Impiego dell'elaboratore sul luogo di lavoro e tutela penale della *privacy*[*]

1. La diffusa prassi del monitoraggio delle *e-mail* e della navigazione in Rete dei dipendenti

Tra i tanti profili della *privacy*, oggetto di attenzione da parte delle diverse Autorità nazionali preposte alla tutela dei dati personali, particolare rilievo hanno assunto in questi ultimi anni quelli connessi all'attività lavorativa, in conseguenza delle sempre più ampie possibilità di intrusione nella sfera personale dei lavoratori consentite dallo sviluppo tecnologico. A destare preoccupazione è per lo più la consapevolezza che l'impiego dell'elaboratore elettronico per lo svolgimento delle proprie mansioni espone il lavoratore al rischio di un monitoraggio costante e 'invisibile' della sua attività, sia durante l'orario di lavoro – ad es. mediante appositi programmi, in grado di registrare il numero di tasti digitati in un determinato arco di tempo (c.d. *keystroke-monitoring*) – sia in un momento successivo: il datore di lavoro può infatti agevolmente consultare sul *server* dell'azienda tutte le tracce lasciate dal lavoratore in occasione dello svolgimento di ogni singola operazione sul suo terminale, ed è quindi in condizione di sapere, ad esempio, quali e quanti messaggi di posta elettronica il lavoratore ha inviato o ricevuto, quali siti della Rete ha visitato e per quanto tempo si è protratto il collegamento. Un controllo di questo tipo, tra l'altro, può non esaurirsi in una verifica dell'effettivo adempimento della prestazione lavorativa, ma può arrivare ad interessare momenti di vita privata del lavoratore, rispetto ai quali deve essere assicurato il diritto alla riservatezza anche sul luogo di lavoro.

L'estensione della prassi del monitoraggio dell'uso degli strumenti elettronici da parte dei lavoratori è ben testimoniata da diverse indagini conoscitive svolte negli ultimi anni negli Stati Uniti: un Paese nel quale le aspettative di riservatezza dei dipendenti sembrano ritenute necessariamente soccombenti rispetto alle esigenze di sicurezza, imperanti in ogni ambito (dalla singola impresa considerata alla Nazione nel suo complesso).

[*] Il presente contributo è risultato di una riflessione comune degli autori; tuttavia i §§ 1 e 2 sono stati redatti da Claudia Pecorella e il § 3 da Riccardo De Ponti.

Da un'indagine svolta nel 2001 dalla *Privacy Foundation* dell'Università di Denver (Colorado)[1] risultava che al monitoraggio sistematico delle e-mail e dell'uso di Internet – regolarmente utilizzati per l'attività lavorativa – fossero sottoposti 14 milioni di lavoratori negli Stati Uniti e 27 milioni in tutto il mondo (che corrispondevano a più di un terzo e ad oltre un quarto della *on-line workforce*, rispettivamente, statunitense e mondiale)[2]. Un sensibile aumento del ricorso a controlli routinari sull'uso delle risorse elettroniche è emerso poi dall'indagine svolta qualche anno dopo dall'*American Management Association (AMA)* e dall'*ePolicy Institute*: su un campione di 526 società americane, ben il 76% ammetteva di monitorare le connessioni a Internet dei dipendenti e tra esse il 65% dichiarava di utilizzare appositi programmi per impedire la connessione con alcuni siti ritenuti inappropriati (siti pornografici, *social network*, siti di intrattenimento, siti commerciali, siti sportivi, etc.). Quanto alla posta elettronica, il 55% delle società interpellate risultava procedere alla conservazione e alla lettura dei messaggi inviati e ricevuti e una percentuale di poco inferiore (il 50%) era solita accedere ai documenti presenti nel *computer* del lavoratore. Nella maggioranza dei casi le società dichiaravano di aver previamente informato i lavoratori sia dei controlli effettuati sui loro documenti (nell'80% dei casi) o sulla corrispondenza (86% dei casi), sia del monitoraggio sui siti visitati (89% dei casi)[3]. Quanto a quest'ultimo aspetto, l'indagine effettuata due anni dopo, su un campione più ristretto di società americane (304), nel confermare per lo più i risultati dell'indagine precedente, metteva in evidenza come la pratica di informare preventivamente il lavoratore sul monitoraggio della attività da lui svolta servendosi degli strumenti informatici non fosse esente da critiche, risultando in molti casi (ben il 70%) affidata ad una più o meno 'attenta' lettura, da parte del lavoratore, dell'*employee handbook* messo a sua disposizione all'inizio del rapporto di lavoro. Solo il 27% delle società interpellate riteneva opportuna una politica di sensibilizzazione dei lavoratori sul corretto uso degli strumenti elettronici e un'adeguata informazione sui controlli previsti[4].

D'altra parte, la mancata informazione ai dipendenti sull'attività di controllo svolta nell'ambito lavorativo e persino l'espresso riconoscimento del carattere riservato della corrispondenza gestita attraverso il servizio di posta elettronica dell'azienda non sembrano avere rilevanza decisiva nel giudizio sulla legittimità del monitoraggio comunque effettuato dal

[1] La *Privacy Foundation* è stata istituita all'interno del *Privacy Center* dell'Università di Denver: maggiori informazioni sulla sua composizione e sulla sua attività sono reperibili sul sito www.privacyfoundation.org.

[2] Cfr. A. SCHULMAN, *The Extent of Systematic Monitoring of Employee E-mail and Internet Use* (9 luglio 2001), in *www.sonic.net*. L'autore è *Chief Researcher* del *Workplace Surveillance Project* presso la *Privacy Foundation.*

[3] Cfr. AMERICAN MANAGEMENT ASSOCIATION-THE EPOLICY INSTITUTE, *2005 Electronic Monitoring & Surveillance Survey*, in *www.Businesswire.com* (18 maggio 2005).

[4] Cfr. AMERICAN MANAGEMENT ASSOCIATION-EPOLICY INSTITUTE RESARCH, *2007 Electronic Monitoring & Surveillance Survey*, in www.amanet.org.

datore di lavoro. In diverse occasioni, infatti, la giurisprudenza americana ha negato l'esistenza in quelle situazioni di una legittima aspettativa di *privacy* in capo al lavoratore, ritenendo, da un lato, che "nessuna persona ragionevole considererebbe l'intercettazione delle *mail* inviate attraverso il sistema di posta elettronica dell'azienda come un'invasione reale e altamente lesiva della *privacy* del lavoratore" e, dall'altro lato, che "l'interesse della società a prevenire affermazioni inopportune e non professionali o addirittura attività illegali attraverso il suo sistema di posta elettronica prevale sull'interesse alla riservatezza che il dipendente possa avere nelle affermazioni di quel tipo da lui svolte"[5]. Si comprende così come una recente informativa sul tema, diffusa da un'associazione americana per la tutela della riservatezza (la *Privacy Rights Clearinghouse*), si concluda con l'invito ai lavoratori a rivolgersi al legislatore federale affinché venga finalmente adottata una disciplina chiara della materia[6].

Maggiore sensibilità per le tematiche che coinvolgono la riservatezza del lavoratore sul luogo di lavoro si riscontra nei Paesi europei, nei quali è in corso un ampio dibattito, a livello sia nazionale sia comunitario, sulla necessità di un corretto bilanciamento tra le esigenze di controllo del datore di lavoro e il diritto alla *privacy* del lavoratore, ritenuto comunque meritevole di salvaguardia anche nel contesto lavorativo.

Come si è anticipato, la questione del monitoraggio sull'utilizzo da parte dei dipendenti del servizio di posta elettronica e di navigazione in Internet, attraverso le risorse informatiche dell'azienda, è stata per lo più affrontata – in assenza di normative specifiche al riguardo – dalle autorità preposte alla protezione dei dati, proprio per il rischio, legato a questo tipo di controllo, che vengano acquisite dal datore di lavoro "informazioni anche sensibili di lavoratori o di terzi, non necessariamente legate all'attività lavorativa"[7].

In questo ambito, punto di riferimento comune a tutti i Paesi dell'Unione Europea è l'attività del "Gruppo di lavoro sulla protezione dei dati", un organismo europeo indipendente con finalità consultive, costituito in applicazione dell'art. 29 della direttiva 95/46/CE sulla tutela

---

[5] Così SMYTH V. PILLSBURY, January 18, 1996 (United States District Court for the Eastern District of Pennsylvania), in www.loundy.com. In precedenza, in termini analoghi, BOURKE V. NISSAN, July 26, 1993 (Court of Appeal of the State of California), in *www.loundy.com*, nella quale pure si esclude l'illiceità della condotta del datore di lavoro non avendo egli conosciuto il contenuto di una *mail* attraverso una vera e propria 'intercettazione', essendosi limitato a stamparne una copia da un dispositivo elettronico di memoria. Sulla distinzione, rilevante ai fini dell'applicazione dell'*Electronic Communications Privacy Act of 1986*, tra intercettazione di una comunicazione in atto (nella quale non è ricompressa la comunicazione memorizzata su un supporto elettronico – *stored electronic communication*) e accesso abusivo a un dispositivo che fonisce un servizio di comunicazione elettronica (U.S.C. *section* 2701 (a)), v. R. DUNNE, *Computers and the Law*, Cambridge University Press, 2009, p. 247 ss.

[6] Cfr. PRIVACY RIGHTS CLEARINGHOUSE, *Employee Monitoring: Is There Privacy in the Workplace? – Fact Sheet 7*: Workplace Privacy 1993-2009, in www.privacyrights.org,

[7] Così giustifica il suo intervento in materia il Garante della *privacy* italiano, nella Relazione annuale al Parlamento sull'attività svolta: v. Relazione 2007 – *Garanzie e sicurezza nel trattamento dei dati: l'attività dell'autorità*, 16 luglio 2008, in *www.garanteprivacy.it.*

delle persone fisiche, con riguardo al trattamento di dati personali nonché alla libera circolazione di tali dati[8]. Del tema che qui interessa il Gruppo di lavoro si è occupato una prima volta, in modo marginale, all'interno del "Parere 8/2001 sul trattamento dei dati personali nel contesto dell'occupazione"[9]: in quella occasione si è cercato di individuare a quali dei principi della direttiva 95/46CE deve ritenersi condizionata la legittimità della raccolta, della conservazione e dell'impiego dei dati personali nel contesto professionale. Con riguardo, in particolare, al momento della raccolta, è stata sottolineata l'esigenza che l'acquisizione dei dati attraverso il controllo sui dipendenti, oltre a dover essere resa nota ai lavoratori, persegua una finalità legittima, rispetto alla quale risulti sia necessaria, sia proporzionata; altamente problematico resta invece il profilo del consenso al trattamento dei dati, ove necessario, perché rileverebbe solo un consenso *liberamente* prestato, ed è ritenuto tale solo quello che può essere ritirato "senza pregiudizio per i propri interessi".

Il Gruppo di lavoro è poi tornato sull'argomento, l'anno successivo, nel "Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro", diretto a "rendere uniforme l'applicazione dei provvedimenti nazionali presi in forza della direttiva 95/46/CE" [10], alla luce anche della giurisprudenza della Corte europea dei diritti dell'uomo nel frattempo intervenuta (sulla quale, v. *infra*, § 2.1).

In questo documento sono contenute alcune indicazioni particolarmente significative, che possono assumersi a premesse di partenza incontestabili di ogni analisi avente ad oggetto questa delicata materia: prima fra tutte, l'affermazione che "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". Si tratta di una precisazione apparentemente superflua, che può però risultare importante ogniqualvolta quell'argomento venga invocato – come nella (scarsa) giurisprudenza italiana sul tema - per legittimare l'arbitrio del datore di lavoro nell'espletamento dei controlli sull'uso degli strumenti informatici da parte dei suoi dipendenti.

Con riguardo ai controlli sulla navigazione in Internet, si sottolinea poi la "particolare utilità [delle] soluzioni di natura tecnologica" funzionali alla prevenzione degli abusi, nella consapevolezza che "un divieto globale per i dipendenti d'impiegare Internet a fini personali

[8] Tale organismo, spesso indicato come Gruppo di lavoro "Articolo 29" sulla protezione dei dati, proprio in ragione delle sue origini, è composto da rappresentanti delle autorità competenti per la protezione dei dati nei diversi Stati membri.

[9] Il parere, approvato il 13 settembre 2001, è reperibile all'indirizzo: http://europa.eu.int/comm/internal_market /en/dataprot/wpdocs/wp48en.pdf.

