TRIBUNALE MILANO
10 MAGGIO 2002
(ORDINANZA)
GUP: PELLEGRINO

Diritti della personalità • Segretezza della corrispondenza • Posta elettronica aziendale in uso al lavoratore • Accesso da parte di terzi • Violazione della sfera privata • Esclusione • Fattispecie: informazioni relative alla violazione di doveri inerenti al rapporto di lavoro tratte dalla corrispondenza elettronica e conseguente licenziamento del lavoratore

L'accesso da parte di terzi alla casella di posta elettronica aziendale in uso al lavoratore, sebbene protetta da codici identificativi, non costituisce violazione della sfera privata del lavoratore, non essendo in tal caso configurabile un diritto all'utilizzo esclusivo e privato.

Il Giudice per le indagini preliminari, dott. Andrea Pellegrino,
Visti gli atti del procedimento,
verificata la ritualità delle notifiche e degli avvisi,
sentite le parti intervenute all'udienza camerale del 29.4.02,
a scioglimento della riserva ivi assunta

OSSERVA

Con atto presentato presso gli uffici della Procura della Repubblica di Milano in data 7.11.01, l'avv. (—), nella sua qualità di difensore procuratore speciale di A., sporgeva denuncia querela nei confronti dei sigg.ri C.G. e R.F. (la prima, responsabile del reparto di project management della ditta (—); il secondo, legale rappresentante della predetta società) per il reato p. e p. dagli artt. 110, 616,61 n. 11 c.p. nonché per tutti gli altri reati eventualmente ravvisabili dall'Autorità Giudiziaria.

In fatto l'esponente deduceva che la A. in data 13.8.01 aveva ricevuto da parte del proprio datore di lavoro (ditta (—) presso la quale aveva svolto in qualità di impiegata mansioni di consultant/account sin dalla data di assunzione avvenuta l'1.9.00) raccomandata datata 6.8.01 del seguente letterale tenore: « il giorno 31 luglio u.s., la Sua responsabile, durante le normali e periodiche operazioni di lettura della casella aziendale di posta elettronica (cui fanno riferimento i clienti di (—), per i progetti a Lei assegnati) al fine di verificare eventuali messaggi ricevuti durante il Suo periodo di assenza per ferie, si imbatteva in comunicazioni inerenti soluzioni internet inequivocabilmente relative a progetti estranei a quelli attualmente gestiti da (...)... ».

Con successiva missiva del 29.8.01 la A. veniva licenziata dalla ditta (...) per presunta violazione dei doveri inerenti al rapporto di lavoro (licenziamento che la lavoratrice impugnava con rivendicazioni economiche).

Nella denuncia-querela l'esponente deduceva che la condotta della C. e del R. presentava aspetti di rilevanza penale (art. 616 c.p.) avendo i medesimi fatto accesso alla corrispondenza della lavoratrice; corrispondenza

— quella contenuta all'interno della sua casella di posta elettronica, al pari di quella effettuata per via epistolare, telegrafica, telefonica ovvero effettuata con ogni altra forma di comunicazione a distanza — la cui segretezza è garantita costituzionalmente. Né si poteva ritenere la ricorrenza di una causa di giustificazione (esercizio di un diritto o adempimento di un dovere) dal momento che in nessun caso — con l'ovvia eccezione, nella specie non ricorrente, dell'ipotesi in cui si abbia motivo di ritenere che in essa siano contenuti elementi comprovanti fatti illeciti che interessino in modo diretto l'agente — è consentito al datore di lavoro di controllare il contenuto dei messaggi di posta elettronica. Ad ogni buon conto occorreva evidenziare che:

i messaggi inviati dai clienti erano, senza dubbio identificabili tra quelli contenuti nella casella postale (e ciò si deduceva dal fatto che la stessa società aveva assegnato tali clienti alla A. e le relative comunicazioni erano state oggetto di altri e precedenti controlli da parte della responsabile sig.ra C.);

il controllo delle missive dei clienti era superfluo considerato che gli stessi erano in ferie;

il controllo dei messaggi a carattere privato fu compiuto quando la A. era in ferie evidentemente a sua insaputa e con l'avallo dei responsabili della società;

non vi era alcuna fondata ragione, al momento del controllo della corrispondenza destinata alla A., da parte della società, per ritenere che in essa vi fossero contenuti elementi comprovanti fatti illeciti interessanti in modo diretto la società stessa.

In data 21.1.02 il P.M. avanzava richiesta di archiviazione del procedimento con la seguente motivazione: « le caselle di posta elettronica recanti quali estensioni nell'indirizzo E-MAIL @(...).it, seppur contraddistinte da diversi « username » d identificazione e password di accesso, sono da ritenersi equiparate ai normali strumenti di lavoro della società e quindi soltanto in uso ai singoli dipendenti per lo svolgimento dell'attività aziendale agli stessi demandata; considerando quindi che la titolarità di detti spazi di posta elettronica debba ritenersi riconducibile esclusivamente alla società... p.q.m. ...*omissis* ».

L'opposizione risulta inaccoglibile mentre, di contro, l'archiviazione deve essere disposta ritenuta l'infondatezza della notizia di reato.

Dopo aver sgombrato il campo da impropri riferimenti alla normativa contenuta nella legge n. 675/96 relativa al ben diverso (ed assolutamente inconferente) problema della tutela del trattamento dai dati personali, una breve ma doverosa premessa s'impone.

La fattispecie dedotta avanti a questo giudice presenta aspetti di novità nell'ambito di una disciplina che solo da tempi relativamente assai recenti ha iniziato a fare la propria comparsa nelle aule giudiziarie.

Non può negarsi come la nascita e la diffusione di una nuova tecnologia precedono sempre e significativamente l'affermarsi di una cultura comune e standardizzata nell'utilizzo ad ogni livello del nuovo strumento. La preoccupazione della prima fase è solo quella di acquisire la padronanza, a volte anche solo parziale, dell'uso tecnico del nuovo mezzo o strumento senza alcun interesse (o attenzione) nel valutare le modalità di integrazione semiotica o antropomorfa della nuova tecnologia (cfr. il recente esempio della telefonia mobile). A questa regola non è certamente sfuggita la « posta elettronica » di internet.

In attesa di una codificazione dei comportamenti ai fini dell'omologazione e dell'accettazione di un uso standardizzato dello strumento, molte sono le problematiche che si sono affacciate con la nascita della « buca delle lettere elettronica », tra queste dividendole per aree tematiche e con specifico riferimento all'utilizzo di tale strumento da parte del lavoratore si possono elencare le seguenti:

a) utilizzo anche per fine privato dell'indirizzo di posta elettronica da parte del lavoratore con eventuale esposizione dello stesso sulla carta da visita intestata a proprio nome;

b) possesso di un indirizzo « generalista » e che la posta ivi indirizzata può avere come destinatario un qualunque altro dipendente con conseguente incertezza sulla « consegna »;

c) mancata individuazione del mittente (in possesso di un indirizzo in codice o con sigla) che non provvede a sottoscrivere il messaggio ovvero che non si preoccupa di farsi riconoscere rendendosi di fatto anonimo.

Limitando sostanzialmente la nostra analisi alla prima problematica, va detto innanzitutto come non possa mettersi in dubbio il fatto che l'indirizzo di posta elettronica affidato in uso al lavoratore, di solito accompagnato da un qualche identificativo più o meno esplicito, abbia carattere personale, nel senso cioè che lo stesso viene attribuito al singolo lavoratore per lo svolgimento delle proprie mansioni.

Tuttavia, « personalità » dell'indirizzo non significa necessariamente « privatezza » del medesimo dal momento che, salve le ipotesi in cui la qualifica del lavoratore lo consenta o addirittura lo imponga in considerazione dell'impossibilità o del divieto di compiere qualsiasi tipo di controllo/intromissioni da parte di altri lavoratori che rivestano funzioni o qualifiche sovraordinate (fattispecie che potrebbe effettivamente indurre a qualche dubbio), l'indirizzo aziendale, proprio perché tale, può sempre essere nella disponibilità di accesso e lettura da parte di persone diverse dall'utilizzatore consuetudinario (ma sempre appartenenti all'azienda) a prescindere dalla identità o diversità di qualifica o funzione: ipotesi, frequentissima, è quella del lavoratore che « sostituisce » il collega per qualunque causa (ferie, malattia, gravidanza) e che va ad operare, per consentire la continuità aziendale, sul personal-computer di quest'ultimo anche per periodi di tempo non limitati.

Così come non può configurarsi un diritto del lavoratore ad accedere in via esclusiva al computer aziendale, parimenti è inconfigurabile in astratto, salve eccezioni di cui sopra, un diritto all'utilizzo esclusivo di una casella di posta elettronica aziendale.

Pertanto il lavoratore che utilizza — per qualunque fine — la casella di posta elettronica, aziendale, si espone al « rischio » che anche altri lavoratori della medesima azienda che, unica, deve considerarsi titolare dell'indirizzo — possano lecitamente entrare nella sua casella (ossia in suo uso sebbene non esclusivo) e leggere i messaggi (in entrata e in uscita) ivi contenuti, previa consentita acquisizione della relativa password la cui finalità non è certo quella di « proteggere » la segretezza dei dati personali contenuti negli strumenti a disposizione del singolo lavoratore bensì solo quella di impedire che ai predetti strumenti possano accedere persone estranee alla società;

E che detto rischio, per essere « operativo », non debba essere preventivamente ed espressamente ricordato al lavoratore è una evenienza che può ritenersi conseguenziale alle doverose ed imprescindibili conoscenze

informatiche del lavoratore che, proprio perché utilizzatore di detto strumento, non può ignorare questa evidente e palese implicazione.

