenzionali

Art. 4, Statuto dei Lavoratori versione previgente

2° Comma

«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 (i.e. DTL), dettando, ove occorra, le modalità per l'uso di tali impianti»

I c.d. controlli preterintenzionali

Art. 4, Statuto dei Lavoratori
versione previgente

3° e 4° Comma

«Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.

Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale».

5. La giurisprudenza sui c.d. controlli difensivi

Corte di Cassazione 3 aprile 2002, n. 4746

«Ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 l. n. 300 del 1970, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre **devono ritenersi certamente fuori dell'ambito di applicazione della norma sopra citata i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi)**, quali, ad esempio, i sistemi di controllo dell'accesso ad aule riservate o, come nella specie, gli apparecchi di rilevazione di telefonate ingiustificate»

Corte di Cassazione 17 luglio 2007, n. 15892

«Il **controllo a distanza sull'attività dei lavoratori, di carattere difensivo**, in quanto **diretto ad accertarne comportamenti illeciti**, non è soggetto agli oneri contemplati dall'art. 4 dello statuto dei lavoratori, **solo se questo controllo è diretto alla tutela di beni estranei al rapporto di lavoro**. Trova invece applicazione detto articolo se il controllo difensivo tende ad accertare l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro. **I dati acquisiti in violazione di detto articolo non possono essere legittimamente posti a fondamento di un licenziamento**»

Corte di Cassazione 23 febbraio 2010, n. 4375

«In tema di controllo del lavoratore, **i programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi ad Internet** sono necessariamente apparecchiature di controllo nel momento in cui, in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e in via continuativa durante la prestazione, l'attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento, anche in relazione al rispetto delle direttive aziendali che limitano le connessioni telematiche predettte per finalità personali; ne consegue che **i dati acquisiti da tali programmi, ove per gli stessi non siano rispettate le condizioni legittimanti di cui all'art. 4 comma 2 l. n. 300 del 1970 (quali l'accordo con le rappresentanze sindacali o la commissione interna o, in mancanza, l'autorizzazione dell'ispettorato del lavoro), non sono utilizzabili nel procedimento disciplinare** instaurato nei confronti del lavoratore in relazione a violazioni disciplinari emergenti da tali dati»

Corte di Cassazione 28 gennaio 2011, n. 2117

«In tema di controllo a distanza dei lavoratori, il **divieto previsto dall'art. 4 stat. lav. di installazione di impianti audiovisivi od altre apparecchiature** per il controllo a distanza dell'attività dei lavoratori, riferendosi alle sole installazioni poste in essere dal datore di lavoro, **non preclude a questo, al fine di dimostrare l'illecito posto in essere da propri dipendenti, di utilizzare le risultanze di registrazioni video operate fuori dall'azienda da un soggetto terzo, del tutto estraneo all'impresa e ai lavoratori dipendenti della stessa, per esclusive finalità «difensive» del proprio ufficio e della documentazione in esso custodita**, con la conseguenza che tali risultanze sono **legittimamente utilizzabili nel processo** dal datore di lavoro. (Nella specie, i lavoratori, addetti a mansioni di sorveglianza dei locali della propria impresa, erano abusivamente entrati nell'attiguo ufficio appartenente ad una diversa impresa e tale condotta era stata ripresa dall'impianto di videoregistrazione ivi installato; il datore di lavoro, presa contezza dell'accaduto, aveva licenziato i lavoratori utilizzando, a sostegno della propria decisione, il filmato; la S.C., in applicazione del principio di cui alla massima, ha confermato la decisione di merito che aveva ritenuto ammissibile la produzione della registrazione)»

Corte di Cassazione 23 febbraio 2012, n. 2722

«E' **estranea all'applicazione dell'art. 4 dello statuto dei lavoratori** la condotta del datore di lavoro che pone in essere una **attività di controllo sulle strutture informatiche aziendali** (nella specie, controllo della mail del dipendente) **che prescinde dalla pura e semplice sorveglianza sull'esecuzione della prestazione lavorativa degli addetti** ed è, invece, **diretta ad accertare la perpetrazione di eventuali comportamenti illeciti dagli stessi posti in essere** (nella specie, avente ad oggetto il licenziamento per giusta causa adottato nei confronti di un quadro direttivo di banca, accusato di aver fornito a soggetti terzi estranei informazioni di carattere riservato riguardanti un cliente della banca stessa, tramite posta elettronica, e di aver così attuato, grazie a tali informazioni, operazioni finanziarie da cui aveva tratto vantaggi personali, la Corte ha ritenuto corretta la condotta ispettiva del datore, atteso che nella specie entrava in gioco il diritto del datore di lavoro di tutelare il proprio patrimonio, che era costituito non solo dal complesso dei beni aziendali, ma anche dalla propria immagine esterna, così come accreditata presso il pubblico)»

Corte di Cassazione 1° ottobre 2012, n. 16622

«L'effettività del divieto di controllo a distanza dell'attività dei lavoratori richiede che **anche per i cd. controlli difensivi trovino applicazione le garanzie dell'art. 4, comma 2, l. 20 maggio 1970 n. 300**; ne consegue che se, per l'esigenza di evitare attività illecite o per motivi organizzativi o produttivi, il datore di lavoro può installare impianti ed apparecchi di controllo che rilevino anche dati relativi alla attività lavorativa dei dipendenti, **tali dati non possono essere utilizzati per provare l'inadempimento contrattuale** dei lavoratori medesimi».

Corte di Cassazione 17 febbraio 2015, n. 3122

«In tema di controllo del lavoratore, **le garanzie procedurali** imposte dalla L. n. 300 del 1970, art. 4, comma 2, espressamente richiamato dal D.Lgs. n. 196 del 2003, art. 114, per l'installazione di impianti e apparecchiature di controllo richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, dai quali derivi la possibilità di verifica a distanza dell'attività dei lavoratori, **trovano applicazione ai controlli, c.d. difensivi, diretti ad accertare comportamenti illeciti dei lavoratori**, quando, però, tali comportamenti riguardino **l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, e non, invece, quando riguardino la tutela di beni estranei a rapporto stesso**; ne consegue che **esula dal campo di applicazione della norma il caso in cui il datore abbia posto in essere verifiche dirette ad accertare comportamenti del prestatore illeciti e lesivi del patrimonio e dell'immagine aziendale**».

Corte di Cassazione 27 maggio 2015, n. 10955

«La **creazione da parte del datore di lavoro** di un **falso profilo "facebook"** attraverso il quale "chattare" con il lavoratore al fine di verificare l'uso da parte dello stesso del telefono cellulare durante l'orario di lavoro, **esula dal campo di applicazione dell'art. 4 della legge 20 maggio 1970, n. 300**, trattandosi di **un'attività di controllo che non ha ad oggetto l'attività lavorativa ed il suo esatto adempimento ma l'eventuale perpetrazione di comportamenti illeciti da parte del dipendente, idonei a ledere il patrimonio aziendale sotto il profilo del regolare funzionamento e della sicurezza degli impianti**. (Nella specie il lavoratore era già stato in precedenza sorpreso al telefono, lontano dalla pressa cui era addetto, che, rimasta incustodita per oltre dieci minuti, si era bloccata).»

Corte di Cassazione 12 ottobre 2015, n. 20440

«Gli artt. 2, 3 e 4, L. cit. impongono modi d'impiego, da parte del datore di lavoro, delle guardie giurate, del personale di vigilanza e di impianti ed attrezzature per il controllo a distanza. I relativi divieti riguardano il controllo sui modi di adempimento dell'obbligazione lavorativa ma non anche comportamenti del lavoratore lesivi del patrimonio e dell'immagine aziendale. **Non sono perciò vietati i cosiddetti controlli difensivi, intesi a rilevare mancanze specifiche e comportamenti estranei alla normale attività lavorativa nonchè illeciti**. Controlli eseguibili anche mediante agenzie investigative private (Cass. 4 marzo 2014 n. 4984, 23 febbraio 2012 n. 2722, 14 febbraio 2011 n. 3590, 7 giugno 2003 n. 9167, 3 aprile 2002 n. 4746, 17 ottobre 1998 n. 10313, 25 gennaio 1992 n. 829).