[10] Cfr. Gruppo di lavoro sulla protezione dei dati – Articolo 29, *Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro*, adottato il 29 maggio 2002, in *www.europa.eu.int/comm/privacy*.

appare irragionevole". Più in generale, si attribuisce "importanza fondamentale", in un'ottica preventiva, all'informazione del dipendente sull'impiego e sulla finalità "di qualsiasi apparecchiatura e/o dispositivo di rilevamento" che riguardino la sua postazione di lavoro, nonché sull'eventuale individuazione di un abuso del mezzo informatico di comunicazione da parte sua, salvo che ricorrano ragioni particolari – che, alla luce dell'esperienza, vengono ritenute difficilmente ipotizzabili[11] – nelle quali appaia giustificato proseguire la sorveglianza in segreto. Indicazioni, queste, che non possono evidentemente non assumere rilevanza ai fini di un'eventuale valutazione della legittimità dell'attività di monitoraggio concretamente realizzata, sotto il profilo della sua necessità e proporzionalità allo scopo[12].

Muovendo inoltre dalla considerazione che il fatto di avvisare in anticipo il dipendente non è "sufficiente a giustificare qualsiasi infrazione dei suoi diritti in tema di protezione dei dati", si perviene alla conclusione che "il controllo della corrispondenza di un lavoratore o del suo impiego dell'Internet può ritenersi necessario unicamente in circostanze eccezionali" e che i dati eventualmente raccolti per questa via non possono essere utilizzati per finalità diverse e incompatibili con quella originaria (così, ad esempio, se il controllo era funzionale alla rilevazione di *virus* informatici, i dati ottenuti non possono essere successivamente usati per valutare il comportamento del dipendente).

Quanto al delicato problema del consenso al monitoraggio prestato dal dipendente, dopo aver ribadito che "il ricorso all'assenso va limitato ai casi in cui il dipendente dispone di una scelta veramente libera", si perviene alla conclusione che "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 (…) la possibilità di legittimare il controllo della posta elettronica in base a tale assenso risulta estremamente limitata". Anche in questo caso si tratta di una precisazione molto importante, alla quale non sembra essere rivolta la dovuta attenzione nel dibattito in corso su questo argomento.

Spostando l'attenzione sull'ordinamento italiano, si nota come il tema della legittimità dei controlli effettuati dal datore di lavoro sull'uso delle risorse elettroniche dell'azienda, ancorché oggetto di alcune pronunce giurisprudenziali, sia stato sino ad oggi di scarso interesse da parte della dottrina penalistica; la presenza e la diffusione del fenomeno anche nel nostro Paese è del

[11] Si afferma, infatti, in proposito, che "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" (p. 5 del Documento di lavoro in versione italiana).

[12] A questo riguardo si esclude, ad esempio, che possa essere ritenuto proporzionato "un controllo a tappeto dei singoli casi di impiego della posta elettronica e dell'Internet da parte del personale", con l'unica eccezione della effettiva necessità del controllo per "garantire la sicurezza del sistema" e sempreché non siano sufficienti sistemi meno intrusivi per la *privacy* del lavoratore, come quelli già oggi resi disponibili dalla tecnologia (es. dispositivi 'di blocco', piuttosto che di controllo) (p. 18 del Documento di lavoro in versione italiana).

resto confermata dalla necessità, percepita dal Garante per la protezione dei dati personali, di dettare delle linee-guida in materia, alla luce "delle segnalazioni pervenute negli anni e dei ricorsi presentati nel 2006".

Con un provvedimento del 1° marzo 2007[13] il Garante, dopo aver fornito alcune indicazioni pratiche per il bilanciamento delle contrapposte esigenze in gioco, prescrive ai datori di lavoro pubblici e privati l'adozione di una serie di misure che garantiscano una chiara e completa informazione ai dipendenti sull'uso che possono fare degli strumenti elettronici messi a loro disposizione e sui controlli previsti, nonché alcuni accorgimenti, anche tecnici, per ridurre sia il rischio di abusi, sia le eventuali intrusioni nella sfera personale del lavoratore. Si fa comunque espresso divieto di effettuare "la lettura e la registrazione *sistematica* dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto strettamente necessario per svolgere il servizio *e-mail"*, e "la riproduzione o l'eventuale memorizzazione *sistematica* delle pagine *web* visualizzate dal lavoratore"[14].

Coerentemente con la sua funzione, il Garante si è preoccupato di indicare in quali casi il controllo della corrispondenza elettronica e della navigazione in Rete risulti rispettoso della disciplina di protezione dei dati personali e della legislazione di settore, individuata principalmente nello Statuto dei lavoratori (l. 20 maggio 1970 n. 300); nessuna considerazione viene invece dedicata alla eventuale rilevanza penale di quelle condotte. Ed è proprio su questo aspetto che vogliamo soffermare ora l'attenzione, distinguendo la trattazione dei profili di liceità del controllo sulla corrispondenza, inviata e ricevuta dal lavoratore presso l'indirizzo personale di posta elettronica attribuitogli dal datore di lavoro, da quelli relativi al controllo sulla navigazione in Internet, realizzata dal dipendente servendosi del sistema informatico dell'azienda.

2. Le condizioni di liceità del controllo sulla corrispondenza del lavoratore

A differenza di quanto avviene con il monitoraggio della navigazione in Rete (sul quale v. *infra*, § 3) il controllo del datore di lavoro sulla corrispondenza dei dipendenti interferisce con il

[13] Cfr. *Linee-guida per posta elettronica e Internet*, in *Gazz. Uff.* 10 marzo 2007 n. 58; *Foro it.*, 2007, III, 214 ss., nonché sul sito del Garante: *www.garanteprivacy.it*. Perplessità su questo provvedimento del Garante, per le interferenze che produce con la disciplina contenuta nella legge 300/1970 (Statuto dei lavoratori) sono manifestate da M. DEL CONTE, *Internet, posta elettronica e oltre: il Garante della* privacy *rimodula i poteri del datore di lavoro*, in *Dir. inf.*, 2007, 497 ss. Questioni attinenti al controllo della posta elettronica del lavoratore sono state successivamente sottoposte all'attenzione del Garante e risolte, rispettivamente, con i provvedimenti del 2 aprile 2008 e del 21 gennaio 2010 (consultabili sul sito appena menzionato).

[14] Così il provvedimento del Garante del 1° marzo 2007, *Linee-guida* cit. (corsivo aggiunto). Nel settore pubblico le indicazioni del Garante sono state riprese all'interno di una direttiva della Presidenza del Consiglio dei Ministri del 16 maggio 2009 (direttiva n. 02/09), avente ad oggetto l'utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro. Cfr. *www.governo.it/GovernoInforma/Dossier/pa_internet_direttiva/index.html.*

diritto alla libertà e alla segretezza "della corrispondenza e di ogni altra forma di comunicazione", che nell'art. 15 della Costituzione è dichiarato inviolabile e del quale sono ammesse limitazioni "soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge". Un diritto che la Corte costituzionale fa rientrare "tra i valori supremi costituzionali" e che, "per la stretta attinenza della libertà e della segretezza della comunicazione al nucleo essenziale dei valori della personalità", viene considerato "parte necessaria di quello spazio vitale che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana"[15].

Il particolare riconoscimento che riceve questa "speciale forma di manifestazione del pensiero di una persona nei suoi esclusivi rapporti con un'altra persona"[16] ha come presupposto che la comunicazione sia indirizzata a soggetti determinati e individuati e che sia trasmessa con modalità che escludono in linea di massima la conoscibilità da parte di terzi, sì da salvaguardarne, per quanto possibile, la segretezza. Un requisito che ricorre, secondo "quanto abitualmente si ritiene", anche qualora non vi possa essere certezza sulla esclusività della comunicazione perché, ad es., si utilizzi un impianto telefonico che oltre all'apparecchio principale abbia delle derivazioni o consenta comunque un inserimento in linea attraverso il centralino per lo smistamento delle chiamate. Decisiva è la circostanza che possa ammettersi una "presunzione di riservatezza del messaggio", in quanto il mezzo prescelto per la comunicazione presenti "tutte quelle normali cautele che sono necessarie per la garanzia costituzionale"[17].

Quanto poi alla estensione della tutela attribuita dalla Costituzione alle comunicazioni, se non vi è difficoltà a individuarne il momento di inizio e di conclusione quando si tratta di comunicazioni che richiedono la contemporanea partecipazione dei soggetti coinvolti (si pensi ad una telefonata), qualche precisazione richiede la corrispondenza epistolare, dovendosi stabilire a partire da quando e fino a quando il documento nel quale sia incorporata la espressione di pensiero che si vuole comunicare diviene oggetto di tutela costituzionale. Tradizionalmente, si suole attribuire carattere di corrispondenza ad un messaggio solo dal momento nel quale esso esce dalla materiale disponibilità del mittente - venendo inviato attraverso il mezzo di trasmissione prescelto - e fino al momento in cui il destinatario abbia

[15] Così C. cost. 26 febbraio 1993 n. 81, che richiama la precedente sentenza dell'11 luglio 1991 n. 366. In precedenza, nel senso che il "diritto garantito dall'art. 15 Cost. possa essere compresso solo nei limiti effettivamente richiesti da concrete, gravi esigenze di giustizia", C. cost. 4 aprile 1973 n. 34.

[16] Cfr. A. PACE, *Commento all'art. 15 Cost.*, in G. AMATO, A. PACE, F. FINOCCHIARO, *Rapporti civili (artt. 13-20), Commentario della Costituzione a cura di G. Branca*, Bologna, Zanichelli, 1977, p. 81, nota 6.

[17] Così A. PACE, *op. cit.*, p. 88, nota 5; in senso più ampio, A. VALASTRO, *La tutela penale delle comunicazioni intersoggettive, fra evoluzione tecnologica e nuovi modelli di responsabilità*, in *Riv. it. dir. proc. pen.*, 1999, 997 ss.

preso conoscenza del suo contenuto: in questo frangente si ritiene esaurita la fase della 'comunicazione' vera e propria. Prima e dopo questi momenti, l'eventuale abusiva cognizione da parte di terzi del contenuto del messaggio non verrà in considerazione come violazione di corrispondenza, risultando semmai applicabile la normativa sui segreti documentali o sui dati personali (v. *infra*, § 2.3).

Rispetto a messaggi intersoggettivi trasmessi con modalità idonee a precluderne la conoscenza da parte di estranei, l'art. 15 Cost. riconosce, in capo sia al mittente che al destinatario, un diritto soggettivo alla segretezza della comunicazione, che può subire limitazioni solo in forza di un provvedimento dell'autorità giudiziaria e con le garanzia stabilite dalla legge. E poiché questa situazione giuridica soggettiva è stata dal Costituente qualificata come "inviolabile", deve ritenersi che, nel dubbio, essa debba essere considerata prevalente rispetto ad altre libertà o poteri costituzionalmente rilevanti, con i quali venga eventualmente a confliggere[18]. A questo proposito, la Corte costituzionale ha avuto occasione di precisare che tale diritto "non può subire restrizioni o limitazioni da alcuno dei poteri costituiti se non in ragione dell'inderogabile soddisfacimento di un interesse pubblico primario costituzionalmente rilevante, sempreché l'intervento limitativo posto in essere sia strettamente necessario alla tutela di quell'interesse"[19].

Al di fuori dei casi nei quali eccezionalmente la legge ne preveda delle limitazioni, opera dunque un generale divieto d'interferenza sia per le pubbliche autorità che per i privati, alla stregua del quale appare problematica – per quello che qui più ci interessa – la rilevanza che può essere attribuita all'eventuale rinuncia al diritto stesso da parte del suo titolare nell'ambito di un rapporto essenzialmente non paritario, qual è il rapporto di lavoro subordinato. Certo è che, stanti le garanzie delle quali la Costituzione circonda la libertà di esprimersi, un potere di interferenza nelle comunicazioni private del lavoratore non può essere attribuito al datore di lavoro per il solo fatto di essere proprietario degli strumenti attraverso i quali quelle comunicazioni si realizzano: su questo punto, come si è visto, si è pronunciato con chiarezza il Gruppo di lavoro sulla protezione dei dati nel "Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro" del maggio 2002[20]. Qui si può solo aggiungere che il potere di disporre del mezzo di comunicazione consente al datore di lavoro di impedirne l'utilizzo da parte di terzi, ma non gli attribuisce alcun diritto a prendere cognizione

[18] Così, ancora, A. PACE *op. cit.*, p. 96 e p. 100, nella quale si parla a questo proposito di una "presunzione di 'preferenza' che discende dall'inviolabilità della situazione in esame".
[19] Così C. cost. 11 luglio 1991 n. 366 *cit*.
[20] V. *retro*, § 1.

del contenuto dei messaggi comunicati servendosi di quel mezzo, pur in assenza di qualsivoglia autorizzazione da parte sua.