Né si può ritenere che l'assimilazione della posta elettronica alla posta tradizionale, con consequenziale affermazione « generalizzata » del principio di segretezza, si verifichi nel momento in cui il lavoratore utilizzi lo strumento per fini privati (ossia extralavorativi), atteso che giammai un uso illecito (o, al massimo, semplicemente tollerato ma non certo favorito) di uno strumento di lavoro può far attribuire a chi, questo illecito commette, diritti di sorta.

A questo punto, peraltro, il problema muta prospettiva perché non riguarda più l'individuazione ed il diritto di chi « entra » nel computer (e nell'indirizzo di posta elettronica) altrui avendo possibilità di leggere i messaggi di posta elettronica non specificamente a lui destinati, bensì diventa quello di « tutelare » il diritto di chi invia il messaggio (a qualunque contenuto: ossia a contenuto privato ovvero lavorativo) credendo che il destinatario dello stesso sia e possa essere esclusivamente una determinata persona (o una cerchia determinata di persone). È evidente che questa situazione può trovare tutela rendendo chiaro al proprio interlocutore che l'indirizzo di posta elettronica è esclusivamente aziendale (e, quindi, al di là dell'uso di intestazioni apparentemente personali del lavoratore-principale utilizzatore, lo stesso non è un indirizzo privato secondo quanto precedentemente detto); cosa che può avvenire o usando un inequivoco identificativo aziendale (indirizzato ad un destinatario virtuale) in aggiunta ad altro identificativo personale-nominativo ovvero provvedendo a segnalare adeguatamente al proprio interlocutore (destinatario reale) la circostanza del carattere « non privato » dell'indirizzo.

Né può ritenersi conferente ogni ulteriore argomentazione che, facendo apoditticamente leva sul carattere di assoluta assimilazione della posta elettronica alla posta tradizionale, cerchi di superare le strutturali diversità dei due strumenti comunicativi (si pensi, in via esemplificativa, al carattere di « istantaneità » della comunicazione informatica — operante come un normale terminale telefonico — pur in presenza di un prelievo necessariamente legato all'accensione del personal e, quindi, sostanzialmente coincidente con la presenza stanziale del lavoratore nell'ufficio ove è presente il desk-top del titolare dell'indirizzo) per giungere a conclusioni differenti da quelle ritenute da questo giudice.

Tanto meno può ritenersi che leggendo la posta elettronica contenuta sul personal del lavoratore si possa verificare un non consentito controllo sulle attività di quest'ultimo atteso che l'uso dell'e-mail costituisce un semplice strumento aziendale a disposizione dell'utente-lavoratore al solo fine di consentire al medesimo di svolgere la propria funzione aziendale (non si possono dividere i messaggi di posta elettronica: quelli « privati » da un lato e quelli « pubblici » dall'altro) e che, come tutti gli altri strumenti di lavoro forniti dal datore di lavoro, rimane nella completa e totale disponibilità del medesimo senza alcuna limitazione (di qui l'inconferenza dell'assunto in ordine all'asserito preteso divieto assoluto del datore di lavoro di « entrare » nelle cartelle « private » del lavoratore ed individuabili come tali, che verosimilmente contengano messaggi privati indirizzati o inviati al lavoratore e che solo ragioni di discrezione ed educazione imporrebbero al datore di lavoro/lavoratore non destinatario di astenersi da ogni forma di curiosità...).

Parimenti irrilevante appare l'ulteriore rilievo che anche la posta tradizionale che presenti caratteri inequivoci di « privatezza », non cessi di assumere detto carattere se fatta recapitare al suo destinatario sul posto di lavoro anziché al proprio domicilio dal momento che in questo caso l'inconfondibilità del carattere di privatezza-esclusività (busta chiusa con nominativo del solo destinatario) della corrispondenza non consente di operare un simile confronto!

Venendo alla fattispecie dedotta in giudizio, si evidenzia come le indagini esperite (assunzione di sommarie informazioni testimoniali rese da P. F., direttore tecnico nonché responsabile del settore informatico per la filiale italiana della (...)) abbiano consentito di acclarare che:

— all'interno della (...) il lavoratore è depositario di un username e di una password (conosciuti dal solo responsabile tecnico) che vengono utilizzati per entrare nel sistema informatico: identificativi che il singolo lavoratore può in qualsiasi momento modificare;

— l'accesso a tutti gli strumenti aziendali (e-mail compresa) è funzionale all'occupazione del dipendente;

— la funzione svolta dagli identificativi non è quella di proteggere i dati personali contenuti negli strumenti a disposizione del singolo lavoratore bensì quella di proteggere i predetti strumenti dall'accesso di persone estranee alla società;

— è prassi comune fra i dipendenti dell'azienda fornire volontariamente i propri dati d'accesso ad altri lavoratori con funzioni societarie equivalenti onde permettere la continuazione delle relative funzioni in propria assenza;

— nel normale uso dello strumento viene anche tollerato un uso extralavorativo della e-mail senza tuttavia che si verifichi un mutamento della destinazione dello strumento, che è quello esclusivo della comunicazione con colleghi e clienti: in ogni caso non viene consentito, anzi è assolutamente vietato, l'utilizzo dello spazio di posta elettronica per motivi personali;

— l'indirizzo di posta elettronica dei dipendenti della società si compone, da sinistra a destra, del nome e del cognome del lavoratore seguiti dal simbolo @ e dal nome della società (...).it.

Tutte queste circostanze di fatto attestanti le consuetudini lavorative all'interno dell'azienda e le condotte dei dipendenti sono conformi alle premesse sopra esposte e consentono di escludere la configurabilità a carico degli indagati di fattispecie delittuose.

Fermo quanto precede, si può concludere ritenendo che:

— la A., così come gli altri lavoratori con mansioni e qualifica pari o assimilabili, era tenuta, secondo una consuetudine che non abbiamo difficoltà a ritenere universale, a segnalare (ovvero a non mantenere segreta nel caso di successiva modificazione) la propria password per consentire a qualunque altro suo collega di poterla adeguatamente sostituire durante la sua assenza dal lavoro;

— la A., nell'utilizzazione della casella di posta elettronica della società, non poteva non sapere che alla medesima, indipendentemente dalla sua presenza in società, vi poteva avere lecito accesso qualunque altro suo collega (e, ovviamente, il datore di lavoro) al fine del disbrigo delle incombenze lavorative connesse alle mansioni (invio e ricezione di comunicazioni di lavoro con colleghi e clienti). Fermo quanto precede, da ultimo va detto che quand'anche — per assurdo, atteso quanto sin qui esposto

— si volesse ritenere che con la loro condotta la C. e il R. nelle rispettive diverse qualità, entrando nella casella di posta elettronica in uso alla lavoratrice abbiano commesso nei confronti della stessa un'illecita intromissione in una sfera personale privata, nondimeno la configurabilità del reato di cui all'art. 616 c.p. verrebbe ugualmente esclusa sotto il profilo soggettivo attesa la totale mancanza di dolo nella loro condotta;

— l'accesso alla casella di posta elettronica dell'A. è avvenuta per motivi assolutamente connessi allo svolgimento dell'attività aziendale, oltre che in assenza della lavoratrice: in una situazione, cioè, nella quale non vi era altro modo per accedere a quelle necessarie informazioni e comunicazioni che, diversamente, se non ricevute ovvero recepite con ritardo, avrebbero potuto arrecare un evidente danno (economico e non solo) per la società.

Da qui il rigetto dell'opposizione e l'archiviazione del procedimento.

Visti gli artt. 408 e segg. C.p.p.

P.Q.M.

rigetta l'opposizione proposta nell'interesse della persona offesa A. in data 14.2.02;

dispone l'archiviazione del procedimento e ordina la restituzione degli atti al Pubblico Ministero.

L'USO DELLA POSTA ELETTRONICA E DI INTERNET SUL LUOGO DI LAVORO: CONFLITTI TRA NORME E NECESSITÀ DI UNA REGOLAMENTAZIONE AD HOC

1. Premessa.

L'introduzione delle nuove tecnologie, tra cui si annoverano gli elaboratori elettronici e i relativi programmi, ivi inclusi quelli necessari al funzionamento della posta elettronica ed al collegamento ad Internet, tra gli strumenti funzionali allo svolgimento dell'attività lavorativa, ha comportato una indiscutibile evoluzione nelle modalità di esecuzione della prestazione lavorativa medesima.

Tuttavia questo cambiamento strutturale, nello svolgimento delle rispettive mansioni e nell'organizzazione aziendale del lavoro, ha aperto questioni interpretative di difficile soluzione con riguardo a diversi profili giuridici: dalla tutela della privacy di coloro che utilizzano tali strumenti, alla tutela giuslavoristica del lavoratore, rispetto ad eventuali possibili ingerenze nella propria sfera privata da parte del datore di lavoro; dai profili penali a quelli di rango costituzionale, concernenti la tutela della corrispondenza.

Le caratteristiche tecniche e le potenzialità intrinseche a tali strumenti pongono, infatti, con una urgenza sempre crescente, problemi di coordinamento e contemperamento tra due sfere di interesse, diametralmente opposte e parimenti meritevoli di tutela.

Da un lato sono innanzitutto individuabili: l'esigenza delle imprese di implementare sistemi di organizzazione del lavoro, basati sul ricorso a

strumenti tecnologicamente avanzati, necessari per mantenere adeguati livelli di competitività sul mercato, che implicano la registrazione di una gran mole di dati, generati dai lavoratori e, al contempo, l'esigenza di evitare che si verifichino abusi, da parte degli stessi lavoratori, nell'uso dei dispositivi hardware e software, che sono parte del patrimonio aziendale e come tali tutelabili dal datore di lavoro[1].