Ciò tanto più vale quando il lavoro dev'essere eseguito, come nel caso di specie, al di fuori dei locali aziendali, ossia in luoghi in cui è più facile la lesione dell'interesse all'esatta esecuzione della prestazione lavorativa e dell'immagine dell'impresa, all'insaputa dell'imprenditore» (conferma sentenza della Corte d'Appello di Torino secondo cui «era lecito il controllo svolto dalla società, al di fuori dei locali aziendali, mediante guardie giurate o con investigatori privati e con **l'uso di uno strumento per la localizzazione e la verifica degli spostamenti degli automezzi (Global Positioning System)**».

6. Il nuovo testo dell'art. 4 dello Statuto dei Lavoratori *ex* art. 23 D.Lgs. 151/2015

Legge delega 10 dicembre 2014 n. 183 (G.U. n. 290 del 15 dicembre 2014)

Art. 1, comma VII, lett. f)

«*Allo scopo di rafforzare le opportunità di ingresso nel mondo del lavoro da parte di coloro che sono in cerca di occupazione, nonché di riordinare i contratti di lavoro vigenti per renderli maggiormente coerenti con le attuali esigenze del contesto occupazionale e produttivo e di rendere più efficiente l'attività ispettiva, il Governo è delegato ad adottare, su proposta del Ministro del lavoro e delle politiche sociali, entro sei mesi dalla data di entrata in vigore della presente legge, uno o più* ***decreti legislativi****, di cui uno recante un testo organico semplificato delle discipline delle tipologie contrattuali e dei rapporti di lavoro, nel rispetto dei seguenti principi e criteri direttivi,* in coerenza con la regolazione dell'Unione europea e le convenzioni internazionali: [...]

f) ***revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore***».

Art. 4, Statuto dei Lavoratori

(come sostituito dall'art. 23, D.lgs. 14 settembre 2015, n. 151 – G.U. n. 221 del 23 settembre 2015)

«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 imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.***

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.***

3. ***Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196****».*

7. Le principali novità introdotte dal *Jobs Act*

In breve: le principali novità introdotte dal Jobs Act

- Confermato l'utilizzo da parte del datore di lavoro degli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori **esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro**, con l'aggiunta della possibilità anche per la **tutela del patrimonio aziendale.**

- Resta la necessità dell'accordo con le rappresentanze sindacali aziendali

  ma

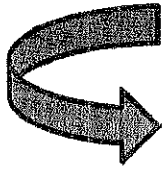
  in caso di imprese con **unità produttive ubicate in diverse province della stessa regione ovvero in più regioni**, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale.

- Confermata, in mancanza di accordo, l'**autorizzazione della Direzione Territoriale del Lavoro**

  Nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, è necessaria l'autorizzazione del **Ministero del lavoro e delle politiche sociali.**

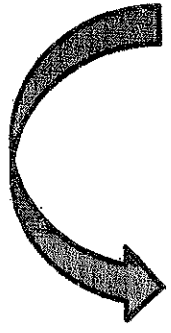
segue

- **Possibilità di utilizzo degli strumenti ad uso del lavoratore per "*rendere la prestazione lavorativa*"** e degli **strumenti di registrazione degli accessi e delle presenze**



senza accordo sindacale o autorizzazione amministrativa

- Utilizzazione «a ***tutti fini connessi al rapporto di lavoro***» (quindi **anche fini disciplinari**) delle informazioni raccolte attraverso:



- ***«impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori»*** *(art. 4, comma 1);*
- ***«strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze»*** *(art. 4, comma 2).*

2 condizioni:

- **dare al lavoratore adeguata informazione** delle modalità d'uso degli strumenti e di effettuazione dei controlli.

- **rispetto della disciplina in materia di *privacy* (D.lgs. 196/2003)**

6. Il nuovo testo dell'art. 4 dello Statuto dei Lavoratori *ex* art. 23 D.Lgs. 151/2015

Art. 4, Statuto dei Lavoratori
1° comma

c 4, Statuto dei Lavoratori: l'art. 23, D.lgs. 151/2015

«***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».*

8. I controlli a distanza: gli impianti audiovisivi e "gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività ei lavoratori"

9. L'installazione di impianti audiovisivi

L'installazione di impianti audiovisivi

- Gli impianti audiovisivi possono essere installati **esclusivamente:**

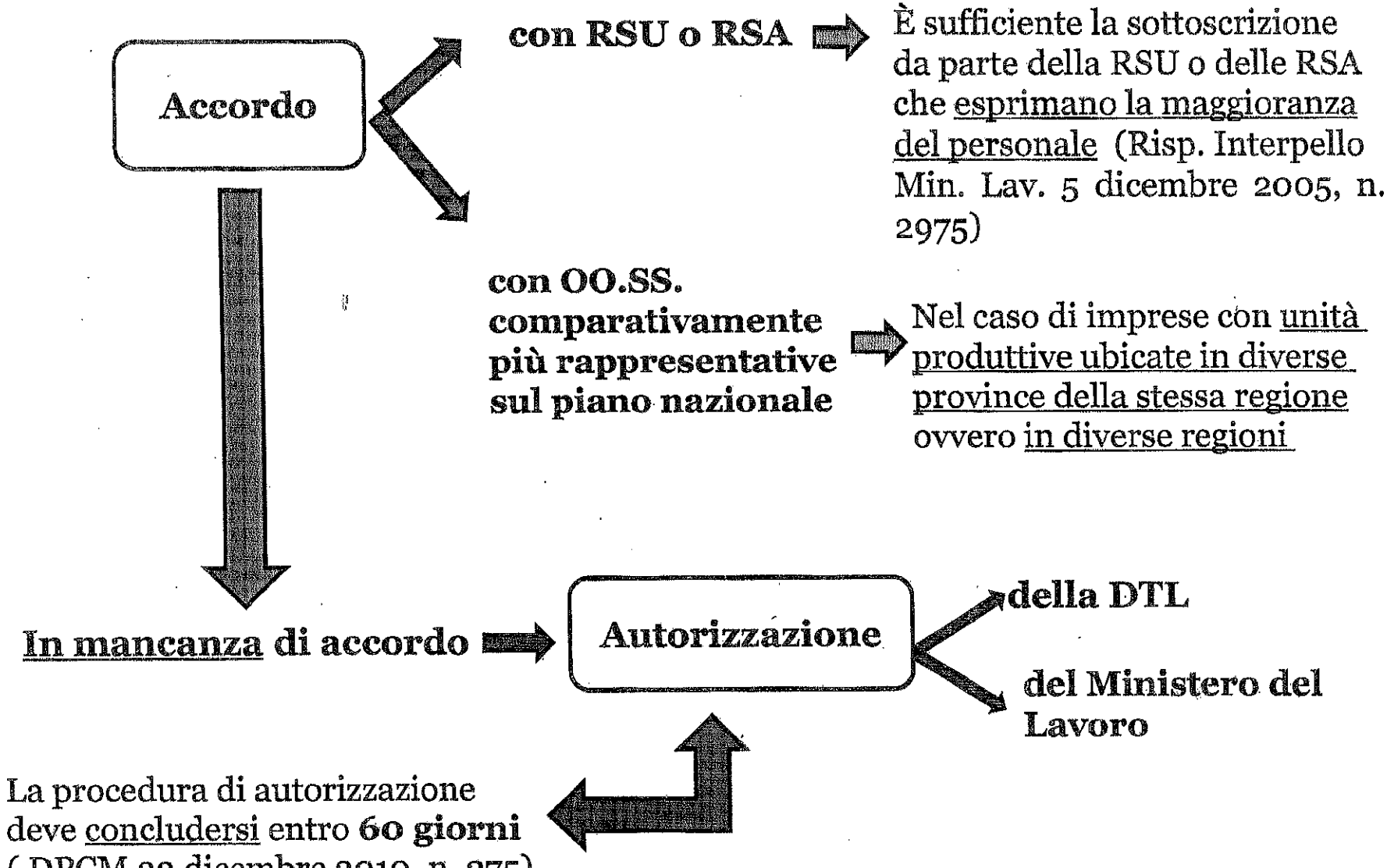
  - per **esigenze organizzative e produttive;**
  - per la **sicurezza del lavoro;**
  - per la **tutela del patrimonio aziendale**

  finalità introdotta dall'art. 23, D.lgs. 151/2015 (già contemplata, tuttavia, dalla Giurisprudenza).