2.1. *L'equiparazione della corrispondenza informatica alle forme tradizionali di corrispondenza*. Il diritto alla libertà e alla segretezza delle comunicazioni private è sancito dall'art. 15 Cost. per "ogni forma di comunicazione" privata, anche diversa dalla corrispondenza vera e propria, tradizionalmente identificata con quella telefonica, epistolare o telegrafica[21]: indiscutibile è dunque la sua estensione anche a quella nuova forma di comunicazione che si realizza attraverso il servizio di posta elettronica.

Benché la Corte costituzionale italiana non abbia avuto ancora occasione di pronunciarsi al riguardo, ai fini del riconoscimento di una totale assimilazione della corrispondenza elettronica a quella 'tradizionale' appare significativa la giurisprudenza della Corte europea dei diritti dell'uomo, che non ha esitato ad estendere ai messaggi di posta elettronica le garanzie di riservatezza sancite, anche per la corrispondenza, dall'art. 8 CEDU[22].

In una pronuncia del 3 aprile 2007 (Copland v. The United Kingdom) la Corte ha infatti ritenuto in contrasto con quella disposizione la lettura da parte del Vicepreside (*Deputy Principal*) dei messaggi di posta elettronica, così come l'intercettazione delle telefonate e della navigazione in Rete, di una dipendente del Carmarthenshire College, amministrato dallo Stato. Nel caso di specie, le ingerenze nella sfera privata della dipendente, da parte di un'autorità pubblica, non erano consentite ai sensi del secondo comma dell'art. 8 CEDU, non sussistendo all'epoca dei fatti, nell'ordinamento inglese, alcuna disposizione di legge che disciplinasse le condizioni in presenza delle quali i lavoratori potessero essere controllati nell'uso del telefono, della casella di posta elettronica e di Internet, messi a loro disposizione per l'espletamento dell'attività lavorativa. A ciò si aggiungeva la circostanza che la dipendente non era stata avvertita di quel possibile controllo e del tutto ragionevole appariva, quindi, da parte sua, l'aspettativa di riservatezza delle sue comunicazioni.

D'altra parte, nessuna rilevanza è stata attribuita dalla Corte alla circostanza che il controllo si sarebbe esaurito nel monitoraggio dei c.d. dati esterni alle comunicazioni ricavabili dalla bolletta telefonica (numero chiamato, data e ora della chiamata e sua lunghezza, così come i siti

[21] Cfr. A. PACE *op. cit.*, p. 93: "una volta costituito un servizio di comunicazione il quale istituzionalmente e tecnicamente trasmetta in via riservata messaggi intersoggettivi [deve] dirsi conseguentemente imposto, all'ente pubblico o al soggetto privato che ne abbia la gestione, il dovere di rispettare la libertà e la segretezza delle comunicazioni inoltrate".

[22] Cfr. Art. 8 CEDU: "*Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui*".

Internet visitati, giorno, ora e durata del collegamento), nonché dei soli indirizzi delle e-mail inviate o ricevute, senza lettura del loro contenuto. A parere della Corte, già espressasi al riguardo in un caso di intercettazione telefonica, anche queste informazioni devono essere considerate "elemento integrale delle comunicazioni effettuate", sì che la loro indebita acquisizione comporta una violazione della sfera privata altrui[23].

Nell'ordinamento italiano l'espressa equiparazione tra le forme tradizionali di corrispondenza e l'*electronic mailing* è stata sancita per la prima volta dal legislatore penale che, in occasione dell'introduzione nel codice penale di diverse figure di reato informatico con la legge 547/1993, ha sentito la necessità di ampliare la nozione di corrispondenza rilevante "agli effetti della legge penale", contenuta nell'ultimo comma dell'art. 616 c.p., per includervi, accanto a quella "epistolare, telegrafica o telefonica", originariamente contemplata, anche quella "*informatica o telematica*, ovvero effettuata con ogni altra forma di comunicazione a distanza". Conseguentemente, anche la corrispondenza elettronica può essere oggetto dei fatti di "violazione, sottrazione e soppressione di corrispondenza", repressi dall'art. 616 c.p., ancorché la scelta del legislatore di soddisfare le nuove esigenze di tutela penale, estendendo l'applicabilità di una fattispecie costruita intorno a forme diverse di corrispondenza – e rimasta invariata nella sua formulazione –, abbia creato alcuni problemi interpretativi, come tra breve vedremo[24].

In questa sede appare necessario precisare che cosa debba intendersi per 'corrispondenza informatica' ai fini di quella disposizione, avendo riguardo alle diverse fasi nelle quali si articola la trasmissione di un messaggio elettronico, a partire dal momento nel quale viene registrato nella memoria interna del sistema informatico, fino al momento in cui perviene a conoscenza del destinatario. Sotto questo profilo, oggetto delle condotte descritte nell'art. 616

[23] Cfr. Malone c. Royaume-Uni (2 agosto 1984), avente ad oggetto l'intercettazione delle telefonate di un antiquario sospettato di ricettazione, effettuate dalla polizia su mandato del ministro dell'Interno: in questa occasione la Corte ha ritenuto che, in assenza di una disciplina espressa, costituisse violazione dell'art. 8 CEDU la comunicazione alla polizia, senza il consenso dell'abbonato, dei dati relativi ai numeri telefonici chiamati - dei quali erano state raccolte le tracce con un apposito apparecchio di registrazione - poiché tali numeri sono parte integrante delle comunicazioni telefoniche. Si veda anche la sentenza Halford c. Royaume-Uni del 1997, avente ad oggetto delle telefonate private sul luogo di lavoro, che erano state intercettate senza che la lavoratrice fosse stata avvisata e in presenza quindi di una sua legittima aspettativa circa il loro carattere privato; anche in questo caso la Corte ha dovuto prendere atto della assenza, all'epoca dei fatti, di previsioni di legge che autorizzassero il controllo da parte dell'autorità pubblica.

[24] Con la stessa legge 547/1993 sono state introdotte nuove figure di reato a tutela delle comunicazioni informatiche nel loro 'profilo dinamico', sulla falsariga di quelle già contemplate dal codice penale per le comunicazioni telegrafiche e telefoniche (artt. 617–617-ter). In particolare, l'art. 617-*quater* c.p. punisce "chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe". Questa norma trova applicazione ogniqualvolta si sia presa cognizione del contenuto della comunicazione privata intromettendosi fraudolentemente nella fase della sua trasmissione e non già attraverso la lettura del supporto nel quale quel contenuto era stato fissato: ipotesi, quest'ultima, di violazione della corrispondenza ai sensi dell'art. 616 c.p.

c.p. risulta essere: a) il messaggio registrato nella memoria del *computer* del mittente – di solito in un apposito archivio –, in attesa di essere trasmesso al *server* del fornitore del servizio di posta elettronica (c.d. *e-mail provider*) utilizzato dal mittente stesso; b) il messaggio proveniente dal mittente e presente nella memoria del *server* dell'*e-mail provider*, in attesa di essere trasmesso all'elaboratore del *provider* utilizzato dal destinatario (se diverso da quello del mittente); c) il messaggio trasmesso dal *provider* del mittente e presente nella memoria del *server* dell'*e-mail provider* del destinatario (se diverso da quello del mittente), in attesa di essere ricevuto da quest'ultimo, in occasione del primo collegamento alla sua 'casella postale' (*account*); d) il messaggio finalmente giunto a destinazione, presente nella memoria del *computer* del destinatario e in attesa di essere letto da quest'ultimo. Similmente a quanto si è detto per la corrispondenza epistolare, quando il destinatario giunge a conoscenza del contenuto del messaggio elettronico, la comunicazione si è realizzata e i dati dai quali il messaggio è composto ricevono tutela dall'ordinamento in quanto tali e non più per la libertà e segretezza che doveva essere assicurata alla loro comunicazione[25].

L'equiparazione tra la tradizionale corrispondenza epistolare e la posta elettronica deve ritenersi operante con riguardo non solo alle caselle (c.d. *account*) di posta liberamente create dall'individuo presso uno dei tanti gestori del servizio (c.d. *service provider*) accessibili dalla Rete (si pensi a yahoo!, libero, alice, gmail, etc.), ma anche a quella 'personale' che al dipendente sia stata attribuita sul luogo di lavoro. La circostanza che l'indirizzo (il c.d. dominio) presso il quale è attivato l'*account* personale del lavoratore corrisponda a quello del datore del lavoro – sia esso il nome di una società, di uno studio professionale o quello dello stesso datore di lavoro – non incide sul carattere privato che comunque deve essere riconosciuto ai messaggi che per il suo tramite il lavoratore inoltra e riceve. Ciò che conta è solo il fatto che al lavoratore sia attribuita una specifica casella di posta, contraddistinta dal suo nome e direttamente accessibile attraverso una *password* a lui soltanto nota[26]: tutte le comunicazioni effettuate servendosi di quella casella devono essere considerate riservate e quindi oggetto delle garanzie previste per le comunicazioni private dall'art. 15 Cost. Non solo: riservati devono anche essere considerati i c.d. dati esterni alla comunicazione informatica gestita attraverso quella casella di

[25] Così, ad esempio, con riguardo ai dati che compongono i messaggi di posta elettronica già letti ed eventualmente conservati nell'apposito archivio previsto dai programmi di gestione della corrispondenza elettronica, non sarà più applicabile l'art. 616 c.p., bensì la norma sul danneggiamento informatico (art. 635-bis c.p.) nel caso in cui vengano cancellati o altrimenti manomessi; allo stesso modo, sarà applicabile la norma sulla rivelazione del contenuto di documenti segreti (art. 621 c.p.) qualora il loro contenuto – destinato a rimanere segreto – sia oggetto di un'indebita rivelazione, etc. Sul tema, C. PECORELLA, *Il diritto penale dell'informatica,* II ed., Padova, Cedam, 2006, p. 295 s.

[26] Per l'ipotesi frequente, nella quale il lavoratore renda conoscibile a terzi la sua *password*, per garantire l'accesso alla sua casella di posta in situazioni di emergenza, v. *infra*.

posta, come espressamente riconosciuto dalla Corte costituzionale, in linea con la già ricordata giurisprudenza della Corte europea dei diritti dell'uomo[27].

Si tratta ora di vedere se e in quali casi il mancato rispetto di questa sfera di riservatezza da parte del *datore di lavoro* – e/o di altra persona da lui autorizzata – assuma rilevanza penale nell'ordinamento italiano.

2.2. *Controllo 'in tempo reale' e tutela penale della* segretezza *della corrispondenza.* La prima forma di controllo da considerare è quella che si realizza sulla posta elettronica quando il processo comunicativo non si è ancora esaurito, perché il messaggio non è ancora pervenuto a conoscenza del destinatario. Per queste ipotesi, come si è anticipato, il codice penale italiano prevede una specifica figura di reato, diretta a reprimere la violazione, la sottrazione e la soppressione di corrispondenza da parte di persona diversa da quella alla quale la corrispondenza è diretta (art. 616 c.p.)[28]. Tuttavia, a differenza delle condotte di sottrazione, distrazione, distruzione e soppressione della corrispondenza altrui (ossia, ad altri diretta), che possono avere ad oggetto qualsiasi tipo di corrispondenza (anche quella 'aperta', come nel caso di una cartolina postale), la violazione della *segretezza* della corrispondenza, consistente nel fatto di "prendere cognizione" del contenuto di messaggi ad altri inviati, assume rilevanza solo nei confronti della corrispondenza 'chiusa', qual è, tipicamente, la lettera inserita in una busta suggellata.

L'applicazione di questa disposizione nei casi di controllo 'in tempo reale' della posta elettronica del lavoratore dipende dunque dalla possibilità di qualificare come corrispondenza 'chiusa' il messaggio elettronico inviato e ricevuto attraverso il sistema informatico del datore di lavoro: una possibilità che è stata sino ad oggi esclusa dalla giurisprudenza, in quei pochi casi nei quali ha avuto occasione di pronunciarsi, aventi ad oggetto la presa visione, da parte del datore di lavoro o comunque del superiore gerarchico del lavoratore, dei messaggi da quest'ultimo ricevuti o inviati servendosi del proprio indirizzo di posta elettronica aziendale[29].