Dall'altro si staglia il diritto del lavoratore a non vedere invasa la propria sfera personale, tutelata non più soltanto dalle norme della l. 300/70, poste a salvaguardia della dignità e libertà del lavoratore rispetto al potere di controllo datoriale, ma dalla normativa vigente in materia di tutela della privacy, tesa a garantire all'interessato/lavoratore il controllo sul trattamento e la circolazione delle informazioni che lo riguardano, sotto il profilo dell'*an* e del *quomodo*.

È notorio infatti che già le componenti standard, degli strumenti che rendono possibile l'utilizzo della posta elettronica e di Internet, implicano ad oggi la registrazione automatica di numerosi dati attinenti alla navigazione, nonché la memorizzazione di messaggi in arrivo o in uscita, trasmessi mediante l'account aziendale[2].

Ciò solleva naturalmente problemi di legittimità di tali forme di registrazione, sia con riferimento alla normativa vigente in materia di tutela della riservatezza delle persone rispetto al trattamento dei dati personali, che con riguardo alle disposizioni giuslavoristiche, nonché ai principi costituzionali ed alla legislazione penale, in materia di tutela della corrispondenza.

Poiché nell'ambito del rapporto di lavoro tali normative, cui sottendono *ratio* diverse, devono trovare necessariamente un'applicazione coordinata, nei paragrafi che seguono si è cercato di metterne in evidenza, se pur brevemente, gli aspetti più rilevanti e le difficoltà attuative rispetto alla moderna realtà produttiva.

Dalle riflessioni svolte emerge la necessità di un intervento normativo specifico, che affronti in modo unitario le numerose questioni giuridiche

---

[1] È indubbia la potenzialità di danno per l'impresa, che risiede nell'eventuale abuso di strumenti quali la posta elettronica e Internet, da parte del lavoratore. Al di là infatti della diminuzione di produttività del singolo — che può investire del tempo in attività non comprese nell'ambito delle proprie mansioni — ed all'aumento dei costi aziendali, dovuti alla durata maggiore della connessione, vi sono rischi di diffusione di materiale confidenziale e riservato a terzi, che la velocità del messaggio per posta elettronica certamente agevola, nonché rischi di commissione di veri e propri illeciti, se non addirittura di reati mediante il web. Si pensi ad esempio all'accesso, dalla propria postazione di lavoro, a siti su cui sia pubblicato materiale pornografico o di pedofilia, ovvero su cui si effettuino scommesse illegali ecc. Profili di rischio si presentano inoltre nel caso di partecipazione a chatroom con l'account aziendale, oppure nel caso di realizzazione di comportamenti molesti mediante l'invio di messaggi, all'interno dell'azienda, a colleghi ovvero, al di fuori della stessa, nei confronti di terzi. Tali situazioni sono peraltro rese ancor più complesse dal fatto che spesso al medesimo account corrispondono entità giuridiche distinte (ad esempio più aziende dello stesso gruppo), il che implica un coinvolgimento nelle attività svolte, mediante l'account di posta, di più soggetti giuridici, con evidenti difficoltà di delimitazione e identificazione delle rispettive, eventuali responsabilità.

[2] Occorre inoltre tener presente che in commercio sono disponibili anche software specifici e più complessi (cosiddetti software « spia »), atti a monitorare le attività svolte in rete dall'utente (nel contesto in oggetto, dal lavoratore), ovvero software diretti a delimitare, ab origine, l'ambito di navigazione concesso all'utente, mediante l'inibizione di determinate categorie di siti.

in discussione, dopo aver individuato un punto di possibile equilibrio tra gli opposti interessi in gioco. Poiché tali problematiche sono percepite e condivise anche al di fuori dei confini nazionali, dagli altri Stati membri, è in corso un dibattito comune sull'argomento, che dovrebbe sfociare, in tempi brevi, nella emanazione di un documento unitario, quantomeno a livello dei Garanti per la privacy europei.

Nell'attesa che, a livello comunitario, si disegnino i confini per un nuovo corretto rapporto tra tecnologia, diritti dell'individuo, impresa e lavoro, l'unica via da seguire appare dunque quella della adozione di dettagliate e specifiche policy aziendali, per tentare di adeguare l'attuale prassi produttiva alla complessa serie di adempimenti e divieti, prevista dalla normativa vigente.

2. La legge n. 675/96.

Va detto innanzitutto che la delicatezza del tema del trattamento dei dati personali, nell'ambito del rapporto di lavoro, era già emersa in tutta la sua ampiezza all'indomani dell'entrata in vigore della legge 675/96 (d'ora in poi « la Legge »), anche a prescindere dalla specificità delle questioni relative all'uso di Internet e della posta elettronica.

Anche volendo *limitarsi*, per così dire, ad esaminare il trattamento dei dati che ogni datore di lavoro è tenuto necessariamente ad effettuare, ai fini della gestione del rapporto di lavoro con i propri dipendenti, trattamento che potremmo, pur se impropriamente, definire *off line*[3], era apparsa subito evidente infatti la difficoltà di adeguamento alle prescrizioni del dettato normativo. Nelle odierne organizzazioni aziendali la raccolta ed il trattamento dei dati dei dipendenti non si limitano a quelli conseguenti « ... a specifici obblighi contabili, retributivi, previdenziali, assistenziali e fiscali... »[4], ma riguardano sovente la gestione di numerosi altri aspetti del rapporto: dalla rilevazione delle presenze tramite badge[5] alle « note di qualifica »[6], dalle ulteriori polizze assicurative facoltative che il datore dovesse decidere di stipulare in favore dei dipendenti ai cellulari con uso misto o all'uso della mensa da parte di soggetti la cui confessione religiosa non dovesse ad esempio consentire l'ingerimento di certi alimenti.

Sotto questo profilo quindi l'applicazione della l. 675/96 ha richiesto un difficile lavoro di analisi delle singole situazioni, avente lo scopo di rendere coerenti tali trattamenti con le prescrizioni normative, soprattutto

[3] Con tale espressione si intendono i trattamenti di dati che il Titolare/datore di lavoro svolge nell'ambito della gestione del rapporto di lavoro e che, pur se effettuati anche mediante l'uso di strumenti informatici, non sono necessariamente connessi con l'uso della rete. Per un esame specifico delle problematiche relative all'applicazione della legge sulla privacy nell'uso di Internet, ci si permette di rinviare a A. Stracuzzi, *Il commercio elettronico e l'impresa*, II Edizione 2002, Il Sole-24 Ore, pagg. 185 e ss.

[4] Sono le cause di esclusione dall'obbligo della notificazione, elencate all'art. 7, comma 5-*ter*, legge 675/96.

[5] Su cui il Garante si è espresso con il provvedimento del 2 giugno 1999.

[6] Anche queste oggetto di intervento da parte del Garante, che ha riconosciuto il diritto d'accesso del dipendente, anche se al termine della procedura di valutazione, nonché il diritto di correzione dei dati, se oggettivamente errati.

con riguardo alla distinzione tra dati comuni e sensibili, alla obbligatorietà o meno del conferimento dei dati, alla disciplina del consenso o alle conseguenze di un eventuale diniego dello stesso da parte del lavoratore.

Infatti uno dei principi cardine della disciplina sulla privacy consiste nel fatto che il consenso al trattamento o alla comunicazione dei dati, quando richiesto, deve essere non solo « informato » ma « libero » (art. 11), ovvero « revocabile » in ogni momento e senza conseguenze per l'interessato.[7]

Tuttavia poiché quando si tratta di consenso prestato da soggetti interessati, operanti nell'ambito di un rapporto di lavoro subordinato, il rispetto della effettività di questa circostanza è messo intrinsecamente in dubbio, ne è derivata la necessità di un'applicazione rigorosissima del principio di « pertinenza e non eccedenza » di cui all'art. 9[8], per evitare di incorrere in un uso abusivo dello strumento del consenso, come metodo di dubbia sanatoria di trattamenti « debordanti » e quindi illeciti.

Il che ha implicato per ogni azienda, che volesse realmente qualificarsi *privacy compliant*, la necessità di una revisione delle proprie procedure organizzative, finalizzata all'individuazione delle attività che implicavano trattamenti obbligatori[9] o comunque necessari[10], per i quali quindi il consenso, necessario nel caso di dati sensibili, era da considerarsi « dovuto » ai fini della instaurazione o prosecuzione del rapporto di lavoro, da tenere distinte da quelle relative a trattamenti qualificabili come « facoltativi »[11], per i quali un rifiuto del consenso, necessario anche nel caso di dati comuni, avrebbe comportato semplicemente la esclusione del singolo interessato/dipendente da quella attività, senza conseguenze di rilievo.

In altri termini, l'adeguamento alle prescrizioni della legge sulla privacy ha significato e significa, per il mondo imprenditoriale, l'adozione di una nuova filosofia organizzativa, attraverso la quale tutti i processi aziendali devono essere (ri)pensati e (ri)strutturati in modo conforme alla *ratio* normativa, mediante l'individuazione delle diverse « aree » aziendali di trattamento dei dati, l'analisi dei relativi « flussi » tra un'area e l'altra, la coerente gestione degli incarichi al trattamento da conferire ai singoli dipendenti[12]. Non solo ma la redazione di una corretta informativa, corredata

---

[7] In realtà il consenso quando è funzionale all'adempimento di obblighi specifici da parte del datore di lavoro (es. di natura contributiva o assistenziale) è addirittura obbligatorio. Il rifiuto del consenso, in questi casi, potrebbe configurare inadempimento contrattuale sanzionabile sotto il profilo disciplinare o addirittura integrare gli estremi del giustificato motivo di licenziamento.

