5401/01/IT/def.
WP 55

Documento di lavoro

riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro

Adottato il 29 maggio 2002

Commenti:

* i capitoli relativi ai diversi paesi potranno subire ulteriori cambiamenti decisi di concerto con le delegazioni nazionali

Il gruppo di lavoro è stato costituito in applicazione dell'articolo 29 della direttiva 95/46/CE in quanto organismo europeo indipendente con finalità consultive che si occupa di protezione dei dati e di riservatezza. I suoi compiti sono descritti nell'articolo 30 della direttiva 95/46/CE e nell'articolo 14 della direttiva 97/66/CE.

Alle funzioni di segretariato provvede la Direzione A (Funzionamento ed impatto del mercato interno - Coordinamento - Protezione dei dati) della Direzione generale Mercato interno della Commissione europea, B-1049 Bruxelles, Belgio, ufficio n. C100-6/136.

Sito Web: www.europa.eu.int/comm/privacy

IL GRUPPO DI LAVORO IN TEMA DI PROTEZIONE DEGLI INDIVIDUI PER QUANTO RIGUARDA IL TRATTAMENTO DEI DATI PERSONALI,

costituito in applicazione della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995[1],

visto l'articolo 29 e l'articolo 20, paragrafo 1, lettera a) e paragrafo 3 di detta direttiva,

visto il proprio regolamento interno, in particolare gli articoli 12 e 14,

ha adottato il presente documento di lavoro:

[1] Gazzetta ufficiale L 281 del 23/11/1995, pag. 31, reperibile sul sito:

http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

Documento di lavoro del gruppo di lavoro ex articolo 29[2] riguardante la vigilanza ed i controlli sulle comunicazioni elettroniche effettuate dal posto di lavoro

Progetto di riepilogo

Il presente documento di lavoro integra il parere 8/2001 sul trattamento dei dati personali nel contesto dell'occupazione[3] e contribuisce a rendere uniforme l'applicazione dei provvedimenti nazionali presi nell'ambito della direttiva sulla protezione dei dati 95/46/CE[4]. Esso non pregiudica l'applicazione alla protezione dei dati delle normative nazionali attinenti a detta protezione.

Per studiare tale problematica il gruppo di lavoro ex articolo 29 ha costituito un sottogruppo[5] ed adottato un **documento d'ampia portata** reperibile sull'Internet al seguente indirizzo[6]:

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

Nel presente documento di lavoro il gruppo di lavoro ex articolo 29 esamina la questione dei controlli e della vigilanza sulle comunicazioni elettroniche effettuate

---

[2] Il gruppo di lavoro ex articolo 29 è un gruppo consultivo composto da rappresentanti delle autorità competenti per la protezione dei dati nei diversi Stati membri, il quale agisce in modo autonomo ed ha tra l'altro il compito di esaminare qualsiasi questione riguardante l'applicazione dei provvedimenti nazionali presi in applicazione della direttiva sulla protezione dei dati allo scopo di contribuire a renderne uniforme l'applicazione.

[3] Parere approvato il 13 settembre 2001 e reperibile al seguente indirizzo Internet:

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48en.pdf. Tale parere contiene un'analisi approfondita sull'applicazione al trattamento di dati personali riguardanti attività connesse all'occupazione delle disposizioni della direttiva sulla protezione dei dati (in particolare gli articoli 6, 7 ed 8).

[4] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati; GU L 281 del 23.11.95, pag. 31.

[5] All'attività di tale sottogruppo hanno contribuito le autorità competenti per la sorveglianza di: AT, BE, DE, ES, FR, IR, IT, NL, UK.

[6] Il documento comprende un allegato che riporta le disposizioni più importanti in tema di protezione dei dati vigenti negli Stati membri tali da ripercuotersi in certa misura sulle attività di vigilanza e di controllo delle comunicazioni elettroniche sul posto di lavoro.

dal posto di lavoro, cioè del controllo da parte del datore di lavoro della posta elettronica e dell'impiego d'Internet fatto dai dipendenti.

Alla luce della giurisprudenza della Corte europea dei diritti umani riguardante l'articolo 8 della convenzione per la protezione dei diritti umani e delle libertà fondamentali nonché di altri testi pertinenti di diritto internazionale e delle disposizioni della direttiva 95/46/CE il presente documento di lavoro offre indirizzi interpretativi ed esempi concreti circa quanto costituisce attività legittima di controllo e circa i limiti accettabili della vigilanza sui dipendenti esercitata dal datore di lavoro. Si osservi che in alcuni Stati membri la legislazione può prescrivere livelli di tutela più elevati di quelli contemplati dal presente documento di lavoro.

Quando al mattino si recano a lavorare i lavoratori non abbandonano fuori dell'ufficio o della fabbrica i loro diritti alla riservatezza ed alla protezione dei dati. Essi possono legittimamente attendersi di usufruire di un certo grado di riservatezza sul posto di lavoro, visto che una parte significativa delle loro relazioni con altri essere umani si sviluppa nell'ambiente di lavoro. Questo diritto è tuttavia controbilanciato da altri diritti ed interessi legittimi del datore di lavoro; quest'ultimo ha in particolare il diritto di gestire la sua azienda con una certa efficienza, ma soprattutto il diritto di tutelarsi contro le responsabilità od i danni cui possono dare origine gli atti dei lavoratori. Questi diritti ed interessi costituiscono motivi legittimi atti a giustificare opportuni provvedimenti volti a limitare i diritti del dipendente alla riservatezza. A questi effetti l'esempio più chiaro è dato dai casi in cui il datore di lavoro è vittima di un atto perseguibile penalmente del dipendente.

Per trovare l'equilibrio tra diritti ed interessi diversi occorre tuttavia tener conto di vari principi, ed in particolare di quello della proporzionalità. Dovrebbe essere ovvio che la semplice idoneità presunta di un'attività di controllo e sorveglianza a servire gli interessi del datore di lavoro non basta da sola a giustificare qualsiasi intrusione nella sfera privata del dipendente. Prima di venir applicato sul posto di lavoro qualsiasi provvedimento di controllo deve superare una serie di prove, descritte in modo particolareggiato nel presente documento di lavoro.

La natura di tale valutazione può riassumersi nelle seguenti domande:

a) l'attività di controllo risulta trasparente per i dipendenti?

b) tale attività è necessaria, oppure il datore di lavoro potrebbe ottenere gli stessi risultati con metodi tradizionali di sorveglianza?

c) il trattamento dei dati personali proposto risulta equo nei confronti dei lavoratori?

d) detto trattamento risulta commisurato alle preoccupazioni che cerca di sopire?

Concentrandosi sull'applicazione pratica di tali principi il presente documento di lavoro fornisce un indirizzo per stabilire i contenuti delle politiche perseguite dalle imprese in tema d'impiego della posta elettronica e dell'Internet che datori di lavoro e dipendenti possano considerare una base minima per un'ulteriore elaborazione (tenendo conto delle caratteristiche particolari di una data impresa, delle sue dimensioni e della normativa nazionale nei settori connessi alla protezione dei dati).

Nell'esaminare l'impiego dell'Internet per fini privati il gruppo di lavoro ex articolo 29 è del parere che **prevenire gli abusi debba considerarsi più importante che**

individuarli, ovverosia che l'interesse del datore di lavoro sia servito meglio prevenendo gli abusi dell'Internet piuttosto che individuando i casi in cui essi hanno luogo. In questo contesto risultano di particolare utilità le soluzioni di natura tecnologica. Un divieto globale per i dipendenti d'impiegare Internet a fini personali appare irragionevole e non tiene conto del grado in cui l'Internet può aiutarli nella vita di tutti i giorni.

Il gruppo di lavoro desidera dar risalto all'importanza fondamentale del fatto che il datore di lavoro informi il dipendente in merito (i) alla presenza, all'impiego ed alla finalità di qualsiasi apparecchiatura e/o dispositivo di rilevamento messi in funzione per quanto riguarda la stazione di lavoro del dipendente, e (ii) agli abusi dei mezzi elettronici di comunicazione (posta elettronica od Internet) eventualmente individuati, a meno che ragioni di sufficiente importanza non giustifichino una prosecuzione della sorveglianza in segreto[7], il che di norma non si verifica. Il software può fornire con facilità e rapidità le informazioni del caso, grazie ad esempio ad una finestra che avvisi il dipendente del fatto che il sistema ha rilevato un impiego non autorizzato della rete e/o ha preso provvedimenti per impedirlo.