Muovendo dalla premessa che l'indirizzo di posta elettronica attribuito al lavoratore "può sempre essere nella disponibilità di accesso e lettura da parte di persone diverse dall'utilizzatore

[27] Cfr. C. cost. 26 febbraio 1993 n. 81, cit. La tutela della segretezza dei 'dati esterni' è affidata alle disposizioni penali sulle intercettazioni (artt. 617 ss. c.p.).

[28] Il primo comma dell'art. 616 c.p. dispone che "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 € 30 a € 516".

[29] Cfr. T. Milano, 10 maggio 2002, Ceriani, in *Foro it.* 2002, II, 385 ss.; T. Torino, sez. distaccata di Chiasso, 20 giugno 2006, Tramalloni, in *Dir. Internet*, 2007, 275 ss. con nota di M. VIOLANTE; *Foro it.* 2007, II, 132, nonché Cass. V, 19 dicembre 2007, Tramalloni, in *DII* 2008, 64 ss.; *Nuova giur. civ. commentata*, 2008, I, 957 ss. con nota di A. SITZIA; *Cass. pen.*, 2008, 4670 con nota di S. ATERNO; *Foro it.*, 2008, II, 137 s.

consuetudinario (ma sempre appartenenti all'azienda) a prescindere dall'identità o diversità di qualifica o funzione"[30], i giudici italiani hanno ritenuto che i messaggi inviati o ricevuti dal lavoratore, servendosi di quell'indirizzo, abbiano carattere di corrispondenza 'chiusa' solo nei confronti di soggetti *esterni* all'azienda che, in quanto tali, non sono legittimati "all'accesso ai sistemi informatici di invio o di ricezione dei singoli messaggi"[31]. Più precisamente, per la giurisprudenza quella corrispondenza non potrebbe dirsi 'chiusa' e quindi segreta rispetto a chi abbia la legittimazione all'uso del sistema informatico adoperato per la sua comunicazione – in ragione della proprietà del mezzo stesso o sulla base delle norme interne che ne regolano l'utilizzo –, perché tale legittimazione "abilita alla conoscenza delle informazioni in esso custodite"[32]. La circostanza che il dipendente debba digitare la propria *password* per accedere alla *sua* casella di posta elettronica viene considerata ininfluente perché, coerentemente con le premesse, a quella cautela viene attribuita la sola finalità di impedire che al servizio di corrispondenza elettronica posto a disposizione del lavoratore "possano accedere persone estranee alla società"[33].

In base a questa impostazione teorica, che comunque non nega in linea di principio che anche la corrispondenza informatica possa avere carattere 'chiuso', laddove sia indirizzata ad un *account* personale di posta[34], sarebbe lecita la lettura della corrispondenza del lavoratore da parte di chiunque sia 'legittimato' all'uso della sua *password* e quindi all'accesso ai messaggi presenti nella sua casella di posta. Sul piano pratico, ciò significa legittimare l'intrusione del datore di lavoro e/o del superiore gerarchico, ai quali - come spesso avviene – il lavoratore abbia consegnato una copia della propria *password*, per consentire l'accesso alla sua casella di posta in situazioni di emergenza che non consentano l'intervento diretto del lavoratore, oppure che risultino autorizzati dalla normativa interna ad accedere al *server* di posta aziendale, sul quale sono memorizzate le *password* dei dipendenti e i messaggi in transito sui loro *account* personali.

[30] Così T. Milano, 10 maggio 2002, Ceriani, *cit*,, 387.
[31] Così Cass. V, 19 dicembre 2007, Tramalloni, *cit.* 957.
[32] Così Cass. V, 19 dicembre 2007, Tramalloni, *cit. ibidem.*
[33] Così T. Milano, 10 maggio 2002, Ceriani, *cit*,, *ibidem.*
[34] Sulla possibilità di distinguere, anche con riferimento alla corrispondenza informatica, tra corrispondenza 'aperta' e 'chiusa' ai sensi dell'art. 616 c.p., v. C. PECORELLA, *Il diritto penale dell'informatica* cit., p. 296 ss. *Contra,* G. FIANDACA, E. MUSCO, *Diritto penale. Parte speciale*, vol. II, tomo primo, II ed., 2007, secondo i quali "la prima parte dell'art. 616 c.p., facendo riferimento alla *corrispondenza chiusa*, impedisce, di fatto, l'estensione anche alla corrispondenza telematica se non in violazione del divieto di analogia. E le stesse difficoltà sussistono anche per le altre condotte incriminate dalla norma (…) Sembra difficile poter qualificare la corrispondenza telematica come corrispondenza chiusa o aperta, termini che fanno, infatti, riferimento a oggetti fisicamente tangibili, quali le buste da lettera" (p. 260 s.). Nel senso che "l'invio di un messaggio via *e-mail* costituisce certamente corrispondenza chiusa", dovendosi guardare alla "volontà di esclusione dei terzi, quale desumibile dalle modalità trasmissive adottate", A. VALASTRO, *La tutela penale delle comunicazioni intersoggettive*,cit., p. 1002.

Tuttavia, questa soluzione giurisprudenziale solleva non poche perplessità, non essendo chiaro quale sia il fondamento della 'legittimazione' di quei soggetti alla lettura della corrispondenza del lavoratore, che nella ricostruzione operata dai giudici sembra doversi cogliere in una sorta di condivisione, con il dipendente, della sua casella 'personale' di posta elettronica, dal momento che la corrispondenza in essa presente sarebbe da essi liberamente consultabile. Una condivisione che certo poco si concilia con l'apparente individualità dell'indirizzo di posta assegnato al lavoratore e contrassegnato da una chiave d'accesso a lui esclusivamente attribuita; diverso sarebbe il caso ove esistessero diversi *account* di posta per specifiche aree di lavoro, protette all'esterno da un'unica *password*, comune a tutte le persone che vi appartengono e che hanno necessità di utilizzare il servizio di *electronic mailing* per esigenze lavorative: nessuna aspettativa di riservatezza potrebbe creare un sistema di questo tipo, nel quale sarebbe chiara a tutti la utilizzabilità per fini esclusivamente lavorativi del mezzo di comunicazione messo a disposizione dal datore di lavoro.

Viceversa, la situazione nella quale si trova il dipendente, titolare di una casella di posta personale, porta a ritenere del tutto ragionevole la sua aspettativa alla segretezza dei messaggi inviati e ricevuti attraverso di essa[35], negli stessi termini nei quali, sul luogo di lavoro, il dipendente può pacificamente contare sulla riservatezza delle proprie conversazioni telefoniche e della corrispondenza epistolare a lui esclusivamente indirizzata. Né tale aspettativa può essere negata perché altre persone sono in grado di accedere a quei messaggi: come si è visto, la circostanza che il telefono aziendale sia dotato di un centralino per lo smistamento delle telefonate, che renda di fatto possibile l'ascolto delle comunicazioni altrui, non giustifica la violazione della riservatezza delle conversazioni effettuate dal dipendente servendosi di quel mezzo. Dovendosi poi escludere che la proprietà del mezzo attribuisca al datore di lavoro il diritto di prendere conoscenza dei messaggi personali del lavoratore, l'unica interferenza che il lavoratore può attendersi, nella sua corrispondenza informatica sul posto di lavoro, è quella eccezionalmente resasi indispensabile per proseguire l'attività lavorativa in sua assenza: è proprio per quelle situazioni, infatti, che al lavoratore viene chiesto di depositare, in forma riservata, una copia della *password* necessaria per accedere alla sua casella di posta. Questa particolare ipotesi, tuttavia, non consente di ritenere 'aperta' la corrispondenza del lavoratore nei confronti del datore di lavoro e/o del superiore gerarchico, per il solo fatto che ad essi è stata consegnata dal dipendente la chiave per accedere alla sua casella di posta; dovrebbe piuttosto ritenersi che il lavoratore, così facendo, abbia *consentito* all'accesso alla propria casella da parte

[35] Sottolinea questo aspetto il Garante per la protezione dei dati personali, nel provvedimento del 21 gennaio 2010 (*"Posta elettronica aziendale e* privacy *del dipendente"*).

del datore di lavoro e/o del suo superiore gerarchico, se e in quanto ricorrano le condizioni per le quali quel consenso gli è stato chiesto.

Non è dunque in discussione, la natura 'chiusa' o 'aperta' della corrispondenza del lavoratore, perché quella corrispondenza deve ritenersi 'chiusa' nei confronti di chiunque, sia esso esterno o interno all'impresa. Viene piuttosto in rilievo il consenso prestato dal lavoratore alla lettura dei suoi messaggi di posta elettronica da parte di determinate persone e in presenza di certe circostanze; un consenso che giustificherebbe e quindi renderebbe lecita la violazione di corrispondenza ai sensi dell'art. 616 c.p., altrimenti realizzata nei confronti del dipendente, anche e proprio da quelle persone che la giurisprudenza italiana ritiene, invece, senza una plausibile ragione, incondizionatamente 'legittimate' all'accesso alla sua casella di posta elettronica. E' dunque alle condizioni di validità di quel consenso che deve ora rivolgersi la nostra attenzione.

Come opportunamente evidenziato dal Gruppo di lavoro sulla protezione dei dati, problematica appare l'attribuzione di rilevanza al consenso prestato dal lavoratore nei confronti di comportamenti del datore di lavoro che limitino o compromettano dei suoi diritti: il consenso può infatti ritenersi 'liberamente' dato solo da chi può negarlo "senza pregiudizio per i propri interessi" (*retro*, § 1).

La questione appare ancor più delicata laddove, come nel caso che ci interessa, sia in gioco un diritto del lavoratore al quale la Costituzione attribuisce carattere inviolabile e che, in quanto rientrante tra i diritti della personalità, avrebbe "gli attributi (coessenziali a tali diritti) della assoluta intrasmissibilità, irrinunciabilità, indisponibilità e imprescrittibilità"[36].

La consapevolezza della oggettiva incapacità del lavoratore ad esprimere un libero consenso sul luogo di lavoro ha in passato indotto il legislatore italiano a prevedere, nell'art. 4 dello Statuto dei lavoratori (l. 300/1970), che siano le rappresentanze sindacali aziendali (o, in mancanza di queste, la commissione interna) - e non già i lavoratori - a dover dare il consenso necessario per l'installazione di "impianti o apparecchiature di controllo" dai quali possa derivare un controllo a distanza dei lavoratori, e quindi, in ultima analisi, un possibile pregiudizio per la loro dignità personale[37]. L'inefficacia, a quei fini, del consenso dei singoli

[36] Così A. PACE, op. cit., 97.

[37] L'art. 4 della l. 300/1970, dopo aver posto, nel primo comma, il divieto di utilizzare "impianti audiovisivi e altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori", stabilisce nel secondo comma che "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". In merito a questa disposizione e alla sua

lavoratori viene ribadita dalla giurisprudenza, per la quale "l'unico consenso cui il legislatore ha voluto condizionare (…) la legittimità dell'uso e delle installazioni degli impianti di controllo è esclusivamente quello collettivo delle rsa, ovvero della c.i., ovvero ancora dell'Ispettorato del lavoro, essendo il bene tutelato dalla disposizione la 'personalità' del singolo, colto nella ricchezza della sua posizione esistenziale"[38]. Conseguentemente, è stata in diverse occasioni dichiarata l'illiceità dell'installazione di apparecchiature di controllo (indiretto) in violazione dell'art. 4 Stat. lav., a nulla rilevando la circostanza che "le maestranze fossero a conoscenza dell'esistenza degli impianti potenzialmente idonei al controllo né la circostanza che gli impianti stessi abbiano funzionato per un determinato periodo di tempo senza contestazioni da parte dei lavoratori"[39], così come l'esistenza di un "eventuale preavviso dato ai lavoratori"[40].