[8] L'art. 9 stabilisce, fra l'altro, che i dati devono essere raccolti e registrati per scopi legittimi e determinati, devono essere trattati in modo lecito e soprattutto devono essere pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti.

[9] Trattamenti necessari per l'adempimento di obblighi previsti dalla legge, da un regolamento o dalla normativa comunitaria (art. 12, comma 1, lett. *a*).

[10] Trattamenti necessari per l'esecuzione di obblighi derivanti da un contratto (art. 12, comma 1, lett. *b*), ad es. la stipula di polizze sanitarie ulteriori rispetto a quelle obbligatorie, per scelta organizzativa aziendale.

[11] Trattamenti di dati relativi ad attività aziendali ulteriori e facoltative, come ad es. corsi di formazione interni, distribuzione di houseorgan ecc.

[12] L'adempimento della disciplina della privacy in azienda è in realtà affidato ai dipendenti che, in ogni loro attività, devono rispettare le scelte organizzative adottate dal Titolare/azienda. Il Titolare, che deve impartire le istruzioni per iscrit-

di idonee richieste di consenso agli interessati, dovrebbe infatti essere l'atto finale di un processo molto più complesso, riguardante anche l'avvenuta organizzazione ed adozione delle necessarie misure di sicurezza, in conformità con i risultati delle attività descritte sopra.

Tenendo conto di tutto ciò, non v'è dubbio che la questione dell'uso della posta elettronica e di Internet in azienda riveste un carattere di particolare complessità, dovendo essere esaminata e gestita, ai sensi privacy, secondo i criteri indicati sopra e con la massima attenzione.

Prescindendo per ora dalle problematiche del « controllo » datoriale e della possibile o meno liceità dello stesso, si deve considerare che la semplice « conservazione », come pure la « cancellazione » e la « distruzione » di dati, rappresentano operazioni di trattamento, ai sensi privacy, che devono essere regolamentate e gestite conformemente alle disposizioni della legge 675/96[13].

L'attività di registrazione dei dati relativi alle *e-mail*, nonché la memorizzazione — mediante l'utilizzo dei file log — dei siti visitati e/o degli indirizzi web raggiunti, nonché, a seconda dei casi, di altre tipologie di dati, deve essere qualificata come « trattamento » di dati personali, rilevante ai sensi della legge 675/96 e successive modifiche[14]. In altre parole, la registrazione ed archiviazione delle informazioni relative alla posta elettronica, indipendentemente dalla presa di cognizione del contenuto del singolo messaggio, nonché il controllo sull'accesso ad Internet, sono attività sottoposte agli adempimenti ed alle regole dettate dalla normativa vigente in materia di privacy.

Non dovrebbero quindi sussistere dubbi sul fatto che il datore di lavoro, prima di procedere all'effettuazione delle operazioni di trattamento (pertanto prima di rendere operative le funzioni di memorizzazione dei sistemi informativi a propria disposizione), dovrà innanzitutto dare espressamente atto dell'esistenza di tali tipologie di trattamenti nella notificazione all'Autorità Garante di cui all'art. 7 della citata legge, nonché informare in modo chiaro e completo il dipendente, circa le modalità e le finalità del trattamento effettuato con tali tipologie di dati, nonché chiedere il relativo consenso scritto, laddove necessario, in conformità in particolare agli artt. 10, 11, 12, 22 della legge 675/96. In ogni caso il trattamento dovrà essere svolto nel rispetto dei principi fondamentali dettati dall'art. 9 della legge 675/96 ed essere « protetto » da adeguate misure di sicurezza (nel rispetto delle disposizioni di cui all'art. 15, commi 1 e 2, ed al DPR 318/99).

Nel tentativo di dare un quadro preciso della questione, proviamo a partire dalla realtà tecnologica e dalla prassi organizzativa.

---

to, può decidere se nominare anche alcuni responsabili interni, cui affidare, *ex* art. 8, l'incarico di controllare il rispetto della disciplina adottata.

[13] Si intende, per « trattamento »: qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, 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 (art. 2, punto *b*).

[14] A questo proposito è opportuno dare atto del fatto che i dati attinenti ai siti visitati, in certe circostanze potrebbero addirittura essere qualificati come dati sensibili, ai sensi dell'art. 22 della legge 675/96, non essendo da escludere la consultazione di siti connotati politicamente o dal punto di vista religioso o sindacale (basti pensare ai siti appartenenti a partiti o a sindacati).

I sistemi informativi, da quelli più semplici a quelli « integrati »[15], sono strutturati in modo tale da realizzare automaticamente la registrazione/conservazione (quindi il « trattamento ») di qualsiasi messaggio di posta elettronica e di qualsiasi accesso ad Internet, effettuato da qualsiasi utente dei sistemi stessi.

I messaggi di posta, sia in entrata che in uscita, arrivano nel server aziendale e vi rimangono quantomeno[16] fino a quando non vengano scaricati dagli utenti/dipendenti, sui propri Personal Computer o inviati ai rispettivi destinatari dal server medesimo. Il sistema può essere infatti progettato in modo che, mediante lo « scaricamento » o l'invio, il messaggio venga cancellato dal server, oppure che questo venga duplicato, rimanendo sia nel server che nel PC. In ogni caso, il fatto che i messaggi in entrata vengano scaricati, dai destinatari, sui rispettivi singoli PC e cancellati dal server centrale, non impedisce che nel server stesso rimanga necessariamente traccia registrata dei seguenti dati (sia in entrata che in uscita): indirizzo del mittente, nome del destinatario, oggetto, data, ora e generalmente volume dei dati trasmessi e degli eventuali allegati. Il contenuto dei messaggi, sia quelli ricevuti che quelli inviati, viene inoltre generalmente archiviato/conservato dall'utente sul proprio PC che, in quanto tale, è in ogni caso un bene aziendale contenente dati, del cui trattamento, ai sensi privacy, risponde il Titolare/azienda.

Se si considera che nei messaggi di posta elettronica (di cui, in mancanza di una regolamentazione aziendale *ad hoc*, viene notoriamente fatto un uso assolutamente promiscuo[17]) possono essere contenuti dati sensibili di ogni genere, certamente debordanti rispetto a quanto stabilito dall'Autorizzazione Generale n. 1, in materia di trattamento dei dati sensibili nell'ambito dei rapporti di lavoro, nonché rispetto alle prescrizioni dell'art. 9, appare evidente la imprescindibile necessità di elaborare rigorose policy aziendali, aventi lo scopo, in attesa della approvazione dell'auspicato codice deontologico[18], di regolamentare l'uso di tale strumento, in modo da renderlo, per quanto possibile, conforme alle prescrizioni della legge 675/96.

In mancanza di una disciplina normativa specifica e di una regolamentazione aziendale, l'uso della posta elettronica per motivi « non esclusiva-

---

[15] Quelli realizzati mediante l'implementazione dei cosiddetti sistemi ERP (Enterprise Resources Program).

[16] L'adozione delle diverse forme di registrazione e scaricamento dei messaggi di posta è una scelta aziendale, adottata generalmente a livello di responsabile del centro EDP. Per la delicatezza della funzione sarebbe consigliabile nominare il responsabile EDP anche responsabile privacy, in modo da sensibilizzare la funzione sulle conseguenze delle scelte organizzative.

[17] La posta elettronica, a meno di espliciti divieti aziendali, viene generalmente utilizzata anche per messaggi di carattere privato. Dagli auguri di compleanno ai messaggi agli amici o ai colleghi, fino ai messaggi di carattere politico/sociale: è quasi impossibile non aver ricevuto, negli ultimi 12 mesi, almeno un appello relativo alla pace nel mondo, alle manifestazioni di piazza, alla raccolta di firme contro la lapidazione nei paesi musulmani ecc.

[18] Il codice deontologico in materia di rapporti di lavoro, previsto dalla legge 467/2001 (che ha modificato la legge 675/96), dovrà occuparsi di trattamenti « necessari per finalità previdenziali o per la gestione del rapporto di lavoro, prevedendo anche specifiche modalità per l'informativa all'interessato e per l'eventuale prestazione del consenso relativamente alla pubblicazione di annunci per finalità di occupazione e alla ricezione di curricula contenenti dati personali anche sensibili » (art. 20, comma 2, lett. *b*).

mente professionali »[19], prassi ampiamente tollerata nella grande maggioranza delle aziende, implica paradossalmente il rischio, per il Titolare/azienda, di dover rispondere di trattamento di dati comuni e sensibili, di cui non conosce, né potrebbe[20], la natura e la tipologia ma che sono « conservati » negli strumenti elettronici aziendali, spesso mescolati con i messaggi inerenti l'attività professionale e per i quali devono tuttavia applicarsi tutte le relative norme della Legge[21].

Viceversa, sempre dal punto di vista « privacy », la gestione dell'accesso ad Internet del dipendente, pur costituendo analogo potenziale trattamento di dati comuni e sensibili[22] e, come tale, ricadente nelle medesime prescrizioni normative, risulta meno problematico per due ragioni. Da un lato la registrazione/conservazione degli accessi ai diversi siti è limitata al server centrale, quindi all'area EDP (più facilmente controllabile sotto il profilo delle misure di sicurezza) e non rimane « archiviata » nei singoli PC, dall'altro l'azienda può, al limite, decidere di eliminare tale funzione, per tutto il personale o per buona parte, evitando il trattamento in quanto tale. Può inoltre essere adottata la soluzione intermedia dell'installazione di appositi software che impediscano l'accesso ai siti considerati « a rischio », in modo da lasciare libero soltanto l'accesso ai siti necessari per svolgere l'attività lavorativa. In ogni caso, poiché l'interessato/dipendente deve essere correttamente informato anche del « non trattamento » che lo riguarda, la policy dovrà riportare e descrivere esattamente le scelte di gestione degli accessi ad Internet adottate dall'azienda.

