TRIBUNALE PERUGIA
20 FEBBRAIO 2006
GIUDICE: ANGELERI
PARTI: N.N.
ABC SPA

Lavoro subordinato • Dipendente • Abuso risorse informatiche • Accertamento mediante verifica del pc del dipendente • Violazione artt. 4 e 8 Statuto lavoratori • Non sussiste

La condotta del datore di lavoro il quale effettui una verifica sul pc del dipendete per accertarne l'eventuale abuso non integra la violazione degli artt. 4 e 8 dello Statuto dei lavoratori in quanto costituisce non un controllo a distanza sull'attività del lavoratore bensì un controllo differito nel tempo di tipo difensivo contro condotte illecite.

Lavoro subordinato • Dipendente • Abuso risorse informatiche dell'azienda • Accesso a siti pornografici durante orari di lavoro • Sospensione cautelare dal servizio • Illegittimità • Reintegrazione in via d'urgenza.

L'abuso da parte del dipendente (nel caso di specie giornalista) delle risorse informatiche dell'azienda per accedere in maniera massiccia (418.000 visite in meno di un mese) a siti pornografici non è tale da giustificare la sospensione del servizio in assenza di determinate e specifiche contestazioni in ordine ad effettivi disservizi della rete informatica aziendale ovvero di calo di rendimento nella prestazione di lavoro.

VERIFICHE SULL'ACCESSO AD INTERNET DEI DIPENDENTI E CONTROLLI DIFENSIVI

Il Tribunale di Perugia, nell'ordinanza in commento, confermata in sede di reclamo, ha affrontato alcune tematiche molto interessanti.

Si trattava, nel caso di specie, di un licenziamento per giusta causa, intimato in quanto il lavoratore (un giornalista) aveva fatto un uso massiccio del computer aziendale e della connessione a Internet per ragioni estranee alla prestazione lavorativa, uso verificato mediante l'accesso ai *file* di *log*[1] di sistema, che tenevano traccia del numero, della durata, e della tipologia dei siti visitati (si trattava per la gran parte di siti a sfondo pornografico).

La problematica analizzata dal Tribunale di Perugia involge il controllo dell'attività lavorativa, sia sotto il profilo regolato dallo Statuto dei Lavo-

* L'ordinanza per esteso è pubblicata in questa *Rivista*, 2006, p. 809.

[1] I *file* di *log* sono generati automaticamente, e in essi si registrano le operazioni fatte dal sistema o dall'utente durante la sua sessione di lavoro, ovvero gli accessi effettuati.

ratori, sia per ciò che concerne la normativa in materia di trattamento dei dati personali, che, per la verità, viene ad essere sostanzialmente negletta dal Giudicante.

Il Tribunale, difatti, sembra appiattire la disciplina del trattamento dei dati personali in ambito lavorativo al solo disposto dell'art. 4 e dell'art. 8 dello Statuto dei lavoratori[2], eludendo i profili legati alla liceità del trattamento, con riguardo al D.lgs. 196/03[3].

Questa ricostruzione (che probabilmente dipende anche dalle prospettazioni e dalle eccezioni formulate dalle parti) deve essere attentamente meditata, sotto diversi profili.

1. Potere datoriale di controllo e art. 4 della L. 300/1970.

In primo luogo, Il Tribunale ha affrontato il problema del controllo eseguito dall'azienda sull'uso del computer assegnato al lavoratore, per ciò che concerne, in particolare, i *log file* delle connessioni ad Internet.

Il Giudice ha ritenuto che detto controllo debba rientrare non già in una forma diretta o indiretta di verifica dell'attività lavorativa, ma si sostanzi in un cd. « controllo difensivo », volto ad accertare le condotte illecite dei lavoratori.

Prima di affrontare il problema della definizione e dei limiti di tale tipologia di controlli, occorre soffermarsi, più in generale, sull'estensione dei poteri del datore di lavoro, con riguardo alla verifica dell'attività dei lavoratori.

Il potere di controllo del datore di lavoro[4], prima dello Statuto dei lavoratori, trovava il suo fondamento sugli artt. 2086 e 2104 del Codice Civile, in quanto l'imprenditore, quale creditore della prestazione lavorativa, poteva accertare che il dipendente eseguisse la prestazione stessa con la diligenza richiesta dalla natura di quest'ultima[5].

A seguito dell'entrata in vigore dello Statuto dei Lavoratori, il potere di controllo viene circoscritto nei suoi aspetti più « polizieschi », e viene « procedimentalizzato », al precipuo fine di rafforzare la libertà e la dignità del lavoratore[6].

---

[2] Legge 20 maggio 1970, n. 300, in *Gazz. Uff.*, 27 maggio 1970, n. 131.

[3] In generale, sul trattamento dei dati personali nel rapporto di lavoro, vd. P. Chieco, *Privacy e lavoro. La disciplina del trattamento dei dati personali*, Bari, 2000; M. Aimo, *Privacy, Libertà di espressione e rapporto di lavoro*, Napoli, 2003; A. Bellavista, in *Il Codice dei dati personali*, a cura di F. Cardarelli-S. Sica-V. Zeno-Zencovich, Milano, 2004, p. 397 ss.

[4] Sul potere di controllo, vd. F. Tofoletto, *Nuove tecnologie informatiche e tutela del lavoratore*, Milano, 2006, p. 1 ss.

[5] Cfr. A. Bellavista, *Sorveglianza, privacy e rapporto di lavoro*, in *Dir. Internet*, 5/2006, p. 437, il quale correttamente nota che « tutto il controllo possibile risultava logicamente e giuridicamente giustificato e trovava il suo limite solo nella subordinazione tecnico-funzionale del prestatore di lavoro ».

[6] L'osservazione è di A. Maresca-S.L. Monticelli, in *Trattato di Diritto Amministrativo*, Vol. XXXVI, *La protezione dei dati personali*, a cura di G. Santaniello, Padova, 2005, p. 538; vd. anche A. Bellavista, *Sorveglianza, cit.*, p. 438; W. Sarasella, in *Codice della Privacy*, coord. da V. Italia, Tomo I, Milano, 2004, p. 1459; sull'art. 4 dello Statuto dei lavoratori vd. anche A. Usai, *Osservazioni in tema di controllo dell'attività dei lavoratori attuato mediante sistemi informatici*, in questa *Rivista*, 1991, p. 247, ed Autori ivi citati.