Una soluzione di questo tipo si impone anche per ottenere il consenso del lavoratore alla lettura della sua corrispondenza, che si renda necessaria per il proseguimento dell'attività lavorativa in sua assenza: indifferente, al riguardo, è il fatto che quella intrusione debba realizzarsi accedendo direttamente alla casella di posta del dipendente – attraverso la *password* da lui comunicata - oppure prendendo visione dei messaggi di posta attraverso il *server* aziendale. Anche in questo secondo caso, infatti, le garanzie di cui gode il diritto alla segretezza delle proprie comunicazioni private non consentono di ritenere equivalente al consenso del lavoratore la conoscenza, da parte sua, della possibilità tecnica di realizzare per quella via una intrusione nella sua sfera di riservatezza; ma neanche potrebbe dirsi implicito il suo consenso nella accettazione di condizioni di lavoro che includano espressamente la possibilità di lettura della posta elettronica dei lavoratori, ovvero l'espresso divieto di fare uso personale della casella di posta. Al di fuori di casi in cui sia limitato da un atto motivato dell'autorità giudiziaria, il diritto alla segretezza della propria corrispondenza privata, riconosciuto dall'art. 15 Cost., può venir meno solo per effetto di un consenso validamente prestato dal suo titolare: nell'ambito lavorativo ciò si traduce nella necessaria ricerca delle condizioni che garantiscano la libertà del lavoratore nella sua decisione di consentire ad altri l'accesso alla propria casella di posta elettronica. D'altra parte, se si riconosce che la libertà e la segretezza della propria corrispondenza rientrano "tra i valori supremi costituzionali"[41], nessuna limitazione potrà ad esse imporsi in considerazione del diritto di proprietà del datore di lavoro sul mezzo di

importanza ai fini della valutazione della legittimità del monitoraggio da parte del datore di lavoro dell'uso di Internet da parte dei dipendenti, v. *infra*, § 3.

[38] Così P. Catania 21 ottobre 1996, Jovino c. Costa, in *Dir. lav.*, 1997, II, 213.

[39] Così Cass. 18 febbraio 1983, n. 1236, Soc. off. meccaniche Vimercati c. Quagliarello, in *Foro it.*, 1985, I, 2076 nota di A. ROSSI.

[40] Così Cass. 6 marzo 1986, n. 1490, Soc. Italcementi c. Filcea, in *Or. giur. lav.*, 1986, 919.

[41] Così C. cost. 81/1993 cit.

comunicazione utilizzato dal lavoratore, ma neppure dei poteri di direzione, controllo e disciplina ad esso attribuiti dalla legge nell'ambito del rapporto di lavoro[42].

Così stando le cose, si comprende perché particolare interesse assumano le soluzioni che la tecnologia mette a disposizione, per far fronte ad esigenze lavorative sopravvenute senza violare la riservatezza della corrispondenza del lavoratore: soluzioni in gran parte suggerite dal Garante della *privacy* nel suo provvedimento del 1° marzo 2007, in quanto ritenute "utili per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza". Opportuno viene considerato, ad esempio, oltre all'impiego di indirizzi di posta condivisi tra più lavoratori di una stessa area di lavoro (in alternativa o in aggiunta all'indirizzo personale del lavoratore), come evidenziato in precedenza, anche il ricorso a quelle "apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (…), messaggi di risposta contenenti le 'coordinate' (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura". Una misura di questo tipo consentirebbe di non trascurare eventuali messaggi lavorativi urgenti, dei quali, per qualsivoglia ragione, il lavoratore non possa direttamente prendere conoscenza, senza dover accedere agli *account* personali dei dipendenti. Non solo: consentirebbe anche di risolvere un ulteriore problema, che sin qui abbiamo trascurato, collegato all'eventuale consenso, validamente prestato del lavoratore, alla lettura della propria corrispondenza: quel consenso, infatti, potrebbe giustificare la violazione di corrispondenza altrimenti realizzata dal datore e/o dal superiore gerarchico nei confronti del lavoratore, ma nessun rilievo potrebbe avere rispetto alla violazione da essi commessa nei confronti del mittente di un messaggio pervenuto alla casella di posta del lavoratore, e il cui contenuto sia a lui ancora sconosciuto.

2.3. *Il controllo sui messaggi archiviati*. Resta a questo punto da chiedersi se e a quali condizioni il datore di lavoro (o altra persona da lui autorizzata) possa leggere i messaggi contenuti nella casella di posta del dipendente, che non costituiscono più 'corrispondenza' in quanto la comunicazione si sia già conclusa. Messaggi che il lavoratore ha già inviato o che ha già letto, se ne era il destinatario, ma che siano ancora presenti nel suo *account* di posta, ovvero nella memoria del *server* di posta aziendale.

La circostanza che l'accesso all'*account* del lavoratore sia presidiato dalla sua *password* personale induce a ritenere che ogni intrusione che non sia consentita dal titolare integri un

[42] Il riferimento è agli artt. 2086, 2094, 2104 e 2106 c.c.

accesso abusivo ai sensi dell'art. 615-ter c.p.[43]. Benché, infatti, il legislatore italiano non abbia specificamente previsto che l'accesso abusivo possa riguardare, oltre che il sistema informatico nel suo complesso, anche una parte soltanto della sua memoria, che sia specificamente protetta da una misura sicurezza, non vi sono ostacoli letterali alla possibilità di ritenere che il reato si realizzi anche attraverso questa modalità, ogniqualvolta sussistano esigenze di tutela della riservatezza di dati e/o programmi, per l'accesso ai quali sia necessaria una specifica *password*, eventualmente diversa da quella richiesta per accedere al sistema[44].

A ciò si aggiunga che l'art. 615-ter c.p. punisce non solo l'introduzione ma anche la *permanenza* abusiva in un sistema informatico protetto, "contro la volontà espressa o tacita" del titolare dello *jus excludendi*. Con questa sottofattispecie il legislatore italiano ha voluto reprimere quelle ipotesi nelle quali l'introduzione in un sistema informatico protetto (o in una sua parte specificamente protetta) sia autorizzata, ma appaia pericolosa per l'interesse tutelato la permanenza all'interno del sistema, stante la possibilità di svolgere qualunque operazione consentita all'utente legittimo (compresa la lettura dei dati esistenti)[45].

Una permanenza abusiva di questo tipo potrà essere ravvisabile ogniqualvolta il datore di lavoro, avendo (eccezionalmente) accesso alla casella di posta del lavoratore, per far fronte ad esigenze lavorative improcrastinabili, ne approfitti per leggere la corrispondenza archiviata del lavoratore, che risulti *ictu oculi* priva di attinenza con quelle esigenze lavorative che sole hanno legittimato il suo ingresso in quella parte riservata e protetta del sistema informatico utilizzato dal dipendente.

Un'ultima considerazione, deve riguardare la diversa ipotesi, nella quale la lettura dei messaggi archiviati venga realizzata attraverso il *server* di posta aziendale, sul quale quei messaggi siano conservati, e senza che sia necessaria la digitazione della *password* del lavoratore, perché altrimenti si avrebbe accesso abusivo. In questi casi il messaggio di posta riceve tutela penale, come già anticipato, attraverso le disposizioni sulla inviolabilità dei segreti documentali, che però si limitano a sanzionare la rivelazione (non già l'*acquisizione*) del segreto[46]. Tuttavia, la possibilità per il datore di lavoro di conservare sul *server* di posta

[43] Sotto la rubrica "Accesso abusivo a un sistema informatico o telematico", l'art. 615-ter c.p. – inserito nel codice penale con la legge 547/1993 in precedenza richiamata – punisce con la reclusione sino a 3 anni "Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo".

[44] In proposito, cfr. C. PECORELLA, *Il diritto penale dell'informatica* cit., p. 339 ss.

[45] Diffusamente sul punto, C. PECORELLA, *Il diritto penale dell'informatica* cit., p. 349 ss.

[46] Ci riferiamo, in particolare, all'art. 621 c.p., con il quale si punisce "chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela, senza giusta causa, ovvero l'impiega a proprio o altrui profitto,… se dal fatto deriva nocumento". Tale disposizione è oggi applicabile anche ai segreti contenuti su un supporto informatico, in considerazione dell'aggiunta, ad opera della legge 547/1993 già richiamata, di un nuovo secondo comma del

aziendale i messaggi di posta transitati sui singoli *account* dei dipendenti è condizionata sia al rispetto delle disposizioni dello Statuto dei lavoratori che, come si è visto, vieta l'installazione di apparecchi che, per quanto funzionali all'organizzazione dell'attività lavorativa, possono tuttavia anche tradursi in uno strumento di controllo di quest'ultima, sia alle disposizioni del Codice sulla *privacy* (d.lgs. 30 giugno 2003 n. 196) per l'inevitabile raccolta di dati personali che consegue alla lettura della corrispondenza dei lavoratori.

3. Le condizioni di liceità del controllo sulla navigazione in Internet da parte dei dipendenti

In questa seconda parte del lavoro ci si interroga sulla liceità del controllo effettuato dal datore di lavoro sull'utilizzo dei *computer* connessi ad Internet da parte dei dipendenti; in particolare, oggetto di attenzione sono quelle situazioni in cui sia assente qualunque esigenza di riservatezza rispetto al *contenuto* delle informazioni consultate in Rete[47]. Se, infatti, attraverso Internet possono instaurarsi delle vere e proprie comunicazioni (si pensi agli scambi di *e-mail*, o all'utilizzo di strumenti di discussione in tempo reale, quali le *chat*), è tuttavia anche possibile che la navigazione comporti soltanto l'acquisizione di informazioni messe a disposizione del pubblico attraverso *computer* (*server*) collegati alla Rete. In questi casi, non intercorrendo una comunicazione *privata* tra due persone, ci si trova al di fuori dell'ambito di operatività dell'art. 15 Cost., in quanto l'eventuale controllo operato dal datore di lavoro avrebbe ad oggetto trasmissioni di dati prive del requisito della *riservatezza*, con conseguente inapplicabilità delle norme relative alla violazione delle comunicazioni e della corrispondenza di cui all'art. 616 e seguenti del codice penale, che puniscono la violazione delle sole comunicazioni dotate dei requisiti della *personalità*, o della *segretezza*[48].

Come si è visto (*retro*, § 1) il problema del controllo sulla navigazione in Rete dei dipendenti da parte del datore di lavoro appare tutt'altro che teorico: l'esperienza mostra quanto sia forte l'interesse ad effettuare controlli di questo tipo, soprattutto in contesti altamente

---

seguente tenore: "agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi".

[47] Recentemente, su questo tema, BELLAVISTA, *La Cassazione e i controlli a distanza sui lavoratori,* in *Riv. giur. lav. prev. soc.,* 2010, 2, 462; GALLARDI, *Il controllo sugli accessi ad internet al vaglio della Cassazione,* in *Riv. it. dir. lav*. 2010, 565; PERINA, *L'evoluzione della giurisprudenza e dei provvedimenti del garante in materia di protezione dei dati,* in *Riv. it. dir. lav.,* 2010, 305; BARRACO-SITZIA, *Il problema dei "controlli difensivi" del datore di lavoro:* estne saepe ius summum malitia?, in *Lav. giur.,* 2010, 991.

[48] Nel senso che, ai fini dell'applicabilità degli artt. 617 ss. c.p., le comunicazioni intercettate debbano essere *"comunicazioni chiuse, alle quali si può accedere soltanto violando la segretezza che le tutela",* Cass. V, 19 maggio 2005 n. 4011, in *Dir. giust.,* 2006, 13, 78.

tecnologizzati e quanto diffusi essi siano in Paesi – come ad esempio gli Stati Uniti – nei quali la legge non ponga limiti al loro svolgimento[49].

Tante sono le ragioni che inducono il datore di lavoro a monitorare l'utilizzo di Internet da parte dei dipendenti: esiste, in primo luogo, un interesse datoriale ad assicurarsi che i dipendenti utilizzino la connessione alla Rete solo per ragioni lavorative e che non se ne servano per fini personali durante l'orario di lavoro. In secondo luogo, il datore di lavoro può avere un legittimo interesse a controllare il traffico dei dati per garantire il buon funzionamento della rete aziendale (per limitare i danni, nell'ipotesi di diffusione di programmi *virus*, o per prevenire il rischio di atti dolosi, in occasione dell'introduzione da parte di estranei nella rete stessa). Va poi considerato che l'utilizzo scorretto dello strumento informatico da parte dei dipendenti potrebbe comportare una responsabilità del datore di lavoro nei confronti di terzi o quantomeno un suo coinvolgimento, sia pure indiretto, nell'attività illecita del dipendente[50]. A fronte di tutte queste plausibili ragioni del datore di lavoro sta l'interesse, di segno opposto, del lavoratore a non essere controllato e monitorato durante l'orario di lavoro.