Per completare il quadro descrittivo delle situazione, bisogna aggiungere che spesso i server che gestiscono il sistema aziendale possono non essere situati presso la sede del Titolare del trattamento, ma presso « web farm » esterne che forniscono, in outsourcing, tale servizio, con conseguente trattamento all'esterno, da parte di terzi, dei dati.

Infine si deve aggiungere che, altrettanto spesso le aziende decidono, per ovvi motivi di contenimento dei costi, di implementare un unico sistema informativo che gestisca le attività di tutte le aziende del Gruppo, con conseguente trattamento, da parte dell'azienda presso cui è installato il sistema, dei dati di tutte le altre aziende che, sotto il medesimo account di posta elettronica, transitano sul sistema stesso.

In questo caso, come nel precedente, sarà necessario redigere un incarico a responsabile che tenga conto, di questa tipologia di dati e di trattamenti e darne una adeguata informativa agli interessati.

Questa lunga descrizione degli aspetti tecnico-organizzativi ha lo scopo di evidenziare come l'uso degli strumenti tecnologici in azienda, crea pro-

---

[19] Per alcune considerazioni circa il cosiddetto « margine di tolleranza » che l'imprenditore è tenuto a rispettare si rimanda al par. 4, nota 51.

[20] Per le motivazioni che saranno esposte nei successivi paragrafi, l'imprenditore non può, in ogni caso, avere accesso ai messaggi « privati ». Per tale ragione è necessario stabilire regole precise per la registrazione ed archiviazione dei messaggi privati da parte del dipendente stesso, in modo che risultino separabili dai messaggi professionali.

[21] Poiché la conservazione di tali dati è comunque effettuata all'interno degli strumenti elettronici aziendali, il datore di lavoro/Titolare è tenuto a rispettare le norme della legge 675/96, in materia di notificazione, informativa, consenso, misure di sicurezza (tra cui idonei backup) ecc.

[22] Mediante la ricostruzione del percorso di navigazione, con la registrazione dell'accesso ai diversi siti, tra i quali possono esservi quelli di carattere politico, sindacale, pornografico ecc.

blematiche complesse, difficilmente immaginabili preventivamente ed in astratto, che mettono a dura prova anche la tenuta di leggi « recenti », come la legge 675/96.

È pur vero che, se ci limitiamo all'uso esclusivamente professionale, si può correttamente sostenere che si tratti di trattamenti « necessari », quindi non « debordanti » ai sensi dell'art. 9 della Legge, in quanto intrinseci alle necessità produttive di una qualsiasi moderna organizzazione aziendale. Certamente sarebbe impensabile oggi eliminare l'uso della posta elettronica e di Internet dall'attività lavorativa, non soltanto per l'azienda, che vedrebbe retrocedere la propria posizione sul mercato, ma anche per il dipendente, che vedrebbe diminuire notevolmente la possibilità di sviluppo professionale e la propria conseguente competitività sul mercato del lavoro.

Ciò non toglie che, per rendere lecito il trattamento e pur trattandosi di dati comuni, sarà necessaria una idonea informativa, che dia conto anche delle misure di sicurezza adottate, corredata del consenso del dipendente, che sarà da qualificarsi, in questo caso, come « necessario »[23].

Nel caso viceversa di « uso privato » della posta elettronica e di Internet, i relativi trattamenti di dati sia comuni che sensibili saranno certamente « debordanti » e questi ultimi non potranno sicuramente essere considerati « coperti » dall'Autorizzazione Generale n. 1 del Garante[24]. Soltanto una policy aziendale, che vieti o, in ossequio al principio del « margine di tolleranza », stabilisca nel dettaglio l'uso « privato » della posta, prevedendo ad esempio file separati di archiviazione da gestire ad esclusiva cura del dipendente, potrà sollevare l'impresa dalle responsabilità penali e civili conseguenti alla violazione delle norme della legge 675/96.

In mancanza di una dettagliata regolamentazione aziendale, un'interpretazione rigorosa della legge n. 675/96 rischierebbe quindi di porre in una posizione di illiceità l'intero mondo imprenditoriale, a prescindere dal fatto che i dati raccolti vengano o meno utilizzati o anche solo esaminati dal datore di lavoro e quindi prima ancora di porsi il problema del monitoraggio e del rispetto degli articoli 4 e 8 della legge n. 300/70.

In Italia, come negli altri Paesi appartenenti alla UE, la materia è allo studio dell'Autorità Garante, che ha annunciato la preparazione di un « provvedimento generale, in particolare per quel che concerne il controllo delle e-mail dei lavoratori dipendenti... » ed ha dichiarato anche di aver « ...posto in essere alcuni specifici accertamenti di carattere preliminare in riferimento ai profili dell'informativa ai lavoratori interessati, del principio di proporzionalità nel trattamento dei dati, della trasparenza dei controlli... »[25]. Non è dato sapere se il provvedimento annunciato coinciderà o meno con il codice deontologico in materia di rapporti di lavoro, previsto dalla legge 467/2001, che dovrà occuparsi di trattamenti « necessari per finalità previdenziali o per la gestione del rapporto di lavoro, prevedendo anche specifiche modalità per l'informa-

[23] Necessario per l'adempimento del contratto, secondo l'organizzazione della produzione stabilita dall'azienda.

[24] Per un confronto con le posizioni di altri Paesi, si rimanda alla sentenza della Corte di Cassazione francese ed al Regolamento federale della Svizzera, citati rispettivamente nei successivi paragrafi 4 e 5.

[25] Relazione 2001 del Garante della privacy, presentata l'8 maggio 2002, pag. 47.

tiva all'interessato e per l'eventuale prestazione del consenso relativamente alla pubblicazione di annunci per finalità di occupazione e alla ricezione di curricula contenenti dati personali anche sensibili » (art. 20).

Del resto l'argomento è talmente delicato che le Autorità Garanti della protezione dei dati degli Stati membri stanno procedendo in parallelo, nell'attività di studio per l'elaborazione di codici o normative che regolino il settore ed hanno costituito un Gruppo di lavoro, il cosiddetto « Articolo 29 »[26], che avrebbe dovuto elaborare una decisione comune entro il mese di maggio del 2002[27].

In un primo parere, adottato il 13 settembre 2001[28], il Gruppo ha confermato che ogni rilevazione, uso o memorizzazione di informazioni sui lavoratori con mezzi elettronici rientra nel campo d'applicazione della legislazione di protezione dei dati ed ha confermato la doverosa applicazione dei principi cardine della privacy (finalità, trasparenza, legittimità, proporzionalità, sicurezza ecc.). In particolare il parere ha ribadito che i lavoratori devono essere dettagliatamente informati su quali dati vengono raccolti su di loro (direttamente o per altre vie), i dati devono essere rilevati esclusivamente per finalità determinate, esplicite e legittime e devono essere pertinenti e non eccedenti rispetto alle finalità. A proposito del consenso, il Gruppo di lavoro ha ritenuto che, « ...se un datore di lavoro deve trattare dati personali come conseguenza necessaria e inevitabile del rapporto di lavoro, sbaglia se cerca di legittimare il trattamento mediante il consenso. Il ricorso al consenso va limitato ai casi in cui il lavoratore è effettivamente libero di scegliere e può successivamente ritirare il proprio consenso senza pregiudizio »[29].

Per quanto concerne l'interazione tra diritto del lavoro e diritto della protezione dei dati, il parere stabilisce che quest'ultimo e le prassi e il diritto del lavoro non operano separatamente e senza interferenze, ma è necessario un bilanciamento che contribuisca allo sviluppo di soluzioni che proteggano adeguatamente gli interessi dei lavoratori.

Passando a trattare la questione del controllo o monitoraggio dei lavoratori rispetto all'uso della posta elettronica e di Internet, il Gruppo di lavoro ha ritenuto che ogni controllo deve essere una risposta proporzionata del datore di lavoro ai rischi che corre, tenendo in dovuto conto la riservatezza del lavoratore e gli altri interessi legittimi di questi. Tutti i dati personali detenuti o utilizzati durante i controlli devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità che giustificano il controllo. Quest'ultimo deve essere, in ogni caso, trasparente (cioè informato) ed eseguito nel modo meno invasivo possibile.

3. Lo Statuto dei Lavoratori.

Nell'affrontare la questione del « controllo », da parte del datore di lavoro, non si può prescindere naturalmente dall'esaminare la legge n.

[26] Il Gruppo, costituito ai sensi dell'art. 29 della direttiva 95/46/CE e composto da rappresentanti dei Garanti della protezione dei dati degli Stati membri, ha carattere consultivo e indipendente.

[27] Relazione 2001, pag. 47

[28] Parere 8/2001 (5062/01 WP 48).

[29] Parere 8/2001, sommario in Relazione 2001, pag. 323.

300/70, la cui applicabilità è fatta espressamente salva dalla legge n. 675/96[30].

In particolare l'art. 4 dello Statuto vieta l'installazione e l'utilizzo di apparecchiature che abbiano, come unica finalità, quella del controllo a distanza dei lavoratori[31].

La norma citata, in ogni caso, non vieta in assoluto ogni forma di controllo da parte del datore di lavoro: essa dispone infatti che, nel caso in cui gli impianti e le apparecchiature, richieste da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, comportino anche la possibilità del controllo a distanza da parte del datore di lavoro, sia necessaria, per la legittimità dell'uso di tali strumenti, l'adozione di una specifica procedura. In queste ipotesi, il datore di lavoro infatti deve informare il lavoratore dell'esistenza di tali strumenti di controllo a distanza ed ottenere il consenso all'utilizzo degli stessi da parte delle rappresentanze sindacali aziendali, ovvero delle commissioni interne oppure, in mancanza di accordo con queste ultime, dovrà superare il vaglio dell'Ispettorato del lavoro[32].

