ARTICOLO SU INTERNET – E. MAIL E POTERI DI CONTROLLO DEL DATORE DI LAVORO

Autori:
ALESSANDRO VASTA
AURELIO LONIGO

1. Il Problema

Il rapido sviluppo tecnologico degli ultimi decenni se da un lato ha contribuito a migliorare le capacità produttive ed organizzative delle imprese, dall'altro ha certamente posto nuovi problemi in termini di rapporti con i lavoratori.

E' indubbio infatti che gli strumenti informatici e telematici rappresentino oggi indispensabili **mezzi di produzione**, posti dall'azienda a disposizione dei dipendenti per agevolarne e renderne più efficiente la prestazione lavorativa; peraltro tali strumenti, proprio a causa delle caratteristiche tecniche di funzionamento, rischiano di diventare un potenziale (ed a volte involontario) strumento di controllo sull'attività dell'utente (ad es. si pensi ai servers che registrano i files di *log* o la *cache memory* degli accessi ad Internet).

Ciò ha riproposto in termini assolutamente nuovi l'ormai noto **contrasto** fra il legittimo esercizio del potere direttivo del datore di lavoro, con il connesso potere di controllo, ed i contrapposti diritti di riservatezza, libertà e dignità dei lavoratori.

Infatti, da un lato il datore di lavoro avverte oggi più che mai l'esigenza di adottare misure a protezione dei propri strumenti informatici, nonché di verificarne il corretto utilizzo, sanzionando quegli usi scorretti che non solo possono integrare la violazione del dovere di diligenza e fedeltà nell'esecuzione del rapporto di lavoro, ma altresì compromettere il patrimonio aziendale od esporre la società a responsabilità verso terzi[1]; dall'altro il lavoratore,

[1] E' necessario sottolineare che tale diritto del datore di lavoro si trasforma in onere, qualora voglia godere della tutela penale riconosciuta dagli artt. 615 ter e 615 quater del Codice Penale, posti a tutela del "domicilio informatico". In particolare l'**art. 615 ter, Codice Penale** (Accesso abusivo ad un sistema informatico o telematico) dispone: "*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*
La pena è della reclusione da uno a cinque anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militar o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

vista l'accresciuta potenzialità "invasiva" di queste tecnologie, sente più pressante l'esigenza di tutela della propria sfera personale e della propria dignità.

Tutto ciò coinvolge questioni che attengono all'applicazione della normativa giuslavoristica dettata a difesa della dignità e della libertà dei lavoratori (i.e. art. 4 e 8 della Legge 20 maggio 1970, n. 300, di seguito lo "*Statuto dei lavoratori*"), delle norme penali volte a tutelare la corrispondenza privata (i.e. art. 615 codice penale) ed infine del complesso di norme disciplinanti il corretto trattamento dei dati personali (D. lgs. 30.06.2003 n. 196 "Codice in materia di protezione dei dati personali", di seguito il "*Codice privacy*").

In questo articolo, si presterà specifica attenzione a due strumenti comunemente messi a disposizione del lavoratore per l'esecuzione della prestazione lavorativa: **(i)** la posta elettronica aziendale e **(ii)** gli strumenti informatici che consentono l'accesso al *world wide web*. Nel far ciò verrà preso in esame sia lo stato della normativa che la concreta applicazione data ad essa dalla giurisprudenza, tentando, ove possibile, di suggerire delle soluzioni ai notevoli problemi posti.

2. Il Quadro Normativo

2.1 Il potere gerarchico e di controllo del datore di lavoro

Il fondamento del potere del datore di lavoro, quale "capo" dell'impresa[2], di esercitare un controllo sulla regolare ed esatta esecuzione della prestazione di lavoro dei propri dipendenti, risiede in alcune norme del codice civile, le quali gli attribuiscono il diritto di verificare:

- il rispetto della diligenza richiesta ai sensi dell'**art. 2104, comma 1, c.c.,** secondo cui: "*Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale*";
- il rispetto delle istruzioni impartite ai sensi dell'**art. 2104, comma 2, c.c.** secondo il quale: "*il dipendente deve inoltre osservare le disposizioni per l'esecuzione e la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende*";
- il rispetto dell'obbligo di fedeltà di cui all'**art. 2105 c.c.**, ai sensi del quale: "*il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con*

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio." L'**art. 615 quater Codice Penale** (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici) dispone: "*Chiunque, al fine di procurare a sè o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a lire dieci milioni.*
La pena è della reclusione da uno a due anni e della multa da lire dieci milioni a venti milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617quater."

[2] L'**art. 2086 c.c.** individua nell'imprenditore " *il capo dell'impresa e da lui dipendono gerarchicamente i suoi collaboratori*"

l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio".

L'inosservanza di tali obblighi può portare, da parte del datore di lavoro, al legittimo esercizio del potere disciplinare, previsto dall'**art. 2106 c.c.**[3] e dall'art. 7 dello Statuto dei lavoratori[4]. Tali poteri di cui gode il datore di lavoro, per mantenersi legittimi, devono peraltro essere contemperati con il rispetto delle libertà fondamentali del lavoratore, riconosciute e tutelate principalmente dallo Statuto dei lavoratori.

2.2 – La Normativa a tutela dei lavoratori

Viene di conseguenza in rilievo la normativa dettata dalla **Legge 20 maggio 1970, n. 300**, meglio nota come "Statuto dei lavoratori" [5] ed in particolare, ai nostri fini il dettato dell'**art. 4 dello Statuto dei lavoratori**[6] il quale sancisce innanzitutto il divieto assoluto ed inderogabile di utilizzo "*di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori"* (c.d. *Controllo intenzionale*), salvo poi ammettere l'uso di impianti e apparecchiature da cui derivi anche solo la possibilità di controllo a distanza dell'attività dei lavoratori ad una duplice condizione: (i) che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, e (ii) che siano installati previo accordo con le rappresentanze sindacali aziendali, oppure in mancanza di

---

[3] **Art. 2106 c.c.**: "*L'inosservanza delle disposizioni contenute nei due articoli precedenti può dar luogo all'applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione e in conformità delle norme corporative*":

[4] Dispone **art. 7 dello Statuto dei Lavoratori**. (Sanzioni disciplinari): "*Le norme disciplinari relative alle sanzioni, alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alle procedure di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti. Esse devono applicare quanto in materia è stabilito da accordi e contratti di lavoro ove esistano.*
Il datore di lavoro non può adottare alcun provvedimento disciplinare nei confronti del lavoratore senza avergli preventivamente contestato l'addebito e senza averlo sentito a sua difesa.
Il lavoratore potrà farsi assistere da un rappresentante dell'associazione sindacale cui aderisce o conferisce mandato.
Fermo restando quanto disposto dalla legge 15 luglio 1966, n. 604, non possono essere disposte sanzioni disciplinari che comportino mutamenti definitivi del rapporto di lavoro; inoltre la multa non può essere disposta per un importo superiore a quattro ore della retribuzione base e la sospensione dal servizio e dalla retribuzione per più di dieci giorni.
In ogni caso, i provvedimenti disciplinari più gravi del rimprovero verbale non possono essere applicati prima che siano trascorsi cinque giorni dalla contestazione per iscritto del fatto che vi ha dato causa.
Salvo analoghe procedure previste dai contratti collettivi di lavoro e ferma restando la facoltà di adire l'autorità giudiziaria, il lavoratore al quale sia stata applicata una sanzione disciplinare può promuovere, nei venti giorni successivi, anche per mezzo dell'associazione alla quale sia iscritto ovvero conferisca mandato, la costituzione, tramite l'ufficio provinciale del lavoro e della massima occupazione, di un collegio di conciliazione ed arbitrato, composto da un rappresentante di ciascuna delle parti e da un terzo membro scelto di comune accordo o, in difetto di accordo, nominato dal direttore dell'ufficio del lavoro. La sanzione disciplinare resta sospesa fino alla pronuncia da parte del collegio.
Qualora il datore di lavoro non provveda, entro dieci giorni dall'invito rivoltogli dall'ufficio del lavoro, a nominare il proprio rappresentante in seno al collegio di cui al comma precedente, la sanzione disciplinare non ha effetto. Se il datore di lavoro adisce l'autorità giudiziaria, la sanzione disciplinare resta sospesa fino alla definizione del giudizio.
Non può tenersi conto ad alcun effetto delle sanzioni disciplinari decorsi due anni dalla loro applicazione."

[5] L'eventuale violazione di alcune sue norme potrebbe avere riflessi negativi in relazione altresì aulla valutazione di ottemperanza o meno della condotta del datore di lavoro a quanto disposto dal **D. Lgs. 30 giugno 2003, n. 196**, *Codice in materia di protezione dei dati personali.* In merito basti evidenziare che lo stesso Codice, al Titolo VIII, Capo III – Divieto di controllo a distanza e Telelavoro, afferma che "*resta fermo quanto disposto dall'art. 4 della legge 20 maggio 1970, n. 300*".

[6] L'art. 4, commi 1 e 2 recita:" *E' vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. 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 solo 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 dove occorra le modalità per l'uso di tali impianti….. [omissis]."*

queste con la commissione interna od ancora, in difetto di accordo, a seguito di provvedimento dell''Ispettorato del lavoro, che detti le modalità per l'uso di tali impianti." (c.d. "*controllo preterintenzionale*").

Altra norma che può assumere rilevanza nel caso di specie, soprattutto con riferimento alla possibilità di controllo degli accessi ad Internet, è l'**art. 8 dello Statuto dei lavoratori**, il quale vieta al datore di lavoro, sia in fase di assunzione che nel corso di svolgimento del rapporto, di effettuare alcuna indagine "*sulle opinioni politiche, religiose e sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore".*

Il rispetto di tali fondamentali norme è garantito tramite il riconoscimento di poteri di intervento delle associazioni sindacali, volto ad ottenere la cessazione immediata dalla condotta illecita, nonché tramite l'applicazione di sanzioni penali a carico del datore di lavoro.