A titolo di raccomandazione pratica si può considerare la possibilità che i datori di lavoro forniscano ai dipendenti due linee di posta elettronica:

a) la prima, per scopi puramente professionali, soggetta a possibili controlli nei limiti stabiliti dal presente documento di lavoro,

b) la seconda linea, destinata a scopi puramente privati (eventualmente sostituibile dall'autorizzazione ad impiegare la posta elettronica), sarebbe sottoposta unicamente ai normali provvedimenti di sicurezza e controllata solo in casi eccezionali per individuare eventuali abusi.

Il gruppo di lavoro ex articolo 29 ha rilevato alcune divergenze tra le normative nazionali attinenti alla protezione dei dati, che riguardano soprattutto le deroghe consentite al diritto fondamentale alla segretezza della corrispondenza ovvero il campo d'applicazione e gli effetti dei sistemi collettivi di rappresentazione e codecisione dei dipendenti. Cionondimeno il gruppo di lavoro non ha rilevato tra le normative nazionali attinenti alla protezione dei dati divergenze tali da costituire seri ostacoli alla definizione di un'impostazione comune, ed ha quindi pubblicato il presente documento di lavoro che sarà sottoposto a revisione negli anni 2002-2003 alla luce dell'esperienza compiuta e dei progressi registrati in questo campo.

---

[7] Un buon esempio sarebbe quello di casi di controllo occulto debitamente giustificato.

1. LA VIGILANZA SUL POSTO DI LAVORO - UNA SFIDA PER LA SOCIETÀ

La vigilanza sui lavoratori ha recentemente attirato una considerevole attenzione da parte dei mezzi di comunicazione ed è attualmente oggetto di un dibattito pubblico nella Comunità. Effettivamente la graduale introduzione nell'intera Comunità della posta elettronica sul posto di lavoro ha attirato l'attenzione di datori di lavoro e dipendenti sul rischio di una violazione della sfera privata sul posto di lavoro.

Nell'esaminare il problema della vigilanza occorre tener sempre presente che per quanto i lavoratori abbiano il diritto ad una certa *privacy* sul posto di lavoro tale diritto va controbilanciato con quello del datore di lavoro a controllare il funzionamento della sua impresa ed a difendersi contro atti dei dipendenti che rischino di porre a repentaglio suoi interessi legittimi (ad esempio quando la responsabilità del datore di lavoro sia chiamata in questione per le azioni dei dipendenti).

Se è vero che le nuove tecnologie costituiscono un'evoluzione positiva per quanto riguarda le risorse a disposizione dei datori di lavoro, gli strumenti di vigilanza elettronica si prestano ad essere utilizzati in modi che ledono i diritti e le libertà fondamentali dei dipendenti. Non va dimenticato che con l'arrivo delle tecnologie dell'informazione è di vitale importanza che i lavoratori godano tutti degli stessi diritti, indipendentemente dal fatto che lavorino in linea o no.

Va parimenti dato risalto al fatto che l'evoluzione delle condizioni di lavoro rende oggi più difficile stabilire una netta separazione tra le ore di lavoro e la vita privata. In particolare con lo sviluppo dell'"ufficio in casa" molti dipendenti continuano a lavorare a casa utilizzando infrastrutture informatiche messe o no a loro disposizione dal datore di lavoro a tale scopo.

La dignità umana del lavoratore va anteposta a qualsiasi altra considerazione. Nell'esaminare questo problema è importante non dimenticarsi di questo fatto e degli effetti negativi che le attività di vigilanza possono produrre sulla qualità della relazione professionale tra i dipendenti ed il datore di lavoro nonché il lavoro stesso.

In considerazione di tutti questi fattori non è sorprendente che questa problematica sia in primo piano nel dibattito pubblico, ed urge contribuire ad interpretare uniformemente alla luce della recente giurisprudenza della Corte europea dei diritti umani le disposizioni della direttiva 95/46/CE e quelle con le quali essa è recepita nelle legislazioni nazionali.

Il gruppo di lavoro è quindi del parere che sarebbe utile far parte delle informazioni e delle raccomandazioni che figurano nel seguito al settore pubblico ed a quello privato. Giova rilevare che il presente documento di lavoro copre qualsiasi attività riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro (tanto il controllo in tempo reale quanto l'accesso ai dati archiviati).

2. STRUMENTI GIURIDICI INTERNAZIONALI

2.1 ARTICOLI 8 E 10 DELLA CONVENZIONE EUROPEA PER LA SALVAGUARDIA DEI DIRITTI DELL'UOMO E DELLE LIBERTÀ FONDAMENTALI

Articolo 8.

1. Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza.

2. Non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto se non laddove tale ingerenza sia contemplata dalla legge in quanto provvedimento che, in una società democratica, risulti necessario per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui.

Articolo 10.

1. Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni od idee senza ingerenza alcuna da parte delle autorità pubbliche ed indipendentemente dalle frontiere. Il presente articolo non impedisce che gli Stati sottopongano ad un regime di autorizzazione le imprese di radiodiffusione, di cinema o di televisione.

2. L'esercizio di queste libertà, comportando doveri e responsabilità, può essere sottoposto a determinate formalità, condizioni, restrizioni o sanzioni disposte dalla legge e necessarie in una società democratica per la sicurezza nazionale, l'integrità territoriale o l'ordine pubblico, la prevenzione di disordini e reati, la protezione della salute o della morale, la protezione della reputazione o dei diritti altrui, oppure per impedire la divulgazione d'informazioni confidenziali oppure ancora per garantire l'autorità e l'imparzialità del potere giudiziario.

Tutti gli Stati membri e l'Unione europea sono vincolati dalle disposizioni della convenzione europea per la salvaguardia dei diritti umani e delle libertà fondamentali. Tradizionalmente questi diritti sono stati esercitati in senso verticale (vale a dire dall'individuo nei confronti dello Stato), ma attualmente è in corso un dibattito riguardante la misura in cui essi possano essere esercitati in senso orizzontale (vale a dire tra individui). È tuttavia chiaro che questi diritti sono in linea di massima ben reali.

Il gruppo di lavoro è quindi del parere che, all'atto di esaminare l'applicazione dei provvedimenti nazionali presi nell'ambito della direttiva 95/46/CE allo scopo di contribuire all'applicazione uniforme di detti provvedimenti, occorra rifarsi ai principi più importanti espressi dall'attuale giurisprudenza della Corte europea dei diritti umani in rapporto a tale disposizione, in particolare per quanto riguarda la segretezza della corrispondenza.

Nelle sentenze sinora pronunciate la Corte ha reso chiaro che dalla protezione della "vita privata" sancita dall'articolo 8 non esulano la vita professionale in quanto lavoratore dipendente né la vita al di fuori delle mura domestiche.

Il caso **Niemitz contro Germania** riguardava la perquisizione dell'ufficio del ricorrente effettuata da un'autorità governativa. Il governo ha provato ad argomentare che l'articolo

8 non garantisce alle persone la protezione contro la perquisizione del loro ufficio dato che la convenzione opera una netta distinzione tra vita privata e mura domestiche da un lato e vita professionale e locali destinati all'attività professionale dall'altro.

La Corte ha respinto questa tesi dichiarando:

"Del rispetto della vita privata deve parimenti far parte in certa misura il diritto di stabilire e sviluppare relazioni con altri esseri umani. ***Non sembra inoltre esservi alcuna ragione di principio per la quale si debba considerare tale interpretazione della nozione "vita privata" tale da escludere attività di natura professionale o commerciale****, giacché dopo tutto è nel corso della propria vita lavorativa che la maggior parte delle persone ha una possibilità significativa, se non la più significativa, di sviluppare relazioni con il mondo esterno. Questa tesi è confortata dal fatto che, come la Commissione ha correttamente fatto rilevare, non è sempre possibile distinguere chiaramente quali tra le attività svolte da un individuo rientrino nell'ambito della sua vita professionale o commerciale e quali no"*[8]

Più precisamente, nel caso **Halford contro Regno Unito** la Corte ha statuito che l'intercettazione delle chiamate telefoniche svolte dai dipendenti sul posto di lavoro costituisce una violazione dell'articolo 8 della convenzione. Un particolare interessante è costituito dal fatto che la sig.ra Halford disponesse di due telefoni, uno dei quali era destinato all'impiego privato. L'impiego di tali telefoni non era soggetto ad alcuna restrizione né oggetto di alcuna istruzione.