Dal punto di vista giuslavoristico, non dovrebbe esservi dubbio sul fatto che i sistemi informatici, laddove realizzino o consentano forme di controllo a distanza dei lavoratori, rientrino nell'ambito di applicazione dell'art. 4, comma 2, dello Statuto dei Lavoratori, ancorché tale norma sia stata formulata quando la tecnologia su cui si fondano i meccanismi di funzionamento della posta elettronica e di Internet ancora non esistevano.

Si potrebbe addirittura aggiungere che il problema non riguarda soltanto l'uso della posta elettronica e di Internet, ma l'uso degli elaboratori (PC) in quanto tali, soprattutto in considerazione del fatto che, in applicazione delle misure di sicurezza privacy imposte dal D.P.R. 318/99, al dipendente devono essere attribuiti, per l'accesso al sistema, una *login* ed una *password*, mediante le quali è possibile ricostruire qualsiasi attività da questi effettuata sui documenti archiviati nel sistema, ivi inclusi la data e l'ora.

Per quanto concerne il tipo di controllo attuabile, la casistica giurisprudenziale sembrerebbe lasciar intendere che devono considerarsi vietati tutti quei sistemi automatizzati che permettano di risalire all'identità del singolo dipendente, in una ricostruzione « aggregata » di informazioni relative all'attività da questo svolta[33], mentre risultano permessi quei con-

[30] Art. 43, comma 1.

[31] Art. 4, comma 1, « È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori ».

[32] Art. 4, comma 2, « Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti [...] ».

[33] Ad es.: l'installazione di centralini telefonici elettronici (Pret. Milano, 4.10.88, Pret. Roma, 13.01.88, Pret. Roma, 18.09.86); l'elaborazione da parte di un PC di dati storici (Pret. Milano, 5.10.84); l'installazione di un elaboratore che, dopo aver registrato tutte le operazioni svolte da un operatore attraverso un codice individuale, sia in grado di effettuare una ricostruzione ed un'analisi di tali dati aggregati (Pret. Firenze, 20.03.90).

trolli, ritenuti non lesivi della dignità del lavoratore, effettuati per area o settore o comunque non riconducibili all'attività del singolo individuo[34].

Sono considerati consentiti inoltre i cosiddetti « controlli difensivi », cioè quelli che non riguardano (direttamente o indirettamente) l'attività lavorativa, ma sono diretti ad accertare eventuali condotte illecite del lavoratore.

In questo contesto si deve tener presente che gli strumenti informatici, quali posta elettronica e Internet, si possono prestare, abbastanza agevolmente, a forme più o meno gravi di abuso da parte dei dipendenti, quando non addirittura di veri e propri reati[35]. È noto che l'eventuale abuso della strumentazione aziendale (inteso come utilizzo degli strumenti dell'azienda per fini diversi da quelli attinenti all'esecuzione della propria prestazione lavorativa), di per sé può già essere considerata una violazione dei doveri di diligenza e fedeltà, che la legge impone al prestatore di lavoro subordinato[36].

Una pronuncia di merito[37], con riferimento alla valutazione della legittimità delle sanzioni disciplinari e del licenziamento di una lavoratrice, disposto da una società, a causa dell'uso smodato delle connessioni ad Internet, precisa infatti che « la condotta della lavoratrice non solo e non tanto ha provocato costi aziendali non necessari (si badi che nel caso in esame le connessioni non sono state sporadiche e quindi comprensibili e giustificabili, ma cospicue e regolari). Data la sua entità ha integrato gli estremi di un rilevante inadempimento degli obblighi contrattuali di lavoro: in altri termini, quale che fosse la ragione (Internet o qualsiasi altra cosa), per tutte quelle ore la lavoratrice non ha effettuato la prestazione per la quale era retribuita ».

Di recente la Corte di Cassazione, pronunciandosi (forse per la prima volta) in materia di controllo a distanza dei dati telefonici, ha escluso l'operatività del divieto di cui all'art. 4, legge 300/70, poiché il comportamento del datore di lavoro doveva essere interpretato come « ...teso a controllare la condotta illecita del dipendente e non l'attività lavorativa svolta dal medesimo »[38]. Purtroppo la Suprema Corte non ha minimamente approfondito la materia, la qual cosa sarebbe stata di grande utilità, ai fini della soluzione delle problematiche qui esposte. Basti considerare infatti che gli strumenti che consentono un « controllo difensivo », come ad es. le registrazioni telefoniche o la posta elettronica, sono inevitabilmente anche in grado di controllare l'attività lavorativa del dipendente e pertanto non consentono di escludere a priori l'applicazione della procedura prevista dal secondo comma dell'art. 4.

---

[34] Ad es.: il badge che rileva soltanto la presenza o meno sul luogo di lavoro (Trib. Milano, 26.03.94; Pret. Torino, 23.01.92 ecc.); il centralino telefonico elettronico quando ad ogni apparecchio corrispondano più persone (Pret. Milano, 2.07.81); l'installazione di un sistema di comando di apertura delle porte, di aree c.d. segregate, che rilevi soltanto il possesso dell'autorizzazione all'accesso e non l'identità del singolo (Pret. Milano, 2.07.81).

[35] A tal fine si suole distinguere tra i reati commessi *con* Internet, da quelli commessi *su* Internet, dove fra i primi possono annoverarsi ad es. pedofilia, violazione della privacy altrui ecc. e fra i secondi, ad es. il *dowload* di software o di qualsiasi altra opera dell'ingegno non autorizzato ecc.

[36] Cfr. artt. 2104, 2105 e 2086 del codice civile.

[37] Tribunale Milano, Sezione Lavoro, del 14.06.2001, in *Guida al Lavoro* 2001, con nota di G. Bulgarini D'Elci.

[38] Cass. Sez. Lav. 3.04.2002.

La dottrina[39] è in prevalenza orientata nel sostenere che, in ogni caso, la registrazione degli accessi ad Internet da parte dei lavoratori, così come la memorizzazione di tutti i messaggi di posta elettronica in entrata e in uscita dal server[40], pur essendo propedeutica all'esercizio del potere di controllo e disciplinare del datore di lavoro (di per sé normativamente previsto)[41], deve avvenire nel rispetto della procedura di cui all'art. 4, nonché nel rispetto di ulteriori disposizioni dello Statuto dei Lavoratori. Infatti, anche dopo aver ottenuto il benestare dell'Ispettorato o il consenso espresso delle rappresentanze sindacali, il datore di lavoro potrà, a fronte di un abuso degli strumenti aziendali, comminare una sanzione disciplinare, solo ove abbia rispettato la procedura di cui all'art. 7 dello Statuto dei Lavoratori. Dovrà infatti essere stato redatto e reso accessibile a tutti i lavoratori il codice disciplinare, in conformità con i contratti collettivi applicabili; inoltre il datore di lavoro dovrà contestare l'addebito nelle forme previste dall'art. 7 citato ed infine applicare la sanzione, che dovrà, in ogni caso essere proporzionata all'addebito contestato[42].

La descrizione dei limiti di lecito utilizzo dei beni aziendali, quindi di posta elettronica e Internet, dovranno pertanto essere specificati in modo puntuale nel codice disciplinare, altrimenti ben difficilmente si potrà procedere alla contestazione dell'inadempimento del lavoratore[43].

Di diversa opinione sono altri autori che, nell'intento di evitare al datore di lavoro il compito di avventurarsi in « ...complesse trattative sindacali dagli esiti necessariamente alquanto incerti »[44], suggeriscono di considerare « ...leciti, a prescindere dall'esistenza — a monte — di qualunque accordo sindacale stipulato ai sensi dell'art. 4 Stat. Lav. », quei controlli « ...focalizzati non già sullo svolgimento dell'attività lavorativa da parte del dipendente, ma soltanto sul tipo di impiego che il dipendente stesso fa dello strumento informatico posto a sua disposizione dal datore di lavoro ».

Tale interpretazione, fondata sul tentativo di affrontare in modo « pragmatico » l'attuale realtà produttiva, si basa naturalmente sulla necessità che vengano adottate in azienda regole univoche, circa le modalità di utilizzo degli strumenti informatici e le finalità per le quali questi vengono messi a disposizione dei dipendenti, che siano portate a conoscenza di tutto il personale « ...con strumenti idonei, analoghi a quelli utilizzati per il codice disciplinare di cui all'art. 7 Stat. Lav. ».

Con riguardo alla disciplina dettata dallo Statuto dei Lavoratori, occorre inoltre considerare l'art. 8, il quale impone al datore di lavoro il

---

[39] L. NOGLER, *Potere di controllo e utilizzo privato di telefono aziendale*, in nota a sent. Cass. Sez. Lav. 3.04.2002, *Guida al Lavoro* n. 21, 2002.

[40] Si deve ricordare che la funzione di registrazione dei messaggi di posta elettronica in entrata e in uscita, così come la memorizzazione dei percorsi effettuati in rete può essere considerata una caratteristica tecnica standard dei server di gestione di posta elettronica e Internet, che opera indipendentemente da una specifica volontà di controllo da parte del datore di lavoro.

[41] Cfr. artt. 2086, 2104 e 2105 del codice civile.

[42] Cfr. art. 2106 del codice civile.

[43] È tuttavia fatto salvo il caso in cui l'inadempimento integri una fattispecie di reato: in tale ipotesi infatti il procedimento disciplinare potrà essere instaurato anche se la specifica violazione commessa non fosse indicata espressamente nel codice disciplinare. Cfr. F. TOFFOLETTO, *La sanzione scatta solo se c'è un codice*, pubblicato in *Il Sole-24 Ore* del 28/05/2001, n. 145.