Ed infatti **l'art. 28** dello Statuto dei lavoratori, dispone che: "*Qualora il datore di lavoro ponga in essere comportamenti diretti a limitare od impedire l'esercizio dell'attività e della libertà sindacale…. su ricorso degli organismi locali delle associazioni sindacali nazionali che vi abbiano interesse, il giudice del luogo ove è posto in essere il comportamento denunziato…. ordina con decreto motivato la cessazione immediata del comportamento illegittimo e la cessazione degli effetti."*

La violazione di quanto disposto dagli articoli richiamati è punita ai sensi del combinato disposto dagli artt. 113, 114 e 171[7] del Codice Privacy e dell'**art. 38** dello Statuto dei lavoratori con l'ammenda da Euro 154 ad Euro 1549 o con l'arresto da 15 giorni ad un anno la condotta di chiunque violi gli articoli 4 ed 8 della Legge 300/1970[8].

2.3 Normativa a protezione dei dati personali

a) Il Codice Privacy

Il D. Lgs. 30 giugno 2003 n. 196, *Codice in materia di protezione dei dati personali* (di seguito il "Codice Privacy") è entrato in vigore il 1 gennaio 2004 ed ha abrogato, tra le altre norme, anche la previgente Legge 31 dicembre 1996 n. 675 sulla "*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*".

---

[7] **Art. 113 del Codice Privacy** (Raccolta di dati e pertinenza): "*Resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n.300*". **Art. 114 del Codice Privacy** (Controllo a distanza): "*Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n.300*". **Art. 171 del Codice Privacy**: "*La violazione delle disposizioni di cui agli articoli 113, comma 1, e 114 è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300*".

[8] Trattasi in realtà della pena base: il medesimo articolo prevede infatti che "*…Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicabili 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'art. 36 del codice penale"*

Oggetto principale della tutela è il **Dato personale**, definito dall'articolo 4 come "*qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".*

I Dati Personali si possono distinguere, principalmente, in :

a) "**Dati sensibili"** i quali ineriscono alla sfera più intima della persona, e che l'art.4 del Codice Privacy definisce come quelli "……*idonei a rivelare l'origine razziale o etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati idonei a rivelare lo stato di salute e la vita sessuale".*

b) **"Dati comuni"**, i quali si ricavano, a contrario, dalla definizione dei dati sensibili, come quei Dati Personali che non appartengono strettamente alla vita intima della persona, ma riguardano informazioni meno pregnanti e riservate, quali l'indirizzo, la residenza, la sede, la retribuzione, ecc.

Oltre alle norme di carattere generale comunque applicabili ai rapporti di lavoro, il Codice Privacy detta delle previsioni specifiche in materia al Titolo VII, *Lavoro e Previdenza sociale*. In particolare, con riferimento alle fattispecie in esame, l'art. 114 in materia di *Controllo a distanza* si limita a rinviare alla disciplina dettata dall'art. 4 dello Statuto dei lavoratori.

- **<u>Principi ed obblighi imposti dal Codice Privacy</u>**

I principi cardine a cui ogni trattamento di dati personali deve conformarsi sono enunciati all'**art. 11** del Codice Privacy, il quale recita:

"*I dati personali oggetto del trattamento devono essere:*

a) *trattati in modo lecito e secondo correttezza;*
b) *raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;*
c) *esatti, e se necessario, aggiornati;*
d) *pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;*
e) *conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.*

Tali principi costituiscono il parametro di riferimento cui qualsiasi trattamento di Dati personali si deve uniformare. Ai nostri fini, rilevano il dovere di liceità e correttezza del trattamento (c.d. **principio di liceità**), il dovere di trattare i dati per scopi legittimi, manifesti, determinati (c.d. **principio di finalità**), il dovere di trattare solo i dati strettamente pertinenti e non eccedenti rispetto al perseguimento delle finalità (lecite) di trattamento (c.d. **principio di proporzionalità**), nonché, infine, il dovere di conservarli per un tempo non eccedente a quello necessario al perseguimento degli scopi per i quali sono stati raccolti (c.d. **principio di conservazione e c.d. "diritto all'oblio"**):

A questi principi deve aggiungersi altresì il c.d. **principio di necessità,** espressione della novella legislativa del 2003[9], ai sensi del quale "*i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità*". L'applicazione concreta di tale norma comporta che il trattamento di dati personali non è lecito se le finalità del trattamento possono essere perseguite con dati anonimi o solo indirettamente identificativi[10].

Oltre a queste prescrizioni di carattere generale, la Legge pone a carico del Titolare[11] o, in caso di delega, del Responsabile[12], una serie di obbligazioni specifiche. Fra queste, per quanto di nostro interesse, rilevano:

I. l'obbligo di **informativa** all'interessato[13] e la raccolta del **consenso**[14] al trattamento dei dati, ove necessari.
II. l'obbligo di individuare gli **incaricati** del trattamento impartendo loro specifiche **istruzioni di trattamento**[15].

---

[9] Art. 3 Codice Privacy.
[10] Sono qualificati direttamente identificativi i dati personali che permettono l'identificazione diretta dell'interessato – cfr. art. 4, comma 1, lett. C) D. lgs. 196/2003
[11] Tale è la "*persona fisica, la persona giuridica, la pubblica amministrazione, e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità e modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza*".
[12] Tale è la "*persona fisica, la persona giuridica, la pubblica amministrazione, e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento di dati personali".*
[13] Cfr. **art. 13 del Codice Privacy**, secondo cui l'interessato, cioè la persona cui si riferiscono i dati, deve essere previamente informato, oralmente o per iscritto, circa: a) le finalità e modalità del trattamento; b) la natura obbligatoria o facoltativa del conferimento dei dati; c) le conseguenze di un eventuale rifiuto di rispondere; d) i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza e l'ambito di diffusione dei medesimi; e) i diritti di cui all'art. 7; f) gli estremi identificativi del Titolare e, se designato, del Responsabile.
[14] Cfr. **art. 23 del Codice Privacy** che enuncia il principio della necessità di un consenso dell'interessato libero, specifico, informato, espresso e documentato per iscritto, per il legittimo trattamento dei suoi dati personali, tranne nei casi in cui da tale consenso sia possibile prescindere, e **l'art. 26 del Codice Privacy**, che prescrive il consenso scritto per il trattamento dei dati sensibili.
[15] Cfr. **art. 30 del Codice Privacy** (Incaricati del trattamento): "*1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. 2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento*

III. l'obbligo di adozione delle **misure di sicurezza**[16]**.**

- **Sanzioni**

A fronte delle previsioni normative ricordate, il Codice Privacy prevede specifiche sanzioni penali o amministrative. In particolare interessano in questa sede **l'art. 167** il quale sanziona la condotta di chiunque *"Salvo che il fatto costituisca più grave reato, …, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli art. 18, 19, 23, 123, 126 e 130[17]"* punendolo *"…se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi, o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi"*[18].

L'art. **169**[19] sanziona con l'arresto sino a due anni o l'ammenda da diecimila a cinquantamila euro l'omessa adozione delle misure minime di sicurezza.

Sanzioni amministrative sono applicate in caso di violazione dell'obbligo di fornire all'interessato, o alla persona presso la quale i dati sono raccolti, l'informativa prevista dall'art. 13 del Codice, e consistono in una sanzione da tremila a diciottomila euro[20].

Quanto all'eventuale responsabilità civile sorgente per i danni cagionati da un illecito trattamento dei Dati Personali, il Codice Privacy, richiamando espressamente quanto previsto dall'articolo 2050 del codice civile, equipara l'attività di trattamento dei dati personali ad una "*attività pericolosa*" ed inverte l'onere della prova a carico del Titolare: ciò significa che non spetterà al danneggiato fornire la prova del fondamento del suo diritto, ma sarà il Titolare del

---

consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima."

[16] Cfr. **art. 31 e ss. del Codice Privacy**, secondo cui sussiste un obbligo di custodire e controllare i dati personali, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta. L'indicazione invece di **misure di sicurezza minime** (la cui mancata adozione comporta l'applicazione di sanzioni penali) é contenuta nel **Disciplinare Tecnico, Allegato B al Codice Privacy**.

[17] In particolare l'**art. 23 del Codice Privacy** prevede l'obbligo di ottenere il consenso dell'interessato al trattamento di dati personali da parte di soggetti privati o pubblici.

[18] Il medesimo articolo prevede sanzioni più gravi in caso di violazione delle norme relative a trattamenti di dati particolari (sensibili o relativi a provvedimenti giudiziari) o in caso dalla violazione derivi nocumento per l'interessato.

[19] Cfr. **art. 169 del Codice Privacy** (Misure di sicurezza): "*1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro. 2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non ecce-dente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. L'organo che im-partisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto ap-plicabili.*"

[20] Cfr. **art. 161 del Codice Privacy** (Omessa o inidonea informativa all'interessato): "*1. La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da tremila euro a diciottomila euro o, nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi specifici ai sensi dell'articolo 17 o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati, da cinquemila euro a trentamila euro. La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizio-ni economiche del contravventore.*"

trattamento dei dati che potrà liberarsi dalla responsabilità civile solo provando di aver adottato tutte le misure idonee ad evitare il danno cagionato[21].

Si ricorda infine quanto previsto dall'**art. 171** che nel sanzionare la violazione delle condotte di cui all'art. 114 del Codice Privacy (Controllo a distanza) rinvia alle sanzioni previste dall'art. 38 dello Statuto dei Lavoratori.

b) Il Gruppo di lavoro dei Garanti Europei

La disciplina oggi prevista dal Codice Privacy in materia di rapporti di lavoro è peraltro destinata ad essere integrata dalla prossima elaborazione ed adozione di un *Codice di deontologia e buona condotta* espressamente previsto dall'art. 111 dello steso Codice Privacy[22]. Nell'elaborazione di tale documento si dovrà probabilmente far riferimento non solo agli eventuali orientamenti elaborati dall'Autorità Garante per la protezione dei dati personali, ma altresì alle raccomandazioni del c.d. "Gruppo di lavoro sulla protezione dei dati"[23].