La sig.ra Halford sosteneva che l'intercettazione delle sue chiamate telefoniche configurasse una violazione dell'articolo 8 della convenzione. Il governo proponeva la tesi che per le chiamate telefoniche effettuate dalla sig.ra Halford dal suo posto di lavoro non valesse la protezione accordata dall'articolo 8 poiché lei non poteva avere alcuna ragionevole aspettativa di riservatezza in relazione a tali chiamate. Nel corso dell'audizione in tribunale gli avvocati del governo hanno espresso il parere che un datore di lavoro debba in linea di massima avere la possibilità di controllare, senza informarne preventivamente il dipendente, le chiamate fatte da quest'ultimo sui telefoni messi a sua disposizione dal datore di lavoro.

A parere della Corte tuttavia *"risulta chiaro dalla giurisprudenza che le chiamate telefoniche effettuate da sedi commerciali possano, alla pari di quelle effettuate da casa, rientrare nell'ambito delle nozioni di "vita privata" e "corrispondenza" a termini dell'articolo 8, paragrafo 1 (omissis).*

Non vi sono elementi atti a provare che la sig.ra Halford, in quanto utente del sistema interno di telecomunicazioni, abbia ricevuto un avviso di qualunque tipo circa il fatto che le chiamate effettuate a partire da tale sistema potessero essere oggetto d'intercettazioni. A parere della Corte lei poteva ragionevolmente attendersi una certa riservatezza per tali chiamate…".[9]

Nella nozione di "corrispondenza" rientrano non soltanto lettere scritte su carta, ma anche altre forme di comunicazione elettronica ricevute sul posto di lavoro o da esso

---

[8] 23 novembre 1992, serie A n. 251/B, paragrafo 29; grassetto aggiunto in sede di redazione

[9] 27 maggio 1997.

inviate, quali chiamate telefoniche effettuate a partire da sedi commerciali od in esse ricevute ovvero *e-mails* ricevuti od inviati per mezzo dei *computers* dell'ufficio.

Alcuni interpreti fanno notare che ciò sembra anche implicare che (per quanto questo non fosse precisato nella sentenza) se un dipendente è avvisato in anticipo dal datore di lavoro circa la possibilità d'intercettazione delle sue comunicazioni egli possa perdere le sue aspettative di riservatezza con la conseguenza che in tal caso le intercettazioni non costituirebbero una violazione dell'articolo 8 della convenzione. Il gruppo di lavoro non è del parere che il fatto di avvisare in anticipo il dipendente sia sufficiente a giustificare qualsiasi infrazione dei suoi diritti in tema di protezione dei dati.

In termini più generali, dalla giurisprudenza relativa all'articolo della convenzione europea per la salvaguardia dei diritti umani e delle libertà fondamentali possono evincersi tre principi:

a) I lavoratori hanno una legittima aspettativa di riservatezza sul posto di lavoro, che non è pregiudicata dal fatto che essi usino mezzi di comunicazione o qualsiasi altra infrastruttura commerciale di proprietà del datore di lavoro.

   Tuttavia il fatto che il datore di lavoro fornisca ad un dipendente informazioni adeguate al proposito può ridurre le legittime aspettative di riservatezza di quest'ultimo.

b) Il principio generale di segretezza della corrispondenza copre le comunicazioni sul posto di lavoro, ed in questo ambito rientrano plausibilmente la posta elettronica ed i *files* ad essa acclusi.

c) La tutela della vita privata comprende in certa misura anche il diritto a stabilire e sviluppare relazioni con altri esseri umani. Il fatto che tali relazioni interessino in larga misura l'ambiente di lavoro pone alcuni limiti alle legittime esigenze del datore di lavoro in fatto di provvedimenti di vigilanza.

L'articolo 10 risulta parimenti rilevante, per quanto in misura minore, giacché disciplina la libertà d'espressione e quella d'informazione e sancisce il diritto dell'individuo a ricevere ed a fornire informazioni ed idee senza interferenze delle autorità pubbliche. La rilevanza dell'articolo 10 sembra trovare espressione nelle considerazioni formulate dalla Corte nel già menzionato caso Niemitz contro Germania. Come ha dichiarato la Corte, sul posto di lavoro le persone sviluppano una parte significativa delle loro relazioni con il mondo esterno ed è quindi indubbio che in tale contesto il loro diritto alla libertà di espressione abbia un ruolo da svolgere.

2.2 CONVENZIONE SULLA PROTEZIONE DELLE PERSONE RISPETTO AL TRATTAMENTO AUTOMATIZZATO DI DATI DI CARATTERE PERSONALE (OIL/108)

Tale convenzione è stata aperta alla firma il 28 gennaio 1981 ed ha costituito il primo strumento giuridico legalmente vincolante nel campo della protezione dei dati. Nell'ambito della convenzione i firmatari sono tenuti a fare quanto necessario nell'ambito della loro legislazione nazionale per applicare i principi stabiliti dalla

convenzione così da garantire che sul loro territorio siano rispettati i diritti umani fondamentali di tutti gli individui per quanto riguarda il trattamento dei dati personali[10].

Altri importanti documenti riguardanti la convenzione 108 che hanno rilievo in questo contesto sono:

- la raccomandazione (89) 2 del Consiglio d'Europa sulla protezione dei dati personali utilizzati a fini d'occupazione[11];
- la raccomandazione (97) 5 del Consiglio d'Europa sulla protezione dei dati di natura medica[12];
- la raccomandazione (86) 1 del Consiglio d'Europa sulla protezione dei dati personali utilizzati a fini previdenziali [13];
- la raccomandazione (95) 4 del Consiglio d'Europa sulla protezione dei dati personali nel campo dei servizi di telecomunicazione, con particolare riferimento ai servizi telefonici.

2.3. CARTA DEI DIRITTI FONDAMENTALI DELL'UNIONE EUROPEA

Articolo 7. ***Rispetto della vita privata e della vita familiare.***

Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.

Articolo 8. ***Protezione dei dati a carattere personale.***

1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o ad un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

La carta dei diritti fondamentali dell'Unione europea sembra seguire nelle grandi linee i principi stabiliti dalla Corte europea dei diritti umani; il concetto di segretezza della corrispondenza è stato ampliato ed è diventato il concetto di "segretezza delle comunicazioni" di nuova generazione, con cui si mira a garantire alle comunicazioni elettroniche un grado di protezione identico a quello tradizionalmente goduto dalla posta.

---

[10] Si veda anche la raccomandazione (89) 2 del Consiglio d'Europa sulla protezione dei dati personali utilizzati ai fini di occupazione, reperibile in inglese o francese sul sito: http://cm.coe.int/ta/rec/1989/89r2.htm

[11] Reperibile sul sito http://cm.coe.int/ta/rec/1989/89r2.htm

[12] Reperibile sul sito http://cm.coe.int/ta/rec/1997/97r5.html

[13] Reperibile sul sito http://www.legal.coe.int/dataprotection/Default.asp?fd=rec&fn=R(86)1E.htm

Accordando alla protezione dei dati una natura sostanzialmente differenziata l'articolo 8, integra inoltre la protezione concessa dall'articolo 7. Questo risultato riveste particolare importanza per quanto riguarda la questione dei controlli sulla posta elettronica.

2.4. UFFICIO INTERNAZIONALE DEL LAVORO (UIL)

Il codice di condotta in tema di protezione dei dati personali dei lavoratori (1997) stilato dall'Ufficio internazionale del lavoro stabilisce quanto segue:

"5. Principi d'indole generale

5.1. I dati personali vanno trattati nel rispetto delle leggi ed in modo corretto, nonché unicamente per motivi direttamente pertinenti all'occupazione del dipendente.

5.2. In linea di massima i dati personali vanno utilizzati unicamente per gli scopi per i quali sono stati originariamente raccolti.

5.3. Se s'intende trattare dati di natura personale per finalità diverse da quelle per le quali essi sono stati originariamente raccolti il datore di lavoro dovrà garantire che essi non vengano impiegati in modo incompatibile con dette finalità originarie e dovrà prendere i provvedimenti del caso per evitare qualsiasi errore d'interpretazione causato da un cambiamento di contesto.

5.4. I dati di natura personale raccolti in relazione a provvedimenti di carattere tecnico od organizzativo volti a garantire la sicurezza ed il corretto funzionamento di sistemi informatici automatizzati non devono essere impiegati per controllare il comportamento dei lavoratori.