La libertà deve essere intesa quale autonomia da condizionamenti esterni di altri soggetti, mentre la dignità come decoro e rispettabilità personali[7].

In particolare, l'art. 4 dello Statuto dei lavoratori al primo comma vieta l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori, mentre al secondo comma delimita la possibilità di installazione degli impianti e delle 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.

Detti impianti, difatti, 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 (ora, Direzione del Lavoro), dettando, ove occorra, le modalità per l'uso di tali impianti,.

Per attrezzatura di controllo può intendersi « qualsiasi congegno o parte di congegno dotato di potenzialità (o suscettibile di essere usato in funzione) di controllo, ovunque collocato e inserito, e non necessariamente caratterizzato da una sua distinta ed autonoma struttura o da una esclusiva destinazione al controllo »[8].

La violazione di detta norma è punita (con sanzione penale) dall'art. 171 del Codice della Privacy, mediante rinvio alla sanzione di cui all'art. 38 della L. 300/1970[9].

Si deve distinguere quindi tra un divieto assoluto di installazione di impianti di controllo (al primo comma) e un divieto relativo per i controlli « preterintenzionali » (al secondo comma)[10].

La norma è caratterizzata, senza dubbio, da un evidente giudizio di sfavore nei confronti degli strumenti di controllo, che, al secondo comma, vengono consentiti soltanto all'avverarsi di una duplice condizione: che essi siano richiesti per proteggere degli interessi, espressamente indicati e ritenuti meritevoli di tutela, e che siano adottati soltanto in seguito alla procedura di accordo *ad hoc*[11].

La giurisprudenza, dopo aver rilevato, in un primo momento, che tra i controlli a distanza potessero comprendersi soltanto quelli continui, o comunque attuabili in qualunque momento dal datore di lavoro[12], è arrivata poi a estendere progressivamente (in ottica di più penetrante tutela del lavoratore) il concetto, ritenendo rilevante la mera possibilità di controllo a distanza, ed arrivando a argomentare come il concetto di

---

[7] Vd. G. GENTILE, *Innovazioni tecnologiche e art. 4 dello Statuto dei lavoratori*, in *Dir. lav.*, 1996, p. 473.

[8] Così A. ROSSI, *La libertà e la professionalità dei lavoratori di fronte alle nuove tecnologie informatiche*, in *Quest. giust.*, 1983, n. 2, p. 220.

[9] In virtù dell'intricato (e superfluo) gioco di rimandi introdotto dagli artt. 171 e 179, comma secondo, del D.lgs. 196/2003; sul punto cfr. F. TOFFOLETTO, *op. cit.*, p. 22.

[10] Cfr. U. ROMAGNOLI, *Osservazioni sugli artt. 4 e 6 dello Statuto dei lavoratori*, in *Giur. it.*, 1971, IV, p. 130; G. GENTILE, *op. cit.*, p. 481; per la giurisprudenza, vd. Pretura Milano, 20 dicembre 1984, in *Orient. giur. lav.*, 1985, p. 688.

[11] Cfr. A. BELLAVISTA, in *Il Codice*, cit., p. 431.

[12] Cfr. Pret. Venezia, 26 giugno 1973, in *Not. giurispr. lav.*, 1974, p. 150.

distanza sia da intendere non soltanto in senso fisico, ma anche in senso temporale[13].

Questo assetto normativo non è stato intaccato dal Codice della Privacy che, difatti, all'art. 114, afferma che « resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300 ».

Non può quindi dubitarsi dell'applicazione ai trattamenti di dati svolti in ambito lavorativo anche del disposto dell'art. 4 dello Statuto dei lavoratori; difatti, per ciò che riguarda la disciplina lavoristica, la *voluntas legis* è stata evidentemente orientata nel senso di non contrapporsi, ma di aggiungersi, alle regole statutarie, delle quali è stata formalmente ribadita la vigenza[14].

Occorre verificare se questa disciplina possa trovare applicazione anche alle possibilità di controllo offerte dalla diffusione pervasiva dell'informatica.

La risposta non può che essere positiva.

Fin dalle storiche sentenze del Tribunale di Milano[15], infatti, è stato argomentato come le possibilità di controllo offerte dalle nuove tecnologie informatiche dovessero essere ricomprese tra le « altre apparecchiature », cui si riferisce l'art. 4 dello Statuto dei lavoratori.

Era già stato sottolineato[16], oltre un decennio fa, che « l'elaboratore elettronico è in grado di svolgere un controllo continuo, capillare e totale ». Questa affermazione, già allora pienamente condivisibile, è tanto più vera adesso, se rapportata da un lato alla potenza di calcolo[17], cresciuta esponenzialmente, ed alla capacità di memorizzazione dei computer, e dall'altro alla crescita tumultuosa di Internet, fino ad arrivare a ciò che oggi viene definito « Web 2.0 ».

Alcuni ritengono peraltro di effettuare un ulteriore distinzione, qualora il controllo venga effettuato non già da un apparecchiatura esterna (il *router*, il *proxy server*, il *server* medesimo), ma attraverso del *software* installato direttamente sul computer in dotazione al dipendente, in quanto in questo caso « si potrebbe ritenere che non ci si trovi dinanzi ad una apparecchiatura di controllo, cui fa riferimento l'art. 4 St. lav., cioè ad una apparecchiatura distinta e distinguibile dagli ordinari strumenti di lavoro, e quindi, separabile dagli strumenti di lavoro »[18].

---

[13] Vd. Pret. Milano, 5 dicembre 1984, in *Riv. it. dir. lav.*, 1985, II, p. 209; per la dottrina, cfr. G. Santoro Passarelli, *Osservazioni in tema di art. 3 e 4 Stat. lav.*, in *Dir. lav.*, 1986, I, p. 491; G. Gentile, *op. cit.*, p. 477; F. Toffoletto, *op. cit.*, p. 25. Per una casistica giurisprudenziale sulle apparecchiature ritenute illegittime, vd. A. Maresca-S.L. Monticelli, *op. cit.*, p. 551.

