UNIVERSITA' DEGLI STUDI DI CAMERINO

Scuola di Scienze e Tecnologie
Corso di laurea in Informatica

Corso di perfezionamento in "Esperto in Digital Forensics"

Nuove reti aziendali :diritti di controllo del datore di lavoro e privacy del dipendente.

CANDIDATO

Cinzia Grucci

RELATORE

Avv. Di Minco

a.a. 2011/2012

INTRODUZIONE

L’evoluzione incessante delle tecnologie dell’informazione e della comunicazione dei Sistemi Informativi Automatizzati sia in ambito privato sia in quello della Pubblica Amministrazione richiedono dinamiche rapide e continue nell’espletamento delle conoscenze attualmente disponibili al loro interno. Il tema quindi della “sicurezza” relativa alle nuove tecnologie dell’informazione sta sempre più imponendosi, assumendo rilevanza strategica. Con il termine “Sicurezza Informatica” si intende l’insieme delle misure di carattere organizzativo, tecnologico e procedurale mirate ad assicurare la protezione dei sistemi informatici e delle informazioni in essi contenuti, riguardo a determinate minacce. A tale proposito, la **gestione del Sistema informativo** e la sua **struttura organizzativa** diventano un argomento prioritario e con esso il **contesto normativo esistente**,con indicazioni su come affrontare le problematiche della Sicurezza dei Sistemi Informativi Automatizzati e su come realizzare e gestire adeguate misure di protezione. Il concetto di gestione dell’informazione, sta assumendo una crescente importanza ; per poter essere svolta nel modo più efficiente ed efficace possibile, qualsiasi attività richiede, in diversa misura, di poter disporre dell’informazione giusta al momento giusto. E’ pertanto necessario dedicare grande attenzione alla progettazione e realizzazione del proprio sistema informativo, inteso non solo come insieme degli strumenti ICT necessari ad

automatizzare determinate attività, ma in senso più ampio come insieme di tutti gli elementi, dati, persone, procedure, infrastruttura tecnologica, principi, che in qualche modo interagiscono con le informazione trattate in una data organizzazione.-

NUOVI SCENARI TECNOLOGICI IN MATERIA DI RETI

L'ambiente informatico aziendale è in rapida evoluzione in risposta alla "consumerizzazione" del settore Information Tecnology, al fenomeno della "mobilità" dei supporti connessi alla rete e al "cloud computing".- Queste tendenze introducono nuove opportunità di business ma anche rischi e vulnerabilità. Il valore e il peso delle nuove tendenze non devono essere sottovalutati né demonizzati come forieri di nuovi rischi, ma risorse aziendali e integrità dei dati devono essere protetti. In passato lo scopo della rete era quello di connettere gli utenti alle risorse I.T. in un'architettura client/server ed i modelli di rete erano in gran parte prevedibili; oggi le esigenze della periferia della rete si sono evolute, data la presenza di svariati dispositivi mobili che si connettono alla rete aziendale da diverse posizioni. Non sempre , inoltre, è possibile escludere tali connessioni, nonostante una policy di sicurezza di rete tendenzialmente orientata alla chiusura in tal senso.Anche le applicazioni sono in rapida evoluzione ; sono

virtualizzate; possono essere utilizzate in server diversi e persino in “data –center” diversi. Al contempo, la rete aziendale “si estende” e ricorre al “cloud” anche per applicazioni di collaborazione come “dropbox” o “Google document”. Di conseguenza i gestori del server non hanno più precisa contezza di quali dispositivi si connettano alla rete o da quale posizione. Le applicazioni in uso non sono più limitate a quelle rese disponibili dai gruppi I.T.- I dati non sono più al sicuro nei data –center ma attraversano il mondo su “smart phone” e tablet p.c. e risiedono nel cloud, fuori dalla portata dei gruppi I.T.-

D’altro canto, anche le caratteristiche delle minacce esterne sono mutate. Non più attacchi alle reti effettuati in modo massiccio, dunque appariscenti e verificabili in tempi brevi, ma attacchi più complessi, articolati, e soprattutto mirati e intercettabili dopo diverso tempo dall’azione criminosa. Dal punto di vista della sicurezza di rete e del suo sistema difensivo, maggiori sono le informazioni di contesto disponibili, maggiori sono le risorse da cui attingere per bloccare un attacco alla rete , maggiore è la sicurezza della rete stessa. A quest’ultimo fine, pertanto, è consigliato l’utilizzo di un “sistema di sicurezza integrato”, ovvero realizzato mediante la correlazione di informazioni da diversi sistemi.