Al riguardo viene in rilievo il "*Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche" sul posto di lavoro"* adottato il 29 maggio 2002. Il documento parte dal presupposto che il lavoratore può legittimamente attendersi di usufruire di un certo grado di riservatezza sul posto di lavoro, dato che una parte significativa delle sue relazioni con gli altri esseri umani si sviluppa nell'ambiente di lavoro. Tale diritto deve peraltro essere controbilanciato dall'interesse legittimo del datore di lavoro di gestire la sua azienda con efficienza e di tutelarsi contro responsabilità o danni, anche verso terzi.

I Garanti sottolineano come la soluzione debba necessariamente essere individuata in un **bilanciamento** degli interessi contrapposti e rispondere alle seguenti valutazioni:

- prevenire gli abusi deve considerarsi più importante che individuarli;
- un divieto globale per i dipendenti di utilizzare Internet ed e-mail a fini personali appare irragionevole e non tiene conto del grado in cui tali strumenti possano aiutarli nella vita di tutti i giorni;

---

[21] Cfr **art. 15 del Codice Privacy**, secondo cui:"*Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 c.c.",* il quale a sua volta recita:"*Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di aver adottato tutte le misure idonee a evitare il danno".*

[22] Il meccanismo dell'elaborazione ed adozione di codici deontologici, anche di concerto con le organizzazioni di categoria interessate, è uno strumento già utilizzato in passato al fine di integrare il complesso normativo in materia di protezione dei dati personali con norme disciplinanti nel dettaglio settori di rilievo o particolarmente delicati (basti pensare ai codici in materia di attività giornalistica, scopi storici, scopi statistici e di ricerca scientifica, finanziamenti e credito al consumo).

[23] Il gruppo di lavoro è stato costituito in applicazione dell'art. 29 della Direttiva 95/46/CE in quanto organismo europeo indipendente con finalità consultive in materia di protezione dei dati e riservatezza. A tale organismo partecipano le Autorità Garanti per la protezione dei dati personali istituite nei paesi facenti parte l'Unione Europea e pertanto i documenti di lavoro elaborati dal Gruppo ed i relativi orientamenti costituiscono un concreto strumento di interpretazione della normativa nazionale e di valutazione delle relative evoluzioni.

Quanto alla posta elettronica:

- qualsiasi forma di controllo deve risultare assolutamente indispensabile (ad es. al fine di riscontrare un'eventuale attività criminosa, virus informatici, garantire la sicurezza dei sistemi, mantenere lo scambio di corrispondenza in caso di assenza del dipendente);
- i dati raccolti devono essere trattati per uno scopo determinato, esplicito e lecito: pertanto i dati raccolti ad es. per garantire la sicurezza dei sistemi non potranno poi essere utilizzati per altri finalità, quali ad es. il controllo del comportamento del lavoratore;
- l'attività di controllo deve essere trasparente, ovvero effettuata in modo chiaro ed esplicito e non occulto. In particolare il datore di lavoro dovrà fornire ai dipendenti una politica interna sull'utilizzo degli strumenti che risulti accessibile, chiara ed accurata ed informi i dipendenti indicando, tra l'altro:
  - modalità e tempi di utilizzo da parte dei dipendenti dei sistemi informatici e telematici di proprietà dell'azienda per comunicazioni personali o private (ad es. limiti di tempo e durata dell'impiego);
  - finalità di un'eventuale attività di vigilanza;
  - la procedura volta a garantire il rispetto delle regole con indicazione dei provvedimenti e delle infrazioni;
  - l'eventuale presenza di copie di back up dei sistemi e la durata della loro conservazione.

Quanto all'utilizzo di Internet:

- il datore di lavoro deve informare immediatamente il dipendente di qualsiasi uso improprio degli strumenti aziendali rilevato (ad es. ricorrendo a software che prevedano finestre di "pop up" con indicazione del tempo di connessione ad internet, ecc.);
- la prevenzione di una navigazione impropria deve essere preferita ad un'attività di controllo successivo;
- l'eventuale attività di controllo deve, se possibile, essere svolta senza analizzare il contenuto dei siti visitati: una verifica dei tempi di connessione o dei siti più visitati da un dipartimento può essere sufficiente a rilevare eventuali abusi i quali, una volta individuati, possono giustificare un'ulteriore attività di controllo;
- in ogni caso il datore di lavoro deve:
  - informare i dipendenti delle eventuali condizioni in cui è consentito l'impiego privato di internet;
  - informare i dipendenti dei sistemi adottati per impedire l'accesso a determinati siti e per individuare i casi di abuso;

- indicare la portata dei controlli e se essi possano riguardare singole persone o se in determinate circostanze il contenuto dei siti possa essere registrato e/o visionato.

2.4 Normativa penale

Con particolare riferimento alle ipotesi di accesso alla posta elettronica ed alla navigazione Internet del dipendente possono altresì venire in rilievo alcune fattispecie penali di cui al Titolo XII, Capo III, Sezione V del Codice Penale, "Delitti contro la inviolabilità dei segreti),

In particolare **l'art. 616 c.p.**[24] il quale sanziona diverse fattispecie di violazione della corrispondenza altrui quali **(i)** il venire a conoscenza di corrispondenza chiusa, ovvero **(ii)** la rimozione della corrispondenza dal luogo in cui si trova (privandone così il destinatario della legittima disponibilità) od **(iii)** il trattenerla ritardandone così il recapito, ed ancora **(iv)** il danneggiamento materiale della stessa o **(v)** la sua sottrazione per impedirne la consegna. Ad estendere l'applicazione delle fattispecie penali alle ipotesi in esame provvede l'**ultimo comma** dell'art. 616 c.p. il quale stabilisce che per corrispondenza si deve intendere, agli effetti delle disposizioni del codice penale relative ai delitti contro l'inviolabilità dei segreti, "*quella epistolare, telegrafica, telefonica, informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza*"[25].

Assume altresì rilievo l'art. **617 quater c.p., comma 1,** il quale punisce l'intercettazione delle comunicazioni con mezzi informatici o telematici, ovvero il loro impedimento totale o parziale con interruzioni provocate da qualsiasi forma di ingresso nel sistema, o nel dialogo fra sistemi[26]. In particolare per intercettazione si deve intendere la presa di cognizione, totale o parziale, della comunicazione, la quale deve pervenire al legittimo destinatario perché, altrimenti, ricorrerebbero le altre ipotesi previste dalla norma,

---

[24] Cfr. art. 616 c.p. (Violazione, sottrazione e soppressione di corrispondenza): "*Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prendere o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, e' punito, se il fatto non e' preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da lire sessantamila a un milione.*
Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, e' punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni.
Il delitto e' punibile a querela della persona offesa.
Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza".

[25] Infine l'art. 623 bis c.p. estende l'applicabilità del complesso delle norme poste a tutela dell'inviolabilità dei segreti "*a qualunque altra trasmissione a distanza di suoni, immagini od altri dati*".

[26] L'art. 617 quater c.p., comma 1, recita: "Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto od in parte, il contenuto delle comunicazioni di cui a primo comma…." Tale delitto è punibile a querela della persona offesa; sono tuttavia perseguibili d'ufficio ove ricorrano determinate circostanze aggravanti giustificate dalla lesione di interessi facenti capo allo Stato o ad altri enti pubblici, ovvero alla qualifica di funzionario pubblico o di investigatore privato rivestita dall'autore del fatto.

quali l'interruzione o l'impedimento. Essa deve poi avvenire "fraudolentemente", cioè con l'utilizzazione di artifizi o raggiri[27].

3. La dottrina e la giurisprudenza

L'assenza di una normativa specifica che disciplini in maniera adeguata e moderna le fattispecie in esame, individuando in modo preciso facoltà o divieti, modalità o limiti per un corretto bilanciamento degli interessi giuridici in gioco, ha contribuito al proliferare di opinioni ed orientamenti in sede dottrinaria e giurisprudenziale; ad oggi, sul tema, si evidenziano **contrapposte tendenze**[28]:

- da un lato la **dottrina maggioritaria**[29], più incline ad assicurare soluzioni garantiste e tutelanti la posizione dei lavoratori, ritiene che gli strumenti che permettono un monitoraggio delle e-mail o degli accessi ad Internet devono senz'altro considerarsi strumenti di controllo a distanza, in quanto consentono al datore di lavoro di controllare e ricostruire l'attività dei dipendenti. Tali strumenti tecnologici devono pertanto essere attivati nel rispetto della procedura prevista dall'art. 4 dello Statuto dei lavoratori, nonché di quanto previsto dall'art 8 del medesimo Statuto, e quindi di concerto con le rappresentanze sindacali o con l'ispettorato del lavoro;

- di orientamento opposto una **dottrina minoritaria**[30], benché autorevole, secondo la quale la disciplina di cui all'art. 4 dello Statuto dei lavoratori deve applicarsi solo a sistemi di controllo aventi carattere estrinseco ed eventuale rispetto allo svolgimento della prestazione lavorativa (es. impianti di videosorveglianza); di conseguenza la norma non troverebbe applicazione all'installazione ed utilizzo di strumentazione informatica e telematica che rappresenti uno strumento essenziale di produzione;

---

[27] Le condotte indicate all'art. 617 quater c.p. sono sostanzialmente identiche a quelle desumibili dall'art. 616 c.p., il quale sanziona la condotta di chi prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto od in parte, la distrugge o sopprime . Mentre però nell'art. 617 quater l'oggetto della tutela penale è la comunicazione, cioè la trasmissione di un messaggio, costituito da idee, sentimenti, propositi, notizie, diverso dalla corrispondenza, nell'art. 616 c.p. oggetto di tutela è il risultato della comunicazione quale appare fissato in un documento materiale o in altro mezzo tecnico, destinato ad essere trasmesso e da altri ricevuto. Per esemplificare, chi prende abusivamente cognizione del contenuto di una comunicazione altrui memorizzata in un dischetto per elaboratore risponde del reato di cui all'art. 616 c.p., mentre chi si immette in una rete telematica, venendo a conoscenza di messaggi in corso di comunicazione, pone in essere il reato di cui all'art. 617 quater c.p.. La condotta deve presentare connotati di frode, e cioè deve consistere nella utilizzazione di artifizi o di raggiri.