5.5. Le decisioni relative ad un dipendente non devono essere basate unicamente sul trattamento automatico dei dati di natura personale relativi a tale dipendente.

5.6. I dati di natura personale raccolti per mezzo di controlli elettronici non devono costituire gli unici fattori presi in considerazione ai fini della valutazione delle prestazioni di un dipendente.

(Omissis)

6.14.

(1) Qualora siano soggetti a vigilanza i dipendenti andranno informati in anticipo delle ragioni di tale vigilanza, del calendario, del metodo e delle tecniche impiegati e dei dati che s'intende raccogliere; il datore di lavoro deve inoltre ridurre al minimo l'invasione della sfera privata dei dipendenti.

(2) Controlli segreti saranno consentiti unicamente qualora:

a) risultino conformi alla legislazione nazionale, ovvero

b) vi siano ragionevoli motivi per sospettare un'attività criminale od altri gravi misfatti.

(3) Una vigilanza continua andrà consentita unicamente qualora risulti necessaria per finalità sanitarie e di sicurezza ovvero per la protezione di beni materiali.

(Omissis)

12.2. Laddove esistano e garantendo il rispetto delle legislazioni e delle prassi nazionali, i rappresentanti dei lavoratori andranno informati e consultati:

a) in merito all'introduzione od alla modifica di sistemi automatizzati che trattino i dati di natura personale relativi ai dipendenti,

b) prima che venga introdotta qualsiasi forma di vigilanza elettronica sul comportamento dei lavoratori sul posto di lavoro

c) circa le finalità, i contenuti ed il modo di distribuire e d'interpretare eventuali questionari e tests relative ai dati personali dei lavoratori".

3. SORVEGLIANZA E CONTROLLO DELLE COMUNICAZIONI ELETTRONICHE SUL POSTO DI LAVORO NEL CONTESTO DELLA DIRETTIVA 95/46/CE

Il seguente documento di lavoro si basa sull'applicazione dei principi che figurano nella direttiva 95/46/CE in rapporto alla problematica in questione, tenendo conto dell'articolo 8 della Convenzione europea per la protezione dei diritti umani e delle libertà fondamentali il quale prescrive il rispetto della corrispondenza nonché della vita privata.

Sul posto di lavoro il datore di lavoro può disporre di molte forme di vigilanza, ciascuna delle quali presenta specifici problemi. Il presente documento verte su due di tali forme, per le quali valgono principi analoghi: il controllo della posta elettronica e la sorveglianza dell'accesso ad Internet.

Punto di partenza è la conferma di quanto stabilito nel parere 8/2001, secondo il quale la direttiva 95/46/CE si applica all'elaborazione di dati personali nel contesto di un'attività di lavoro dipendente come in qualsiasi altro contesto[14]. Oltre alla direttiva 95/46/CE, di portata più generale, può avere rilievo anche la direttiva 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni. Tale direttiva completa nei dettagli ed integra la direttiva 95/46/CE per quanto riguarda l'elaborazione dei dati personali nel settore delle telecomunicazioni. Oltre che nel campo d'applicazione della direttiva 95/46/CE il controllo delle comunicazioni elettroniche, inclusi *e-mail* ed accessi ad Internet, da parte dei datori di lavoro può così rientrare, o, anche in quello della direttiva 97/66/CE, attualmente oggetto di revisione nel contesto della revisione più generale della normativa comunitaria sulle telecomunicazioni. Nei casi cui si applica tale direttiva possono rivestire particolare importanza l'articolo 5 (che verte sulla riservatezza delle comunicazioni) e l'articolo 6 (sui dati relativi alle chiamate ed alla fatturazione).

3.1 PRINCIPI D'INDOLE GENERALE APPLICABILI AL CONTROLLO DELLA POSTA ELETTRONICA E DELL'INTERNET

I principi enunciati nel seguito in merito alla tutela dei dati sono tratti dalla direttiva 95/46/CE e vanno applicati quando si debba prendere in esame il trattamento dei dati personali nell'ambito dei controlli in questione. Il rispetto di tutti i principi che seguono è indispensabile perché qualsiasi attività di controllo risulti legittima e giustificata.

3.1.1. NECESSITÀ

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. A tal fine occorre prendere in attenta considerazione metodi tradizionali di vigilanza, tali da rappresentare una minore intrusione nella sfera privata delle persone, facendovi eventualmente ricorso prima d'impegnarsi in qualsiasi forma di controllo delle comunicazioni elettroniche.

Il controllo della corrispondenza di un lavoratore o del suo impiego dell'Internet può ritenersi necessario unicamente in circostanze eccezionali. Il controllo della posta

[14] Reperibile sul sito http: //europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48en.pdf

elettronica di un lavoratore può ad esempio risultare necessario per ottenere conferma o prova del fatto che esso abbia compiuto determinate azioni, tra le quali rientrerebbe un'eventuale attività criminosa del lavoratore, se ed in quanto ciò risulta indispensabile al datore di lavoro per difendere i propri interessi come ad esempio nel caso in cui abbia una responsabilità subordinata per le azioni del lavoratore. Tra le attività lecite rientrerebbe altresì la rilevazione della presenza di virus informatici e più generalmente qualsiasi attività del datore di lavoro mirante a garantire la sicurezza del sistema.

Giova ricordare che l'apertura della posta elettronica di un dipendente può rendersi necessaria anche per motivi diversi dal controllo e dalla vigilanza, come quello di mantenere lo scambio di corrispondenza nel caso in cui il dipendente sia assente (ad esempio per malattia o per ferie) e non vi sia altro modo (come la funzione *autoreply* o l'inoltro automatico) per ottenere tale risultato.

Il principio della necessità comporta altresì l'obbligo per un datore di lavoro di non conservare i dati per un tempo più lungo di quello necessario allo scopo dichiarato dell'attività di controllo.

3.1.2. FINALITÀ

Questo principio si riferisce al fatto che i dati vanno raccolti per uno scopo determinato, esplicito e legittimo, evitando di trattarli in un secondo momento in modo incompatibile con tali finalità. In questo contesto il riferimento al principio di compatibilità significa ad esempio che qualora l'elaborazione dei dati sia giustificata per motivi attinenti alla sicurezza del sistema i dati così elaborati non potranno in un secondo momento venir trattati per un altro scopo, quale ad esempio il controllo del comportamento del dipendente.

3.1.3. TRASPARENZA

Questo principio comporta l'obbligo per il datore di lavoro di essere chiaro ed aperto circa le sue attività; non è consentito alcun controllo occulto della posta elettronica da parte del datore di lavoro, fatti salvi i casi in cui una legge dello Stato membro lo consenta nell'ambito dell'articolo 13 della direttiva[15]. Ciò ha maggiore probabilità di verificarsi nei casi in cui si è individuata una specifica attività criminosa (in rapporto alla necessità di ottenere degli elementi di prova e in subordine al rispetto delle norme giuridiche e procedurali degli Stati membri), ovvero in cui le disposizioni nazionali che stabiliscono le necessarie salvaguardie autorizzino il datore di lavoro ad agire in un certo modo per rilevare eventuali infrazioni alla legge sul posto di lavoro.

Tale principio può altresì scindersi in due aspetti distinti:

3.1.3.1. OBBLIGO DI FORNIRE INFORMAZIONI AL TITOLARE DEI DATI

Questo costituisce forse l'esempio più rilevante di applicazione pratica del principio della trasparenza alla problematica in questione. Esso comporta per il datore di lavoro l'obbligo di fornire ai suoi dipendenti una dichiarazione

[15] L'articolo 13 della direttiva consente agli Stati membri di prendere provvedimenti legislativi per restringere il campo d'applicazione degli obblighi e dei diritti stabiliti da alcuni articoli della direttiva laddove questa restrizione costituisca un provvedimento necessario a salvaguardare importanti interessi pubblici quale la sicurezza nazionale oppure la necessità di prevenire, indagare, rilevare e perseguire reati, oppure ancora la protezione dei titolari dei dati ovvero dei diritti e delle libertà altrui.

prontamente accessibile, chiara ed accurata della politica che persegue in tema di controlli della posta elettronica e dell'Internet.