Una “rete futura” deve garantire sicurezza a tutti i livelli della rete, dalla sede centrale alle filiali, per i dipendenti in sede e per i collaboratori che utilizzano dispositivi cablati, wireless o V.P.N.- Un’architettura di policy estesa a tutta la rete consente di creare, distribuire e monitorare regole di sicurezza basate su un linguaggio contestuale, del tipo “chi – cosa – dove – quando - come”.

L’applicazione di tali regole può includere azioni come il blocco dell’accesso ai dati o ai dispositivi, oppure ad es. l’avvio della crittografia dei dati. Si pensi ad es. al dipendente che si connette alla rete dallo smartphone aziendale e viene identificato, così come vengono identificati e circoscritti i privilegi concessi a quel determinato utente e al dispositivo assegnato a quest’ultimo. Il “motore per le policy”, infatti, non solo stabilisce le policy applicate a quel dispositivo e a quell’utente, ma condivide anche tali policy con tutti i punti nella rete , oltre ad aggiornare immediatamente le informazioni quando in rete compare un nuovo dispositivo. E’ evidente che un sistema siffatto è potenzialmente idoneo a ledere la privacy dell’utente cui il dispositivo è assegnato, come pure è potenzialmente idoneo ad offrire al datore di lavoro anche degli strumenti per operare un controllo a distanza sull’operato dei lavoratori.

Le “reti di nuova generazione” sono anche in grado di offrire risposte alle preoccupazioni per la sicurezza correlate al “cloud computing”. Anche in una rete distribuita estesa basta poco per reindirizzare in modo intelligente il traffico web, per applicare policy di controllo e sicurezza “granulari” (1). Come tutto questo si coniughi e/o si scontri con le esigenze di privacy aziendale e con quelli dei lavoratori dipendenti è il nodo che si cercherà di affrontare nel presente lavoro. Il Garante della privacy non si è disinteressato alla questione, avendo predisposto un VADEMECUM (2) ovvero uno strumento per cominciare ad approfondire i potenziali rischi del cloud , decidere quali tipi di dati (anche quelli personali o addirittura sensibili) trasferire e per quali scopi. Il CLOUD è un insieme di

tecnologie e di modalità di fruizione di servizi informatici che favoriscono l'utilizzo e l'erogazione di software , la possibilità di conservare ed elaborare grandi quantità di informazioni via internet. Il Cloud offre, a seconda dei casi, il trasferimento della conservazione o dell'elaborazione dei dati dai computer degli utenti ai sistemi del fornitore. Consente, inoltre, di usufruire di servizi complessi senza doversi necessariamente dotare né di computer o altri hardware avanzati né di personale in grado di programmare o gestire il sistema. Tutto può essere demandato all'esterno, in outsourcing, e a un costo potenzialmente limitato in quanto le risorse informatiche necessarie per i servizi richiesti possono essere condivise con altri soggetti che hanno le stesse esigenze. La tecnologia, come sempre, procede più velocemente del legislatore, e non solo in Italia. Manca ancora un quadro normativo in tema di privacy, di tutela sia civile che penale.

Alcune utili novità per il settore delle telecomunicazioni sono state introdotte lo scorso maggio con il d.lgs. n. 69 del 28.5.2012. , normativa che obbliga i gestori di telefonia e di rete nonché i providers a notificare alle competenti autorità nazionali (e in taluni casi anche agli utenti) tutte le violazioni di sicurezza che comportino la distruzione, la perdita o la diffusione indebita di dati personali trattati nell'ambito della fornitura del servizio.

Nel caso di "cloud computing", il cliente di servizi cloud , che è il **titolare del dato**, ha il diritto/dovere di esercitare un potere di controllo nei confronti del **responsabile del trattamento** che è il "cloud provider", verificando la corretta esecuzione delle istruzioni impartite in relazione ai dati personali trattati (2) (pag.

15 del documento), essendo comunque anch'egli responsabile di eventuali violazioni commesse dal fornitore, dal momento che il Codice della privacy prevede, tra l'altro, che il titolare eserciti un potere di controllo nei confronti del responsabile del trattamento (in questo caso il "cloud provider") verificando l'esatto adempimento delle istruzioni impartite in tema di trattamento dei dati personali.