[14] D'altronde, la norma costituisce solamente la conferma di un dato pacifico: sul punto vd. A. Bellavista, in *Il Codice*, cit., p. 430; R. Del Punta, *Diritti della persona e contratto di lavoro*, in *http://www.csmb.unimo.it/adapt/bdoc/2006/22_06/06_22_85_DANNO_ALLA_PERSONA.pdf*. Occorre ricordare che già l'art. 43, comma secondo, della L. 31 dicembre 1996, n. 675, disponeva che « rimangono ferme le disposizioni della legge 20 maggio 1970, n. 300, e successive modificazioni ».

[15] Pretura di Milano 5 dicembre 1984, in *Foro it.*, 1985, II, 285; vd. anche W. Sarasella, *op. cit.*, p. 1456 ss.

[16] Così G. Gentile, *op. cit.*, p. 487.

[17] La potenza di calcolo dei microprocessori, a partire dagli anni '80, secondo la c.d. « Legge di Moore » (in realtà un'osservazione empirica), tende a raddoppiare ogni diciotto mesi.

[18] Così A. Maresca-S.L. Monticelli, *op. cit.*, p. 552; vd. altresì T. Padovani, *Il controllo a distanza dell'attività lavorativa svolta mediante elaboratori elettronici*, in *Riv. it. dir. lav.*, 1985, II, p. 255; R.

Il computer, in particolare, essendo un mero strumento di lavoro, non rientrerebbe nell'ambito di applicazione dell'art. 4 L. 300/1970[19].

Una tale tesi non appare accoglibile, in quanto eccessivamente restrittiva; non è condivisibile, infatti, l'affermazione secondo cui gli strumenti di lavoro non possano anche fungere da apparecchiature di controllo.

Al contrario, il controllo del lavoratore effettuato direttamente via *software* sul computer del dipendente[20] è idoneo a presentare modalità di compromissione della sfera di libertà del dipendente pari se non superiori rispetto ad un controllo effettuato con apparecchiature esterne, e dunque anche sotto questo profilo la distinzione si appalesa ingiustificata, tanto più che la *ratio* della norma è palesemente ispirata alla finalità che la vigilanza sui dipendenti « vada mantenuta in una dimensione umana e quindi non esasperata dall'uso di tecnologie che possano eliminare ogni zona di riservatezza e di autonomia nello svolgimento del lavoro »[21].

La Cassazione ha, peraltro, da qualche anno, identificato una categoria di controlli che sarebbero sostanzialmente estranei all'ambito applicativo dell'art. 4 dello Statuto dei Lavoratori.

Si tratta dei cc.dd. « controlli difensivi », vale a dire i controlli posti in essere dal datore di lavoro al fine di prevenire ovvero reprimere quei comportamenti dei lavoratori che si concretino in un uso scorretto dei beni aziendali.

In particolare, la Suprema Corte ha ritenuto che « ai fini della operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 L. n. 300 citata, 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 controllo dell'accesso ad aree riservate, o, appunto, gli apparecchi di rilevazione di telefonate ingiustificate »[22].

ZALLONE, *Art. 4 statuto dei lavoratori e nuove tecnologie: profili interpretativi*, in *Orient. giur. lav.*, 1984, p. 682; anche A. USAI, *op. cit.*, p. 261 ritiene che « salvo casi particolari, in cui il controllo operato tramite gli elaboratori elettronici per il tipo particolare di lavoro riesca a dare il quadro completo ed analitico non solo di tutta l'attività, ma anche delle pause e dei tempi in cui il dipendente svolge il suo lavoro, generalmente gli strumenti informatici sono inidonei a costituire un mezzo di lesione della riservatezza e della dignità del lavoratore ».

[19] Vd. per la giurisprudenza Pret. Milano, 12 luglio 1988, in *Or. giur. lav.*, 1988, p. 936.

[20] Si pensi alla memorizzazione della cronologia delle pagine web visitate, ai *cookies*, alle informazioni sui *file* aperti e sul loro contenuto, per non considerare ipotesi ben più invasive, quali i cc.dd. *keylogger*, vale a dire quella particolare tipologia di software (o di hardware aggiuntivo) che memorizza tutti i caratteri digitati dall'utente, giungendo anche a « scattare » delle istantanee (*snapshot*) del video, memorizzabili in formato grafico - per la definizione vd. *http://it.wikipedia.org/wiki/Keylogger*.

[21] Così M. FEZZI, *Calcolatori elettronici e controllo a distanza dell'attività del lavoratori*, in *Lavoro 80*, 1983, II. p. 569.

[22] Così Cass., 3 aprile 2002, n. 4746, in *Mass. giur. lav.*, 2002, p. 644, con nota di BERTOCCHI; *in Riv. giur. lav.*, 2003 II, p. 71; *contra* Cass., 17 giugno 2000, n. 8250, in *Giust. civ. mass.*, 2000, p. 1327 (ancorché riguardante impianti audiovisivi); per la dottrina, cfr. G. GENTILE, *op. cit.*, p. 500, il quale peraltro rileva che i controlli difensivi, in quanto volti a tutelare beni diversi, quali la proprietà e la salute, consentano in ogni caso di controllare altri aspetti del comportamento del lavoratore, e pertanto dovrebbe comunque trovare applica-

Parte della dottrina è fortemente critica nei confronti dei *dicta* della Suprema Corte (condivisi, come già rilevato, in maniera integrale dal Tribunale di Perugia), per una serie di argomentazioni che si ritengono condivisibili.

In particolare, è proprio l'individuazione di attività di controllo che sarebbero estranee al dettato della norma a destare perplessità, dal momento che « l'espressione ''attività dei lavoratori'' contenuta nell'art. 4 dello Statuto dei lavoratori, riguarda, secondo l'opinione prevalente, tutta l'attività, sia lavoratoria sia posta in essere ad altri fini, estranei alla sfera solutoria »[23], ed inoltre è assai improbabile che il controllo teso alla verifica dell'attività illecita si svolga a « comparti stagni », senza interessare anche la prestazione lavorativa lecitamente resa[24].