- **previo accordo sindacale** o, in mancanza, **autorizzazione** della DTL o del Ministero del Lavoro

10. Procedura per l'installazione

Procedura per l'installazione



segue

Il nuovo art. 4 tiene conto delle **realtà produttive dislocate su più territori**

Novità rilevante: consente di ovviare alle criticità rappresentate dalla normativa previgente

proliferazione di accordi e tavoli sindacali separati su base locale ⟹ con possibili decisioni opposte, per fattispecie identiche, nelle diverse realtà geografiche

Contenuti dei provvedimenti autorizzativi

Su istanza dell'impresa ⟶ (corredata dalla planimetria dei locali ove sarà installato l'impianto e da relazione tecnica dell'impianto medesimo)

↓

la DTL o il Ministero del Lavoro, **previa verifica** volta ad accertare che l'installazione sia finalizzata alle esigenze di cui all'art. 4, Statuto dei Lavoratori (produttive ed organizzative, sicurezza del lavoro, tutela del patrimonio)

↓

emetterà il provvedimento di autorizzazione, eventualmente, **indicando condizioni di utilizzo dell'impianto da installare** (anche se il nuovo art. 4 non contiene più l'esplicito riferimento a tale possibilità)

↓

nel provvedimento potranno, ad esempio, essere riportate le raccomandazioni rilasciate dal **Garante *Privacy*** con il **provvedimento dell'8 aprile 2010** in materia di videosorveglianza:

- informazione ai lavoratori della presenza di telecamere;
- nomina di un incaricato della gestione delle video riprese;
- posizionamento delle telecamere verso le "zone a rischio" cercando, nei limiti del possibile, di non collocarle in maniera unidirezionale verso i lavoratori in attività;
- conservazione delle immagini per un periodo temporale limitato (fatte salve specifiche esigenze);
- avvertenza che una eventuale implementazione degli strumenti di controllo è soggetta ad una nuova autorizzazione o ad un nuovo accordo collettivo.

11. Gli strumenti "esonerati"

Non è soggetto ad accordo sindacale/autorizzazione amministrativa l'utilizzo di

- **strumenti utilizzati per rendere la prestazione lavorativa:** strumenti informatico-tecnologici quali pc, *tablet, smartphone,* sistema di rilevazione GPS, ecc.

- **strumenti di registrazione degli accessi e delle presenze:** *badge*, sistemi di accesso alle aree di parcheggio aziendale, ecc.

- ✓ La normativa sui controlli viene finalmente adeguata all'attuale realtà tecnologica;
- ✓ vengono ridotte le incertezze dando copertura legislativa agli approdi cui è giunta la Giurisprudenza ed il Garante *Privacy*

Utilizzabilità «***a tutti i fini connessi al rapporto di lavoro***» purché:

- il lavoratore riceva adeguata informativa ;
- vengano rispettate le norme sulla privacy.

Art 4, Statuto dei Lavoratori
2° comma

«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»***

Art 4, Statuto dei Lavoratori
3° comma

*«**Le informazioni raccolte** ai sensi dei commi 1 e 2 sono **utilizzabili a tutti i fini connessi al rapporto di lavoro** a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196».*

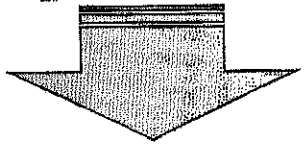
12. Utilizzabilità delle informazioni raccolte

Utilizzabilità delle informazioni

Il nuovo art. 4 consente espressamente al datore di lavoro l'utilizzo delle informazioni raccolte tramite:

- ***«impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori»*** *(art. 4, comma 1);*

- ***«strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze»*** *(art. 4, comma 2)*



Per **«tutti i fini» connessi al rapporto di lavoro:**

anche disciplinari (ma non solo: a titolo esemplificativo, per la valutazione del rendimento; ecc.).

13. Condizioni di utilizzabilità delle informazioni

Condizioni di utilizzabilità delle informazioni

1) **Fornire al lavoratore una adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli;**

2) **Rispettare la normativa sulla *privacy* (D.lgs. 30 giugno 2003, n. 196).**

14. L'adeguata informazione: policy aziendali

1) «L'adeguata informazione»

Il lavoratore deve ricevere un particolareggiata e chiara informativa sulle **modalità d'uso degli strumenti** e di **effettuazione dei controlli**

Nel nuovo contesto normativo diventano fondamentali

***policy* aziendali**

per disciplinare l'uso di internet, del computer e della posta elettronica ed in genere di tutti gli strumenti informatici dati in dotazione ai dipendenti, specificando:

- ✓limiti entro i quali è consentito un uso dello strumento dato in dotazione;
- ✓siti internet la cui consultazione è vietata;
- ✓conseguenze disciplinari applicabili in caso di uso contrario alla *policy* interna

15. Provvedimento del Garante privacy del 30 luglio 2015, n. 456

Provvedimento del Garante *privacy* del 30 luglio 2015, n. 456

«***Il datore di lavoro***, *pur avendo la facoltà di verificare l'esatto adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro da parte dei dipendenti,* ***deve*** *in ogni caso* ***salvaguardarne la libertà e la dignità*** *e, in applicazione dei principi di liceità e correttezza dei trattamenti di dati personali,* ***informare in modo chiaro e dettagliato circa le consentite modalità di utilizzo degli strumenti aziendali e l'eventuale effettuazione di controlli anche su base individuale. L'assenza di una esplicita policy al riguardo può determinare una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione***».

16. Il rispetto della normativa sulla privacy

2) Il rispetto della normativa sulla *privacy* (D.lgs. 196/2003)

- ❑ Rispetto delle **garanzie in materia di protezione dei dati**
- ❑ Rispetto dei **principi generali**:
  - ✓ **necessità**
  - ✓**correttezza**
  - ✓**finalità**
  - ✓**pertinenza**
  - ✓**non eccedenza**
- ❑ Rispetto delle **prescrizioni e linee guida elaborate dal Garante *Privacy***

17. Principio di necessità, art. 3 D. lgs. 196/2003

18. Principio di correttezza, finalità e pertinenza, art. 11, D.lgs. 196/2003

19. Deliberazione n. 13 del 1° marzo 2007 – Linee guida del garante per posta elettronica e internet

21. Provvedimento n. 345 del 04 giugno 2015

22. Provvedimento del 30 luglio 2015, n. 456

23. Violazione dell'art. 4 dello Statuto dei Lavoratori:

a) inutilizzabilità del dato acquisito dal datore di lavoro attraverso gli accertamenti svolti sul lavoratore;

b) responsabilità penale

24. La legittimità degli accertamenti operati dal datore di lavoro tramite agenzia investigativa al fine di verificare la non idoneità della malattia a determinare uno stato di incapacità lavorativa

24.La legittimità degli accertamenti operati dal datore di lavoro tramite agenzia investigativa al fine di verificare la non idoneità della malattia a determinare uno stato di incapacità lavorativa

La legittimità degli accertamenti operati dal datore di lavoro tramite agenzia investigativa al fine di verificare la non idoneità della malattia a determinare uno stato di incapacità lavorativa del lavoratore risulta oramai un dato assolutamente consolidato e pacifico.

In particolare la Corte di legittimità, tornata più volte a pronunciarsi sulla questione, ha chiarito che le disposizioni dell'art. 5 St. Lav. sul divieto di accertamenti del datore in ordine all'infermità per malattia o infortunio del dipendente e sulla facoltà di effettuare il controllo delle assenze solo attraverso i servizi ispettivi degli istituti previdenziali competenti, non precludono la contestazione delle certificazioni mediche prodotte dal lavoratore e in genere degli accertamenti di carattere sanitario attraverso la prova di ogni circostanza idonea a dimostrare l'insussistenza della malattia o la non idoneità di quest'ultima a determinare uno stato di incapacità lavorativa (Cass., 14 aprile 1987, n. 3704; Cass., 26 febbraio 1994, n. 1974; Cass., 7 giugno 1995, n. 6399 e Cass., 2 novembre 1995, n. 11355).

In altre parole, si riconosce al datore di lavoro il diritto di prendere conoscenza di comportamenti del dipendente, che, seppur estranei allo svolgimento dell'attività lavorativa, sono comunque rilevanti sotto il profilo della correttezza e buona fede nell'adempimento delle obbligazioni derivanti dal rapporto di lavoro.