In sostanza , nonostante una recente normativa (3) , abrogando i commi da 19 a 19.8 dell'allegato B al D.lgs. 196/03, non obblighi più il titolare del trattamento (sia egli datore di lavoro privato o pubblico, sia egli persona fisica o giuridica) a redigere annualmente (entro il 31 marzo) il Documento Programmatico sulla Sicurezza, e nonostante - come anzi accennato nella doverosa panoramica delle evoluzioni tecnologico-organizzative attuali - le innovazioni informatiche e della tecnica d'impresa rendano i previsti controlli sempre più difficili, sul datore incombe comunque l'onere di assicurarsi che siano adottate misure tecniche e organizzative atte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati; di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta; di modifica dei dati in conseguenza di interventi non autorizzati o non conformi alle regole (4) (5) . E infatti sia i soggetti pubblici sia le imprese private TITOLARI di TRATTAMENTI non devono dimenticare che i soggetti INTERESSATI al trattamento (le persone cui i dati trattati si riferiscono) hanno ex lege (vedi art. 7 e ss. – titolo II° parte 1° del d.lgs. 196/03) precisi diritti , tutti riconducibili al generale diritto alla protezione dei

dati che li riguardano (art. 1 d. lgs. 196/03) ed esplicitantisi nella conoscenza di origine, modalità, finalità, soggetti che trattano i dati nonché diritto di rettifica, cancellazione e trasformazione in forma anonima, nel caso di violazione di legge. Il titolare del dato, pertanto, sia esso impresa sia soggetto pubblico,si trova a dover "proteggere" la rete aziendale in maniera "attiva" (incombendogli veri e propri obblighi di verifica e controllo) senza tuttavia ledere il diritto alla riservatezza dei dipendenti, i cui dati, peraltro e tra l'altro, deve difendere da attacchi informatici, virus, intrusioni illecite sia fisiche sia telematiche etc.-(5)

In particolare, si pone il problema dei POTERI DI CONTROLLO DEL TITOLARE DEL TRATTAMENTO e dei conseguenti LIMITI AI PREDETTI POTERI per esigenze legate al diritto alla privacy del lavoratore.

FONTI NORMATIVE

NORME alla base DELLA TUTELA della PRIVACY dei LAVORATORI sono:

gli artt. 2 -3 – 21 e 41 della Carta Costituzionale ;

l'art. 615 ter del Codice penale "Accesso abusivo ad un sistema informatico o telematico" ;

l’art. 616 del Codice penale “Violazione, sottrazione e soppressione di corrispondenza”(che merita una valutazione particolare affrontando una tematica specifica, benché ugualmente riconducibile alla tutela della riservatezza) ;

l’art. 2087 del Codice Civile ;

l’art. 4 della legge 300/70 (Statuto dei Lavoratori) ;

l’art. 29 Direttiva 95/46/CE ;

l’art. 114 del d.lgs.196/03 (normativa sulla privacy) .

Nell’ambito del rapporto di lavoro la privacy non è un diritto assoluto ; esso va bilanciato con altri diritti o interessi legittimi vuoi del datore di lavoro vuoi degli altri lavoratori. Il problema è stato affrontato dal “Gruppo di lavoro europeo per la tutela delle persone con riguardo al trattamento dei dati personali “ così come costituito dall’art. 29 della Direttiva 95/46/CE. Il fatto che certi dati personali (e i relativi diritti) siano inseriti nell’organizzazione aziendale comporta la necessità di accertare una parziale intrusione nella propria sfera privata, dovuta al fatto che il datore di lavoro detiene comunque un diritto/dovere di controllo sul funzionamento della propria impresa (5). Il problema del bilanciamento di questi opposti interessi viene risolto (a livello di normativa europea) (6) indicando al datore di lavoro una serie di **principi** cui deve uniformarsi nello svolgimento della sua attività di controllo :

a) principio di necessità. Ogni forma di controllo deve essere indispensabile rispetto ad uno scopo preordinato ;

b) principio di finalità. I dati trattati devono essere utilizzati per il fine originario che deve essere determinato a priori, esplicito e legittimo ;

c) principio di trasparenza. Il datore di lavoro deve dichiarare le attività di controllo, senza, quindi, effettuare c.d. controlli occulti ;

d) principio di proporzionalità e non eccedenza. Il trattamento deve rispettare i confini prestabiliti dallo scopo per cui viene effettuato, cioè deve essere proporzionato al rischio aziendale affrontato ;

e) principio di accuratezza e conservazione dei dati. I dati devono essere veritieri ed aggiornati e non devono essere conservati per un periodo superiore a quello necessario ;

f) principio di sicurezza. Il dato deve essere tenuto al sicuro attraverso strumenti tecnologici e organizzativi, tali da tutelarlo da attacchi esterni. E' evidente come, soprattutto in quest'ultimo principio, i poteri di controllo e verifica da parte del datore di lavoro possano rivestire carattere di ambivalenza, di fatto possono essere potenzialmente lesivi proprio di quella privacy dei lavoratori i cui dati sono finalizzati a tutelare.