Ne consegue, pertanto, che questa distinzione comunque possa non essere ritenuta idonea a legittimare dei controlli (anche di tipo difensivo) effettuati senza essere preceduti dal previo accordo di cui al comma secondo dell'art. 4, accordo che contribuirebbe altresì non solo alla necessaria trasparenza dell'attività datoriale, ma anche alla riduzione della medesima al minimo indispensabile, per raggiungere le finalità legittimamente perseguite[25].

D'altronde, giurisprudenza di merito quasi coeva all'ordinanza in commento[26] è di segno diametralmente opposto, ritenendo imprescindibile

---

zione il secondo comma dell'art. 4 L. 300/1970.

[23] Così A. Bellavista, in *Il Codice*, cit. p. 434; vd. anche A. Usai, *op. cit.*, p. 255; G. Gentile, *op. cit.*, p. 477, che evidenzia come non a caso la norma si riferisca all'attività del lavoratore, e non all'attività lavorativa, poiché quest'ultima è da individuarsi quale attività direttamente collegata all'espletamento delle mansioni, mentre la prima costituisce un concetto di portata più ampia, « in quanto comprende l'intero comportamento umano nel luogo di lavoro ». L'A. (p. 495) opera altresì una chiara distinzione tra il controllo dell'attività lavorativa, e il controllo del risultato, quest'ultimo certamente lecito, in quanto rientrante nel diritto del datore di lavoro alla prestazione cui il dipendente è contrattualmente tenuto; cfr. altresì F. Rotondi, *Controllo a distanza dell'attività lavorativa*, in *Dir. prat. lav.*, 2006, XXXIII, p. 1822 ss.

[24] A. Usai, *op. cit.*, p. 264 ritiene che i controlli difensivi possano essere considerati leciti « senza difficoltà », in riferimento alla scriminante dell'esercizio del diritto, o della legittima difesa, « se attuati mediante strumenti in grado di selezionare esclusivamente i comportamenti illeciti del lavoratore ». Vi è anche chi (E.O. Policella, *Il monitoraggio elettronico dei dipendenti per scopi difensivi*, in *Dir. internet*, 2007, I, p. 87) ritiene di individuare una distinzione tra controlli difensivi *ex post*, conseguenti alla necessità di fronteggiare una condotta illecita (certa o verisimile), che sarebbero sottratti al dettato dell'art. 4, e controlli *ex ante*, effettuati in via preventiva, per i quali sarebbe invece imprescindibile l'adozione della procedura concordata.

[25] In questa sede non viene affrontato l'affine problema del controllo della posta elettronica del dipendente, anche sotto il profilo del delitto di cui all'art. 616 c.p.; sul punto per la giurisprudenza vd. Trib. Milano, 10 maggio 2002, *http://www.infogiur.com/giurisprudenza/control_e_mail_trib_mi_02.asp*; Trib. Milano, sez. distaccata di Chivasso, 15 settembre 2006, *http://www.penale.it/page.asp?mode=1&IDPag=381*; Comunicato stampa n. 23 del Garante del 12 luglio 1999, *http://www.garanteprivacy.it/garante/doc.jsp?ID=47997*; per la dottrina vd. L. Nogler, *Posta elettronica aziendale: conta anche la privacy del lavoratore*, in *Guida al lavoro*, 2002, n. 22, p. 10; F. Toffoletto, *op. cit.*, p. 15 ss.; E.O. Policella, *op. cit.*, p. 89.

[26] App. Milano, 30 settembre 2005, in *Dir. prat. lav.*, 2006, X, p. 569; cfr anche Trib. Milano, 31 marzo 2004, in *Orient.. giur. lav.*, 2004, p. 648; Trib. Torino, 9 gennaio 2004, in *Giur. piem.*, 2005, I, p. 131; per la dottrina vd. F. Toffoletto, *op. cit.*, p. 27 ss.; E.O. Policella, *op. cit.*, p. 85; M. Gobbato-S. Tagliabue, *Il controllo dei lavoratori: stato dell'arte al-*

l'obbligo di rispettare la procedure di cui al secondo comma dell'art. 4 dello Statuto dei lavoratori, anche laddove si installi un *software* con finalità di controllo difensivo.

Occorre sottolineare, peraltro, come nel caso di specie il Tribunale, con un singolare *obiter dictum*, pur ritenendo i controlli svolti come estranei all'art. 4, precisi nondimeno che « il controllo dei dati relativi alla ''navigazione'' in internet effettuata dal personal computer in uso al ricorrente fosse pienamente conforme alla previsione dell'art. 4, secondo comma della legge n. 300/70, sopra riportato. Infatti, l'art. 8 dell'accordo stipulato il 7 aprile 2004 tra la ABC SPA. e il competente organismo di rappresentanza dei lavoratori, il comitato di redazione, prevedeva che tutti gli accessi dalle singole postazioni verso indirizzi internet fossero mantenuti in un apposito *log* di sistema ».

2. Potere di controllo e art. 8 della L. 300/1970.

Il Tribunale affronta altresì i profili connessi alla violazione dell'art. 8 dello Statuto dei lavoratori.

Il Giudicante ritiene di superare la questione affermando che « il controllo eseguito dalla convenuta sul numero e la durata degli accessi a siti internet compiuti dallo N.N. in un determinato lasso temporale aveva il solo scopo di accertare se questi fosse venuto meno ai suoi doveri; non era invece diretto a indagare sulle sue inclinazioni o, in senso lato, sulle sue opinioni, per acquisire in modo illecito quelli che oggi la disciplina sulla cosiddetta privacy o riservatezza definisce ''dati sensibili''. Di conseguenza, la fattispecie concreta esula dall'ambito di applicazione dell'art. 8 ».

L'articolo 8 della legge 20 maggio 1970, n. 300[27] stabilisce il divieto, per il datore di lavoro, sia ai fini dell'assunzione, che nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.