La possibilità di contestare gli accertamenti medici si fonda sul fatto che gli stessi costituiscono in ogni caso il risultato di un apprezzamento valutativo; dunque, anche se provenienti da soggetti pubblici, sono privi di efficacia probatoria privilegiata (Si veda Cass., 6 marzo 1990, n. 1750, in FI, 1990, I, 2486 e Cass., 4 aprile 1997, n. 2953, secondo cui la certificazione medica non può costituire una prova assoluta dell'effettivo stato di malattia del lavoratore, dal momento che troppo sovente essa viene strumentalizzata per il perseguimento di fini illeciti e che tale circostanza è contestabile al lavoratore attraverso un procedimento disciplinare qualora indici gravi e concordanti facciano dubitare dell'effettiva sussistenza dello stato morboso).

In particolare la Suprema Corte di Cassazione Sezione Lavoro, con la nota sentenza n. 6236 del 2001 ha confermato un consolidato orientamento secondo il quale nei casi di lavoratore assente dal lavoro perché in malattia è consentito al datore di lavoro di avvalersi di ogni circostanza di fatto, come ad esempio di investigatori privati, per verificare l'esistenza della malattia stessa o la non idoneità di quest'ultima a determinare uno stato di incapacità lavorativa, e quindi a giustificare l'assenza.

Preme, infatti, rilevare che l'insussistenza della malattia può essere desunta anche da circostanze diverse da un accertamento sanitario, quali quelle relative al comportamento tenuto dal lavoratore durante il periodo della pretesa malattia, la cui conoscenza può essere acquisita dal datore di lavoro, mediante indagini svolte direttamente dal lui stesso o da persone da lui incaricate, nel rispetto dei limiti cui è assoggettata qualsiasi indagine privata sulla vita e sui comportamenti altrui. (Nel caso di specie, analogo al presente procedimento, un lavoratore, assentatosi dal lavoro esibendo un certificato medico recante una diagnosi di "sindrome influenzale", veniva licenziato sulla base degli accertamenti compiuti da un'agenzia investigativa che il datore, insospettito da episodi pregressi, aveva ingaggiato). (Trib. Perugia 17/9/2005, ord., Giud. Angeleri, in Riv. it. dir. lav. 2006, con nota di Elisa Benedetti, "*Accertamenti non sanitari sulla malattia del lavoratore ed efficacia probatoria del certificato medico*", 101).

Preme, infatti, rilevare che secondo l'orientamento assolutamente consolidato della giurisprudenza nel caso si verifichino assenze reiterate, di breve durata e che appaiano di carattere "strategico", il datore di lavoro potrà contestare la simulazione e la strumentalità del ricorso alla malattia, anche sulla base del mero ma fondato sospetto che la documentazione medica prodotta dal lavoratore sia inattendibile e senza che sia necessario procedere al preventivo controllo ex art 5 dello Statuto. Tale controllo preventivo non è dunque un passaggio obbligato per mettere in discussione la sussistenza dello stato morboso: data la piena sindacabilità di tutti i referti medici, spetterà al giudice verificarne l'attendibilità avvalendosi dei poteri istruttori attribuitigli dalla legge (Cass., 13 febbraio 1990, n. 1044 e Cass., 10 novembre 1997, n. 11095).

E' evidente tuttavia come non si possa limitare la possibilità di sindacare gli accertamenti compiuti sul lavoratore dichiaratosi ammalato al solo controllo sanitario *ex post*, che potrebbe rilevarsi tardivo e inefficace sia per le malattie che non lasciano postumi evidenti, sia a fronte di patologie accertabili solo attraverso un'accurata analisi del paziente, il quale potrebbe aver tratto in inganno il medico accentuando i sintomi o tacendo l'anticipata guarigione. Il giudice potrà dunque non utilizzare tali mezzi quando la fondatezza o l'infondatezza delle risultanze delle certificazioni mediche siano dimostrabili altrimenti, magari con ricorso ad accertamenti fattuali svolti da agenzie private abilitate come nel caso di specie.

La possibilità concessa al datore di lavoro di avvalersi di fatti della vita del lavoratore che rivelino l'insussistenza della malattia non contrasta né con quanto previsto dall'art. 5 dello Statuto, in quanto lo stesso fa riferimento ai soli accertamenti di carattere sanitario come specificato in rubrica, né tantomeno con l'art. 8, poiché le eventuali indagini del datore di lavoro non riguarderebbero in alcun modo fatti che si possono ritenere non rilevanti ai fini della valutazione dell'attitudine professionale del dipendente; né è ipotizzabile un'estensione analogica delle due norme.

Il datore di lavoro può dunque legittimamente irrogare il licenziamento sulla base delle risultanze della verifica dell'agenzia investigativa né può ravvisarsi alcuna violazione della *privacy*, considerando che a norma dell'art. 24, D.lgs. 30 giugno 2003, n. 196, il trattamento dei dati personali effettuato per far valere un diritto in giudizio è lecito anche senza il consenso dell'interessato (nello stesso senso si è espresso il Garante per la protezione dei dati personali nel respingere il ricorso di un lavoratore licenziato a fronte della documentazione raccolta da un'agenzia investigativa da cui risultava l'insussistenza della malattia addotta per giustificare la propria assenza, *Newsletter*, 8 – 14 gennaio, *GL*, 2001, 3, 25).

REGOLAMENTO AZIENDALE PER L'UTILIZZO DEL SISTEMA INFORMATICO

INDICE

PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone *...nome azienda...*ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche della nostra Azienda deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, *...nome azienda...* ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password deve essere attivata per l'accesso alla rete, per l'accesso a Lotus Notes, per lo screen saver e per il collegamento a Internet. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte dell'..... (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,...).*

Il custode delle parole chiave riservate, per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita dell' ..... (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,...*), in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal responsabile dei sistemi informatici della *...nome azienda...* L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita dell' ..... (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,...).*

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ...), se non con l'autorizzazione espressa dell' ..... (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,...).*

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente ..... (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,...)* nel caso in cui vengano rilevati virus.

UTILIZZO DELLA RETE DI *(...NOME AZIENDA...)*

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

..... (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,...)* può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stamparti comuni. In caso di necessità la stampa in corso può essere cancellata.

GESTIONE DELLE PASSWORD

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite da ..... (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,...)*È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi (come previsto dal punto 5 del disciplinare tecnico allegato al Codice della privacy, d.lgs.vo n.196/2003) con contestuale comunicazione al Custode delle Parole chiave (*....inserire il nome della persona...).(n.b.: in molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica al custode; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dall'incaricato entro i termini massimi: in questi casi vanno adattate le istruzioni contenute nel presente regolamento)*

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; ; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato (punto 5 del disciplinare tecnico).

La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle Parole chiave, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o persona dalla stessa incaricata (*Responsabile, responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali ...*)

UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato (punto 22 del disciplinare tecnico). Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati sensibili e giudiziari (punto 21 del disciplinare tecnico) devono essere custoditi in archivi chiusi a chiave.

UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli da ..... (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,...)* e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc...), in caso di allontanamento, devono essere custoditi in un luogo protetto.

USO DELLA POSTA ELETTRONICA

La casella di posta, assegnata dall'Azienda all'utente, è uno **strumento di lavoro.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica aziendale *.....@.....it (oppure .com)* per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per *(...nome azienda....)* deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

> La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto (tutelato in base all'art. 6 bis del r.d. 29.6.1939 n.1127), e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, ...).

Per la trasmissione di file all'interno di *(...nome azienda....)* è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all' ..... (*individuare la figura e la sua qualificazione: responsabile del trattamento*

informatico, responsabile dei sistemi informatici aziendali,...). Non si devono in alcun caso attivare gli allegati di tali messaggi.

USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dall' ..... (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,...).*

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del disciplinare tecnico allegato al d.lgs.vo n. 196/2003.

NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

data

Iunio Valerio Romano
Coordinatore Aree Vigilanza presso Direzione territoriale del lavoro di Lecce *

Mobile working e controllo a distanza, il GPS quale strumento di lavoro

La nuova disciplina del controllo a distanza dei lavoratori e i nuovi strumenti di lavoro, quali ad esempio il GPS, impongono, in assenza di precise indicazioni in materia, di trovare il giusto equilibrio tra interesse aziendale e l'inevitabile compressione dei diritti fondamentali dei lavoratori

L'art. 23, D.Lgs. n. 151/2015, in attuazione di quanto disposto in sede delegante dalla legge n. 183/2014 (cfr. art. 1, c. 7, lett. f)., al fine di adeguare la normativa vigente all'evoluzione tecnologica e alle più recenti prescrizioni comunitarie, ha riscritto l'art. 4, legge n. 300/1970 e l'art. 171 del D.Lgs. n. 196/2003, in tema di impianti audiovisivi e altri strumenti di controllo. Come chiarito dal Ministero del lavoro, la norma, lungi dal "liberalizzare" i controlli a distanza sui luoghi di lavoro, ha, pertanto, rivisitato la relativa disciplina in considerazione delle innovazioni tecnologiche degli ultimi anni, rispondendo alle indicazioni fornite dal Garante privacy (cfr. comunicato stampa del 18 giugno 2015).

In realtà, la nuova disposizione, nel ribadire che gli strumenti di controllo a distanza possono essere installati solo per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale[1] ed esclusivamente previo accordo sindacale o, in assenza, previa autorizzazione della Dtl o del Superiore Ministero, sembra, tuttavia sostituire al principio generale del divieto quello positivo dell'utilizzabilità, pur nel rispetto delle cautele di legge.

Nel fare ciò, il nuovo art. 4 della legge n. 300/1970 chiarisce che non possono essere considerati "strumenti di controllo a distanza" gli strumenti che vengono assegnati al lavoratore "per rendere la prestazione lavorativa", ossia gli "attrezzi di lavoro". In tal caso, anche per la relativa consegna non sarà necessario l'accordo sindacale, in quanto si è fuori dall'alveo delle prescrizioni legali.

Il vero problema, in assenza di una posizione ufficiale del Ministero del lavoro, è capire cosa si debba intendere per strumento necessario a "rendere la prestazione lavorativa", atteso che il discrimine può essere sottile e l'assenza di accordo o autorizzazione, se dovuti, possono comportare una responsabilità di natura penale. Peraltro, trattandosi di contravvenzione, tale responsabilità sarà rilevante anche se colposa, fatta salva la buona fede dovuta a "ignoranza" ingenerata da norme equivoche o comportamenti contraddittori della pubblica amministrazione (cfr. principio espresso da Corte Cost. 24 marzo 1988, n. 364).

DISTANZA

Nella previsione di cui all'art. 4 della L. n. 300/1970, il concetto di "distanza" deve essere inteso sia nella dimensione spaziale (luogo distante e nascosto) che in quella temporale (momento successivo e segreto).

La normativa attuale

L'art. 4, legge n. 300/1970, nella sua attuale formulazione, dispone che gli impianti audiovisivi e gli altri strumenti di controllo 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 pos-

** Il presente contributo è frutto esclusivo del pensiero dell'Autore e non è in alcun modo vincolante per l'Amministrazione di appartenenza.*

1. Nel patrimonio aziendale vanno ricompresi non solo i beni materiali ma anche quelli immateriali, come le banche dati dei clienti e dei fornitori, i progetti dei futuri prodotti da lanciare sul mercato, ecc.

sono 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 trattasi possono essere installati previa 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 (Direzione generale per le relazioni industriali e per la tutela del lavoro).

Dal punto di vista sanzionatorio, in assenza di preventivo accordo[2] o preventiva autorizzazione[3] alla mera installazione (e non solo alla successiva messa in uso[4]) dello strumento di controllo a distanza, resta la sanzione penale di cui all'art. 38, L. n. 300/1970 (cfr. art. 171 D.Lgs. n. 196/2003)[5].

La novità, in linea con quanto disposto dal Legislatore delegante, in ottemperanza alle raccomandazioni europee e ai più recenti orientamenti giurisprudenziali, risiede nella previsione di cui ai cc. 2 e 3 del citato art. 4, in forza dei quali non rientrano nella prescrizione di cui al comma 1 gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e gli strumenti di registrazione degli accessi e delle presenze. Peraltro, le informazioni raccolte attraverso gli strumenti di cui ai commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro, quindi anche disciplinari, a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, nel rispetto di quanto disposto dal D.Lgs. n. 196/2003.

Il concetto di strumento atto a rendere la prestazione lavorativa

L'espressione "per rendere la prestazione lavorativa", utilizzata dal Legislatore del 2015, si riferisce agli strumenti di lavoro con riguardo ai quali l'accordo o l'autorizzazione preventivi all'installazione non servono se, e nella misura in cui, gli stessi possono essere considerati il mezzo attraverso cui il lavoratore adempie la prestazione (ad es. computer, tablet, cellulari, ecc.). Ciò significa che, nel momento in cui lo strumento in questione è modificato, con l'aggiunta ad esempio di specifici software di localizzazione o filtraggio, per controllare in un certo qual modo la prestazione lavorativa, si è fuori dall'ambito della previsione in esame. In tale ipotesi, infatti, da strumento che "serve" al lavoratore per rendere la prestazione, esso diviene apparecchiatura atta a consentire al datore di lavoro di controllare la stessa. In tal

2. *Sul punto è interessante citare Cass. Pen., sez. III, 11 giugno 2012, n. 22611, secondo cui "non commette reato il datore di lavoro che installa telecamere che riprendono i dipendenti, ai quali è stato fatto firmare un foglio contenente la relativa autorizzazione". La Suprema Corte ha, infatti, espressamente statuito che, "se è vero che non si trattava né di autorizzazione della RSU né di quella di una commissione interna, logica vuole che il più contenga il meno sì che non può essere negata validità ad un consenso chiaro ed espresso proveniente dalla totalità dei lavoratori e non soltanto da una loro rappresentanza". Tale arresto, contrario al consolidato orientamento giurisprudenziale, si fonda sul principio di effettività della norma e sulla inesistenza di disposizioni normative che disciplinino le modalità di acquisizione del consenso da parte dei lavoratori interessati dalle azioni di controllo datoriali; per cui, opinare nel senso di una non valida manifestazione di assenso da parte di tutti i lavoratori perché non idoneamente rappresentati in sede sindacale "avrebbe un taglio di un formalismo estremo tale da contrastare con la logica", anche perché l'interpretazione della stessa "deve sempre avvenire avendo presente la finalità che essa intende perseguire".*

3. *Il termine entro cui l'istanza di autorizzazione ai sensi dell'art. 4, L. n. 300/1970 deve essere evasa è di gg. 60 (cfr. D.P.C.M. 22.12.2010, n. 275). Peraltro, i tempi di rilascio sono certamente più brevi laddove, come chiarito nella nota prot. n. 7162/2012 MLPS, sia consentita dalla documentazione prodotta la rilevazione delle specifiche dell'impianto, senza che risulti necessario l'accertamento tecnico preventivo dello stato dei luoghi.*

4. *Cfr. Cass. Sez. Lav. 16 settembre 1997, n. 9211, secondo cui la struttura della norma non impone una partecipazione psicologica del datore di lavoro di tipo doloso, giacché appare sufficiente che lo stesso sia in colpa, rilevando, piuttosto, le circostanze oggettive della idoneità dell'impianto o dell'apparecchiatura a consentire il controllo illecito. In considerazione di ciò, è stata ritenuta illecita la condotta della mera installazione di impianti idonei al controllo a distanza, sebbene non ancora attivati, essendo in sé integrativa dell'ipotesi di reato la potenziale idoneità della strumentazione prescelta dal datore di lavoro.*

5. *L'autore della violazione, salvo che il fatto non costituisca più grave reato, è punito con l'ammenda da euro 154 a euro 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 può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo. In tale ipotesi, è disposta la pubblicazione della sentenza. Nell'ipotesi base può trovare applicazione l'istituto della prescrizione obbligatoria ex art. 15 del D.Lgs. n. 124/2004, per cui il personale ispettivo del Ministero del lavoro e delle politiche sociali, che accerta la violazione, prescriverà il tempestivo ripristino della legalità o con il raggiungimento dell'accordo con le rappresentanze sindacali ovvero con la rimozione degli impianti e delle apparecchiature di controllo a distanza illecitamente installate. La nuova disposizione non contiene, invece, più la previsione del possibile contenzioso amministrativo da attivare a mezzo ricorso.*

L'AUTORIZZAZIONE ALL'INSTALLAZIONE DI IMPIANTI AUDIOVISIVI E ALTRI STRUMENTI DI CONTROLLO

L'autorizzazione amministrativa è conseguente alla verifica che l'installazione delle apparecchiature di controllo a distanza sia finalizzata all'esigenze enucleate dal Legislatore (produttive ed organizzative, sicurezza del lavoro, tutela del patrimonio aziendale).