Ai dipendenti andrà offerta un'informazione completa circa le circostanze specifiche atte a giustificare un tale provvedimento eccezionale, ed inoltre circa l'ampiezza e il campo d'applicazione di tali controlli. Tra queste informazioni dovrebbero figurare elementi quali:

1. la politica aziendale in tema di *e-mail* ed Internet, con una descrizione particolareggiata della misura in cui infrastrutture di comunicazione di proprietà dell'impresa stessa possono venir utilizzate dai dipendenti per comunicazioni personali o private (ad esempio limiti di tempo e durata dell'impiego);

2. motivi e finalità di un'eventuale attività di vigilanza; laddove il datore di lavoro abbia espressamente consentito l'impiego delle infrastrutture di comunicazione dell'impresa per fini privati le comunicazioni private possono in un numero estremamente ridotto di casi essere sottoposte a sorveglianza, ad esempio per garantire la sicurezza del sistema d'informazione (rilevamento della presenza di virus informatici);

3. particolari dei provvedimenti presi, vale a dire chi, cosa, come, quando;

4. particolari di qualsiasi procedura volta a garantire il rispetto delle regole, con indicazione del modo e del momento in cui ai dipendenti possono venir notificate eventuali infrazioni alle politica aziendale e delle possibilità loro offerte di rispondere alle accuse eventualmente mosse contro di loro.

Il gruppo di lavoro desidera a questo proposito fare rilevare che sotto il profilo pratico è consigliabile che il datore di lavoro informi immediatamente il dipendente di qualsiasi uso improprio delle comunicazioni elettroniche rilevato, a meno che importanti motivi non giustifichino la prosecuzione della sorveglianza[16], il che non si verifica. Per fornire facilmente e con rapidità le informazioni richieste si può ricorrere a dispositivi software quali finestre contenenti avvertimenti, che appaiono improvvisamente sullo schermo avvisando il dipendente che il sistema ha rilevato un uso non autorizzato della rete. In tal modo è possibile risolvere un numero sorprendentemente elevato di malintesi.

Un ulteriore esempio del principio di trasparenza è la pratica dei datori di lavoro d'informare e/o consultare i rappresentanti dei lavoratori prima d'introdurre politiche che tocchino questi ultimi. Giova far notare che le decisioni in tema di controlli sui dipendenti, inclusa la sorveglianza delle comunicazioni elettroniche da essi effettuate o ricevute, rientrano nel campo d'applicazione della recente direttiva 2002/14/CE purché vi rientri anche l'impresa interessata. La direttiva stabilisce in particolare la necessità d'informare e consultare i dipendenti in merito alle decisioni atte a determinare cambiamenti sostanziali nell'organizzazione del lavoro o nelle relazioni contrattuali. La legislazione nazionale od accordi collettivi possono stabilire modalità operative che risultino ancor più favorevoli ai dipendenti.

---

16 Un buon esempio di ciò è fornito dai casi di controlli occulti debitamente giustificati.

Gli accordi collettivi possono non solo obbligare il datore di lavoro ad informare e consultare i rappresentanti dei lavoratori prima di avvalersi di sistemi di vigilanza, ma anche subordinare quest'ultimo provvedimento alla preliminare approvazione dei rappresentanti dei lavoratori.

Gli accordi collettivi possono parimenti stabilire il campo d'applicazione e la portata dell'impiego dell'Internet e della posta elettronica consentito ai dipendenti, nonché particolari relativi al controllo di tale impiego.

3.1.3.2. OBBLIGO D'INFORMARE LE AUTORITÀ DI VIGILANZA PRIMA DI PROCEDERE A QUALSIASI OPERAZIONE DI TRATTAMENTO DEI DATI PARZIALMENTE OD INTEGRALMENTE AUTOMATICA O QUALSIASI SERIE DI TALI OPERAZIONI.

Questo costituisce un altro modo per garantire la trasparenza perché i lavoratori possono sempre verificare nei registri relativi alla protezione dei dati ad esempio quali siano le categorie dei dati, le finalità ed i destinatari che si presumono interessati dall'attività di elaborazione di dati personali dei dipendenti svolta dal datore di lavoro.

3.1.3.3. DIRITTO D'ACCESSO

In forza della direttiva 95/46/CE[17] un lavoratore dipendente ha, alla pari di qualsiasi altra persona, il diritto di accedere ai dati personali che lo riguardano trattati dal suo datore di lavoro ed all'occorrenza di richiedere la rettifica o la cancellazione od il congelamento dei dati che non ottemperino alle disposizioni della direttiva, in particolare a causa del loro carattere incompleto od inesatto.

La possibilità per i dipendenti di accedere senza costrizioni agli schedari elettronici dei datori di lavoro ad intervalli ragionevoli e senza ritardi o spese eccessive costituisce un potente strumento di cui si può avvalere il singolo dipendente per garantire che le attività di controllo sul posto di lavoro restino

---

[17] Articolo 12: gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento:

a) liberamente e senza costrizione, ad intervalli ragionevoli e senza ritardi o spese eccessivi:

- la conferma dell'esistenza o meno di trattamenti di dati che la riguardano, e l'informazione almeno sulle finalità dei trattamenti, sulle categorie di dati trattati, sui destinatari o sulle categorie di destinatari cui sono comunicati i dati;

- la comunicazione in forma intelligibile dei dati che sono oggetto dei trattamenti, nonché di tutte le informazioni disponibili sull'origine dei dati;

- la conoscenza della logica applicata nei trattamenti automatizzati dei dati che la interessano, perlomeno nel caso delle decisioni automatizzate di cui all'articolo 15, paragrafo 1;

b) a seconda dei casi, la rettifica, la cancellazione od il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto od inesatto dei dati;

c) la notificazione ai terzi ai quali sono stati comunicati i dati di qualsiasi rettifica, cancellazione o congelamento, effettuati conformemente alla lettera b), se non si dimostra che è impossibile o implica uno sforzo sproporzionato.

legittime ed eque nei suoi confronti. Tale accesso agli archivi del datore di lavoro potrà tuttavia rivelarsi problematico in alcune circostanze eccezionali, come ad esempio nel caso dell'accesso ai cosiddetti dati valutativi.

A questo proposito il gruppo di lavoro ha già espresso un primo parere[18] e potrà formulare ulteriori principi informatori in futuro alla luce dell'esperienza compiuta.

3.1.4. LEGITTIMITÀ

Questo principio subordina la possibilità di svolgere qualsiasi operazione di trattamento dati al fatto che essa si prefigga una finalità legittima a norma dell'articolo 7 della direttiva 95/46/CE e delle disposizioni con le quali essa è stata recepita nelle legislazioni nazionali. Particolare rilievo ai fini di questo principio assume l'articolo 7, lettera f) della direttiva in quanto esso dispone che a norma della direttiva il trattamento dei dati riguardanti un dipendente può essere consentito unicamente quando sia finalizzato al perseguimento di interessi legittimi da parte del datore di lavoro e non infranga i diritti fondamentali dei lavoratori.

La necessità del datore di lavoro di tutelare la sua impresa da seri pericoli, impedendo ad esempio la trasmissione d'informazioni confidenziali ad un concorrente, può costituire un tale interesse legittimo.

Nel contesto delle attività di vigilanza e di controllo il trattamento di dati riservati risulta particolarmente problematico poiché l'articolo 8 della direttiva non consente di conciliare interessi opposti secondo quanto disposto dall'articolo 7, lettera f) della direttiva stessa. Il secondo paragrafo, lettera b) dell'articolo 8 fa tuttavia riferimento al "trattamento … necessario per assolvere gli obblighi ed i diritti specifici del responsabile del trattamento in materia di diritto del lavoro, nella misura in cui il trattamento stesso sia autorizzato da norme nazionali che prevedono adeguate garanzie".

Il trattamento di dati delicati connessi ad attività di vigilanza e controllo rappresenta un problema spinoso, che ha rilievo non solo per le attività di lavoro dipendente. Effettivamente esso costituisce una problematica d'indole generale sulla quale il gruppo potrà pronunciarsi in futuro.

In termini pratici, attività di vigilanza direttamente miranti a trattare dati riservati relativi ai dipendenti non risulterebbero legittime a norma di quanto disposto dalla direttiva 95/46/CE e sarebbero quindi inaccettabili a meno che esse non fossero specificamente autorizzate da disposizioni nazionali di legge tali da offrire adeguate garanzie. Sembra tuttavia altrettanto inaccettabile impedire o rendere estremamente difficile qualsiasi attività di vigilanza (che in molti casi risulta non soltanto legittima ma addirittura desiderabile, come nel caso di quelle direttamente miranti a garantire la sicurezza del sistema) per il semplice motivo che ciò può rendere inevitabile il trattamento di alcuni dati di natura riservata.