Dal punto di vista tecnologico, il controllo sulla navigazione da parte dei dipendenti può realizzarsi in vario modo. Esistono numerosi strumenti specificamente progettati per il controllo delle operazioni svolte dall'utente del *computer*, le cui caratteristiche possono essere le più diverse: si può trattare di strumenti, tanto *hardware* quanto *software*, da installare sul *computer* affidato al dipendente oppure da collocare all'interno della rete informatica in un qualunque punto del percorso del flusso dati, che va dal singolo *computer* fino al *server* con il quale viene instaurata la connessione. Tali strumenti di controllo possono essere più o meno invasivi, potendo arrivare, nel caso estremo, a registrare ogni operazione compiuta dal lavoratore (ogni singola pressione dei tasti ed ogni movimento del *mouse*) così come il tempo di consultazione del *web* ovvero a permettere una osservazione da remoto ed all'insaputa dell'utente di quanto viene visualizzato sullo schermo del suo terminale.

Anche senza ricorrere ad appositi strumenti di controllo, l'acquisizione di informazioni relative alla navigazione effettuata è resa possibile dagli strumenti necessari (o comunque di comune impiego) per il collegamento alla Rete: una forma di controllo meno invasiva rispetto alla precedente, ma che consente comunque di raccogliere numerosi dati relativi all'utilizzo di

[49] Per una sommaria descrizione del problema negli Stati Uniti, cfr. AMY ROGERS, *You Got Mail But Your Employer Does Too: Electronic Communication and Privacy in the 21st Century Workplace*, 5 J. TECH. L. & POL'Y 1 (2000); per un'analisi comparata, cfr. LAWRENCE E. ROTHSTEIN, *Privacy or Dignity: Electronic Monitoring in the Workplace*, 19 N.Y.L. SCH. J. INT'L & COMP. L. 379 (2000) e, nella dottrina italiana, STANCHI, *Privacy, rapporto di lavoro, monitoraggio degli accessi ad Internet, monitoraggio delle e-mail e normative di tutela contro il controllo a distanza*, in AA.VV., *I poteri del datore di lavoro nell'impresa*, CEDAM, 2002, 102 ss.; TOFFOLETTO, *Nuove tecnologie informatiche e tutela del lavoratore*, Giuffrè, 2006, 35 ss.

[50] Sul punto STANCHI, *Privacy*, *cit.*, 118.

Internet da parte del lavoratore. Si pensi, ad esempio, ai programmi *browser*, che compilano normalmente un elenco degli indirizzi dei siti visitati[51] - consultabile dagli utenti successivi – e raccolgono quindi dati relativi alla navigazione in ogni singolo sito[52], nonché al *server* DNS[53], che può essere configurato in modo tale da conservare traccia degli indirizzi *web* selezionati. Benché non strettamente indispensabile per la navigazione in Internet, può tuttavia essere presente anche un *server proxy*[54], in grado di registrare informazioni relative a tutte le connessioni *web* effettuate, quali gli indirizzi dei *computer* coinvolti, l'indirizzo della pagina richiesta, la quantità di dati trasmessi, la pagina di provenienza etc.; allo stesso modo, attraverso l'utilizzo di un *firewall*[55], possono essere impostate regole particolari di monitoraggio per registrare connessioni verso specifici indirizzi *web*.

Alcuni degli strumenti citati (in primo luogo il *browser*) devono essere necessariamente collocati nel luogo in cui si trova l'utente e quindi, nel caso che a noi interessa, sono sempre nella sfera di controllo del datore di lavoro, che potrebbe, senza alcuna difficoltà, visualizzare in qualsiasi momento le registrazioni relative alle connessioni effettuate dal dipendente. Altri strumenti possono trovarsi, indifferentemente, nella disponibilità del datore di lavoro o in quella del fornitore dell'accesso alla Rete (*provider*).

In sintesi, il controllo da parte del datore di lavoro non trova alcun limite tecnico: al contrario, gli stessi strumenti che permettono la navigazione in Rete possono fungere contemporaneamente da strumento di controllo, e normalmente svolgono anche tale funzione, salvo che siano specificamente configurati per non effettuare alcuna registrazione.

3.1. *Controlli tecnologici e Statuto dei lavoratori.* Il primo e più rilevante *corpus* normativo contenente norme relative al controllo dei lavoratori sul luogo di lavoro è costituito dallo Statuto dei lavoratori che, pur essendo stato emanato in un periodo nel quale una diffusione delle tecnologie informatiche come quella attuale non era forse nemmeno prevedibile, contiene una dettagliata disciplina volta a prevenire i possibili risvolti negativi di un uso intenso della

[51] La *history* consiste in un elenco dei siti visitati che facilita all'utente il ritrovamento delle informazioni in precedenza reperite.

[52] I cosiddetti *cookies* sono brevi codici alfanumerici che i siti web inviano al programma *browser* perché questo li invii come riferimento ad ogni successivo contatto ai fini di una individuazione, anche se anonima, dell'utente.

[53] Il sistema DNS (acronimo di *Domain Name System*) permette l'associazione degli indirizzi numerici Internet (indirizzi IP) agli indirizzi in formato alfanumerico. Il server DNS viene consultato dal *browser* per conoscere l'indirizzo IP corrispondente all'indirizzo richiesto dall'utente.

[54] Un server *proxy* funge da "intermediario" tra due *computer* in una rete: ad esempio se un utente richiede una pagina contenuta in uno specifico server web, il browser può essere configurato in modo da indirizzare la richiesta non direttamente al server ma ad un *proxy* che si occupa di prelevare tale pagina e inoltrarla al *computer* dell'utente. Lo scopo di tale sistema è normalmente quello di effettuare una copia locale delle pagine più richieste, in modo da poterle fornire più velocemente in caso di richieste successive, di fornire esclusivamente le pagine provenienti da siti web approvati oppure ancora di tenere traccia di tutte le pagine visitate.

[55] Il *firewall* è un componente di una rete informatica che ha la funzione primaria di impedire le trasmissioni di dati indesiderate.

tecnologia a fini di controllo, nel contesto di una più generale sfiducia verso modalità invasive (tecnologiche o meno) di sorveglianza sui lavoratori. Tali norme andavano a 'correggere' l'impianto originario del codice civile del 1942, nel quale il potere del datore di lavoro di controllare l'attività dei lavoratori derivava dalle disposizioni degli artt. 2086 e 2104, che prevedono la subordinazione gerarchica dei lavoratori all'interno dell'impresa e l'obbligo degli stessi di sottostare alle disposizioni dell'imprenditore; in base a tali norme, l'utilizzo di strumenti di controllo sarebbe sempre lecito, in quanto espressione del potere, teoricamente illimitato, di controllare l'attività dei lavoratori.

Con lo Statuto dei lavoratori sono stati introdotti limiti stringenti alle modalità con le quali il datore di lavoro può effettuare il controllo dei dipendenti: si è previsto il divieto di controllo mediante guardie giurate, l'obbligo di comunicare ai lavoratori il nominativo del personale addetto alla vigilanza sull'attività lavorativa, il divieto di indagini sulle opinioni ed il divieto - particolarmente rilevante ai nostri fini - di utilizzo di strumenti per il controllo a distanza dei lavoratori. Rispetto al generale potere di controllo, derivante dagli artt. 2086 e 2104 c.c., le limitazioni introdotte dallo Statuto si configurano quali eccezioni: le modalità di controllo da esso non espressamente vietate o sottoposte a condizione devono essere considerate lecite o comunque senza limiti ulteriori. In particolare, lo Statuto non pone limiti al controllo effettuato di persona dal datore di lavoro sull'attività lavorativa dei dipendenti né, ovviamente, vieta di controllare il risultato dell'attività lavorativa, per valutarne l'adeguatezza rispetto alle mansioni attribuite al dipendente.

Per quanto riguarda gli strumenti di controllo a distanza sul luogo di lavoro (originariamente per lo più identificati con gli impianti di videosorveglianza a circuito chiuso), il legislatore del 1970 si è dimostrato consapevole del rischio che il loro impiego possa rendere disumano il luogo di lavoro, per effetto di un controllo costante ed illimitato mediante strumenti *"totalizzanti e capaci di afferrare ogni momento dell'attività dei lavoratori"*[56]. Le apparecchiature di controllo "a distanza" apparivano pericolose per la *"dignità e la libertà"* dei lavoratori, che lo Statuto mira a proteggere, in quanto non consentivano al lavoratore di conoscere in quale momento fosse effettivamente controllato, a differenza di quanto avviene in occasione di un controllo effettuato di persona dal datore di lavoro o dai suoi incaricati. Inoltre, tali strumenti permetterebbero, con una spesa relativamente contenuta, di tenere sotto controllo contemporaneamente e costantemente la totalità dei lavoratori: un risultato altrimenti difficilmente raggiungibile, se non impiegando risorse umane ed economiche sproporzionate al fine perseguito. In sostanza, il controllo a distanza poteva causare nel lavoratore la sensazione di

[56] BELLAVISTA, *Controlli elettronici e art. 4 dello Statuto dei Lavoratori*, in *Riv. giur. lav.*, 2005, 775.

essere controllato costantemente, con conseguente azzeramento del suo spazio di autonomia, anche al di là di quanto necessario per lo svolgimento della prestazione lavorativa e con effetti disumanizzanti sul suo comportamento.

Per queste ragioni l'art. 4 Stat. lav. prevede, nel primo comma, un divieto assoluto di utilizzare *"impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori"*[57]; si ammette, tuttavia, nel secondo comma che strumenti di controllo *"dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori"* – quindi non finalizzati a tale controllo – e che siano *"richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro"* possano essere installati, ma solo in presenza di un accordo con le rappresentanze sindacali, ovvero, qualora questo non venga raggiunto, con il consenso dell'Ispettorato del lavoro.

Tale soluzione è un ulteriore segnale della sfiducia del legislatore nei confronti dell'utilizzo di strumenti di controllo, e una conferma del giudizio di pericolosità degli stessi. È significativo che venga richiesto il coinvolgimento delle rappresentanze sindacali, non ritenendosi sufficiente il consenso dei singoli lavoratori, che potrebbero essere spinti, dalla disparità di forza contrattuale, ad acconsentire a forme di controllo non giustificate da effettive esigenze produttive o di sicurezza. Come già accennato, il fatto che lo Statuto limiti le possibilità di controllo attraverso *"apparecchiature o impianti"* consente, per esclusione, di affermare la liceità di controlli sull'attività dei lavoratori effettuati *"di persona"* (direttamente dal datore o mediante l'opera di altri subordinati[58]), salvo il rispetto delle altre norme dello Statuto relative ai controlli.

Della disposizione appena esaminata è stata criticata la formulazione, che renderebbe problematico il coordinamento fra quanto disposto nel primo comma – il divieto di *uso* di apparecchiature per finalità di controllo – e quanto invece previsto nel secondo comma – il divieto di *installare* apparecchiature che *possono* avere tale finalità, in assenza di determinate condizioni: la lettera della legge consentirebbe di ritenere ammissibile la mera installazione di strumenti aventi la specifica finalità di controllo, purché non seguita da un loro effettivo

[57] Dispone infatti l'art. 4 Stat. lav. che *"È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati 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"*.

[58] Il controllo può essere effettuato anche da persone diverse da quelle specificamente addette alla vigilanza dell'attività lavorativa, i cui nominativi debbono essere comunicati ai lavoratori ai sensi dell'art. 3 l. 300/1970: cfr. Cass. lav., 12 agosto 1998, n. 7933 (CED 517990), in *Notiz. giur. lav.*, 1998, 697.

utilizzo[59]. A questa possibile conclusione, tuttavia, si è giustamente contrapposta la necessità di una lettura della disposizione che dia conto proprio della differenza dei termini in essa impiegati per pervenire ad affermare la sussistenza di un divieto generale sia dell'uso, sia della mera installazione di strumenti di controllo, risultando quest'ultimo derogabile solo in presenza di accertate esigenze produttive[60].

La violazione di tali divieti è oggi sanzionata penalmente mediante un complesso sistema di rinvii[61], dai quali si ricava che si tratta di un reato contravvenzionale, punito con la pena dell'arresto fino a tre mesi o dell'ammenda fino a 206 euro.

Quanto alla nozione di *"controllo a distanza"*, la giurisprudenza ne ha accolto un'accezione piuttosto ampia, ritenendo violato il divieto posto dall'art. 4 Stat. lav. in tutte le seguenti ipotesi: installazione di un congegno di sicurezza, all'ingresso del locale *garage* messo a disposizione dei dipendenti, che, essendo attivabile mediante un tesserino personale, consente di risalire all'orario di uscita di ciascun dipendente[62]; effettuazione di un controllo, mediante telecamera a circuito chiuso, di una dipendente sospettata di sottrarre denaro dalla cassa di un pubblico esercizio[63]; installazione di un impianto televisivo a circuito chiuso, ancora non attivato e dell'esistenza del quale i dipendenti erano consapevoli[64], indipendentemente dal fatto che il controllo fosse destinato ad essere discontinuo perché esercitato in locali dove i lavoratori si sarebbero trovati solo saltuariamente[65].