[28] Per una panoramica in materia si veda anche E. BARRACO, *Potere di controllo del datore di lavoro, privacy e nuovi strumenti informatici*, in *Lav. nella Giurisp*., 9, 2005.

[29] Fra gli altri A. BELLAVISTA, *Poteri dell'imprenditore e privacy del lavoratore*, in *I poteri del datore di lavoro nell'impresa*, Milano, 2002, p.41; A. STANCHI, *Privacy, rapporto di lavoro, monitoraggio degli accessi ad internet, monitoraggio delle e-mail e normative di tutela contro il controllo a distanza. Alcuni spunti per una riflessione interpretativa*, in *I poteri del datore di lavoro d'impresa*, Padova, 2002.

[30] Fra gli altri P. ICHINO, *Il contratto di lavoro*, III, in *Trattato di diritto civile e commerciale Schlesinger*, Milano, 2003, p.234; C. PISANI, *Il computer e l'art. 4 della Statuto dei lavoratori*, in *Nuove tecnologie e tutela della riservatezza dei lavoratori*, Milano, 1988, p. 43.

- una parte della **giurisprudenza** più recente (contrariamente all'orientamento precedente, più incline a soluzioni garantiste per i lavoratori[31]) pare aderire, in alcune pronunce, all'orientamento della dottrina minoritaria, riconoscendo la legittimità dell'attività di controllo del datore di lavoro e dell'utilizzo di strumenti tecnologici, escludendo la necessità di applicazione della procedura di cui all'art. 4 dello Statuto dei lavoratori: in particolare si è teorizzata la legittimità dei c.d. **controlli difensivi**, ovvero dei controlli mirati non a monitorare l'attività lavorativa del dipendente, bensì a prevenire ed individuare eventuali attività illecite dello stesso. Al riguardo, con riferimento all'utilizzo del *telefono aziendale*, la Suprema Corte ha recentemente riconosciuto la legittimità dell'installazione di impianti di controllo a distanza diretti non a monitorare l'attività lavorativa del dipendente, bensì ad accertare eventuali usi impropri dello strumento[32].

  Questo orientamento non ha peraltro evitato di sollevare alcune critiche, condivisibili, in considerazione del fatto che "*i controlli difensivi sarebbero inevitabilmente in grado di verificare, oltre all'eventuale comportamento illecito, anche l'adempimento della prestazione lavorativa, e quindi difficilmente potrebbero rimanere distinti da quelli che vertono sull'attività del lavoratore*"[33].

  L' orientamento appena illustrato è lungi peraltro dal potersi considerare consolidato; al contrario si devono segnalare altre recenti pronunce della stessa Cassazione che, nel 2000 e 2003, ha affermato non solo la nullità delle prove (relative a condotte illecite del lavoratore) raccolte dal datore di lavoro mediante l'impiego di mezzi di controllo a distanza non concordati, né autorizzati ai sensi dell'art. 4 dello Statuto dei lavoratori, ma

---

[31] Cfr. **Cass. 18 febbraio 1983, n. 1236**, In *Foro It*., 1985, I, 2076: "*L'installazione in azienda, da parte del datore di lavoro di impianti ed apparecchiature richiesti da esigenze produttive, dai quali derivi anche possibilità di controllo a distanza sull'attività lavorativa dei dipendenti, deve essere preceduta da un vero e proprio accordo con le r.s.a., non essendo sufficiente a legittimare l'installazione né il fatto che le maestranze fossero a conoscenza dell'esistenza degli impianti potenzialmente idonei al controllo, né la circostanza che gli impianti abbiano funzionato per un periodo senza contestazioni…*"; **Cass. 21 agosto 1986, n. 1490**, in *Giut. It*. 1987, I, 1, 1102: "*Il divieto del controllo a distanza posto al datore di lavoro dall'articolo 4 dello Statuto dei lavoratori, è assoluto e pertanto non può ritenersi escluso né dalla circostanza che le eventuali apparecchiature non siano ancora funzionanti, né che i lavoratori ne siano stati preavvertiti…*"; **Cass. 16 settembre 1997, n. 9211**, in *Riv. Giur. Lav*., 1988, II, 58: "*L'installazione in azienda, da parte del datore di lavoro, di apparecchiature di controllo, che è assoggettata ai limiti previsti dall'articolo 4 dello Statuto dei lavoratori, anche se peraltro derivi solamente una mera potenzialità del controllo, senza che peraltro rilevi il fatto che i dipendenti siano a conoscenza dell'esistenza di tali impianti, deve essere preceduta dall'accordo con le rappresentanze sindacali aziendali…*".

[32] Cfr. **Cass. 3 aprile 2002, n.4746**, in *Guida al Lavoro*, 21/2002, p. 10: "*Ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4, legge n. 300/1970, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (c.d. controlli difensivi) quali, ad esempio, i sistemi di controlli dell'accesso ad aree riservate, o, appunto, gli apparecchi di rilevazione di telefonate ingiustificate. L'abuso del telefono aziendale può costituire giustificato motivo soggettivo di licenziamento indipendentemente dall'entità del danno creato al datore di lavoro*". Vedi anche **Tribunale di Torino, 9 gennaio 2004**, in *Giur. Piem*., 2004, p. 131. In tali pronunce la giurisprudenza non affronta peraltro la questione dell'applicazione della procedura di cui all'art. 4 dello Statuto dei lavoratori, ritenendo evidentemente i controlli difensivi sganciati dalla necessità di ottenere il consenso delle rappresentanze sindacali o dell'intervento dell'Ispettorato del lavoro.

[33] Cfr. A. MAGGI, *Il controllo della posta elettronica aziendale*, in *G. Lav*., 2005, n.36. Nel medesimo senso G. BASCHERINI in nota a sentenza Corte d'Appello di Ancona 1 agosto 2003, in *Il lavoro nella giurisprudenza* n. 2/2004.

altresì la sussistenza, a carico del datore di lavoro medesimo, della responsabilità penale per violazione degli artt. 4, comma 2 e 38 dello Statuto dei lavoratori[34].

Anche i giudici di merito hanno seguito tale strada: si veda la pronuncia del Tribunale di Milano del 31 marzo 2004, con cui è stato censurato l'utilizzo di un software di controllo degli accessi ad internet, in quanto implicante interferenze (e quindi un controllo) sull'attività lavorativa dei dipendenti[35], nonché, da ultimo, lo stesso Tribunale meneghino, con decreto del 11 aprile 2005, che ha dichiarato antisindacale l'uso di un programma informatico installato ed utilizzato (senza rispetto della procedura di cui all'art. 4 dello Statuto dei lavoratori) al centralino telefonico dell'azienda (con registrazione delle chiamate in entrata ed in uscita) in quanto permetteva indirettamente il controllo a distanza dei lavoratori[36].

Da queste osservazioni generali si evince dunque un quadro normativo assai complesso e controverso, che suggerisce una certa prudenza nelle soluzione pratiche da prospettare.

4. Valutazioni

Esaurito l'esame dello stato normativo, dottrinale e giurisprudenziale, il quesito da porsi attiene alla possibilità ed ai limiti entro i quali sia consentito al datore di lavoro:

a) il controllo e l'accesso alla casella di posta elettronica assegnata ai propri dipendenti, nonché
b) la verifica e monitoraggio degli accessi ad internet da parte dei propri dipendenti.

Quesito a) - L'accesso alla posta elettronica

[34] Cfr. **Cass., 17 giugno 2000, n.8250**, in *Mass. Giur. Lav.*, 2000, 858, secondo la quale non può essere accolta la domanda proposta nei confronti di una dipendente e avente ad oggetto il risarcimento dei danni derivanti dalla sottrazione di somme custodite nella cassa e fondata sulla produzione di fotogramma proveniente da una telecamera a circuito chiuso installata nell'esercizio ove la dipendente prestava la propria attività lavorativa. **Cass. 3 ottobre 2000, n. 14671**, secondo la quale "*le prove ottenute dal datore di lavoro tramite l'utilizzo, non concordato con le organizzazioni sindacali né autorizzato dall'Ispettorato del lavoro, di mezzi di controllo a distanza sono nulle anche se ritraggono i lavoratori in comportamenti illeciti*". Con riferimento all'installazione di un impianto di telecamere cfr. anche **Cass. Pen., 6 marzo 2003, n. 10268**, in *Dir. Lav.*, 2003, 14, ai sensi della quale "*commette il reato di cui agli artt. 4, comma 2, e 38 legge 30 maggio 1970, n. 300 il datore di lavoro, il quale, senza preventivo accordo con le rappresentanze sindacali, abbia installato delle telecamere che, seppure destinate ad evitare furti, renda possibile il controllo a distanza dell'attività dei dipendenti*".

[35] **Tribunale Milano, 31 marzo 2004**, in *Or. Giur. Lav.*, 2004, p. 108. Si trattava in particolare di un software (installato senza ricorrere alla procedura di cui all'art. 4 dello Statuto dei Lavoratori) che consentiva il monitoraggio della navigazione internet effettuata dai singoli dipendenti ed utilizzato *ad libitum* dal datore di lavoro per verifiche mirate. Secondo il Tribunale i c.d. controlli difensivi "*non costituiscono una categoria a sé, esentata a priori dall'applicabilità delle previsioni dell'art. 4 Statuto dei Lavoratori, benché implicanti anche la raccolta di notizie sull'attività lavorativa, ma semplicemente un modo di definire sinteticamente controlli finalizzati all'accertamento di condotte illecite del lavoratore che non rientrano nell'ambito di applicazione dell'art. 4 S.L. perché non comportano la raccolta **anche** di notizie sull'attività lavorativa*".