La norma è chiaramente volta a delimitare l'ambito valutativo del datore di lavoro, esclusivamente a ciò che è direttamente funzionale alla verifica del livello di perizia e di diligenza necessarie per l'esecuzione della prestazione lavorativa, in coerenza con i principi espressi dagli artt. 3, comma secondo, 4 e 42, secondo comma, della Costituzione[28].

---

la luce delle pronunce del Garante e della recente giurisprudenza, in *http://www.giuristitelematici.it*; si veda anche la Circolare del Ministero del Lavoro n. 6585 del 28 novembre 2006, in *http://www.giuristitelematici.it*.

[27] Fatto espressamente salvo dall'art. 113 del Codice della Privacy.

[28] Sul punto vd. A. Maresca-S.L. Monticelli, *op. cit.*, p. 538 ss., e gli autori ivi citati; cfr. anche G. Elli-R. Zallone, *Il nuovo Codice della privacy*, Torino, 2004, p. 128 ss.; sul punto si vedano altresì l'art. 6 della L. 5 giugno 1990, n. 135 (in *Gazz. Uff.*, 8 giugno 1990, n. 132), in tema di divieto di indagini sulla stato di sieropositività da virus HIV, l'art. 3, commi tre e quattro del D.lgs. 9 luglio 2003 n. 215 (in *Gazz. Uff.*, 12 agosto 2003, n. 186), *Attuazione della direttiva 2000/43/CE per la parità di trattamento tra le persone indipendentemente dalla razza e dall'origine etnica*, nonché l'art. 3 commi dal terzo al sesto, del D.lgs. 9 luglio 2003 n. 216 (in *Gazz. Uff.*, 13 agosto 2003, n. 187), *Attuazione della direttiva 2000/78/CE per la parità di trattamento in materia di occupazione e di condizioni di lavoro*.

L'art. 8 individua dunque una serie di dati che possono essere definiti « supersensibili »[29], in quanto non possono in ogni caso essere raccolti o utilizzati, al di fuori delle ipotesi delineate dall'art. 8, e quindi tutte le volte in cui non presentino una stretta (anzi strettissima) connessione con il rapporto di lavoro.

In altre parole, l'art. 8 individua un vero e proprio limite alla possibilità di trattare dati personali del lavoratore[30].

Il Tribunale, peraltro, pare adottare una definizione « finalistica » del trattamento di dati personali. Il trattamento di dati personali « sensibili », dunque, sussisterebbe soltanto se e a condizione che il titolare (per riprendere la terminologia tipica del D.lgs 196/03) operasse allo specifico fine di ricercare dati cc.dd. sensibili[31].

Questa tesi, se può essere accolta con riguardo all'art. 8 dello Statuto dei Lavoratori (che tale dimensione finalista espressamente individua), non può essere affatto estesa a qualunque trattamento.

Difatti, è palese dalla stessa definizione di « dato sensibile », contenuta nel Codice della Privacy, e dalla (amplissima) accezione che il Codice attribuisce al trattamento[32], che tale elemento per così dire soggettivo sia del tutto insignificante, rilevando, invece, l'oggettiva natura del dato trattato.

Ne consegue, pertanto, che contrariamente a quanto sostenuto dal Tribunale di Perugia, non sembra potersi dubitare che una verifica sulla durata degli accessi, e soprattutto sulla tipologia dei siti a cui il lavoratore abbia acceduto possa certamente configurare un trattamento di dati sensibili, laddove idoneo a rivelare (quantomeno) la vita sessuale dell'interessato.

E ciò comporta, come si argomenterà più oltre, delle importanti conseguenze in ordine alla valutazione della liceità del trattamento.

3. Controlli datoriali e trattamento dei dati personali.

La tesi (propugnata dalla Suprema Corte, e accolta dal Tribunale di Perugia) secondo cui i controlli difensivi, anche quelli effettuati sulla navigazione Internet, siano in sostanza sottratti all'applicazione della disciplina di cui all'art. 4 dello Statuto dei Lavoratori, sembra essere troppo rigida.

È ben vero che la norma in questione si attaglia a un epoca industriale, e si sposa con difficoltà con la rivoluzione informatica e telematica, in atto

[29] La definizione è di A. Bellavista, *Il Codice*, cit., p. 423 ss.

[30] Vd. ancora A. Bellavista, *ibidem*, p. 424.

[31] I dati sensibili, *ex* art. 4, comma primo, lett. *d*) del D.lgs. 196/2003, sono « i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale ».

[32] Si ricorda che l'art. 4, comma primo, lett. *a*) del D.lgs. 196/2003 definisce come trattamento « qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati ».

oramai da più di un decennio, ma è altrettanto vero che proprio la potenziale pervasività dei controlli effettuabili per via informatica e telematica, che possono riguardare ogni aspetto dell'attività del lavoratore, con un monitoraggio continuo e spietato[33], richiederebbe una ben maggiore attenzione dell'interprete, volta a valutare appieno la liceità del trattamento di dati personali del lavoratore, alla luce non del solo art. 4 dello Statuto dei Lavoratori, ma con riguardo ai principi fondanti del Codice della Privacy[34].

D'altronde, non si può dimenticare che è proprio il Codice, all'art. 1, a sottolineare che « chiunque ha diritto alla protezione dei dati personali che lo riguardano »[35].

In altre parole, con la valorizzazione dei principi di necessità, di liceità, di finalità, di proporzionalità, di pertinenza, di accuratezza, andrebbe ricercato quell'equilibro tra l'esigenza del datore di lavoro di verificare l'adempimento della prestazione contrattuale, e l'interesse contrapposto del lavoratore a tutelare la propria sfera, che è il fine ultimo della regolamentazione in materia.

Una visione infatti limitata e settoriale, che non colga la prospettiva del trattamento dei dati personali del lavoratore, ma si limiti ad analizzare la natura e le finalità degli « impianti di controllo », non soltanto è anacronistica, ma addirittura contraria al dato normativo positivo, che da oramai un decennio[36] ha inteso introdurre degli strumenti giuridici volti a consentire all'« interessato »[37] di conservare il controllo sulla circolazione dei propri dati personali, tutelando il « diritto all'autoderminazione informativa »[38].