[44] C. FOSSATI e C. MORPURGO, *Internet e azienda*, inserto *Diritto & Pratica Del Lavoro 1*, 2002, pag. XVII.

divieto di effettuare — direttamente o tramite terzi — indagini sulle opinioni politiche, religiose, o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore, sia all'atto dell'assunzione che nel corso dello svolgimento del rapporto di lavoro[45].

Si deve a questo proposito considerare che il controllo e la registrazione della navigazione nel *web* effettuata dal dipendente, potrebbero rivelare, al datore di lavoro, indirettamente, aspetti attinenti alla personalità del prestatore di lavoro. È necessario pertanto brevemente analizzare se ed in che misura tali fattispecie concrete possano ritenersi comprese nel disposto di cui all'art. 8 citato. Tale norma infatti richiede, per la sua operatività, che il datore di lavoro effettui vere e proprie « indagini » aventi ad oggetto le opinioni del lavoratore di natura politica, sindacale o religiosa, o fatti comunque estranei alla valutazione delle attitudini professionali del lavoratore.

Ciò premesso, non si ritiene che vi siano dubbi sul fatto che il monitoraggio degli accessi ad Internet possa rappresentare una forma di indagine, che tuttavia non implica di per sé una conoscenza diretta delle opinioni di natura politica, religiosa e/o sindacale dei lavoratori, ma che indubbiamente potrebbe costituire, in certi casi, una fonte di indizi in tal senso. Vero è, d'altro canto, che l'obiettivo del monitoraggio è per lo più la verifica del corretto utilizzo degli strumenti di lavoro messi a disposizione del lavoratore. A certe condizioni pertanto si potrebbe sostenere che la registrazione in realtà riguardi dati concernenti il corretto adempimento della prestazione lavorativa.

In questo contesto occorre inoltre tenere presente che la norma citata, prevedendo una sanzione di natura penale in caso di sua violazione, non tollera interpretazioni di natura estensiva o analogica.

4. La segretezza della corrispondenza.

Infine sempre con riferimento alla possibilità di registrazione e di accesso ai messaggi di posta elettronica, inviati dai dipendenti, oltre ai profili di legittimità rispetto alla normativa vigente in materia di privacy e di diritto del lavoro, merita un breve cenno anche la problematica scaturente dai principi costituzionali e dalla legislazione penale, in materia di tutela della corrispondenza.

Infatti, a seguito della equiparazione della corrispondenza telematica o elettronica alla corrispondenza cartacea[46], si è posto il problema della ap-

[45] Per quanto concerne i profili di legittimità della fattispecie in esame, rispetto alla disposizione di cui all'art. 8 dello Statuto dei Lavoratori, Cfr. A. Riccardi, *Internet e controllo del personale*, in *Diritto & Pratica del Lavoro*, n. 3/2001, pag. 191 e ss.

[46] Il concetto di corrispondenza è stato esteso alla corrispondenza informatica, oltre che dal D.Lgs. 513/97 (poi recepito nel D.P.R. 445/00), con la legge 547/93, che ha aggiunto il quarto comma dell'art. 616 codice penale, che recita « Agli effetti delle disposizioni di questa sezione, per corrispondenza s'intende quella epistolare, telegrafica o telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza ».

plicabilità, delle norme dettate in tema di segretezza della stessa, ai messaggi di posta elettronica [47].

Dubbi interpretativi riguardano in particolare le fattispecie di reato dettate agli articoli 616 e 617-*quater*, del codice penale.

Per quanto concerne l'art. 616 c.p.[48], si pone il problema di individuare se ed entro quali limiti possa considerarsi lecito l'accesso, da parte del datore di lavoro o di altri colleghi, al contenuto delle e-mail ricevute e/o spedite dal dipendente, dall'indirizzo di posta elettronica aziendale, a lui concesso in uso[49].

Fermo restando che l'analisi del problema e la ricerca di una soluzione corretta ed equilibrata, rispetto agli opposti interessi in gioco, non può essere svolta senza tenere conto di tutto quanto già premesso, dal punto di vista della tutela della privacy e dello Statuto dei Lavoratori, parte della dottrina sta sostenendo l'inapplicabilità di tale norma, rispetto ai messaggi di posta elettronica, sul presupposto che questi ultimi, non potrebbero essere definiti « corrispondenza chiusa », per la caratteristica tecnica della loro piena visibilità sia al momento dell'invio che al loro arrivo a destinazione[50].

Tale impostazione appare poco convincente se si considera che, per leggere i messaggi e-mail, è comunque necessario compiere una azione specifica di « apertura » degli stessi, anche se mediante un semplice *click*, diversamente resta immediatamente visibile soltanto l'indirizzo del mittente, l'oggetto, la data e l'ora[51]. Tanto più se si considera che, ai fini privacy ed in applicazione del D.P.R. 318/99, le misure di sicurezza da adottare obbligatoriamente impongono l'uso di un codice identificativo e di una *password* personali, che impediscono l'accesso all'elaboratore e quindi alla posta, da parte di terzi diversi dal dipendente assegnatario[52].

Quindi a meno che non si vogliano operare forzature, se da un lato difficilmente la posta elettronica può considerarsi « corrispondenza aperta », dall'altro altrettanto difficilmente potrà trattarsi solo ed esclusivamente di corrispondenza aziendale.

Infatti in mancanza di una specifica regolamentazione aziendale, che disciplini l'uso della posta, si deve dare per scontato che di questa venga

---

[47] Titolo XII, Sezione V del codice penale, ma anche l'art. 15 della Costituzione, secondo il quale « La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili ».

[48] Art. 616, comma 1, c.p. « Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prender cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero in tutto o in parte la distrugge o sopprime, è punito, se il fatto non è 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 ».

[49] Il Garante della privacy peraltro ha, già da tempo, invitato le aziende a prendere posizione chiaramente sulla possibilità o meno dell'uso privato della posta elettronica aziendale.

[50] Fa eccezione il caso in cui il messaggio sia stato criptato all'atto della spedizione: in tal caso potrebbe considerarsi integrato il presupposto di operatività di cui all'art. 616 c.p.

[51] Il fatto che i messaggi di posta siano potenzialmente visibili ai fornitori dei servizi di connessione (i cosiddetti providers) appare ipotesi oltre che remota, data la massa di cui si parla, comunque non esente dalle osservazioni svolte nel testo.

[52] Ai sensi privacy anche i colleghi sono da qualificarsi terzi rispetto ai dati del singolo interessato.

fatto anche un uso « privato », da parte dei dipendenti, in coerenza del resto con quel necessario « margine di tolleranza » richiamato dalla dottrina e dalla giurisprudenza[53].

Sussistono dubbi peraltro anche sulla possibilità, pur con una regolamentazione aziendale, di vietare del tutto l'uso privato della posta, se si tiene conto di quanto ha dichiarato la Commission Nationale de l'Informatique et des Libertés (l'Autorità francese sulla protezione dei dati CNIL), che ha pubblicato un Rapporto sulla sorveglianza elettronica dei lavoratori, in cui fa il punto della situazione in Francia e negli altri Paesi della UE, indicando alcune raccomandazioni pratiche[54].

Il Rapporto riferisce che, a differenza di quanto praticato dalle imprese, la giurisprudenza francese ha elaborato risposte molto chiare in favore della tutela della dignità del lavoratore. In particolare riporta una sentenza della Corte di Cassazione (2.10.2001) in cui si afferma che « ...il dipendente, anche durante l'orario di lavoro e sul luogo di lavoro, ha il diritto al rispetto della sua vita privata [...] il che implica, in particolare, la segretezza della corrispondenza. Il datore di lavoro non può dunque... accedere a messaggi personali inviati dal dipendente o da questi ricevuti attraverso strumenti informatici messi a disposizione del dipendente per svolgere l'attività lavorativa, anche qualora il datore di lavoro abbia preventivamente vietato l'utilizzo del computer per fini non professionali ».

Il Rapporto prosegue affermando che il divieto assoluto di utilizzare la posta elettronica, anche in base alla sentenza sopra citata, non è ammissibile. Il criterio della ragionevolezza e dell'uso socialmente accettabile appare offrire utili indicazioni. L'eventuale utilizzo da parte dell'impresa di dispositivi di controllo individuale comporta la necessità di notificare il trattamento e di conservare i dati per un periodo non eccessivo (individuato in non più di sei mesi), oltre all'esigenza di consultare i rappresentanti del personale e gli organi paritetici sopra menzionati.

Anche nella realtà italiana quindi, un adeguato regolamento aziendale dovrebbe, fermi restando gli adempimenti privacy e le procedure *ex* art. 4 Stat. Lav., stabilire il margine di tolleranza e imporre che le e-mail « private » vengano archiviate dal lavoratore, ad es. in *file* separati, in modo da evitare commistioni e consentire viceversa l'accesso a quelle professionali, per soddisfare le esigenze datoriali di organizzazione del lavoro.

La giurisprudenza italiana si è espressa sul punto una sola volta. Una recente ordinanza, che appare viceversa abbastanza « distratta »[55], ha negato, a questo proposito, la sussistenza del reato, sia per mancanza dell'elemento soggettivo del dolo nella condotta del datore di lavoro, sia sotto il profilo dell'insussistenza degli elementi oggettivi del reato. Dopo aver li-

---

[53] G. Pera, *Il licenziamento per abuso del telefono aziendale*, in *Riv. It. Dir. Lav.* 1999, pag. 652; Cfr. Corte di Cassazione, sez. Lavoro, sent. 3 aprile 2002, n. 4746, in *Guida al Lavoro*, n. 21 del 28 maggio 2002, pag. 10.