Nella medesima ottica si pone la Legge 300/70 (Testo Unico dei Diritti dei lavoratori) che – benché non sia finalizzata in modo diretto a tutelare il diritto di privacy dei lavoratori, tuttavia detta diverse norme volte a tutelare il lavoratore da ingerenze indebite del datore di lavoro che potrebbero limitare la libertà di espressione del pensiero del dipendente e, in ultima analisi, la sua dignità. Si pensi agli artt. 1-3 della Legge 300/70 aventi ad oggetto l'attività

di controllo del datore di lavoro sotto i diversi aspetti dei soggetti, dell'oggetto, delle modalità e della valenza probatoria dei dati emergenti dall'attività di controllo. L'art. 4, in particolare, (7) parla dell'attività c.d. di "controllo a distanza" e disciplina l'uso di "impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dei lavoratori , aventi finalità esclusiva, prevalente o anche solo concorrente, con le necessità di impresa." Infatti, come recita la stessa norma al 2° comma, tali impianti e apparecchiature sono consentiti (previo accordo con le R.S.A. ovvero in mancanza con la Commissione interna ovvero con l'Ispettorato del lavoro), **se necessari** "per esigenze organizzative e produttive, ovvero per la sicurezza del lavoro". Il secondo comma della norma, pertanto, contempera due opposte e diverse esigenze: quelle del lavoratore e quelle del datore di lavoro. Inoltre, i dati ricavati da istallazioni "legittime" , di norma non potrebbero essere utilizzati per fini diversi quali, ad es., l'attività disciplinare contro il dipendente.

Tuttavia, l'interpretazione dell'art. 4 ha prodotto nel corso degli anni copiosa giurisprudenza e negli ultimi tempi la norma è tornata a far parlare di sé, soprattutto in conseguenza dell'evoluzione tecnologica e in riferimento al problema delle reti di telecomunicazione. A fronte di una giurisprudenza assolutamente restrittiva nei confronti del datore di lavoro quale ha caratterizzato più o meno tutto il corso degli anni '90, lo scorso decennio, e forse proprio a causa di un'evoluzione tecnologica che rende sempre più

subdoli gli “attacchi” alla sicurezza delle imprese, la giurisprudenza ha operato un distinguo – da un lato l’attività di controllo inerente in maniera diretta o indiretta l’attività lavorativa, dall’altro controlli volti ad accertare condotte illecite sia del lavoratore sia di soggetti terzi rispetto all’azienda – ritenendo lecite quelle verifiche non dirette a controllare le opinioni, le abitudini, la produttività dei dipendenti. Dottrina e giurisprudenza parlano a tale proposito di controlli difensivi, ritenendoli in molti casi ossequiosi al dettato dell’art. 4 della legge 300/70.

I CONTROLLI “DIFENSIVI”

Il concetto, introdotto dalla giurisprudenza fin dagli anni ’80 , è stato ripreso, per sottolinearne la liceità da parte del datore di lavoro, nel 2002. Con esso si intendevano e si intendono quei “controlli diretti ad accertare condotte illecite del lavoratore” (e non, meramente, “l’attività lavorativa” in senso stretto) quali, ad es., i sistemi di controllo dell’accesso ad aree riservate o gli apparecchi di rilevazione di telefonate ingiustificate. Nel caso al vaglio della suprema Corte nel 2002 il giudice “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” (8).

E’ evidente come il distinguo non sia sempre agevole; i due commi dell’art. 4 sembrano entrare in conflitto anche con il ricorso al concetto del “controllo

difensivo". Basti pensare che nella nozione di condotte illegittime del lavoratore potrebbe rientrare anche l'inadempimento del dipendente rispetto alle obbligazioni contrattualmente assunte (inadempimento che è già di per sé una condotta illecita). Il fine dell'art. 4, tuttavia, è quello di impedire che il datore di lavoro – mediante i c.d. controlli a distanza e/o i telecontrolli- operi un'attività invasiva, disumana e disumanizzante sulla vita lavorativa e anche non lavorativa, semprechè svolta all'interno dell'azienda. Riconoscendo in via generalizzata la liceità del controllo teso alla verifica delle attività illecite dei dipendenti si annullerebbe qualunque efficacia alla norma dell'art.4 vanificandone in via indiretta il primo comma. Non solo, la valutazione sulla (il)liceità della condotta del lavoratore (sia essa effettuata a priori o anche a posteriori) sarebbe un dato soggettivo, cioè lasciato alla libera valutazione di una delle parti in causa –il datore di lavoro (9) .