[36] Il Giudicante, con riferimento alla portata dei controlli difensivi di cui alla sentenza della Cassazione 4746/2002, precisa che "*la Suprema Corte ha ritenuto ammissibile tale tipologia di vigilanza da parte del datore di lavoro, allorché tuttavia, la stessa non riguardi l'attività lavorativa affidata ai propri dipendenti, ambito – quest'ultimo – entro il quale torna invece a trovare applicazione il disposto di cui all'articolo 4, 2° comma dello Statuto dei Lavoratori*".

Con riferimento alla gestione dell'e-mail aziendale, ed alla possibilità di monitorarne l'utilizzo e/o di accedere ai contenuti della posta elettronica, vengono in rilievo problematiche attinenti alla: 1) configurabilità di fattispecie penali di reato; 2) possibile violazione dello Statuto dei lavoratori; 3) possibile violazione della normativa in materia di protezione dei dati personali.

1) Configurabilità di fattispecie penale di reato

Con riferimento all'ipotesi di accesso alla posta elettronica del dipendente (ad es. nel caso di assenza dello stesso) vengono in rilievo le fattispecie penali di cui al Titolo XII, Capo III, Sezione V del Codice Penale, "Delitti contro la inviolabilità dei segreti"). In particolare, l'ipotesi di cui all'art. 616 c.p. ("*Violazione, sottrazione e soppressione di corrispondenza*")[37].

Astrattamente ipotizzabili sarebbero anche le fattispecie di cui all'art. 616, n.2 e 3, c.p. che sanzionano rispettivamente la sottrazione o distrazione, al fine di prenderne o di farne prendere cognizione, di corrispondenza chiusa o aperta altrui, ovvero la distruzione o soppressione, in tutto o in parte, di corrispondenza altrui. Si pensi, ad esempio, ai sistemi che procedano al "filtraggio" delle e-mail in entrata od uscita, giustificati tanto da esigenze "anti-spam" quanto, ad esempio, dalla necessità di proteggere i sistemi dall'ingresso di virus. Il blocco delle e-mail effettuato da tali sistemi, magari connesso ad attività di verifica delle e-mail bloccate al fine di provvedere al loro inoltro al destinatario in caso di "blocco non giustificato", nonché l'eventuale cancellazione delle e-mail ritenute "spamming".

Sulla questione, l'orientamento giurisprudenziale più recente appare volto a negare la ricorrenza degli estremi di reato proprio in ragione della natura della posta elettronica quale bene strumentale all'esercizio dell'attività lavorativa.

In particolare il **Tribunale di Milano**, con sentenza 10 maggio 2002[38], ha negato integri gli estremi del reato di violazione della corrispondenza, di cui all'art. 616, comma primo, c.p., la condotta del datore di lavoro il quale, all'insaputa del lavoratore, controlli la sua posta elettronica, in quanto "***il lavoratore non è titolare di un diritto all'utilizzo esclusivo della posta elettronica aziendale*** *e quindi si espone al rischio che altri lavoratori o il datore di lavoro possano lecitamente entrare nella sua casella e leggere i messaggi*".

L'indirizzo di posta, argomenta il Tribunale, è sì "*personale*" del dipendente (in quanto attribuito al singolo lavoratore per lo svolgimento delle proprie mansioni), ma non è "*privato*". "*L'indirizzo aziendale, proprio in quanto tale, può sempre essere nella disponibilità di accesso*

[37] Con riferimento all'equiparazione fra posta elettronica e corrispondenza epistolare o telefonica lo stesso Garante per la protezione dei dati personali ha precisato che " *la posta via internet, anche con l'uso di mailing list o newsgroup, rientra tra le protezioni che l'art. 15 della Costituzione riserva alla corrispondenza*" – cfr. Parere 12 luglio 1999.
[38] In *Massimario di giurisprudenza del lavoro*, 2002, p. 555.

e lettura da parte di persone diverse dall'utilizzatore consuetudinario. *[…] Come non può configurarsi un diritto del lavoratore ad accedere in via esclusiva al computer aziendale, parimenti* ***non è configurabile in astratto un diritto all'utilizzo esclusivo di una casella di posta elettronica aziendale***". In tale ottica "*non può ritenersi che leggendo la posta elettronica contenuta sul personal computer del lavoratore si possa verificare un controllo non consentito sulle attività del lavoratore stesso in quanto l'uso dell'e-mail costituisce un semplice* ***strumento aziendale*** *che, come tutti gli altri strumenti di lavoro forniti dall'azienda, rimane nella completa e totale disponibilità del datore di lavoro*".

In senso contrario alla citata pronuncia, va peraltro segnalata una recente sentenza del Giudice di Pace di Bari, adito in sede civile, il quale ha negato il principio della libera accessibilità del datore di lavoro alla casella di posta elettronica assegnata ad un determinato soggetto sul luogo di lavoro, anche se, va rilevato, la fattispecie sottoposta al suo esame (il titolare della casella di posta elettronica era una giornalista) presentava peculiarità che non rendono la pronuncia estensibile *sic et simpliciter* a fattispecie più comuni.[39]

La posizione espressa sulla questione dalla pronuncia del Tribunale di Milano appare, a parere di chi scrive, condivisibile.

La casella di posta elettronica assegnata al dipendente al momento dell'assunzione è effettivamente un bene strumentale all'esecuzione della prestazione lavorativa, e come tale deve essere utilizzato dal lavoratore. In tal senso l'accesso alla stessa da parte del datore di lavoro non può ritenersi come accesso a corrispondenza "a lui non diretta", come previsto dalla fattispecie penale astratta di cui all'art. 616 c.p.[40] D'altronde a nessuno verrebbe in mente di sanzionare l'accesso del datore di lavoro alla corrispondenza cartacea archiviata in qualsiasi ufficio di cui si compone l'azienda; ed il fatto che grazie alla tecnologia la corrispondenza oggi assuma natura di "documento informatico"[41] non toglie alla stessa, a parere di chi scrive, natura di "corrispondenza aziendale".

Altro argomento a sostegno dell'esclusione di responsabilità penale deriverebbe dal tenore letterale della norma, la quale sanziona solo la violazione di corrispondenza "chiusa": da ciò l'opinione, autorevolmente sostenuta in dottrina, secondo la quale solo la

---

[39] Vedi sentenza 7 giugno 2005 in *Diritto dell'Internet* - n. 6/2005, Ipsoa ed.; il giudice barese, per discostarsi dalla tesi circa la qualificazione dell'e-mail aziendale personalizzato come semplice strumento aziendale e come tale liberamente accessibile da parte del datore di lavoro, argomenta che:….*il lavoro del giornalista non può confondersi con quello del contabile o di altro utilizzatore di computer aziendale…in quanto il dovere del segreto professionale qualifica diversamente l'attività giornalistica ancorché svolta alle dipendenze dell'imprenditore*."

[40] Lo stesso Tribunale di Milano, *cit*. ha affermato che "*un uso extra lavorativo dell'e-mail aziendale non porta a mutare la destinazione dello strumento in sé*", che è quello di comunicazione con clienti e colleghi nell'esercizio delle proprie mansioni lavorative. In senso conforme M. LANOTTE, nota alla sentenza del Tribunale Milano cit., in *Massimario di giurisprudenza del lavoro,* agosto – settembre 2002, n. 8-9 – Il Sole 24 ore.

[41] L'art. 1 del Decreto Legislativo 7 marzo 2005, n. 82 "*Codice dell'amministrazione digitale*" definisce quale documento informatico "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*".

corrispondenza elettronica inviata in forma criptica sarebbe oggetto di tutela della norma penale[42]. Su questo forse si potrebbe obiettare che i sistemi di posta elettronica, il cui accesso ed utilizzo sia condizionato all'autenticazione mediante "*username e password*" abbiano per ciò ad oggetto "corrispondenza chiusa", in un senso più coerente alla realtà della "corrispondenza informatica o telematica". D'altronde se quanto sostenuto dalla dottrina fosse confermato, ogni tipo di corrispondenza non "criptata" (e ciò rappresenta la maggior parte dei casi, essendo più spesso protetti i documenti informatici allegati alla comunicazione, più che la comunicazione medesima)[43], anche quella realmente privata, sarebbe priva di tutela penale. Il che parrebbe eccessivo.

Salvo quanto sopra, non si può peraltro negare l'evidenza, e cioè la possibilità che il dipendente utilizzi comunque la posta elettronica aziendale per comunicazioni private (sempre nei limiti della liceità e correttezza). Anche in tale ipotesi, quand'anche prendesse cognizione di messaggi personali (inviati o ricevuti dal dipendente per il mezzo della casella di posta elettronica aziendale), pur integrando la condotta l'elemento oggettivo del reato, pare condivisibile la tesi secondo cui il datore di lavoro non sarebbe comunque punibile per insussistenza dell'elemento del dolo nella condotta astrattamente contestata[44].

La costruzione prospettata presuppone peraltro la presenza di **regole interne**[45] chiare e specifiche in merito all'utilizzo della posta elettronica aziendale, che informino in particolare il dipendente del carattere "aziendale" dello strumento, della possibilità di accesso da parte di terzi per fini lavorativi (ad es. del diretto superiore o di altro dipendente espressamente autorizzato) e dell'eventuale divieto di utilizzo della stessa per fini privati[46]. Non mancano difatti decisioni di diverso avviso laddove la contestazione di utilizzo personale dello strumento di lavoro (nella fattispecie del telefono aziendale) appariva sproporzionata "*in considerazione dell'assenza di una precisa disposizione di divieto, di un tolleranza protratta per anni, di un'effettiva contestazione precedente ed in assenza di precedente provvedimento disciplinare*"[47].

---

[42] Cfr. F. TOFFOLETTO, in *I problemi giuridici di internet*, AA.VV., Giuffrè Ed., 2003, I, pag. 358.

[43] Per una definizione di posta elettronica si veda l'art. 4 del D. lgs 30.06.2003, n. 196, secondo il quale si possono qualificare come tale:"*i messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza*".

[44] Nel medesimo senso cfr. M. LANOTTE, *Utilizzo privato della posta elettronica aziendale e poteri di controllo del datore di lavoro*, in *Massimario di giurisprudenza del lavoro*, 2002, n. 8-9.