3.1.5. PROPORZIONALITÀ

In ossequio a questo principio i dati personali, compresi quelli risultanti dall'attività di vigilanza, devono risultare adeguati, pertinenti e non eccessivi ai fini del conseguimento

---

[18] Si veda la raccomandazione 1/2001 sui dati utilizzati per valutare i dipendenti.

dello scopo specificato. La politica aziendale in questo campo andrà calcolata su misura, nonché in funzione del tipo e grado di rischio cui l'impresa interessata deve far fronte.

Il principio di proporzionalità porta quindi ad escludere un controllo a tappeto dei singoli casi d'impiego della posta elettronica e dell'Internet da parte del personale, a meno che ciò non risulti necessario al fine di garantire la sicurezza del sistema. Laddove l'obiettivo individuato può essere conseguito in modo meno intrusivo il datore di lavoro deve prendere in considerazione tale possibilità (evitando ad esempio di ricorrere a sistemi che effettuino controlli automatici e continui).

Il controllo della posta elettronica dovrebbe se possibile limitarsi ai dati riguardanti l'entità dello scambio di corrispondenza e la durata delle comunicazioni piuttosto che interessare anche il contenuto di queste ultime, se ciò risulta sufficiente ad eliminare le preoccupazioni dei datori di lavoro. Qualora l'accesso al contenuto della posta elettronica risulti assolutamente indispensabile si dovrà tener conto della sfera privata non solo degli appartenenti all'organizzazione, ma anche delle persone interne che ricevono i messaggi in questione. Il datore di lavoro non può ad esempio ottenere il consenso delle persone esterne all'organizzazione che inviano *e-mails* ai suoi dipendenti. Nei limiti del possibile il datore di lavoro dovrà fare quanto in suo potere per informare i corrispondenti esterni all'organizzazione dell'esistenza d'attività di controllo, se ed in quanto tali corrispondenti possono subirne le ripercussioni. Un esempio pratico potrebbe essere l'inserimento di avvertenze riguardanti l'esistenza del sistema di controllo in tutti i messaggi indirizzati a destinatari esterni all'organizzazione.

Giacché la tecnologia fornisce al datore di lavoro molte possibilità di valutare l'impiego della posta elettronica fatto dai suoi dipendenti verificando ad esempio il numero di messaggi inviati o ricevuti od il formato di eventuali allegati un'effettiva apertura di tali messaggi risulta non commisurata agli obiettivi perseguiti. E' inoltre possibile servirsi delle tecnologie disponibili per garantire la proporzionalità dei provvedimenti presi da un datore di lavoro allo scopo di salvaguardare contro gli abusi l'accesso ad Internet fornito ai suoi dipendenti avvalendosi di dispositivi di blocco piuttosto che di controllo[19].

I sistemi per il trattamento delle comunicazioni elettroniche andrebbero progettati in modo tale da limitare al minimo strettamente necessario la quantità di dati personali trattata[20].

In merito al problema della proporzionalità giova mettere in rilievo il fatto che il dispositivo dei negoziati collettivi può risultare estremamente utile per decidere quali

---

[19] La pratica fornisce già molti esempi di questo impiego delle tecnologie disponibili.

- Internet: alcune imprese utilizzano uno strumento di software che può venir configurato così da bloccare qualsiasi collegamento a categorie predeterminate di siti Web. Previa consultazione dell'elenco aggregato dei siti visitati dai suoi dipendenti il datore di lavoro può decidere di aggiungerne alcuni all'elenco di quelli già bloccati (eventualmente dopo aver avvertito i dipendenti che i collegamenti con tali siti saranno bloccati a meno che il dipendente non sia in grado di giustificarne la necessità).

- Posta elettronica: altre imprese si avvalgono di un sistema automatico di rinvio ad un *server* isolato per tutti i messaggi di posta elettronica che superino una determinata lunghezza. Il destinatario viene automaticamente informato del fatto che un messaggio sospetto è stato reindirizzato a tale *server* e può esservi consultato.

[20] Progetto di direttiva 97/66, 30.o considerando.

iniziative risultino commisurate ai vari rischi cui si trovano a far fronte i diversi datori di lavoro. E' in tal modo possibile arrivare ad un consenso tra il datore di lavoro ed i dipendenti circa il punto di equilibrio tra i rispettivi interessi.

3.1.6. ACCURATEZZA E CONSERVAZIONE DEI DATI

In ossequio a questo principio qualsiasi dato legittimamente archiviato da un datore di lavoro (una volta fatti salvi tutti gli altri principi menzionati nel presente capitolo) consistente in dati che riguardano l'indirizzo elettronico dei dipendenti ed il loro impiego dell'Internet (poiché questa ne è la fonte o per altro motivo) devono risultare accurati ed aggiornati e non venir conservati per un periodo superiore al necessario. I datori di lavoro dovranno precisare un periodo di conservazione dei messaggi di posta elettronica sui loro *server*s centrali in funzione delle esigenze aziendali. Di norma risulterà difficile giustificare un periodo di conservazione superiore ai tre mesi.

3.1.7. SICUREZZA

Questo principio obbliga il datore di lavoro a prendere i provvedimenti tecnici ed organizzativi del caso per garantire che qualsiasi dato personale da lui detenuto sia sicuro e protetto contro intrusioni dall'esterno. Esso comprende altresì il diritto del datore di lavoro a proteggere il suo sistema contro i virus informatici e può comportare una scansione automatizzata dei dati relativi ai messaggi di posta elettronica ed al traffico Internet.

Il gruppo di lavoro è del parere che, vista l'importanza di mantenere la sicurezza del sistema, una tale apertura automatizzata dei messaggi di posta elettronica non debba considerarsi tale da violare il diritto dei dipendenti alla *privacy*, purché vengano presi adeguati provvedimenti di garanzia. Attualmente ad esempio è possibile per i datori di lavoro servirsi di tecnologie automatizzate che tutelano i loro interessi in fatto di sicurezza senza violare i diritti dei dipendenti alla *privacy*.

Il gruppo di lavoro ex articolo 29 attira l'attenzione sulla funzione dell'amministratore del sistema, un dipendente con considerevoli responsabilità sotto il profilo della protezione dei dati. È estremamente importante che l'amministratore del sistema e chiunque abbia l'accesso ai dati personali relativi ai dipendenti nel corso dei controlli siano soggetti ad un rigoroso obbligo di segretezza professionale per quanto riguarda le informazioni riservate cui hanno accesso.

4. CONTROLLO DELLA POSTA ELETTRONICA

4.1. SEGRETEZZA DELLA CORRISPONDENZA

Come già spiegato nel presente documento, il gruppo di lavoro è del parere che la corrispondenza in linea e quella tradizionale non vadano trattate in modo differente senza validi motivi e che di conseguenza la posta elettronica debba beneficiare della stessa tutela dei diritti fondamentali di cui gode la posta tradizionale su carta[21]. La giurisprudenza della Corte europea dei diritti umani fornisce alcuni orientamenti circa l'applicazione del principio del diritto alla segretezza della corrispondenza in una società democratica. Negli ordinamenti giuridici degli Stati membri tuttavia questo principio viene interpretato in modi lievemente differenti, in particolare per quanto riguarda il campo d'applicazione per le comunicazioni professionali, in termini tanto di contenuto quanto di dati relativi al traffico. Sotto il profilo della tutela dei dati ciò ha importanti ripercussioni quando si debba considerare fino a qual punto siano tollerabili intrusioni nella corrispondenza dei dipendenti.

Il gruppo di lavoro ex articolo 29 è del parere che le comunicazioni elettroniche fatte a partire da locali commerciali possano rientrare nella nozione di "vita privata" e "corrispondenza" a termini dell'articolo 8, paragrafo 1 della convenzione europea. Il margine d'interpretazione a questo riguardo è ridotto giacché questa questione è stata chiaramente risolta dalla Corte nel già menzionato caso **Halford contro Regno Unito**.