[54] Il Rapporto si basa sui risultati di uno studio e di un dibattito sull'argomento conclusosi in Francia nel marzo 2001, consultabile per estratto sul sito www.stracuzzi.it..

[55] Ord. Trib. Milano 10.05.2002 con nota critica di L. Nogler, *Guida al Lav.*, n. 22/2002.

quidato le problematiche privacy come « assolutamente inconferenti » l'ordinanza ha negato il carattere di « privatezza » dell'indirizzo di posta elettronica aziendale, in quanto « ...è inconfigurabile in astratto... un diritto all'utilizzo esclusivo di una casella di posta elettronica aziendale ». Dichiarando che l'obiettivo della *password* « non è certo quello di proteggere la segretezza dei dati personali contenuti negli strumenti a disposizione del singolo lavoratore bensì solo quella di impedire che ai predetti strumenti possano accedere persone estranee alla società », l'ordinanza ha aggiunto che « tanto meno può ritenersi che leggendo la posta elettronica contenuta sul personal computer del lavoratore si possa verificare un non consentito controllo sulle attività di quest'ultimo atteso che l'uso dell'e-mail costituisce un semplice strumento aziendale a disposizione dell'utente-lavoratore al solo fine di consentire al medesimo di svolgere la propria funzione aziendale... e che, come tutti gli altri strumenti forniti dal datore di lavoro, rimane nella completa e totale disponibilità del medesimo senza alcuna limitazione ».

L'ordinanza infine ha concluso sostenendo che l'uso privato della posta (anche se tollerato), non consente una generalizzata affermazione del principio di segretezza, poiché trattasi comunque di uso illecito che, in quanto tale, non può far attribuire, a chi lo commette, diritti di sorta.

Con riferimento all'art. 617-*quater* c.p.[56], relativo all'intercettazione telefonica e telematica, perché la fattispecie di reato possa dirsi integrata è necessario che vi sia l'intento fraudolento da parte dell'autore dell'intercettazione. Tale elemento soggettivo è ritenuto presente qualora l'intercettazione sia effettuata con modalità occulte all'insaputa dell'interessato. È evidente che tale aspetto non possa essere riscontrato *laddove l'autore dell'intercettazione fornisca un'informativa completa di tale prassi, avvallata dal consenso dell'interessato*. Rispetto, quindi, alla registrazione della posta elettronica del dipendente, da parte del datore di lavoro, è necessario predisporre un'informativa *ad hoc* da consegnare al lavoratore ed ottenere il relativo consenso, al fine di escludere l'applicabilità della fattispecie penale sopra descritta.

5. Le policy aziendali.

Nei paragrafi che precedono si è cercato di dare un quadro coordinato delle problematiche giuridiche connesse all'uso degli strumenti tecnologici in azienda, teso a sottolineare la assoluta necessità di un intervento normativo specifico, che affronti le questioni in modo unitario, trovando un punto di equilibrio tra gli opposti interessi in gioco, tutti parimenti meritevoli di tutela.

È superfluo ricordare infatti che il lavoratore ha, da un lato il diritto al rispetto della propria sfera privata e della propria dignità, dall'altro

[56] Art. 617-*quater* « Chiunque fraudolentemente intercetta comunicazioni relative a 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 o in parte, il contenuto delle comunicazioni di cui al primo comma ».

l'obbligo di svolgere le mansioni per le quali è stato assunto con diligenza e fedeltà, osservando le direttive e le istruzioni impartite dal datore di lavoro. Questi, da parte sua, ha il diritto di organizzare la propria attività produttiva come meglio ritiene opportuno e di controllare che le proprie direttive vengano osservate, allo scopo di evitare danni economici (es. contenimento dei costi), o impedire che vengano commessi reati (tramite Internet o la posta elettronica), o che vengano violati segreti aziendali ecc.

Nell'attesa di un intervento normativo *ad hoc* e ferma restando l'assoluta incertezza giurisprudenziale sopra menzionata, la redazione di appropriate *policy* aziendali appare l'unica via percorribile oggi per tentare di rispondere, con il maggior grado di specificità possibile, alla complessa ed intrecciata serie di divieti, obblighi e adempimenti stabiliti dalla legislazione vigente. Da un lato l'obbligo di informazione e gestione, richiesto dalla l. n. 675/96 e dal parere (WP48) dei Garanti europei, per quanto concerne il trattamento dei dati dei dipendenti, effettuato tramite l'uso della posta elettronica e di Internet, nonché l'adozione delle relative misure di sicurezza. Dall'altro lato la necessità di definire, dal punto di vista giuslavoristico, il controllo di carattere « meramente difensivo » sull'uso di tali strumenti aziendali ed il cosiddetto « margine di tolleranza ». Dall'altro lato ancora la necessità di stabilire, in riferimento a tale « margine », le regole relative all'uso privato della posta elettronica e di Internet.

Sotto questo profilo il Rapporto CNIL citato, oltre a quanto già detto circa la posta elettronica, fornisce altre utili indicazioni. Ad es. anche il divieto assoluto di utilizzare Internet per fini non professionali è irrealistico e quindi l'uso deve essere ragionevole, tale da non mettere a rischio la sicurezza dell'impresa né da comprometterne la produttività. È lecito, da parte dell'azienda, installare dispositivi atti a filtrare l'accesso a siti non autorizzati o prevedere, per motivi di sicurezza, il divieto di collegarsi a *forum* di discussione o *chat*. Se vengono registrati i dati di connessione (durata e siti visitati), i relativi archivi (*file log*) devono avere esclusivamente finalità di sicurezza e non di controllo del lavoratore, che deve essere informato dell'esistenza e della durata di conservazione, indicata al massimo in sei mesi. Infine il Rapporto suggerisce di nominare, in cooperazione con le rappresentanze del personale, una figura definita « delegato alla protezione dei dati ed all'utilizzo delle nuove tecnologie nell'impresa », che sarà incaricata di seguire la gestione dei dati personali in termini di sicurezza, diritto di accesso e tutela, ivi incluso il rispetto degli obblighi di notificazione all'autorità garante.

A conferma di questa linea, è interessante notare che la Svizzera, pur non rientrando nell'ambito di operatività della Direttiva 95/46/CE, ha adottato un regolamento tipo, a livello federale, che disciplina in modo organico « la sorveglianza dell'utilizzazione di Internet e della posta elettronica al posto di lavoro ».

Dopo aver descritto gli interessi dell'azienda e quelli del lavoratore, sottolinenando che « non sono utilizzati sistemi di controllo o di vigilanza per sorvegliare il comportamento del lavoratore », il regolamento passa a disciplinare l'utilizzazione di Internet e della posta elettronica. L'accesso a tali strumenti deve essere autorizzato per categorie di impiegati e l'azienda deve decidere se consentire o meno l'uso privato (esiste anche un manuale esplicativo dove, al cap. 5, sono riportati alcuni spunti di rifles-

sione per regolamentare questo aspetto). In ogni caso tale consenso deve essere dato fissando regole concrete ed inequivocabili. Devono essere descritte tutte le misure di sicurezza adottate e devono essere specificati tutti i « protocolli » utilizzati[57], ivi inclusi i file temporanei del contenuto (*cache*) ed i file permanenti di tracce dei siti visitati (*cookies*). Il regolamento vieta all'impresa di esaminare il contenuto di e-mail private[58] e raccomanda di organizzare un servizio e-mail separato, preferibilmente criptato, imponendo ai servizi informatici il rispetto della confidenzialità dei protocolli e delle liste di corrispondenza.

Le modalità ed i limiti del controllo delle violazioni della disciplina dell'uso degli strumenti e dei protocolli è dettagliato in tutti i suoi aspetti, ivi incluso quello sulla posta privata, che deve essere effettuato per campionatura casuale, in maniera anonima e limitato ad un predeterminato periodo di utilizzazione.

Viceversa il controllo degli « affari » è consentito, quindi è espressamente prevista la possibilità di prendere visione della posta elettronica di collaboratori assenti (naturalmente se si tratta della posta professionale). Se non c'è distinzione tra posta professionale e privata (indipendentemente dal fatto che sia stata autorizzata o meno) e la questione risultasse dubbia, è necessario chiarire con il dipendente e l'accesso non è considerato lecito. Il regolamento stabilisce inoltre le modalità di sorveglianza delle prestazioni, la procedura in caso di sospetto reato, le sanzioni in caso di abuso, aggiungendo che « ai fini della protezione dei dati i colleghi di lavoro della persona interessata sono considerati terzi » e che, in materia di protocolli, non esistono obblighi di conservazione, in ogni caso questa non deve superare le quattro settimane.

Infine nel caso di sorveglianza illecita da parte del datore di lavoro, il regolamento riconosce al lavoratore il diritto di avvalersi dei rimedi giuridici civili per lesione illecita della personalità (artt. 28 e ss. c.c.), di agire sul piano penale per violazione della sfera segreta o privata mediante apparecchi di rilevazione delle immagini (art. 179-*quater* c.p.) o per sottrazione di dati personali (art. 179-*novies* c.p.)[59].

ALLEGRA STRACUZZI

[57] Per protocollo si intende il « chi », « cosa », « quando » dei messaggi e-mail e della navigazione su Internet, ovvero le registrazioni di mittente, destinatario, data, ora, indirizzo del sito ecc.

[58] Se il nome dell'utente ed il protocollo non sono separabili è raccomandato l'uso di uno pseudonimo.

[59] Rientrano nella sorveglianza illecita anche la valutazione con identificazione di persone dei protocolli senza constatazione di abuso, la consultazione del contenuto della posta elettronica privata, come anche l'impiego dei programmi spia.