[45] Quale un Codice di condotta (Policy). Si veda sul punto Confindustria, *Linee guida per l'utilizzo dei sistemi informatici aziendali*, 5 luglio 2001, e gruppo di lavoro dei Garanti Europei, *Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro*, 29 maggio 2002.

[46] In merito, con riferimento alla legittimità di licenziamento per abuso di telefono aziendale la Suprema Corte ha rilevato che, fermo restando la legittimità del controllo difensivo del datore di lavoro, in ogni caso la telefonata abusiva era "*oggetto di specifica previsione del codice disciplinare e di specifici richiami da parte dell'azienda*" (Cass. 10 luglio 2002, n. 10062).

[47] Cfr. **Tribunale di Milano, 10 ottobre 2003**, in Riv. Critica di diritto del lavoro, 2004, I, p.117.

Tali regole dovranno inoltre essere portate adeguatamente a conoscenza dei lavoratori ed affisse in luogo accessibile a tutti, in conformità a quanto disposto dall'art. 7 della Statuto dei lavoratori, onde consentire l'operatività delle sanzioni disciplinari previste per le eventuali violazioni. L'informazione dei dipendenti consentirà altresì di escludere l'applicazione dell'ulteriore norma penale che potrebbe venire in considerazione, l'art. 617 quater c.p.[48]: per il concretizzarsi di tale reato, infatti, l'intercettazione da parte del datore di lavoro dovrebbe avvenire in maniera "fraudolenta", ovvero all'insaputa del dipendente.

2) Possibile violazione dello Statuto dei lavoratori.

Qualora le finalità perseguite dal datore di lavoro non vadano oltre la gestione dei sistemi di posta elettronica, a fini di corretto funzionamento e sicurezza degli stessi (si pensi all'impiego di strumenti informatici volti a monitorare l'utilizzo della posta elettronica per proteggersi da attacchi informatici e/ da fastidiosi – e costosi - fenomeni quali lo *spamming*) non si ritiene sussistano ragionevoli motivi per affermare che ciò richiederebbe comunque – viste le potenzialità di controllo sull'attività di invio e ricezione della corrispondenza, nonché sul relativo contenuto – l'adempimento delle procedure di consultazione previste dall'art. 4 dello Statuto dei lavoratori.

A ciò si oppone innanzitutto un basilare principio di ragionevolezza. In secondo luogo, ferme restando le considerazioni già svolte in merito ai c.d. controlli difensivi, la legittimità di tali operazioni, finalizzate unicamente a garantire la sicurezza dei sistemi, pare confermata dal fatto che le stesse rappresentano adempimento di veri e propri obblighi di legge (i.e. le misure di sicurezza previste dal Codice Privacy)[49].

Si può pertanto ragionevolmente ritenere che tali strumenti non rientrino nel divieto di cui all'art. 4 dello Statuto dei lavoratori (con conseguente necessità di raggiungere un accordo con le rappresentanze sindacali o l'intervento dell'Ispettorato del lavoro)[50] in quanto da un lato **(i)** non appaiono diretti a realizzare un controllo a distanza del lavoratore bensì a salvaguardare i sistemi aziendali da rischi informatici e a garantire il corretto funzionamento del sistema (ad es. a fronte della presenza di strumenti di protezione, ad es. anti-spam); dall'altro **(ii)** dato il carattere "aziendale" dell'e-mail (quale strumento di lavoro), dovendosi ritenere consentito un accesso ai contenuti della singola casella di posta elettronica (vedi

[48] Cfr. paragrafo 2.4.
[49] Cfr. D.Lgs. 30 giugno 2003 n. 196, Allegato B, Punto 16: *I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale*. Punto 17: *Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale*. Punto 18: *Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale*.
[50] Non manca tuttavia in dottrina chi, "*tenuto conto della gravi conseguenze che la norma determina in caso di violazioni*", suggerisce un atteggiamento più prudente e, di conseguenza, la ricerca dell'accordo sindacale – cfr. F. TOFFOLETTO, op. cit.

punto 1) che precede), a maggior ragione deve ritenersi lecita un'attività di filtro e monitoraggio generalizzato quale quella posta in essere dalla maggiore parte delle Direzioni di sistemi informativi, soprattutto delle aziende più articolate e complesse.

3) Possibile violazione della normativa in materia di protezione dei dati personali.

Appare innanzitutto indiscussa l'applicazione della normativa in materia di trattamento dei dati personali alla fattispecie in esame, anche alla luce dell'equiparazione dell'e-mail alla corrispondenza epistolare o telefonica. Il trattamento delle e-mail (sia a fini di filtraggio *anti-spam*, che a fini svolgimento dell'attività lavorativa) comporta infatti un potenziale trattamento di dati personali del dipendente[51].

In conformità all'orientamento giurisprudenziale relativo al carattere "aziendale" dello strumento di posta elettronica, il **Garante** per la protezione dei dati personali ha precisato che **la posta elettronica dei dipendenti può essere oggetto di controllo da parte del datore di lavoro per fini connessi allo svolgimento della normale attività lavorativa**[52].

In tale ottica, la stessa previsione e gestione di misure di sicurezza quali le **credenziali di autenticazione** (*username e password*) non devono essere lette come strumenti volti a garantire il carattere "privato" delle e-mail (e quindi della banca dati), bensì come strumenti volti a impedire l'accesso alle banche dati da parte di terzi estranei all'azienda[53]. Le stesse misure minime di sicurezza previste dal Codice Privacy prevedono la figura del soggetto, interno all'azienda, che custodisce le credenziali dei dipendenti al fine di consentire l'accesso alle banche dati anche in assenza o impedimento degli stessi[54] ovvero la possibilità di accedere alle medesime banche dati utilizzando credenziali alternative.

Va inoltre sottolineato che il carattere "aziendale" della posta elettronica non consente peraltro di legittimare un divieto assoluto per i dipendenti di utilizzo della stessa a fini personali. Una tale impostazione si scontra difatti con l'orientamento dei Garanti Europei i quali giudicano irragionevole un divieto globale per i dipendenti di utilizzo di Internet (ed e-mail) per fini personali e giungono a suggerire la possibilità di fornire ai lavoratori due linee di posta elettronica, la prima per scopi puramente personali, la seconda per scopi puramente privati.

---

[51] Trattamento tanto più evidente qualora non si voglia aderire all'orientamento che considera la posta elettronica aziendale esclusivamente uno strumento di lavoro.
[52] Cfr. *Newsletter del Garante*, 19 febbraio 2001: in particolare di trattava del caso di assenza del lavoratore.
[53] Cfr. Tribunale di Milano, *cit.*
[54] Quando l'accesso possa avvenire solo mediante l'utilizzo delle credenziali del dipendente assente.

Come già accennato l'orientamento dei Garanti Europei non ha carattere vincolante ma fornisce un'indicazione di quello che presumibilmente sarà il contenuto del Codice Deontologico in materia di lavoro e previdenza di prossima elaborazione. In conformità con tali indicazioni appare pertanto consigliabile:

- Limitare ogni attività di controllo a quelle **assolutamente indispensabili** (quali attività volte a rilevare attività illecite, la presenza di virus informatici, garantire la sicurezza del sistema informatico aziendale, mantenere lo scambio di corrispondenza in assenza del dipendente o per gestire l'attività lavorativa, ecc.);
- **Informare** i lavoratori in modo chiaro, accurato ed accessibile della politica adottata dalla società precisando: **(a)** se ed in che misura la posta elettronica possa essere utilizzata per fini personali; **(b)** i motivi ed i caratteri di un'eventuale attività di vigilanza; **(c)** i provvedimenti adottabili dall'azienda in presenza di violazioni del Codice di condotta aziendale; **(d)** le misure per la contestazione delle violazioni del Codice di condotta; **(e)** l'eventuale presenza di *back up* sulla banca dati e durata di conservazione degli stessi.
- Effettuare verifiche approfondite sulla posizione del singolo lavoratore solo quando siano già emersi indizi di commissione di illecito[55].
- Evitare attività di controllo per altre finalità (ad es. per raccogliere informazioni riservate sui dipendenti o per controllarne l'attività lavorativa).
- Ove possibile, evitare un accesso continuo ed indiscriminato ai contenuti delle e-mail, limitandosi a verificare il numero dei messaggi inviati/ricevuti ovvero il relativo formato/dimensioni degli stessi.

Accanto all'obbligo di informare il dipendente, ai sensi dell'art. 13 del Codice Privacy in merito al trattamento dei suoi dati personali[56], si pone peraltro la necessità di valutare se sussista o meno l'obbligo di raccogliere il suo **consenso** ai sensi dell'art. 23 del Codice Privacy.

La risposta, a parere di chi scrive, deve essere negativa.

Infatti, a fronte dell'obbligo generale di necessità del consenso per il trattamento dei dati personali, l'art. 24, lett. b) del Codice Privacy dispone che lo stesso non sia necessario

[55] In tali ipotesi inoltre il trattamento di dati personali (neutri o sensibili) del dipendente potrebbe peraltro essere svolto senza la necessità di fornire preventivamente l'informativa ai sensi dell'art. 13 del Codice Privacy, né di raccogliere il consenso al trattamento dei dati in quanto troverebbe applicazione l'esonero previsto dagli art. 13, comma 5, lett. b, e art. 26, comma 4, lett. c), Codice Privacy per il trattamento volto al "*fine di far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento*".

[56] Obbligo da adempiere non solo mediante la predisposizione del Codice di condotta (c.d. Policy) sopra richiamato, ma altresì in sede di assunzione, informando il dipendente del trattamento che verrà fatto dei suoi dati ai fini della gestione del rapporto di lavoro.

quando il trattamento avviene "*per eseguire obblighi derivanti da un contratto del quale è parte l'interessato*". Nel caso in esame non vi è dubbio che il datore di lavoro accede alla posta elettronica nell'ambito del rapporto di lavoro e ne verifica l'utilizzo espletando poteri direttivi connaturali al suo ruolo di "capo dell'impresa": senza contare che tale potere si esplica normalmente sulla posta elettronica aziendale (e non ad es. su una casella di posta privata, es. "*web-mail*").