---

[33] A. BELLAVISTA, *Sorveglianza*, cit., p. 437, evidenza i rischi insiti nelle « innumerevoli potenzialità della tecnologia a fini di controllo », auspicando una « grande e diffusa discussione pubblica sulla portata e sugli effetti delle scelte tecnologiche ». Si pensi, a titolo esemplificativo, alla possibilità di incrociare i dati ottenuti dai *log file* della navigazione o dell'utilizzo del *server* aziendale, con quelli dei *badge* identificativi, magari dotati di *chip* RFID attivo; sull'utilizzo dei *chip* RFID cfr. M. FEZZI, *Le nuove frontiere del controllo sui lavoratori (il chip RFID)*, in *DL* online, *http://www.dielle.it*; A. STANCHI, *L'utilizzo della Radio Frequency Identification (RFid) e le implicazioni* giuslavoristiche, *ibidem*; F. TOFFOLETTO, *op. cit.*, p. 32 ss. Prospettive ancora più inquietanti potranno aprirsi in conseguenza delle possibilità di controllo offerte dall'introduzione di elaboratori conformi alle specifiche denominate *Trusted Computing*. Sul punto vd. G.B. GALLUS-F.P. MICOZZI, *Trusted Computing, traitor tracing, ERM e privacy*, relazione presentata al Convegno E-privacy 2006, *http://e-privacy.firenze.linux.it/atti/e-privacy_2006_Gallus_Micozzi_Traitor_Tracing.pdf*.

[34] Cfr. A. BELLAVISTA, *Sorveglianza*, cit., p. 437, il quale correttamente evidenzia come i principi generali del Codice della Privacy contengano un'evidente presa di posizione a favore del rango prioritario dell'esigenza di tutela della persona e rileva altresì la « vitalità » nel nuovo contesto di norme (quali l'art. 4 dello Statuto dei Lavoratori) pensate per altre realtà; cfr. anche A. BELLAVISTA, *Il Codice*, *cit.*, p. 397 ss.

[35] Anche la Carta dei diritti fondamentali dell'Unione Europea, del 7 dicembre 2000, prevede, con formula analoga, all'art. 8, che « ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano ».

[36] Dall'entrata in vigore della Legge 31 dicembre 1996, n. 675, « Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali », in *Gazz. Uff.*, 8 gennaio 1997, n. 5.

[37] Per utilizzare la termologia adottata dalla L. 675/1996 prima e dal D.lgs. 196/2003 poi.

[38] Cfr. S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, p. 101 ss.

La liceità dei controlli difensivi con il mezzo informatico, pertanto, andrebbe ripensata, tra l'altro, con riguardo al principio di necessità di cui all'art. 3 del Codice, laddove afferma che « 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 »[39].

Questa opzione ricostruttiva, oltre che rispettosa del dato normativo, trova conforto nell'attività del « Gruppo di lavoro *ex* art. 29 »[40], ed in particolare, nell'*opinion* 8/01 *on the processing of personal data in the employment context*[41] e nel « Documento di lavoro riguardante la vigilanza sulle comunicazione elettroniche sul posto di lavoro », adottato il 29 maggio 2002[42].

Quest'ultimo documento offre indirizzi interpretativi ed esempi concreti sull'individuazione dell'attività legittima di controllo e circa i limiti accettabili della vigilanza sui dipendenti esercitata dal datore di lavoro.

Il Documento, pur riconoscendo il diritto del datore di lavoro a controllare il funzionamento della sua impresa, ed a difendersi dalle eventuali attività illecite dei dipendenti, evidenzia che « la dignità umana del lavoratore va anteposta a qualsiasi altra considerazione ».

Il Gruppo di lavoro *ex* art. 29 chiarisce quindi che i principi validi con riguardo al trattamento dei dati personali, come enucleabili dalla Direttiva 95/46/CE, vadano necessariamente applicati anche quando si verta in tema di rapporto di lavoro.

In particolare, si pone l'accento sul principio di necessità[43], in base al quale il controllo dell'impiego da parte del lavoratore dell'accesso a Internet debba intendersi necessario soltanto in circostanze eccezionali, sul principio di finalità, dovendo essere i dati raccolti per uno scopo determi-

---

[39] Vd. anche l'Autorizzazione generale n. 1/2005 al trattamento dei dati sensibili nei rapporti di lavoro - 21 dicembre 2005 (Gazz. Uff. 3 gennaio 2006, Suppl. Ord. n. 1) ove si ribadisce che « prima di iniziare o proseguire il trattamento 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, in conformità all'art. 3 del Codice ». L'Autorizzazione è reperibile sul sito del Garante, al *link http://www.garanteprivacy.it/garante/doc.jsp?ID=1203930*.

[40] Il Gruppo di lavoro è stato istituito dall'articolo 29 della direttiva 95/46/CE. Si tratta di un organo consultivo europeo indipendente, che si occupa della protezione dei dati e della vita privata. I suoi compiti sono stabiliti dall'articolo 30 della direttiva 95/46/CE e dall'articolo 15 della direttiva 2002/58/CE. Il Gruppo può, tra l'altro, « esaminare ogni questione attinente all'applicazione delle norme nazionali di attuazione della presente direttiva per contribuire alla loro applicazione omogenea » e « formulare di propria iniziativa raccomandazioni su qualsiasi questione riguardante la tutela delle persone nei confronti del trattamento di dati personali nella Comunità ».

[41] *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf*.

[42] *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_it.pdf*.

[43] « Questo principio comporta l'obbligo per il datore di lavoro di verificare che qualsiasi forma di controllo risulti assolutamente indispensabile in rapporto ad uno scopo determinato prima di impegnarsi in qualunque attività del genere ».

nato, esplicito e legittimo, sul principio di trasparenza, di legittimità, di proporzionalità[44], di accuratezza e conservazione dei dati, nonché di sicurezza.

Sulla base di tali principi, il Documento sottolinea che « ogniqualvolta ciò risulti possibile la prevenzione va considerata più importante del rilevamento; in altre parole l'interesse del datore di lavoro risulta servito meglio da una spesa destinata a prevenire gli abusi dell'Internet con mezzi tecnici piuttosto che ad individuare casi d'abuso », e che molto spesso non sia necessario analizzare il contenuto dei siti visitati, ma che sia sufficiente verificare il tempo speso nella navigazione in Internet da parte del dipendente.