Il punto che resta da chiarire, e che effettivamente consente un certo margine d'interpretazione, è la misura in cui questo principio possa prestarsi a deroghe e limitazioni, in particolare quando vada opposto ai diritti ed alle libertà di altre persone analogamente tutelati dalla convenzione (per esempio i legittimi interessi del datore di lavoro). **In ogni caso l'ubicazione e la proprietà del mezzo elettronico utilizzato non escludono la segretezza delle comunicazioni e della corrispondenza, quale sancita da principi giuridici fondamentali e costituzioni.**

Il gruppo di lavoro ex articolo 29 desidera tuttavia ricordare che questo problema non riguarda specificamente il trattamento dei dati personali nel contesto occupazionale, ma è di portata generale giacché le leggi ed i regolamenti in tema di protezione dei dati non si applicano in astratto. Si presume che i diritti in tema di protezione dei dati si applichino ad ordinamenti giuridici diversi, nel cui ambito differenti disposizioni di legge stabiliscano altri diritti ed obblighi per gli individui (ad esempio diritto del lavoro). Il gruppo di lavoro ex articolo 29 è cionondimeno convinto del fatto che le soluzioni

---

[21] Una tra le prime raccomandazioni formulate dal gruppo di lavoro, la raccomandazione 3/97 "Anonimato nell'Internet", affermava già che la corrispondenza in linea e quella tradizionale andrebbero trattate nello stesso modo.

Si veda il sito: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp6en.pdf

Il documento della Task Force Internet, il più importante adottato dal gruppo di lavoro sulla riservatezza nell'ambito dell'Internet si è soffermato su questa idea nel capitolo 3, pagina 21.

Si veda il sito: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37en.pdf

proposte nel presente documento di lavoro possono risultare utili nel difficile compito di riconciliare questi interessi contrastanti.

4.2. LEGITTIMAZIONE IN FORZA DELLA DIRETTIVA 95/46/CE

I messaggi di posta elettronica contengono dati personali cui si applicano le disposizioni della direttiva 95/46/CE, ed i datori di lavoro devono di conseguenza avere un legittimo motivo per trattare tali dati. Come è stato ampiamente spiegato nel parere 8/2001 il consenso dei dipendenti deve essere accordato liberamente da persone perfettamente informate, ed i datori di lavoro non dovrebbero fare affidamento su tale consenso in quanto mezzo generale per legittimare i trattamenti in questione.

Il motivo più plausibilmente atto a legittimare controlli della corrispondenza elettronica si può reperire nell'articolo 7, lettera f) della direttiva e consiste nel fatto che tale trattamento risulti necessario per il perseguimento degli interessi legittimi del responsabile del trattamento oppure dei terzi cui vengono comunicati i dati. Prima di esaminare in che modo questa disposizione si applichi agli aspetti in questione giova rilevare che tale legittimazione non può prevalere sui diritti e sulle libertà fondamentali del lavoratore dipendente, tra cui rientra all'occorrenza il diritto fondamentale alla segretezza della corrispondenza.

Il gruppo di lavoro ha già espresso il parere che[22]:

"Laddove un datore di lavoro si trovi nella necessità di trattare dati personali in quanto conseguenza necessaria ed inevitabile del rapporto di lavoro costituisce comportamento fuorviante qualsiasi tentativo di legittimare tale trattamento mediante l'assenso. Il ricorso all'assenso va limitato ai casi in cui il dipendente dispone di una scelta veramente libera ed è di conseguenza in grado di ritirare il proprio assenso senza pregiudizio per i propri interessi".

Poiché i messaggi di posta elettronica contengono dati personali relativi tanto al mittente quanto al destinatario ed i datori di lavoro possono in genere ottenere agevolmente solo l'assenso di una di queste parti (a meno che nella posta elettronica non sia compresa la corrispondenza tra dipendenti), la possibilità di legittimare il controllo della posta elettronica in base a tale assenso risulta estremamente limitata. Considerazioni analoghe valgono per il caso contemplato dall'articolo 7, lettera b) della direttiva, giacché non si verificherà mai che una delle parti allo scambio di corrispondenza abbia concluso con il responsabile del trattamento un contratto a norma di tale disposizione, vale a dire un contratto di controllo della corrispondenza.

Giova a questo punto rilevare che nei casi in cui ad un dipendente sia fornito un indirizzo di posta elettronica per un impiego puramente personale o gli venga consentito l'accesso ad una casella postale in rete l'apertura dei messaggi elettronici pervenuti a tali indirizzi da parte del suo datore di lavoro può venir giustificata unicamente in circostanze estremamente limitate (a prescindere dalla ricerca di virus informatici)[23] ed in circostanze

---

[22] Si veda il paragrafo nel riquadro a pagina 23 del parere 8/2001.

[23] Tra tali casi rientrerebbe lo svolgimento di un'attività criminale da parte del dipendente se ed in quanto l'apertura della posta risulta necessaria al datore di lavoro per difendere i propri interessi, come ad esempio nel caso in cui egli sia civilmente e penalmente responsabile per le azioni del dipendente o sia la vittima dell'attività criminale in questione.

normali non può essere giustificato in riferimento all'articolo 7, lettera f) poiché non rientra tra gli interessi legittimi del datore di lavoro accedere a tali dati. Prevale invece il diritto fondamentale alla segretezza della corrispondenza.

La questione della misura in cui l'articolo 7, lettera f) consente il controllo della posta elettronica dipende quindi dal modo in cui i principi fondamentali spiegati nel capitolo 3.2 si applicano nei singoli casi. Come già indicato nel capitolo 3.1.4 (legittimità), al momento di stabilire la correttezza dell'equilibrio tra questi interessi contrastanti si dovrà tener nel debito conto il rispetto della sfera privata delle persone interessate dal controllo ma estranee all'organizzazione.

4.3 INFORMAZIONI DI MINIMA CHE SI RACCOMANDA ALL'IMPRESA DI FORNIRE AI SUOI DIPENDENTI

Nell'elaborare la propria politica i datori di lavoro devono uniformarsi ai principi esposti nel capitolo 3.1.3 nell'ambito del principio generale di trasparenza[24], tenendo presenti esigenze e dimensioni dell'impresa.

Per quanto riguarda più specificamente la corrispondenza elettronica occorre affrontare i seguenti punti:

a) Eventuale diritto di un dipendente a disporre di un indirizzo *e-mail* per finalità puramente personali, eventuale liceità dell'impiego d'indirizzi *webmail* sul posto di lavoro ed eventuale raccomandazione del datore di lavoro che i dipendenti impieghino un indirizzo *webmail* privato quando vogliano utilizzare la posta elettronica per scopi puramente personali (si veda il capitolo 4.4).

b) Accordi raggiunti con i dipendenti circa l'accesso ai contenuti di un messaggio di posta elettronica, con particolare riferimento ai casi di assenza imprevista del dipendente, e finalità specifiche di tale accesso.

c) Laddove dei messaggi venga fatta una copia di *backup*, durata del periodo in cui tale copia è conservata.

d) Informazioni circa il momento in cui i messaggi di posta elettronica vengono definitivamente cancellati dal *server*.

24

1. Una politica aziendale in fatto di posta elettronica ed uso dell'Internet che descriva in modo particolareggiato in che misura le infrastrutture di comunicazione di proprietà dell'impresa possano essere impiegate per comunicazioni di natura personale/privata da parte dei dipendenti (ad esempio limiti di tempo e durata dell'impiego).

2. Ragioni e finalità di un'eventuale vigilanza. Nel caso in cui il datore di lavoro ha espressamente consentito l'impiego delle infrastrutture di comunicazione aziendali per scopi privati, tali comunicazioni private possono essere oggetto di sorveglianza in circostanze estremamente limitate, come ad esempio per garantire la sicurezza del sistema informatico (lotta ai virus informatici).

3. Particolari dei provvedimenti di sorveglianza presi: chi? cosa? quando?

4. Particolari di qualsiasi procedura volta a garantire il rispetto delle regole, con precisazione delle modalità e delle occasioni in cui verranno notificate ai dipendenti eventuali infrazioni delle politiche aziendali e fornita loro l'occasione di confutare le accuse loro mosse.

e) Questioni di sicurezza.

f) Coinvolgimento dei rappresentanti dei dipendenti nel definire la politica aziendale.

Giova rilevare che al datore di lavoro compete l'obbligo di garantire in permanenza che la sua politica si mantenga in linea con gli sviluppi tecnologici e con il parere dei suoi dipendenti.

4.4 *WEBMAIL*[25]

Il gruppo di lavoro è del parere che una tale politica, consistente nel consentire ai dipendenti l'impiego di un indirizzo privato o di *webmail*, potrebbe contribuire a risolvere in modo pragmatico il problema in questione. Una raccomandazione del datore di lavoro in tal senso chiarirebbe la distinzione tra messaggi di posta elettronica destinati ad uso professionale e quelli con finalità private e ridurrebbe la possibilità che i datori di lavoro invadano la sfera privata dei loro dipendenti. Esso comporterebbe inoltre un costo aggiuntivo nullo o minimo per il datore di lavoro.