Al contrario, è stato ritenuto legittimo, stante il mancato utilizzo di "apparecchiature" o di "impianti", il controllo del dipendente durante l'orario di lavoro da parte investigatori[66] o il controllo effettuato mediante la collaborazione di terzi appositamente incaricati[67]. Si ritiene, sia in dottrina che in giurisprudenza, che il controllo vietato sia quello che si effettua a distanza tanto di tempo quanto di spazio[68], stante la forte potenzialità invasiva di un controllo esercitato

[59] USAI, *Osservazioni in tema di controllo dell'attività dei lavoratori attuato mediante sistemi informatici,* in *Dir. inf.*, 1991, 253.
[60] In questo senso PULITANÒ, *Problemi di imputazione soggettiva e art. 4 dello Statuto dei Lavoratori" (nota a Pretura di Milano, 5 dicembre 1984),* in *Foro it.*, 1985, 2, 293.
[61] L'art. 114 del d.lgs. 196/2003 (cosiddetto "Codice della *privacy*") dispone che *"resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300"*, l'art. 171 del medesimo testo normativo prevede che "*la violazione delle disposizioni di cui [all'articolo] 114 è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300"* il quale, a sua volta, da una parte richiama la sanzione di cui all'art. 650 c.p. e dall'altra dispone che, in caso di condanna, l'autorità giudiziaria debba ordinare la pubblicazione della sentenza nei modi previsti dall'articolo 36 c.p.
[62] Cass. lav., 17 luglio 2007, n. 15892 (CED 598745) in *Or. giur. lav.*, 2008, 318 con nota di CAIRO.
[63] Cass. lav., 17 giugno 2000, n. 8250 (CED 537708) in *Or. giur. lav.*, 2000 3, 613.
[64] Cass. lav., 16 settembre 1997, n. 9211 (CED 508047), in *Dir. lav.*, 1998, 137 con nota di DE BONIS.
[65] Cass. lav., 6 marzo 1986, n. 1490 (CED 444864), in *Or. giur. lav.*, 1986, 919.
[66] Cass. lav., 12 giugno 2002, n. 8388 (CED 555005); Cass. lav., 3 novembre 1997, n. 10761 (CED 509428).
[67] Cass. lav., 14 luglio 2001, n. 9576 (CED 548199).
[68] Pret. Milano, 5 dicembre 1984, in *Riv. it. dir. lav*., 1985, 2, 209.

sugli strumenti di lavoro, per verificare *a posteriori* quale sia stato il comportamento ed il ritmo di lavoro del dipendente.

3.2. *Il computer quale strumento di controllo*. Occorre a questo punto verificare la compatibilità con l'art. 4 Stat. lav. dell'utilizzo sul luogo di lavoro di strumenti di comunicazione informatica e dell'utilizzo di strumenti informatici di controllo, dovendosi peraltro prima stabilire se il *computer*, di per sé, possa essere considerato uno strumento di controllo a distanza.

A questo proposito, si è sostenuto che il controllo svolto mediante il *computer* non sarebbe così invasivo da giustificare la sua riconduzione all'art. 4 dello Statuto, e *"non solo nella fattispecie di cui al primo comma, ma nemmeno in quella di cui al secondo comma dell'art. 4"*[69]: quest'ultimo vieterebbe esclusivamente l'impiego di apparecchi, come le videocamere, in grado di registrare ogni singola azione del lavoratore; al contrario, il controllo sull'utilizzo del *computer* non lederebbe la libertà e dignità del lavoratore in quanto sarebbe in grado di registrare solamente il *"corretto utilizzo degli strumenti messi a disposizione dal datore di lavoro".* Non sembra, tuttavia, che tale impostazione sia condivisibile: se è vero che il controllo svolto attraverso il *computer* è meno invasivo rispetto ad altri, nondimeno anch'esso può arrivare a livelli particolarmente penetranti, considerando l'ingente quantità di tempo che oggi un lavoratore trascorre di fronte al terminale. Inoltre, un controllo sul "solo" utilizzo degli strumenti informatici potrebbe comportare un controllo capillare ed assoluto dell'attività lavorativa, con effettivo annullamento di ogni spazio di autonomia.

Un altro indirizzo dottrinale ritiene che il *computer* non rientri nella previsione dell'art. 4 dello Statuto in quanto *"l'organizzazione informatico-telematica del lavoro"* non potrebbe *"essere sussunta nella nozione di «apparecchiatura di controllo»"*, che comprenderebbe soltanto gli impianti *"non essenziali rispetto alla esecuzione della prestazione"*[70]. Neppure tale tesi appare peraltro condivisibile: se il *computer* fosse esclusivamente finalizzato a controllare l'attività dei lavoratori, il suo utilizzo sarebbe sempre vietato ai sensi del primo comma dell'art. 4; viceversa, se fosse *"richiesto da esigenze produttive"*, il suo impiego potrebbe essere sottratto alla procedura di consultazione e autorizzazione prevista dal secondo comma solo attraverso una interpretazione apertamente *contra legem.* Il bene giuridico tutelato dalla norma (la dignità e la libertà dei lavoratori) può essere leso tanto da una apparecchiatura di controllo *esterna* allo strumento di lavoro, quanto da una *integrata* nello strumento di lavoro: quest'ultima, anzi,

[69] CAIRO, *Internet e posta elettronica in azienda: il potere di controllo del datore di lavoro*, in *Or. giur. lav.,* 2004, 128; svolge considerazioni simili USAI, *Osservazioni*, cit., 255.
[70] ICHINO, *Il contratto di lavoro,* vol. III, in *Tratt. dir. civ. e comm.*, a cura di CICU, MESSINEO, MENGONI, Milano, 2003, 234.

presenta una maggiore potenzialità lesiva[71], data la minore distanza fra strumento di controllo e strumento di lavoro.

A ben vedere, essendo la caratteristica principale del *computer* (che ne ha comportato la diffusione esponenziale cui si è assistito negli scorsi decenni) quella di essere una macchina logica *multifunzionale*, le cui funzionalità non sono predeterminate al momento della progettazione, ma includono tutte quelle che possono essere espresse in un linguaggio di programmazione, non è appropriato chiedersi se il sistema informatico, *in astratto*, sia uno strumento di telecontrollo: è piuttosto necessario accertare se lo specifico *computer* utilizzato sul luogo di lavoro abbia o meno programmi funzionali al controllo dei lavoratori o dai quali possa derivare un controllo a distanza dei lavoratori. Occorre, in altre parole, spostare l'attenzione dal *computer* in sé stesso al *software*[72] in esso installato, essendo quest'ultimo a determinare la funzionalità di ogni specifico *computer*[73]. Questa interpretazione è stata criticata in quanto *"la norma dello Statuto impone il controllo previo sull'«installazione» delle apparecchiature, in funzione di una tutela globale e preventiva contro le innumerevoli possibili scelte di impiego delle stesse"*[74]: tale critica, tuttavia, appare superabile considerando che il *computer*, di per sé, senza *software*, è uno strumento inerte e privo di funzionalità; pertanto, finché non venga installato un *software* dotato di funzionalità (anche potenziali) di controllo, il calcolatore non sarà comunque una *"apparecchiatura dalla quali derivi la possibilità di controllo a distanza"*.

Dovrà quindi ritenersi assolutamente vietato l'utilizzo di programmi direttamente finalizzati al controllo dei lavoratori, che comporterebbe una violazione dell'art. 4 Stat. lav., come nel caso di programmi finalizzati a valutare la produttività dei lavoratori, ovvero il tempo da questi passato alla postazione di lavoro o il ritmo lavorativo[75]. Qualora invece i programmi installati sul *computer* non abbiano la finalità specifica di controllare l'attività dell'utente-lavoratore, ma questo controllo sia comunque possibile per le caratteristiche del *software* in concreto utilizzato, dovrà accertarsi se esistano le necessità *"organizzative, produttive o di sicurezza"* previste dallo Statuto; in caso positivo, sarà necessario attivare la procedura di consultazione prevista dal secondo comma dell'art. 4 Stat. lav.[76].

---

[71] GALLUS, nota a Trib. Perugia, 20 febbraio 2006, in *Dir. inf.*, 2007, 203.
[72] Cfr. Pret. Milano, 5 dicembre 1984, in *Foro it*., 1985, I, 286, con note di ROSSI e PULITANÒ.
[73] ZANELLI, *Impresa, lavoro e innovazione tecnologica*, Milano, 1985, 89 ss.
[74] ICHINO, *op. cit.*, p. 233.
[75] Ritiene ammissibile l'utilizzo di strumenti esplicitamente finalizzati al controllo a distanza, a condizione che siano stati oggetto di accordo ai sensi del secondo comma dell'art. 4 Stat. lav., BELLAVISTA, *Poteri dell'imprenditore e privacy*, in A.A.V.V. *I poteri del datore di lavoro nell'impresa*, CEDAM, 2002, 52.
[76] Cfr. App. Milano, 30 settembre 2005, in *Riv. crit. dir. lav.*, 2006, 899, che ha ritenuto illegittimo, per violazione dell'art. 4 Stat. lav., il licenziamento inflitto a causa della rilevazione del reiterato collegamento a siti Internet, effettuata tramite un programma di controllo non autorizzato.

Come già anticipato, il *computer* connesso ad Internet procede normalmente alla registrazione di rilevanti quantità di dati relativi al suo utilizzo e quindi la sua installazione dovrà sempre essere preceduta dalla procedura di consultazione, soprattutto in un contesto produttivo quale quello attuale, nel quale la connessione alla Rete costituisce spesso uno strumento imprescindibile per lo svolgimento dell'attività lavorativa. L'unica alternativa possibile per il datore di lavoro è, da un punto di vista tecnico, quella di modificare la configurazione degli strumenti informatici, facendo in modo che non vengano raccolte informazioni sull'utilizzo dei *computer* all'interno del luogo di lavoro, oppure facendo in modo che esse risultino anonime; in tale modo il *computer* non costituirebbe più uno strumento dal quale possa derivare il controllo a distanza dei lavoratori. Va sottolineato che la soluzione di rendere anonimi i dati è l'unica possibile nei casi in cui gli strumenti tecnologici di comunicazione non siano di proprietà del datore di lavoro ma di un soggetto terzo che fornisca la connessione ad Internet[77]: in uno scenario del genere, l'impossibilità di assicurarsi che il *provider* non effettui registrazioni relative ai dati trasmessi tramite la Rete impone di fare in modo che i dati arrivino a quest'ultimo in forma già anonima[78].

Questa soluzione, per quanto possa apparire particolarmente onerosa per il datore di lavoro, stante la diffusione delle tecnologie informatiche e la loro indispensabilità per lo svolgimento di quasi ogni attività lavorativa, è imposta dallo Statuto dei lavoratori e consente di rispettare adeguatamente le esigenze di protezione dei lavoratori nei confronti di controlli che, anche se effettuati mediante strumenti di lavoro indispensabili, possono arrivare ad essere eccessivamente invasivi.

3.3. *I controlli difensivi*. Come abbiamo visto, la disciplina relativa ai controlli da parte del datore di lavoro è particolarmente rigorosa: esiste tuttavia un filone interpretativo, di origine giurisprudenziale, che ritiene legittimo il controllo a distanza sull'attività dei lavoratori in un ampio numero di casi, nei quali il datore di lavoro investighi sulla possibile commissione di "atti illeciti" da parte dei dipendenti: sarebbero questi i c.d. *controlli difensivi*[79].

[77] Cfr. CASSANO, *Abusivi collegamenti Internet del lavoratore in azienda e abusivo controllo elettronico dell'azienda sull'attività del lavoratore*, in *Giur. merito*, 2003, 27.

[78] Opzione possibile mediante tecniche di *network address translation* e *network masquerading* che consentono di fare apparire le connessioni come provenienti da un unico indirizzo di rete.