I principi enucleati dal Documento non possono essere ignorati, ed anzi dovrebbero essere approfonditi e considerati sia dalla dottrina che dalla giurisprudenza, alla luce delle analoghe disposizioni del Codice della Privacy, al fine di discernere quali tipologie di controllo del lavoratore possano essere considerate lecite[45].

Non stupisce, infine, che una tale ricostruzione traspaia in maniera evidente dalla « giurisprudenza » del Garante per la protezione dei dati personali, in tema di liceità dei trattamenti di dati personali a fini di controlli difensivi[46].

Il Garante, infatti, sottolinea la centralità del disposto dell'art. 11 del Codice della Privacy, nella parte in cui nella parte in cui prevede che i dati siano trattati in modo lecito, secondo correttezza e nel rispetto dei principi di pertinenza e non eccedenza rispetto alle finalità perseguite.

Ne consegue che l'adozione da parte del datore di lavoro di attività di controllo « difensive », al fine di prevenire un uso scorretto dei beni aziendali, deve muoversi imprescindibilmente entro i limiti tracciati dai principi enucleati in tema di trattamento dei dati personali dal D.lgs 196/2003.

In particolare, la liceità dei controlli andrà valutata sulla base dei principi di trasparenza, di proporzionalità e di non eccedenza, che il Garante ha ritenuto, nei provvedimenti richiamati in nota, violati sia per l'omessa o insufficiente informativa al lavoratore, sia, soprattutto, poiché si sarebbe ben potuto dimostrare la non conformità del comportamento del lavoratore agli obblighi contrattuali in tema di uso corretto degli strumenti affidati sul luogo di lavoro, mediante controlli meno invasivi[47].

Da ultimo, occorre soggiungere che il Garante ha recentemente[48] emanato le « Linee guida in materia di trattamento di dati personali di lavora-

---

[44] Sul punto, il Documento suggerisce, ad esempio, ai fini della salvaguardia di abusi connessi all'accesso a Internet, di adottare dispositivi di blocco, piuttosto che di controllo.

[45] Vd. sul punto F. Toffoletto, *op. cit.*, p. 42 ss.; E.O. Policella, *op. cit.*, p. 89.

[46] Vd. Provvedimento del 2 febbraio 2006, in *http://www.garanteprivacy.it/garante/doc.jsp?ID=1229854*; provvedimento del 18 maggio 2006, in *http://www.garanteprivacy.it/garante/doc.jsp?ID=1299082*; per un commento al primo provvedimento, vd. V. Ferrari, *Il licenziamento del lavoratore che « naviga » su Internet*, in *IUSLabor* 2006, 3, *http://www.upf.edu/iuslabor/032006/Italia.vincenzo.pdf*.

[47] Per gli ulteriori profili relativi al consenso, *ex* artt. 24 e 26 D.Lgs. 196/2003, vd. E.O. Policella, *op. cit.*, p. 92.

[48] Con provvedimento 23 novembre 2006, *http://www.garanteprivacy.it/garante/doc.jsp?ID=1364939*. Le linee guida sono state adottate al fine di « fornire indicazioni e raccomandazioni con riguardo alle operazioni di trattamento effettuate con dati personali (anche sensibili) di lavoratori operanti alle dipendenze di datori di lavoro privati ».

tori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati ».

Le Linee guida, pur non disciplinando in maniera diretta la materia dei controlli datoriali, ribadiscono la necessità del rispetto dei principi di protezione dei dati personali, nell'ambito del rapporto di lavoro.

4. Navigazione in Internet per fini personali e licenziamento per giusta causa.

Il Tribunale, pur avendo rigettato le eccezioni relative alle modalità di controllo delle condotte del lavoratore, ha ritenuto che il licenziamento fosse, nel caso di specie, una misura troppo severa, quale sanzione per una condotta, sia pure certamente scorretta, come quella dell'accesso (che viene definito « smodato ») a Internet per fini personali.

In conclusione, il mero utilizzo (ancorché massiccio) del computer aziendale per la navigazione in siti non attinenti alla propria occupazione, in assenza di ulteriori elementi (danni economici, flessione di produttività, diffusione di virus etc.), non è stato considerato dal Giudicante un inadempimento tale da legittimare il licenziamento in tronco per giusta causa.

Il Tribunale di Perugia, in sede di reclamo, ha, a conferma del provvedimento, ribadito come l'accesso a Internet a fini personali, sia da considerare un comportamento illegittimo, ma che non sia di per sé solo sufficiente a giustificare il licenziamento, e ciò anche nell'ipotesi in cui i collegamenti siano « numerosissimi ».

Occorre sottolineare peraltro che la giurisprudenza di merito offre precedenti radicalmente difformi; in particolare, il Tribunale di Milano[49] ha ritenuto la legittimità del licenziamento (per giusta causa) intimato ad un lavoratore che aveva effettuato collegamenti a Internet di lunghissima durata; la sentenza in parola peraltro non affronta in alcun modo il problema della compatibilità tra verifica dei *log* alla connessione Internet, e l'art. 4 dello Statuto dei Lavoratori.

Si tratta, in sintesi, di una questione di merito, legata in effetti, più che alla navigazione in Internet in sé e per sé considerata[50], ad ulteriori elementi che possano costituire, complessivamente considerati, un grave inadempimento del dovere fondamentale del prestatore di lavoro.

5. Conclusioni.

Le problematiche sottese alle « nuove » potenzialità offerte dal mezzo informatico e dal massiccio uso di Internet sul luogo di lavoro, sia ai fini del controllo dei lavoratori, sia ai fini dell'adempimento delle prescrizioni di cui agli artt. 33 e ss. del Codice della Privacy, nonché alle misure minime di sicurezza di cui all'all. B del Codice medesimo, sono molteplici e complesse.

Cercando di operare una sintesi dell'interazione tra i diversi piani normativi, può ritenersi che la liceità di un controllo (e quindi del trattamento

[49] Trib. Milano, 14 giugno 2001, in *Guida lav.*, 2001, p. 46.