In altri casi (in cui vi sia il concreto rischio di condotte illecite da parte del lavoratore) l'attività di verifica, indipendentemente dal consenso dell'interessato, potrà essere giustificata in forza dell'art. 24, lett. f) del Codice Privacy, secondo il quale il consenso non è necessario quando il trattamento è volto al "*fine di far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento*"[57].

Entrambe le condizioni esimenti dall'obbligo del consenso paiono quindi ricorrere sia nella fase normale del rapporto di lavoro, essendo la posta elettronica uno strumento messo a disposizione del dipendente al fine di consentirgli l'espletamento della prestazione lavorativa, sia in una fase prodromica ad eventuali contestazioni di illeciti contrattuali o di violazioni normative da parte del dipendente medesimo[58].

* * *

<u>Quesito b)</u>: la verifica e monitoraggio degli accessi ad Internet

Anche con riferimento all'ipotesi di controllo degli accessi ad internet da parte dei dipendenti vengono in rilievo due aspetti: 1) la legittimità dell'impiego di strumenti informatici per verificare il corretto utilizzo degli accessi ad internet, alla luce dello Statuto dei lavoratori; 2) la rilevanza della normativa in materia di protezione dei dati personali.

1) Legittimità dell'impiego di strumenti informatici per verificare il corretto utilizzo degli accessi ad internet alla luce dello Statuto dei lavoratori

[57] Cfr. anche *Newsletter del Garante*, 8 luglio 2001 sull'utilizzo dei risultati delle intercettazioni telefoniche nell'ambito di un procedimento disciplinare.

[58] Una responsabilità a carico dell'azienda può derivare dall'obbligo risarcitorio connesso alla commissione di un reato o di un fatto illecito da parte del dipendente. L'**art. 2049 c.c.** dispone infatti che « *padroni e committenti sono responsabili per i danni arrecati dal fatto illecito dei loro domestici e commessi nell'esercizio delle incombenze a cui sono adibiti* ». Pertanto, il terzo danneggiato, può far valere il proprio diritto al risarcimento del danno subito, tanto nei confronti dell'autore del danno stesso (i.e. il dipendente), quanto nei confronti del datore di lavoro. A questa responsabilità di tipo civilistico si potrebbe affiancare altresì una responsabilità di carattere penale laddove la condotta penalmente rilevante (del dipendente) sia resa possibile dalla violazione di un obbligo giuridico del datore di lavoro di impedire determinati eventi dannosi, concretizzando un c.d. "reato omissivo improprio". In caso di reato compiuto dal lavoratore, sarà penalmente perseguibile anche il datore di lavoro, a titolo di concorso nel reato, per non aver impedito il fatto adottando le idonee misure di prevenzione e controllo (l'art. 40, comma 2, c.p. recita: "*Non impedire un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo*".)

Va preliminarmente osservato che l'accesso ad internet (o meglio l'utilizzo di strumenti informatici e telematici a ciò funzionali) rappresenta al giorno d'oggi un importante (ed in alcuni casi indispensabile) **strumento di lavoro**. Esso consente di avere agevolmente accesso a risorse e informazioni, nonché espletare attività, altrimenti non accessibili o eseguibili se non con notevole impiego di tempo e risorse (umane ed economiche). A fronte di ciò, nuovi e rilevanti "**rischi**" si paventano per il datore di lavoro, fra i quali l'esposizione dei propri sistemi informatici, e delle banche dati aziendali, ad accessi non autorizzati e/o a danni e disfunzioni.

Per ovviare a tale situazione, la tecnologia odierna consente di predisporre misure volte a **garantire la sicurezza dei sistemi** attraverso la delimitazione ed il monitoraggio degli accessi internet. In concreto, da un lato si pongono in atto sistemi di "filtraggio", impedendo l'accesso a determinati siti (potenzialmente dannosi), nonché l'esecuzione di determinate operazioni (quali il *download* di file), dall'altro si svolgono attività di monitoraggio sugli accessi internet effettuati, al fine di verificare tempi di connessione e siti *web* visitati (complessivamente e/o per ciascun utente).

Appare peraltro evidente come tale attività di verifica del corretto utilizzo degli strumenti informatici e telematici di accesso ad Internet possa risolversi, se non contenuta e regolamentata, in un'attività di **controllo a distanza** del lavoratore, con conseguente astratta applicazione dell'art. 4 della Legge 300/1970. E non solo: la possibilità di verificare i siti effettivamente visitati da ciascun utente rende astrattamente applicabile anche l'art. 8 della Legge 300/1970.

Sui limiti di liceità del controllo operato dal datore di lavoro la giurisprudenza si è espressa in più occasioni.

In particolare si è ritenuto[59] che l'**abuso di internet** da parte del lavoratore costituisca un rilevante inadempimento degli obblighi contrattuali integrante giusta causa di licenziamento, con possibilità per il datore di lavoro di provare l'utilizzo vietato attraverso i dati registrati dal *provider*, e senza pertanto che tale controllo necessiti della procedura di cui all'art. 4 dello Statuto dei Lavoratori.

Discostandosi dalla giurisprudenza più datata, che in passato ha ritenuto che nella nozione di "altre apparecchiature" di cui all'art. 4 dello Statuto dei lavoratori dovessero farsi

[59] Cfr. **Tribunale di Milano, 8 giugno 2001**, in *D. & L. Riv. Crit. Dir. Lav*., 2001, p. 1067. Cfr. altresì **Corte d'Appello di Ancona, 1 agosto 2003**, in *Lav. Giur*., 2004, p. 135".

rientrare tutti gli strumenti idonei a determinare un controllo a distanza del lavoratore[60], le pronunce più recenti hanno sorvolato in merito alla problematica relativa al controllo a distanza del lavoratore, limitandosi ad affermare il carattere illecito della condotta dello stesso e la conseguente legittimità del licenziamento.

Se da un lato tale orientamento appare conforme alla posizione assunta dalla Corte di Cassazione in tema di c.d. controlli difensivi[61] (ai sensi della quale l'art. 4 dello Statuto dei Lavoratori trova applicazione solo in caso di installazione di apparecchiature di controllo dell'attività lavorativa, e non in caso di controlli diretti ad accertare condotte illecite dei lavoratori), dall'altro si presta ad alcune obiezioni.

- In primo luogo, come già rilevato per la posta elettronica, un controllo dell'attività illecita del lavoratore difficilmente può prescindere anche da un controllo dell'attività lavorativa (lecita) del lavoratore stesso[62]. E' alla luce di tali considerazioni che taluni autori[63] ritengono opportuno che il datore di lavoro si avvalga comunque delle procedura autorizzativa di cui all'art. 4 dello Statuto dei lavoratori. Tale posizione appare quanto più sostenibile in considerazione del fatto che un controllo degli accessi internet può consentire di acquisire informazioni molto dettagliate e personali in merito al dipendente, con possibile violazione dell'art. 8 dello Statuto dei lavoratori che vieta indagini su opinioni politiche, religiose e sindacali del lavoratore.
- In secondo luogo, volendo seguire l'orientamento giurisprudenziale meno recente (maggiormente garantista verso i lavoratori) in materia di controllo c.d. preterintenzionale, si sottolinea come esso sanzioni la mera presenza di strumenti potenzialmente idonei a consentire un controllo a distanza sull'attività del lavoratore[64].
- Infine, come già ricordato, la Suprema Corte[65] si è recentemente pronunciata ancora sulla illegittimità di controlli predisposti dal datore di lavoro - senza assolvere agli obblighi di cui all'art. 4 dello Statuto dei Lavoratori - per contrastare l'attività illecita del dipendente, così come il Tribunale di Milano, con sentenza del 31 marzo 2004, ha censurato l'utilizzo di un software di controllo degli accessi ad internet, in quanto

[60] Cfr. **Pret. Milano, 4 ottobre 1988** con riferimento all'installazione di un centralino telefonico automatico in grado di riprodurre e registrare data, tempo e numero chiamante.
[61] Cfr. paragrafo 3
[62] Cfr. G. BASCHERINI, in *Lavoro nella Giurisprudenza*, 2004, 2.
[63] Cfr. G. BULGANINI, *Licenziamento per abuso di collegamento ad internet e tutela del lavoratore dai controlli a distanza*, in *Riv. Crit. Dir. Lav*., 2001, IV, p. 1067. Difatti, come già evidenziato, l'art. 4 dello Statuto dei Lavoratori, accanto ad un divieto assoluto ed inderogabile di utilizzo di impianti ed apparecchiature destinati al controllo dei lavoratori (c.d. Controllo intenzionale), prevede la legittimità di utilizzo (nel rispetto della procedura ivi indicata) di impianti ed apparecchiature giustificati da esigenze organizzative o produttive, disciplinando quello che viene indicato come "controllo preterintenzionale". La finalità delle apparecchiature non è infatti il controllo del lavoratore, il quale si presenta peraltro come potenziale conseguenza dell'utilizzo delle apparecchiature stesse per diverse (e legittime) finalità organizzative e produttive.
[64] Basti pensare alla presenza di un sistema di telecamere a circuito chiuso, benché non funzionanti, ecc. Cfr. Cass. 18 febbraio 1983, n. 1236, cit.; Cass. 21 agosto 1986, n. 1490, cit.; Cass. 16 settembre 1997, n. 9211, cit.
[65] Cfr. pag. 17, **Cass. 16 luglio 2000, n. 8250**, cit.

implicante interferenze sull'attività lavorativa dei dipendenti, e contestato la condotta del datore di lavoro in quanto ritenuta lesiva dell'art. 4 dello Statuto dei lavoratori[66].

L'oscillare interpretativo della giurisprudenza rende necessario tentare di individuare un criterio che possa fungere da riferimento per chi si trovi ad affrontare questo tipo di problematiche: a parere di chi scrive tale criterio deve consistere nell'evitare interpretazioni eccessivamente rigorose e restrittive di una normativa emanata in contesti sociali, ma soprattutto in presenza di standard tecnologici, molto diversi da quelli attuali.