[79] Ampiamente sui controlli difensivi, BARRACO, *op. cit.*, 244 ss; più recentemente, COLUCCI, *L'art. 4 dello Statuto dei lavoratori: attualità della norma e procedure ispettive*, in *Riv. giur. lav. prev. soc.*, 2010, 2, 275; ZOLI, *Il controllo a distanza del datore di lavoro: l'art. 4, L. n. 300/1970 tra attualità ed esigenze di riforma,* in *Riv. it. dir. lav.*, 2009, 1, 485; DOSSI, *Controlli a distanza e legalità della prova: tra esigenze difensive del datore di lavoro e tutela della dignità del lavoratore*, in *Dir. rel. ind.*, 2010, 1153; CONTI, *La sezione lavoro e la Sezione penale della Corte di Cassazione a confronto su controlli a distanza e controlli difensivi*, in *Mass. Giur. lav.*, 2010, 555; DUI, *Monitoraggio della posta elettronica e accesso a Internet*, in *Lav. giur.*, 2010, 805.

La nozione di 'controllo difensivo', dopo aver trovato un primo riscontro nella giurisprudenza penale, abbastanza risalente[80], che affermava la legittimità di un controllo a distanza effettuato su di un cassiere, sospettato di omissioni nelle registrazioni delle somme incassate, ha più di recente trovato la sua massima espansione in una sentenza della Cassazione civile[81], nella quale (con succinta motivazione[82]) si confermava l'ammissibilità di controlli "*diretti ad accertare comportamenti illeciti dei lavoratori".* Questa pronuncia ha dato origine ad un orientamento interpretativo che riconduce alla nozione di controllo difensivo un numero rilevante di ipotesi, quali il controllo a distanza di tempo sul *computer* del dipendente[83], il controllo sull'effettuazione di telefonate ingiustificate[84] ed anche la videoripresa di una dipendente sospettata di sottrarre denaro dalla cassa[85].

L'individuazione della esatta fisionomia dei controlli difensivi appare problematica, non essendo chiaro quali siano i motivi per cui un comportamento conforme alla fattispecie penale dovrebbe essere ritenuto non punibile, se non addirittura lecito; inoltre, non appaiono sufficientemente definite le condizioni in presenza delle quali il controllo potrebbe essere definito *"difensivo"*: stando alla formula giurisprudenziale più ricorrente, sarebbero oggetto del divieto previsto dall'art. 4 Stat. lav. i controlli riguardanti *"l'attività lavorativa"*, mentre sarebbero leciti *"i controlli diretti ad accertare condotte illecite del lavoratore"*.

Questa formula si presta a numerose critiche. In primo luogo va rilevato che l'espressione *"controlli riguardanti l'attività lavorativa"* è più ristretta di quella utilizzata dal legislatore: è *"attività dei lavoratori"* anche quella svolta nei tempi e nei luoghi non specificamente destinati alla prestazione lavorativa, e pertanto deve considerarsi illegittima l'installazione di strumenti di controllo anche al di fuori degli spazi strettamente finalizzati allo svolgimento della prestazione. In secondo luogo, affermare la liceità dei controlli relativi alle *"condotte illegittime"* dei lavoratori rischia di sottovalutare il fatto che *l'inadempimento* del lavoratore rispetto alle

[80] Cass. IV, 8 ottobre 1985, Gambino, in *Or. giur. lav.* 1986, 318.
[81] Cass. lav., 3 aprile 2002 n. 4746, in *Or. giur. lav*. 2002, 221.
[82] L'intero problema dei controlli difensivi viene risolto con queste poche battute: *"Ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 l. n. 300 citata, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (cd. controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate, o, appunto, gli apparecchi di rilevazione di telefonate ingiustificate. Nella specie […] il tribunale avrebbe dovuto valutare il comportamento del datore di lavoro come inteso a controllare la condotta illecita del dipendente e non l'attività lavorativa svolta dal medesimo".*
[83] Trib. Perugia, 20 febbraio 2006, in *Dir. inf*., 2007, 200 con nota di GALLUS; Trib. Milano 31 marzo 2004, in *Or. giur. lav*., 2004, 108.
[84] Trib. Torino, 9 gennaio 2004, in *Giur. piemontese*, 2004, 131.
[85] Cass. V, 18 marzo 2010, n. 20722, in *Foro it.* 2010, II, 439.

obbligazioni contrattualmente assunte è già di per sé una condotta illecita[86]. Se la finalità del divieto posto dall'art. 4 Stat. lav. è quella di impedire al datore di lavoro di verificare l'adempimento dei lavoratori mediante strumenti "disumani" di controllo a distanza, obbligandolo ad effettuare verifiche mediante controlli di persona e da vicino, affermare la possibilità di un telecontrollo delle attività 'illecite' dei lavoratori comporterebbe una sostanziale disapplicazione della norma. Infine, la generica *finalità* di accertamento di attività illecite da parte dei lavoratori appare un criterio selettivo ambiguo[87]: ritenere scriminante la semplice intenzione soggettiva del datore di lavoro comporterebbe, di nuovo, la sostanziale abrogazione del divieto di cui all'art. 4 Stat. lav.; a risultati ancora più assurdi si giungerebbe qualora si ritenessero giustificati i controlli solo nel caso in cui *ex post* portassero effettivamente alla scoperta di una attività illecita[88].

Se la nozione di "controllo difensivo" nella sua accezione più ampia, appena delineata, appare criticabile, si potrebbe tuttavia cercare di individuare un ambito più ristretto all'interno del quale un controllo di quel tipo non sia in contrasto con gli scopi di tutela dell'art. 4 dello Statuto.

Se quest'ultima disposizione è finalizzata a tutelare la *"dignità del lavoratore"* sul luogo di lavoro, che verrebbe lesa qualora venisse eliminata ogni forma di riservatezza nello svolgimento dell'attività lavorativa, sarebbero ammissibili forme di controllo che risultassero non lesive di quella dignità: questo potrebbe essere il caso di controlli finalizzati ad accertare attività illecite del lavoratore (diverse dal mero inadempimento), a condizione che possa escludersi con certezza che attraverso di essi saranno rilevate anche attività del lavoratore diverse da quelle illecite.

Per fare un esempio, ricorrendo alla casistica giurisprudenziale già citata: il controllo mediante telecamere a circuito chiuso su una lavoratrice sospettata di sottrarre denaro dalla cassa è sicuramente adatto a rilevare l'effettiva sottrazione di denaro, ma allo stesso tempo, prima di effettuare il controllo, non sarà possibile escludere che verranno registrate altre attività della lavoratrice, diverse dal furto. Pertanto, un controllo di tale tipo dovrebbe essere ritenuto illecito ai sensi dell'art. 4 Stat. lav.: se lo si permettesse, ogni singolo lavoratore dovrebbe ritenere che, per il solo fatto di essere (unilateralmente) sospettato dal datore di lavoro di compiere atti illeciti, potrebbe essere sottoposto ad un controllo a sua insaputa, al di là dei limiti previsti dallo Statuto,

[86] Riferisce degli orientamenti della giurisprudenza rispetto alla possibilità che i controlli difensivi riguardino l'inadempimento delle prestazioni lavorative, BARRACO, *Privacy e Potere di Controllo*, in BARRACO-SITZIA, *La tutela della privacy nei rapporti di lavoro,* IPSOA, 2008.

[87] Ritiene che i controlli siano ammissibili se condotti in presenza di concreti elementi di illecito, dopo la supposta commissione di un delitto, in maniera proporzionata all'esigenza difensiva e in presenza di un interesse legittimo del datore di lavoro, POLICELLA, *Il monitoraggio elettronico per scopi difensivi*, in *Dir. Internet*, 2007, 1, 87.

[88] NOGLER, *Sulle contraddizioni logiche della Cassazione in tema di diritto alla riservatezza del lavoratore subordinato*, in *Resp. civ. e prev.*, 1998, 1, 111.

realizzandosi così quella compressione della libertà e della dignità del lavoratore che la norma mira a evitare.

Un rischio di questo tipo non sarebbe invece presente nel caso in cui l'attività di controllo fosse idonea ad accertare *esclusivamente* l'eventuale attività illecita del lavoratore (diversa dal mero inadempimento lavorativo). Si ipotizzi, ad esempio, che un dipendente sia sospettato di sottrarre denaro da una cassa contenuta in uno spazio al quale nessun dipendente ha motivo di accedere: una telecamera puntata su di essa potrebbe rilevare esclusivamente il furto ed in nessun caso potrebbe controllare l'attività lavorativa, né accertare il mero inadempimento da parte del lavoratore[89]. In questa prospettiva il controllo sulle attività illecite dei lavoratori dovrebbe ritenersi ammissibile in quanto *inoffensivo* rispetto al bene giuridico (libertà e dignità del lavoratore) tutelato dalla norma. Questo tipo di interpretazione, peraltro, trova già una conferma in una pronuncia della Cassazione civile nella quale, in tema di controlli difensivi, si afferma che le esigenze *"di evitare condotte illecite da parte dei dipendenti [...] non consentono di espungere dalla fattispecie astratta i casi dei cd. controlli difensivi ossia di quei controlli diretti ad accertare comportamenti illeciti dei lavoratori quando tali comportamenti riguardino [...] l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso ove la sorveglianza venga attuata mediante strumenti che presentano quei requisiti strutturali e quelle potenzialità lesive, la cui utilizzazione è subordinata al previo accordo con il sindacato o all'intervento dell'Ispettorato del lavoro"* [90]. Nel ritenere ammissibili i controlli a distanza sui lavoratori, quando siano volti alla tutela di *"beni estranei al rapporto"* di lavoro e siano privi di *"potenzialità lesive"* rispetto alla dignità del lavoratore, si finisce implicitamente con l'attribuire legittimità alla categoria dei controlli difensivi, limitandone però fortemente l'ambito di possibile impiego ed impedendo che necessità di controllo di "attività illecite" portino ad una eliminazione delle tutele previste dallo Statuto dei lavoratori.

Nell'ottica, che qui più interessa, potrebbe ritenersi ammissibile il controllo diretto a verificare che la connessione alla Rete non venga utilizzata indebitamente da un dipendente che non ha alcuna ragione di accedervi, così come il controllo effettuato su un *server* aziendale contenente dati riservati, per accertare eventuali accessi abusivi ad esso attraverso la rete aziendale: in tali ipotesi il controllo potrebbe rivolgersi esclusivamente al comportamento illecito del dipendente (qualora sussista), senza che vi sia il rischio che il controllo "difensivo" si

[89] Nello stesso senso COLUCCI, *op. cit.*, 275.
[90] Cass. lav., 17 luglio 2007 n. 15892, in *Lav. prev. oggi*, 2007, 1678 con nota di MEROLLA.

tramuti surrettiziamente in un controllo pervasivo sull'attività e sull'adempimento del lavoratore.

3.4. *Le linee guida del Garante per la protezione dei dati personali.* La questione dell'ammissibilità del controllo è stata in questa sede affrontata esclusivamente con riferimento alle norme previste dallo Statuto dei lavoratori, nella convinzione che queste siano tuttora le più rigorose nell'ordinamento italiano in materia di controllo sul luogo di lavoro. Rispetto ad esse, in questo contesto, rimangono "sullo sfondo" le disposizioni previste dalla normativa in materia di tutela dei dati personali[91]. La preminenza delle disposizioni dello Statuto trova conferma nelle linee guida emanate dal Garante per la protezione dei dati personali relative all'uso di Internet e della posta elettronica sul luogo di lavoro. In tale documento, emanato *"per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet"*, si conferma il divieto di controllo sulla navigazione del dipendente. Da una parte, si prevede l'obbligo di comunicare ai dipendenti quali siano gli utilizzi ammessi della Rete (se sia ammesso l'uso personale e, eventualmente, se durante l'orario di lavoro o solo durante le pause etc.) e la possibilità per il datore di lavoro di effettuare "controlli" sulla navigazione; dall'altra parte, si specifica che di tali controlli debbono essere avvertiti i dipendenti; si riconosce poi l'esistenza di un divieto di installazione di strumenti di controllo a distanza e, per quanto riguarda i dati necessari alla navigazione in Internet, si consiglia il trattamento *"in forma anonima o tale da precludere l'immediata identificazione di utenti"*. Si prevede infine l'opportunità di un controllo "*su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree"*, che *"può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo"*, eventualmente *"circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia*", in tal modo riconoscendo l'impossibilità di effettuare un controllo, se non anonimo, sulla navigazione in Internet dei lavoratori.

Claudia Pecorella
Professore associato di Diritto penale
nell'Università di Milano-Bicocca

Riccardo De Ponti
Professore a contratto di
Diritto penale dell'informatica
nell'Università di Milano-Bicocca

[91] L. 31 dicembre 1996 n. 675 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali) oggi sostituita dal d.lgs. 30 giugno 2003 n. 196, (Codice in materia di protezione dei dati personali).