[50] A meno che la stessa non sia espressamente vietata, ovvero del tutto irrilevante al fine dello svolgimento della prestazione lavorativa.

di dati personali dei lavoratori, essendo altamente improbabile che un controllo riguardi dati anonimi, ed in considerazione dell'ampiezza del concetto di « trattamento ») sui lavoratori debba essere valutata in primo luogo con riguardo alle disposizioni dello Statuto dei lavoratori, e, qualora esso sia conforme al disposto statutario, si debba comunque verificare se siano rispettati i principi in tema di trattamento di dati personali, delineati in particolare dall'art. 11 del Codice, con precipua attenzione ai principi di necessità, di trasparenza, di proporzionalità e di non eccedenza.

Non si tratta di valutazioni semplici, ma i riflessi di un eventuale trattamento illecito possono essere pesantissimi, sia in tema di sanzioni penali (*ex* art. 171 del Codice), sia per ciò che concerne l'utilizzabilità, nel corso del procedimento disciplinare e dell'eventuale controversia giudiziaria, della prova acquisita in virtù di un controllo illecito.

Un'occasione preziosa per la regolamentazione della materia (soprattutto al fine di chiarire il confine tra controlli leciti e illeciti) potrebbe essere costituita dall'introduzione, ai sensi dell'art. 111 del Codice della Privacy, di un codice di deontologia e di buona condotta per i soggetti interessati al trattamento dei dati personali effettuato per la gestione del rapporto di lavoro.

In sede di auto-regolamentazione, infatti, potrebbero essere meglio precisati (in maniera condivisa e concordata) i confini della potestà di controllo datoriale, anche con riguardo ai controlli difensivi[51], al fine di un equo contemperamento dei diversi interessi in gioco[52].

GIOVANNI BATTISTA GALLUS

---

[51] Anche in considerazione del fatto che, ai sensi dell'art. 12, comma terzo, del Codice, « il rispetto delle disposizioni contenute nei codici [...] costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici »; sul punto vd. A. BELLAVISTA, *Il Codice*, cit., p. 418 ss.; sottolinea l'importanza della (futura) adozione del Codice deontologico anche E.O. POLICELLA, *op. cit.*, p. 83.

[52] Nelle more della pubblicazione della nota a sentenza, è intervenuto il Provvedimento del Garante della protezione dei dati personali del 1/3/2007 (in *Gazz. Uff.*, 10 marzo 2007, n. 58, reperibile anche sul sito del Garante - http://www.garanteprivacy.it/garante/doc) avente ad oggetto « Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori ». Il Garante pertanto, anziché incentivare l'autoregolamentazione, mediante l'introduzione di un codice di deontologia e buona condotta, ha optato per la via del provvedimento generale, emesso ai sensi dell'art. 154 del Codice della Privacy, con particolare riguardo alla lettera *c*) del medesimo articolo (« Il Garante [...] ha il compito di [...] prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143 »). Il provvedimento riguarda precipuamente il trattamento dei dati personali effettuato dai datori di lavoro, al fine di verificare il corretto utilizzo, da parte del dipendente, della posta elettronica e della rete Internet. Fin dalle premesse, si sottolineano i rischi di « analisi, profilazione e integrale ricostruzione » dell'utilizzo di Internet da parte dei lavoratori, mediante elaborazione dei *log file* della navigazione Internet. Il provvedimento, secondo i primi commentatori (D. MINOTTI, *I nuovi obblighi complicano la revisione del documento programmatico di sicurezza*, in *Guida al Diritto*, 2007, n. 12, p. 119) è decisamente sbilanciato verso la massima tutela dei dati personali del lavoratore, comprimendo in maniera eccessiva le potestà datoriali di controllo, e riducendo, di conseguenza, le possibilità di acquisire elementi di prova utilizzabili nel procedimento disciplinare prima e nel giudizio poi. Il Garante, oltre a richiamare l'importanza dei principi fondanti del Codice, sottolinea come il trattamento debba essere ispirato ad un canone

di trasparenza, e pertanto sarà preciso onere del datore indicare « chiaramente ed in modo particolareggiato » quali siano le modalità di utilizzo degli strumenti informatici, e quale sia l'estensione dei controlli. In secondo luogo, vengono formulate delle vere e proprie « linee guida » (paragrafo 3.2 del Provvedimento), ove si rende sostanzialmente obbligatoria l'adozione delle cc.dd. *privacy policies*, vale a dire di un disciplinare interno (che deve essere adeguatamente pubblicizzato, anche mediante affissione), che individui in maniera particolareggiata le modalità di utilizzo di Internet, la possibilità di utilizzo per ragioni personali, le informazioni che vengono conservate, l'eventuale ambito dei poteri di controllo (da giustificarsi specificatamente), le conseguenze di un eventuale utilizzo indebito delle risorse Internet ed, infine, le prescrizioni sulla sicurezza dei dati e dei sistemi. In terzo luogo, il Garante si occupa, direttamente, delle apparecchiature preordinate al controllo a distanza (paragrafi 4 e 5) tra cui « sono certamente comprese strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica », ritenendo illeciti tutti quei trattamenti che consentano una ricostruzione minuziosa e invasiva dell'attività del lavoratore. Per quanto riguarda invece i controlli preterintenzionali, il Garante, dopo aver richiamato la necessità del rispetto dell'art. 4, comma 2 dello Statuto dei Lavoratori, sottolinea l'importanza di adottare misure preventive volte ad evitare l'abuso degli strumenti Internet. In estrema sintesi, il Provvedimento si inserisce nella linea già tracciata sia nei documenti del Gruppo di lavoro *ex* art. 29, già richiamati, sia nei provvedimenti finora adottati dal Garante stesso, mediante l'introduzione di una specifica e puntigliosa serie di limitazioni alla potestà datoriale di controllo. Questi limiti, se da un lato potranno circoscrivere le prassi volte ad un controllo occulto e pervasivo, dall'altro sicuramente comporteranno dei serissimi problemi con riguardo alla possibilità di provare utilizzi non corretti degli strumenti lavorativi.