1. Il provvedimento deve contenere le informazioni in ordine alle modalità d'uso degli strumenti e di effettuazione dei controlli, tipo informativa in ordine alla presenza di telecamere, nomina di un incaricato della gestione delle video riprese, posizionamento delle telecamere verso le "zone a rischio", conservazione delle immagini per un periodo temporale limitato, avvertenza che l'eventuale implementazione degli strumenti di controllo è soggetta a una nuova autorizzazione o a un nuovo accordo collettivo (cfr. nota Garante della Privacy 8/04/2010).

caso, gli interventi di modifica possono avvenire solo alle condizioni di cui al dettato legislativo, ossia la ricorrenza di particolari e comprovate esigenze che legittimino la preminenza di un interesse su di un altro e l'accordo sindacale (o l'autorizzazione).

Mobile working e controllo a distanza: i sistemi di geolocalizzazione

Il sistema di posizionamento globale (GPS) è un sistema di posizionamento e navigazione satellitare civile che può essere utilizzato dal datore nel rispetto dei principi di necessità, pertinenza e non eccedenza e per il perseguimento di finalità legittime (cfr. Garante privacy, provv. 4 ottobre 2011). Lo stesso Garante Privacy ha chiarito che i datori possono utilizzare gli strumenti GPS con lo scopo di localizzare i dipendenti che lavorano in modalità Mobile Working e sono dotati di telefono aziendale, purché adottino opportuni accorgimenti volti a non invadere la sfera privata degli stessi. L'obiettivo, peraltro, non è tanto il controllo dei movimenti dei dipendenti, quanto quello di garantire il coordinamento e la tempestività degli interventi tecnici in caso di necessità. In tal caso, i datori devono poter accedere solo alle funzioni di geolocalizzazione, mentre il lavoratore deve essere al corrente della possibilità di essere localizzato dal proprio datore di lavoro. Affinché si ricada nella previsione di cui al c. 2 dell'art. 4, L. n. 300/1970, è necessario che lo strumento idoneo al controllo a distanza sia indispensabile ai fini dell'espletamento della prestazione. In tale ottica, nel mobile working, il GPS installato sull'automezzo di trasposto piuttosto che sullo smartphone necessita dell'accordo sindacale ovvero dell'autorizzazione amministrativa ogniqualvolta consenta il controllo a distanza della prestazione lavorativa senza essere esso stesso strumento per l'espletamento della medesima. Ed in vero, laddove il GPS sia installato sul pullman che effettua tragitti non fissi o ancora sui taxi, lo strumento in dotazione al mezzo (o al lavoratore) sarà certamente da considerarsi un "attrezzo di lavoro", atteso che consente ad es. di determinare il tragitto da percorrere. Viceversa, se dovesse essere installato sull'autobus di linea, che opera sempre sulla stessa direttiva, non potrà che essere considerato uno strumento di controllo dell'attività lavorativa e come tale soggetto alle prescrizioni di legge.

Conclusioni

Alla luce di quanto sopra esposto, è evidente che la nuova normativa non consente di fornire una regola omnibus, ma è necessario, di volta in volta, individuare un criterio interpretativo in linea con la ratio normativa, che è quella di trovare il giusto equilibrio tra le misure adottate a tutela degli interessi aziendali e la inevitabile compressione dei diritti fondamentali dei lavoratori, operando una distinzione tra controllo a distanza sugli impianti (soggetto a preventivo accordo o autorizzazione) e controllo a distanza sugli strumenti di lavoro[6].

6. Cfr. Cass. Civ., sez. Lav., 12 ottobre 2015, n. 20440, che ha dichiarato legittimo il licenziamento perpetrato in danno di un lavoratore dopo una serie di controlli svolti con il sistema satellitare GPS. La Suprema Corte ha, peraltro, specificato che le norme dello Statuto dei Lavoratori impongono modi di impiego specifici delle guardie giurate, del personale di vigilanza e delle attrezzature per il controllo a distanza. Tuttavia, i divieti imposti "riguardano il controllo sui modi di adempimento dell'obbligazione lavorativa, ma non anche i comportamenti del lavoratore lesivi del patrimonio e dell'immagine aziendale". Per tale ragione non sono illegittimi i controlli difensivi, quei controlli, in altri termini, che hanno lo scopo di evidenziare comportamenti estranei alla normale attività lavorativa. Tale orientamento, peraltro, è pacifico e consolidato, ha argomenta la citata Corte, tanto quando l'attività lavorativa è espletata al di fuori dei locali aziendali. Per un commento, cfr. F. Negri, in Guida al lavoro n. 45/2105.

Garante per la protezione
dei dati personali
Provvedimento 12 novembre 2015

Controlli del datore sul pc aziendale e privacy

Andrea Stanchi
Avvocato in Milano, StanchiStudioLegale

Il Garante della Privacy specifica le regole per il procedimento di verifica dell'accesso abusivo ai sistemi aziendali attraverso l'analisi dei log di sistema

L'Autorità Garante della Privacy, con provvedimento del 12 novembre 2015, chiarisce che il datore di lavoro può effettuare dei controlli mirati (direttamente o attraverso la propria struttura) al fine di verificare l'effettivo e corretto adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 cod. civ.); tuttavia, nell'esercizio di tale prerogativa, occorre rispettare la libertà e la dignità dei lavoratori, nonché, con specifico riferimento alla disciplina in materia di protezione dei dati personali, i principi di correttezza (secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori), di pertinenza e non eccedenza di cui all'art. 11 comma 1 del Codice; ciò, tenuto conto che tali controlli possono determinare il trattamento di informazioni personali, anche non pertinenti o di dati di carattere sensibile.

Il caso

Un dipendente proponeva ricorso al Garante Privacy contro il trattamento dei propri dati da parte del (ormai ex) datore di lavoro, contenuti nel pc aziendale, sequestrato al medesimo all'atto della sospensione del rapporto di lavoro e successivamente sottoposto a verifica del suo contenuto con contestuale esecuzione di una copia dell'hard disk dell'apparecchio; il dipendente ha in particolare lamentato l'illegittimità della condotta tenuta dal datore di lavoro in quanto lo stesso avrebbe agito in modo del tutto arbitrario in assenza di garanzie circa "l'immodificabilità di quanto contenuto nel pc" procedendo all'indebita acquisizione dei dati "in sua assenza e alla presenza di un terzo estraneo all'azienda (...) in violazione dei principi di pertinenza e non eccedenza".

Il datore di lavoro segue nel procedimento di acquisizione della prova (e per l'aspetto considerate dal provvedimento attinente il trattamento dei dati) un procedimento di documentazione dell'attività e di trattamento dei dati che l'autorità garante considera legittimo in considerazione del diritto di difesa del datore di lavoro, rispetto agli inadempimenti del dipendente (art. 24 Codice Privacy, nonchè 2104 e 2105 cod. Civ.).

Dalla ricostruzione fattuale operata dall'Autorità nel corso del procedimento emergeva:

- che il datore di lavoro si era limitato ad adottare le misure necessarie ad evitare "manomissioni o interferenze che potessero compromettere l'accertamento" delle "gravissime e reiterate violazioni della disciplina sul trattamento dei dati personali oltre che delle norme penali e civili" emerse a carico dell'interessato nel corso del procedimento disciplinare avviato nei suoi confronti dalla società resistente; quest'ultima, dopo aver appreso dell'avvenuta fuga di notizie aziendali riservate, ha accertato, attraverso la "verifica dei log contenuti nel "registro degli eventi"" dei pc in uso ad alcuni dipendenti della società, l'esistenza di "numerosi episodi di accessi indebiti" effettuati sui predetti computer, a partire "almeno dalla fine del mese di marzo 2015", attraverso il "pc aziendale utilizzato in via esclusiva dal ricorrente (...) per lo svolgimento delle proprie mansioni lavorative" e di aver pertanto disposto la sospensione in via cautelativa del medesimo dall'attività lavorativa; il titolare del trattamento ha inoltre comunicato di aver chiesto al dipendente, in occasione della contestazione dei relativi addebiti, la riconsegna del pc poi "inserito in una busta (...) sigillata e custodito al sicuro nei locali aziendali senza essere mai acceso dal mo-