E' evidente che attualmente i sistemi informativi di qualsiasi azienda, per le intrinseche caratteristiche tecniche e di funzionamento, consentono necessariamente, anche in assenza di una espressa finalità di controllo da parte del titolare, di verificare e monitorare la navigazione degli utenti (si pensi ai file di *log* registrati dai server). Richiedere in questi casi la preventiva consultazione delle associazioni sindacali appare francamente eccessivo, in quanto obbligherebbe qualsiasi datore di lavoro che doti la propria organizzazione di un sistema di "navigazione Internet" gestito da server centrali ad attivare la procedura sindacale.

Si presenta evidentemente diversa l'ipotesi in cui il datore di lavoro si doti di sistemi di gestione e monitoraggio degli accessi ad internet più sofisticati, ad es. mediante l'implementazione di software specifici per la verifica della navigazione internet effettuata a livello aziendale. Tali sistemi comportano inevitabilmente, seppure in modo non diretto, un potenziale controllo a distanza sull'attività lavorativa dei dipendenti: essi infatti, attraverso l'elaborazione, scomposizione ed evidenziazione di dati (altrimenti) aggregati in merito agli accessi ai vari siti, consentono di ricavare in maniera immediata, informazioni assai dettagliate in merito a tempi e durata delle connessioni, nonché ai siti effettivamente visitati; proprio il dettaglio delle informazioni acquisibili (tempo, durata, oggetto della navigazione del lavoratore, lecita o illecita che sia), rendono questo strumento potenzialmente molto più invasivo – e quindi più rischioso per la libertà e la riservatezza dei dipendenti – rispetto ad un normale sistema di posta elettronica.

Pertanto solo in questi casi, a parere di chi scrive, appare giustificato ed altamente consigliabile il ricorso alla procedura di consultazione prevista dall'art. 4 dello Statuto dei lavoratori.

Per dovere di completezza si deve infine precisare che nelle ipotesi prese in esame non appaiono sussistere gli estremi per una violazione dell'art. 8 dello Statuto dei Lavoratori che

[66] Il Tribunale censura "*l'ovvietà del diritto del datore di lavoro di effettuare controlli "a distanza" che gli permettano di acquisire anche notizie afferenti l'attività lavorativa e di farlo non solo al di fuori di ogni intesa con i rappresentanti dei lavoratori o di una specifica autorizzazione da parte dell'Ispettorato del Lavoro, ma in totale assenza di criteri oggettivi e trasparenti, per quanto di fonte unilaterale*".

vieta indagini sulle opinioni politiche, religiose e sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale. In merito lo stesso Tribunale di Milano[67] dichiara che "*non costituisce violazione dell'art. 8 dello Statuto dei Lavoratori, che rigorosamente limita il diritto di indagine del datore di lavoro sulle opinioni dei propri dipendenti, la conoscibilità occasionata da un sistema di controllo sull'uso di strumenti informatici aziendali perché la condotta vietata presuppone una volontà diretta all'acquisizione di informazioni precluse al datore di lavoro*".

2) Rilevanza della normativa in materia di protezione dei dati personali.

La stessa normativa in materia di trattamento di dati personali viene in rilievo nel caso in esame. Appare difatti evidente come nelle ipotesi di monitoraggio e verifica esaminate venga posta in essere un'attività di trattamento di dati personali, che – in alcuni casi – possono altresì qualificarsi come sensibili, ai sensi dell'art. 4 del Codice Privacy in quanto, dai siti visitati dal dipendente, potrebbero desumersi informazioni inerenti il suo orientamento politico, filosofico, religioso, oltre ad informazioni relative al suo stato di salute.

In merito, ferme restando le considerazioni di carattere generale già esposte in commento al **Quesito a)**, un'attività di monitoraggio sul corretto utilizzo della navigazione Internet, per potersi considerare lecita sotto il profilo della normativa in materia di protezione dei dati personali, deve innanzitutto essere svolta nel rispetto dei principi di cui all'art. 11 del Codice Privacy e, in particolare, dei principi di **necessità e trasparenza** del trattamento, nonché del **principio di proporzionalità**.

Il controllo tecnologico può difatti essere ritenuto legittimo solo laddove, in presenza di un interesse del datore di lavoro meritevole di apprezzamento e tutela, esso debba ritenersi **indispensabile**, in quanto rappresenta l'unica misura adeguata per evitare danni o pregiudizi all'impresa o a terzi. Inoltre, in virtù del medesimo principio, l'**art. 3 del Codice Privacy**[68] prescrive che ogni tipo di trattamento deve avvenire (ove possibile) mediante l'utilizzo di dati anonimi o indirettamente identificativi.

Alla luce di tali principi appare evidente che, al fine di perseguire una mera finalità di protezione dei sistemi aziendali, un controllo generalizzato e dettagliato sulla navigazione effettuata dal singolo utente si presenta, nella maggior parte dei casi, non necessario, in quanto le medesime finalità possono essere perseguite con trattamenti meno invasivi.[69]

In ossequio inoltre al **principio di trasparenza** i lavoratori devono essere debitamente **informati** in merito a: **(i)** condizioni e modalità di utilizzo di internet; **(ii)**

[67] Tribunale di Milano, 31 marzo 2004, cit.
[68] Cfr. paragrafo 2.3.a)
[69] Cfr. in questo senso il *Documento di Lavoro dei Garanti Europei*, 29 maggio 2002, paragrafo 2.3.b)

sistemi predisposti per disciplinare un corretto uso dello strumento; **(iii)** caratteristiche dei controlli e delle modalità delle eventuali contestazioni. La predisposizione di un **Codice di condotta** sull'utilizzo di Internet e l'adeguata informazione dei dipendenti sono elementi indispensabili al fine di legittimare la contestazione di eventuali condotte illecite e la conseguente irrogazione delle sanzioni previste[70].

Infine la **proporzionalità** del controllo impone che le informazioni raccolte, comprese quelle risultanti dall'attività di vigilanza, devono essere adeguate, pertinenti e non eccessive ai fini del conseguimento dello scopo perseguito. In quest'ottica si sono ritenuti non leciti i controlli "a tappeto" dei collegamenti ad Internet, a meno che ciò non risulti realmente necessario al fine di garantire la sicurezza dei sistemi[71].

Certo è che il rispetto del principio di proporzionalità va altresì valutato in relazione alla tipologia di attività svolta dalla società e dei rischi che su di essa possono incombere a causa di un utilizzo abusivo della navigazione Internet: appare evidente che sostenere la legittimità di un "controllo difensivo" si presenta tanto più agevole quanto più "delicata e riservata" possa oggettivamente qualificarsi l'attività svolta – basti pensare alla necessità di proteggere banche dati contenenti informazioni "top secret" o di know how aziendale, ecc. – e quanto maggiore sia il concreto rischio che dall'attività illecita del dipendente possano derivare danni ai sistemi e, quindi, all'attività economica del datore di lavoro.

In considerazione di quanto sopra, consegue che:

- L'attività di **prevenzione** deve essere preferita all'attività di rilevamento di eventuali abusi: ciò implica che l'attività di controllo deve rappresentare un elemento eventuale e limitato rispetto alle attività di prevenzione, quali la regolamentazione dell'utilizzo degli strumenti, od il "filtraggio" dei siti accessibili dai dipendenti. A tale logica risponde la predisposizione di sistemi volti a segnalare all'utente la rilevazione di un utilizzo sospetto o a prevenire il rischio di eventuali abusi (ad es. la predisposizione di finestre di "*pop up*" che avvertano il dipendente dei tempi di connessione; ovvero meccanismi che comportino l'interruzione della connessione in caso di mancato utilizzo del terminale per un determinato periodo di tempo, ecc.).
- Si dovrà privilegiare una modalità di **controllo anonimo** (ad es. effettuando controlli per dipartimenti od ufficio, ovvero limitando il controllo ai siti visitati senza visibilità sull'utente che vi ha avuto accesso).

[70] Il corretto funzionamento del sistema disciplinare richiede inoltre, come già evidenziato, che le procedure adottate dall'azienda siano portate a conoscenza dei dipendenti in conformità a quanto disposto dall'art. 7 dello Statuto dei Lavoratori (cfr. paragrafo 2.2). Per quanto attiene invece all'esclusione della necessità di acquisire il **consenso** del dipendente al trattamento dei dati personali, ai sensi dell'art. 23 del Codice Privacy, si richiamano le osservazioni già esposte con riferimento alla posta elettronica.

[71] Cfr. ancora il *Documento di Lavoro dei Garanti Europei*, 29 maggio 2002, pag. 18

- Si dovrà **evitare di verificare i contenuti dei siti** visitati dall'utente (ad es. limitando il controllo ai tempi di connessione e contestandone all'utente l'eccessiva durata). Tale scelta appare altamente consigliabile sotto diversi punti di vista: poter esaminare il contenuto dei siti visitati consentirebbe difatti l'acquisizione di informazioni sul dipendente anche altamente personali, quali, ad esempio, informazioni sul suo orientamento politico, sindacale, religioso, ecc.[72]
- Eventuali verifiche più dettagliate potranno trovare giustificazione (in termini di "controllo difensivo") qualora le normali attività di controllo facciano sorgere **sospetti** in merito alla liceità della condotta del lavoratore.

[72] Un tale tipo di controllo, con il conseguente trattamento di dati personali anche "sensibili" appare con evidenza caratterizzato da una maggiore invadenza della sfera personale rispetto, ad esempio, al controllo sull'utilizzo del telefono aziendale effettuato mediante apposite apparecchiature (Cfr. Cass. 3 aprile 2002, n.4746, cit., la quale qualifica come "controllo difensivo" il controllo effettuato "*mediante apparecchi di rilevazione di telefonate ingiustificate*"). Da notare inoltre che il trattamento di tali dati sensibili richiederebbe il consenso scritto del lavoratore e l'autorizzazione del Garante ai sensi dell'art. 26 del Codice.