Il datore di lavoro che adotti una tale politica potrà, in casi specifici nei quali vi siano seri sospetti circa il comportamento di un dipendente, controllare la misura in cui tale dipendente utilizza il proprio PC per fini personali rilevando il tempo speso a corrispondere con indirizzi *webmail.* In tale modo gli interessi del datore di lavoro verranno serviti senza che vi sia alcuna possibilità di rivelare dati personali del dipendente ed in particolare dati delicati.

Una tale politica può inoltre risultare vantaggiosa per i dipendenti poiché darebbe loro la certezza del livello di rispetto della sfera privata che possono attendersi, certezza che può essere assente in codici di condotta più complessi e confusi. Ciò detto occorre parimenti mettere in rilievo che:

a) **il fatto di consentire l'impiego di indirizzi privati o di *webmail* non pregiudica la piena applicazione delle sezioni precedenti di questo capitolo ad altri indirizzi di posta elettronica utilizzati sul posto di lavoro**;

b) all'atto di consentire l'impiego della *webmail* le imprese dovrebbero essere consapevoli che esso potrebbe porre a repentaglio la sicurezza delle reti aziendali, specialmente per quanto riguarda la diffusione di virus informatici;

c) i dipendenti dovrebbero essere consapevoli del fatto che talvolta i *server*s della *webmail* sono ubicati in paesi terzi in cui potrebbe non essere garantita una tutela adeguata dei dati personali degli individui.

Occorre tener presente che queste considerazioni valgono per normali rapporti di lavoro. Regole speciali potranno risultare necessarie in rapporto alle comunicazioni dei dipendenti sottoposti a vincoli di segretezza professionale.

---

[25] Per *webmail* s'intende un sistema di posta elettronica in rete che fornisce una posta elettronica in rete a partire da qualsiasi server POP o IMAP, nell'ambito dei quali la protezione di norma è garantita dal nome dell'utente e da una parola d'ordine.

5. CONTROLLO DELL'ACCESSO ALL'INTERNET

5.1 IMPIEGO PRIVATO DELL'INTERNET SUL POSTO DI LAVORO

Occorre anzitutto rilevare che spetta all'impresa decidere se ed in che misura è consentito ai lavoratori impiegare l'Internet per motivi personali.

Ciò detto tuttavia il gruppo di lavoro è del parere che un divieto assoluto dell'impiego personale d'Internet da parte dei dipendenti si può ritenere poco pratico e non molto realistico poiché non tiene conto della misura in cui l'Internet può essere d'aiuto ai dipendenti nella loro vita quotidiana.

5.2. PRINCIPI RIGUARDANTI IL CONTROLLO DELL'INTERNET

Nell'affrontare il problema del controllo dell'accesso dei dipendenti all'Internet si possono applicare alcuni principi.

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. Se ed in quanto ragionevolmente possibile, la politica perseguita in rapporto all'Internet dovrebbe fare affidamento su mezzi tecnici per ridurre l'accesso piuttosto che sul controllo dei comportamenti, basandosi ad esempio sul blocco di alcuni siti o sull'installazione di avvertenze automatiche per le richieste d'accesso a determinati siti.

Per ridurre al minimo i problemi è importante informare prontamente il dipendente in merito al rilevamento di un impiego sospetto dell'Internet. Anche laddove costituisca un provvedimento necessario qualsiasi controllo deve rappresentare una **risposta commisurata** ai rischi cui deve far fronte il datore di lavoro. In molti casi l'abuso di Internet può essere individuato senza che occorra analizzare il contenuto dei siti visitati. Una verifica del tempo speso a navigare sull'Internet o dei siti più frequentemente visitati da un dipartimento può ad esempio essere sufficiente per rassicurare un datore di lavoro circa il fatto che le sue infrastrutture non sono soggette ad abusi. Qualora queste verifiche d'indole generale portino alla luce possibili abusi dell'Internet il datore di lavoro può considerare la possibilità di ulteriori controlli del settore in questione.

Nel valutare l'impiego dell'Internet fatto dai dipendenti i datori di lavoro d**evono cercare di far prova di prudenza nell'arrivare a determinate conclusioni**, tenendo conto della facilità con cui possono verificarsi visite involontarie di siti Web in seguito a risposte impreviste di motori di ricerca, collegamenti *hypertext* poco chiari, pubblicità fuorvianti ed errori di battitura. In ogni caso i lavoratori hanno il diritto di vedersi presentare i fatti contestati e di avere l'occasione di ribattere alle accuse d'abuso presentate dal datore di lavoro.

5.3 CONTENUTO DI MINIMA RACCOMANDATO DELLA POLITICA AZIENDALE IN TEMA D'INTERNET

1. Le informazioni di cui al capitolo 3.1.3 nell'ambito del principio di trasparenza[26].

26

Riferendosi inoltre più specificamente all'impiego dell'Internet occorrerà trattare in particolare i seguenti punti:

2. il datore di lavoro deve indicare chiaramente ai dipendenti a quali condizioni è consentito l'impiego privato dell'Internet, precisando quale materiale non può essere visionato o copiato e spiegando ai dipendenti queste condizioni e questi limiti;

3. i dipendenti vanno informati circa i sistemi messi in opera per impedire l'accesso a determinati siti e per individuare i casi d'abuso. La portata di tali controlli andrà indicata, precisando ad esempio se essi possono riguardare singole persone o particolari sezioni dell'impresa oppure se in circostanze particolari il contenuto dei siti visitati è visionato o registrato dal datore di lavoro. La politica aziendale dovrà inoltre precisare quale uso può all'occorrenza venir fatto dei dati raccolti in rapporto alle persone che hanno visitato determinati siti;

4. i dipendenti vanno informati circa la partecipazione dei loro rappresentanti all'attuazione di tale politica e all'indagine sulle presunte infrazioni.

CONCLUSIONI

Il gruppo di lavoro ha redatto il presente documento di lavoro per contribuire a rendere uniforme l'applicazione dei provvedimenti nazionali presi in forza della direttiva 95/46/CE nel campo della vigilanza e del controllo delle comunicazioni elettroniche sul posto di lavoro (si vedano i riepiloghi delle disposizioni nazionali che figurano nell'allegato al presente documento).

Il gruppo di lavoro ha rilevato alcune divergenze tra le varie disposizioni nazionali, soprattutto in campi connessi alla protezione dei dati per quanto riguarda le deroghe consentite al diritto fondamentale alla segretezza della corrispondenza nonché il campo d'applicazione e gli effetti del processo di rappresentazione collettiva e codecisione. Il gruppo di lavoro ex articolo 29 desidera cionondimeno dare risalto al fatto che qualsiasi divergenza tra le disposizioni prese dagli Stati membri per recepire nelle proprie legislazioni la direttiva 95/46/CE non costituisce un grave ostacolo ad un'impostazione comune, quale risulta dai principi e dalle buone prassi presentate in questo documento di lavoro.

---

1. La politica aziendale in tema di *e-mail* ed Internet, con una descrizione particolareggiata della misura in cui infrastrutture di comunicazione di proprietà dell'impresa stessa possono venir utilizzate dai dipendenti per comunicazioni personali o private (ad esempio limiti di tempo e durata dell'impiego);

2. motivi e finalità di un'eventuale attività di vigilanza; laddove il datore di lavoro abbia espressamente consentito l'impiego delle infrastrutture di comunicazione dell'impresa per fini privati le comunicazioni private possono in un numero estremamente ridotto di casi essere sottoposte a sorveglianza, ad esempio per garantire la sicurezza del sistema d'informazione (rilevamento della presenza di virus informatici);

3. particolari dei provvedimenti presi, vale a dire chi, cosa, come, quando;

4. particolari di qualsiasi procedura volta a garantire il rispetto delle regole, con indicazione del modo e del momento in cui ai dipendenti possono venir notificate eventuali infrazioni alle politica aziendale e delle possibilità loro offerte di rispondere alle accuse eventualmente mosse contro di loro.

Il sottogruppo sull'occupazione provvederà a garantire che il presente documento di lavoro sia oggetto di costanti revisioni alla luce dell'esperienza compiuta e degli ulteriori sviluppi intervenuti in questo campo nel corso degli anni 2002 e 2003.

Fatto a Bruxelles il 29 maggio 2002

A nome del gruppo di lavoro

Il presidente

Stefano RODOTA