mento della consegna, né consegnato a nessun altro, in attesa dell'incontro congiunto in cui, alla presenza del ricorrente, si sarebbe proceduto all'apertura della busta" e alla successiva attività di verifica del contenuto dell'hard disk; la resistente ha poi rappresentato, stante il rifiuto espresso dall'interessato di partecipare all'"esame del suo pc in contradditorio con la società", di aver effettuato, avvalendosi di una società informatica esterna e in presenza di un fiduciario aziendale, l'"analisi del pc del ricorrente (...), documentando in modo minuzioso (con tanto di corredo fotografico) tutti i singoli passaggi (...) ed illustrandone compiutamente le modalità operative", utilizzando a tale scopo un criterio di ricerca basato su parole chiave relative ai "nomi dei file ed agli indirizzi di rete dei computer coinvolti, senza accedere ai file personali del dipendente" eventualmente presenti, come dimostrato da apposita relazione tecnica redatta in occasione dello svolgimento delle predette operazioni; il datore di lavoro ha infine rappresentato di aver provveduto, al termine delle operazioni di verifica, a reinserire il computer aziendale all'interno della "busta sigillata e custodito intatto all'interno della sede sociale (...) al fine di renderlo disponibile all'autorità giudiziaria sia in sede civile che penale" tenuto conto che l'esito degli accertamenti eseguiti ha fornito conferma degli addebiti mossi al dipendente;

- che lo stesso dipendente era stato informato ed aveva preso atto "nella nomina ad incaricato del trattamento e misure di sicurezza sottoscritto" della facoltà del datore di lavoro "di svolgere verifiche anche periodiche, in ordine al rispetto delle procedure in materia di riservatezza e sicurezza dei dati ed ha validamente manifestato il suo consenso"; le verifiche erano state condotte con modalità assolutamente non invasive limitandosi al controllo dell'hard disk e senza mai accedere alla posta elettronica", utilizzando strumenti tali da garantire l'integrità e la riservatezza di eventuali dati personali del dipendente, che, del resto, "ha sempre osservato (...) un atteggiamento improntato alla massima chiusura ed alla totale assenza di collaborazione", al fine di "tutelare e preservare le fonti di prova che attestano le illecite condotte poste in essere dal medesimo.

Il Garante ha quindi ritenuto la legittimità dell'operato aziendale avendo rilevato che:

- il datore di lavoro ha diritto di effettuare verifiche sull'adempimento corretto della prestazione e per la tutela dei diritti del proprio patrimonio;
- risultava dal materiale acquisito e dalle dichiarazioni del datore di lavoro (assistite da sanzione ai sensi dell'art. 168 del Codice in caso di "Falsità nelle dichiarazioni e notificazioni al Garante") che non fosse stato effettuato alcun accesso a file personali del dipendente eventualmente contenuti nel pc aziendale affidato in uso esclusivo al medesimo, quali posta elettronica o cartelle contenenti dati a lui riferibili, essendosi la Società limitata ad eseguire verifiche selettive sull'hard disk del predetto computer mediante l'utilizzo di parole chiave costituite dai nomi dei file e dagli indirizzi di rete di computer assegnati ad altri dipendenti a danno dei quali risultano essersi verificati episodi di accesso abusivo al relativo sistema informatico di cui il datore di lavoro è venuto a conoscenza; rilevato altresì che nello svolgimento di tali operazioni il titolare del trattamento ha comunque provveduto alla nomina di un fiduciario aziendale che prendesse parte alle operazioni in luogo del ricorrente, che in più occasioni era stato comunque invitato a partecipare, documentando in modo dettagliato, attraverso una relazione depositata nel corso del presente procedimento, tutti i passaggi effettuati, nonché gli esiti che ne sono derivati; rilevato altresì che il titolare del trattamento ha affermato che i dati estratti a seguito di tale verifica sono conservati con la sola finalità di "far valere o difendere un diritto in sede giudiziaria" (come previsto dall'art. 24 comma 1 lett. e) del Codice), manifestando a tale riguardo la disponibilità ad adottare tutte le eventuali misure ritenute necessarie a garantire la tutela dei dati attinenti la vita privata del ricorrente eventualmente presenti sul pc aziendale;
- la finalità esclusiva dei controlli era difensiva e funzionale alla tutela dei diritti dell'impresa.

Alcuni rilievi giuridici

Il provvedimento dell'Autorità è interessante perchè di fatto documenta un procedimento, sia pure non espressamente dichiarato tale, di verifiche (con tecniche di digital forensics) sui sistemi informatici di una impresa e poi su strumenti informatici aziendali affidati a dipendenti in ragione del sospetto, poi dimostratosi fondato, di accessi abusivi da parte di di-

pendenti a informazioni aziendali ai fini di sottrarle.

Il procedimento è ben congegnato e, come ritenuto dal Garante, se ne condivide la ritenuta legittimità in materia di trattamento dati.

Le considerazioni che seguono attengono dunque all'utilizzabilità del caso per fare ragionamenti "di scuola" (e con rilievo pratico) ai fini dell'integrazione dell'acquisizione della prova (di un comportamento illecito operato sui sistemi informativi) nelle successive sedi disciplinari piuttosto che giudiziarie, giuslavoristiche, anche nell'ottica della nuova disciplina dell'art. 4 dello Statuto dei lavoratori.

Quest'ultima norma, novellata dal D.Lgs. n. 151/15, all'art. 23, come si ricorda[1], ha ammesso la verificabilità dell'uso degli strumenti di lavoro, sottraendola alla disciplina negoziata in fase sindacale od amministrativa dei controlli c.d. preterintenzionali, ma ha specificamente condizionato tale legittimità (peraltro complessa ed articolata) al rigoroso rispetto della normativa sul trattamento dei dati.

Considerazioni che si ritengono utili ai lettori per comprendere la difficoltà del procedimento di controllo e la sdrucciolevolezza della materia, la facilità di sbagliare e la necessità di procedervi con grande, grandissima cautela, perchè il minimo errore può comportare non soltanto l'illegittimità del procedimento (e quindi l'inutilità della prova procuratasi), ma anche sanzioni di varia natura per il soggetto che vi procede (da quella amministrativa sino a quella penale).

Gli aspetti che sollevano qualche curiosità sono:

- il domicilio informatico (ai sensi dell'art. 615 ter codice penale, che punisce l'accesso abusivo ai sistemi) presuppone innanzitutto una definizione di tale domicilio. Il che avrebbe richiesto documentare nel procedimento l'esistenza di una policy dettagliata che regolasse l'utilizzo dei sistemi aziendali; ciò non risulta, anche se risulta in modo espresso che il dipendente agisse sul pc professionale che utilizzava in ragione delle proprie mansioni e che -nell'incarico al trattamento dei dati, che costituisce un aspetto dell'organizzazione della struttura legale deputata al trattamento dei dati medesimi in modo lecito- fosse stato informato di quale trattamento poteva effettuare e del correlativo diritto dell'impresa di fare controlli ai fini della verifica del corretto trattamento dei dati;
- l'informativa sul trattamento dei dati ed i controlli risulta solo, come sopra descritto, in ragione dell'incarico al trattamento dei dati. Non vi è notizia se l'impresa avesse effettuato anche una informativa più ampia sulle tipologie di controlli effettuabili e sui terzi ai quali i dati avrebbero potuto essere comunicati per tali ragioni (risulta che i dati siano stati trattati ai fini dei controlli da una azienda esterna);
- non risulta se l'impresa nel procedere a tali controlli si fosse coperta, come ben avrebbe potuto, attraverso il conferimento di mandato ad un avvocato penalista ai fini delle investigazioni difensive (art. 391 bis cod. Proc. Pen.: questo elemento non risulta espressamente, il che non significa non fosse stato fatto, ma nei casi in cui ci si avvalesse di tale modalità, la partecipazione dell'avvocato sarebbe rilevante risultasse e risultasse l'attività dal medesimo compiuta nel documentare tutti i passaggi dell'analisi forense ai fini appunto di documentare la non modificabilità dei dati nel periodo in cui il pc fosse rimasto nelle mani dell'impresa per le suddette indagini[2]; finalità nel caso perseguita dall'impresa medesima e dai suoi consulenti con la conservazione in busta chiusa e sigillata e poi successivamente nella documentazione fotografica e descrittiva dei controlli effettuati dal fornitore di servizi, si deve ritenere per quanto non specificato sulla copia dell'hard disk).

Premessi quindi questi punti che nei casi in cui non vi fosse una preliminare valutazione positiva dell'Autorità Garante (come in quello in commento) potrebbero condurre un giudice -nel rispetto del nuovo art. 4 dello Statuto- a valutazioni a seconda dei casi anche parzialmente diverse sulla tenuta probatoria di quanto acquisito nel procedimento (l'informativa resta un cardine del trattamento dei dati nell'ambito

1. *Non ritorno sul tema ma rinvio agli articoli su questa Rivista: Nel jobs act il nuovo articolo 4 dello Statuto dei lavoratori, in Guida al lavoro, 2015, n. 38, 39; Consultabile la posta elettronica del dipendente sull'email aziendale in Guida al lavoro, Numero 6 - 12 febbraio 2016.*

2. *Sotto questo profilo va ricordato che l'Allegato 6 del Codice Privacy attiene al Codice deontologico per i trattamenti di dati personali effettuati per svolgere investigazioni difensive, che è norma integrativa del Codice ai fini della legittimità delle medesime (cfr: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1565171).*

dell'art. 4, cosiccome la struttura organizzativa dei sistemi -con il suo dovere di rispetto dei principi del trattamento, in particolare di quello di necessità che ridonda sulla struttura organizzativa prescelta appunto- che viene definita dall'impresa medesima in quanto titolare identifica i limiti del diritto di tutela del domicilio informatico e dei beni in esso contenuti), appaiono corrette anche le preoccupazioni seguite dai consulenti dell'impresa di consentire la partecipazione del dipendente alla fase di verifica, in una prospettiva di trattamento dei dati personali (ed il Garante giustamente le valorizza nel provvedimento). La partecipazione del dipendente ha rilievo per offrirgli la possibilità di cooperare nell'identificazione dei file che abbiano contenuto personale e non professionale. Funzione poi giustamente perseguita dall'impresa attraverso l'utilizzo di parole chiave (anche se ovviamente laddove vi fosse una definizione esclusiva del domicilio informatico aziendale nessuna informazione personale potrebbe legittimamente risiedere sul pc aziendale, donde la rilevanza di definire adeguatamente domicilio informatico ed utilizzo degli strumenti aziendali).

Premesse queste indicazioni in tema di trattamento dati, la medesima partecipazione va invece apprezzata giuslavoristicamente in una prosettiva disciplinare, in cui va considerato non solo il diritto dell'impresa ma anche il diritto di difesa -effettivo- del dipendente.

Quest'ultimo è un rilevo che ovviamente non vale in tutti i casi, ma è specificamente pertinente ad una problematica attinente il rapporto di lavoro.

Il tema, infatti, (giuslavoristicamente) non è tanto quello di consentire al dipendente -che durante la procedura di verifica compiuta dal datore di lavoro nell'ambito delle proprie strutture e prerogative per l'acquisizione della prova si trova palesemente in una situazione di minorata possibilità di difesa (appare a chi scrive condivisibile in questo senso la scelta tecnica adottata dalla difesa del dipendente di non parteciparvi e limitarsi a contestare la procedura)- di assistere alle verifiche medesime, ma piuttosto quella di documentare la non modificabilità dei dati acquisiti in modo sicuro e certo, ai fini di consentire poi -nel corso del procedimento disciplinare piuttosto che in giudizio- la ripetibilità, e quindi la verifica e nel caso critica, delle operazioni effettuate (in questo, banalizzando, sta il principio della tecnica c.d. forensics[3]: il mondo digitale per sua natura è alterabile in quanto virtuale e quando venisse effettuata una indagine sull'originale dell'hard disk del pc, questo risulterebbe definitivamente alterato; procedura che appare seguita specificamente nel caso, almeno dalla descrizione che ne fa il provvedimento: ovviamente questa è una semplificazione concettuale, come detto, di procedimenti altamente tecnici, per cui occorre avvalersi di tecnici con documentate competenze; come dicono in tv: don't do this at home!).

Il focus della partecipazione del dipendente si sposta invece sulla procedura disciplinare, nel corso della quale occorre mettere il dipendente in condizione di difendersi adeguatamente. Il che significa allegare alla contestazione la documentazione che consente al medesimo di avere contezza dei rilievi effettuatigli, degli inadempimenti contestatigli e del materiale di supporto di tali contestazioni, ed in tale senso anche apprezzare se il termine legale di 5 giorni, ove non ne esista uno contrattuale diverso, sia idoneo ad una compiuta difesa o meno (cfr. da ultimo Cass. n. 22025/2015, sull'accesso ai documenti di supporto come parte del procedimento disciplinare).

Questa è -nel rapporto di lavoro- una condizione di legittimità del procedimento e di ogni atto conseguente.

La copertura giuridica del diritto al controllo pare poi essere stata condivisibilmente identificata nel diritto del datore di lavoro, nell'ambito come detto del proprio domicilio informatico e della prestazione di lavoro, di verificare l'abuso sospettato (Art. 24 codice Privacy, relative al trattamento in caso di tutela di diritti; nonchè art. 2104 e 2105 cod. Civ.; sotto questo profilo soccorrono anche le Opinion del Data Privacy Working Party del 2001 e del Maggio 2002; nonchè le argomentazioni della decisione nella Causa B RBULESCU v. ROMANIA: 12 gennaio 2016 della Corte Europea dei Diritti dell'Uomo, pure commentate su questa rivista come indicato in nota[4]).

Dovendo trarre la sintesi pratica delle implicazioni che rilevano nel rapporto di lavoro e che emergono dalla decisione:

3. *Cfr. fra i riferimenti: https://en.wikipedia.org/wiki/Computer_forensics.*

4. *Cfr. nota 1.*

- occorre la definizione preliminare del domicilio informatico dell'impresa datrice di lavoro (tramite policy, procedure, direttive: art. 2086 e 2104 c.c.). Ricordando che l'utilizzo dichiaratamente promiscuo dei beni aziendali (ad esempio la possibilità di avere sul pc aziendale cartelle personali ecc.) altera completamente le logiche definitorie del domicilio informatico e dei conseguenti diritti, implicando anche diversi e limitati poteri di controllo;
- occorre la definizione del ruolo del dipendente all'interno dell'organizzazione (tramite lo specifico mansionario o, meglio, l'incarico espresso al trattamento dei dati);
- occorre la ricognizione dei trattamenti dei dati effettuati nell'impresa e la definizione dell'organizzazione dei medesimi, attraverso la verifica delle necessità di trattamento (art. 3 Cod. Privacy), nonchè dei principi di pertinenza e non eccedenza una volta identificati i trattamenti necessari (art. 11 cod. Privacy);
- occorre la disclosure sui trattamenti così identificati mediante l'informativa, che può integrare le policy; nell'ambito di questa vanno espressamente identificate le categorie di soggetti che potranno avere accesso ai dati ed ai quali potranno essere comunicati e le finalità;
- occorre mettere in relazione il risultante dispositivo tecnico/normativo/finalistico con le funzioni che definiscono gli strumenti di lavoro aziendali e analizzare la distinzione di questi dagli strumenti di controllo (ricordando che possiamo assumere che nel mondo digitale sia la funzione a stabilire una relazione di connessione che identifica un dispositivo di controllo e che in conseguenza di ciò lo stesso strumento può assumere vesti diverse a seconda del dispositivo in cui è inserito) per verificare se occorra rispettare le procedure dell'art. 4 l.n. 300/70, comma primo;
- occorre che il controllo sia necessitato (e cioè non si possa prevenire l'abuso dello strumento attraverso scelte organizzative) e che esista un indizio dell'abusività dell'utilizzo che giustifichi il controllo;
- occorre che l'indagine si attenga a regole di verificabilità del comportamento tenuto dagli investigatori (e di ripetibilità);
- occorre naturalmente il rispetto della procedura disciplinare (art. 7 l.n.300/70) per ogni contestazione che emerga dalle verifiche.

Ovviamente, l'utilizzo della tecnica delle indagini difensive (art. 391 bis c.p.p.) apre diversi profili che non appartengono però allo spazio di questa analisi, cosiccome l'utilizzo della tecnica di impiego in azienda di sistemi BYOD (Bring Your Own Device) altera anch'essa completamente le possibilità di indagine considerate dal provvedimento dell'autorità in oggetto e richiederebbe riflessioni diverse che esulano da questa sede.