Appare valida soluzione quella di tentare un'applicazione più ristretta del concetto, che salvaguardi completamente l'interesse primario tutelato dall'art. 4: la dignità del lavoratore sul luogo di lavoro. Si pensi ad es. a controlli finalizzati ad accertare condotte illecite del dipendente diverse dal mero inadempimento contrattuale, qualora si escluda con certezza che possano essere monitorate anche attività del lavoratore diverse da quelle illecite. Così un recente orientamento giurisprudenziale (10) che considera leciti quei controlli a distanza volti a tutelare "beni estranei al rapporto di lavoro" e privi di potenzialità lesive della dignità dei lavoratori.

Merita di essere annoverata tra i c.d. controlli difensivi –e quindi soggetta al distinguo di cui sopra ,cui consegua il connotato della liceità o illiceità – l'attività datoriale di regolamentazione dell'uso di internet nei luoghi di lavoro. E sicuramente oggi, allo stato delle nuove tecnologie, un disciplinare tecnico sull'uso della rete risulta indispensabile, benché di sempre più complessa redazione.

Il datore di lavoro, infatti, può avere diverse legittime ragioni per "monitorare" la navigazione dei dipendenti :

a) verificare che la navigazione sia effettuata per ragioni attinenti al lavoro e non personali ;
b) garantire il buon funzionamento della rete ;
c) evitare di incorrere in eventuale responsabilità qualora il dipendente si connetta a siti o scarichi contenuti illeciti ovvero si comporti in modo da produrre decremento economico visitando siti a pagamento.

D'altronde, il contenuto dei dati controllati potrebbe non rivestire affatto il connotato della riservatezza.

Esistono strumenti tecnologici sia hardware che software, più o meno invasivi, in grado di controllare la navigazione dei dipendenti e comunque, a prescindere dall'utilizzo di tali mezzi specifici, gli strumenti utilizzati per garantire la navigazione in rete sono già di per sé idonei a monitorare la navigazione effettuata dalle maestranze, con conseguente apprensione di diversi dati relativi all'utilizzo della rete da parte dei lavoratori. Si pensi al

lavoro di alcuni browser che conservano nella memoria cache i dati relativi alla visitazione di determinati siti al fine di non “interrogare” nuovamente il web nel caso di connessione. Sia sul server proxy sia nella memoria cache di ogni singolo terminale resta memorizzato il “percorso di interrogazione” , con risparmio di tempo e minori rischi di intasamento e di rallentamento del traffico di rete, ma è evidente che i dati memorizzati possono essere facilmente conosciuti dall’amministratore di rete. Si pensi ad una piccola LAN (rete locale) con un unico accesso a internet condiviso da tutte le postazioni che fanno parte della rete .Si avranno una cache sul server ed una cache per ogni postazione (ovviamente di minore capienza rispetto a quella del server). Al fine di ridurre l’occupazione di banda , qualora due p.c. dovessero visitare per la prima volta un sito a breve distanza di tempo, anziché scaricare entrambi l’intero contenuto della pagina, interverrà un server proxy (un programma che implementa in modo più complesso e sofisticato, lo stesso meccanismo della cache del browser consentendo ai suoi client – i browser configurati per utilizzarlo- di usufruire della sua cache, condivisa fra tutti.) E’ come se il secondo browser potesse accedere alla cache del primo (essendo questa condivisa) ; la pagina viene “downloadata” una volta sola con risparmio di banda e di tempo.(11) E’ evidente però che ciò comporta ripercussioni negative sulla privacy dei singoli client e che l’utente che accede per secondo può venire in contatto con numerose informazioni accessibili al primo utente.

Si pensi al fatto che di norma i browser compilano una cronologia dei siti visitati, consultabile altresì dagli utenti che si connettono successivamente.

Si pensi alla prassi dei cookies ,pezzi di files sotto forma di codici alfanumerici, inviati al browser al fine di "caratterizzare" l'utente, anche se in forma anonima.

Si pensi al server D.N.S. che ha il compito di "tradurre" la URL del sito nel corrispondente indirizzo I.P. (e viceversa).

Persino un'indispensabile e insostituibile strumento per la sicurezza della rete –il firewall- può registrare e monitorare connessioni verso specifici siti web.

Nel 2007 il garante privacy, in conseguenza allo sviluppo tecnologico, diede vita al documento "Linee guida del garante privacy" di cui si farà più ampia menzione in seguito.

Cercare di **conciliare esigenze di sicurezza e controllo** del datore di lavoro –specie alla luce delle nuove tecnologie di cui sopra (cloud, esternalizzazione di rete etc.) - ed **esigenze di tutela della privacy e della dignità** del lavoratore non è un problema dalla soluzione semplice e univoca . le sfumature sono talmente sottili, le variabili così numerose che ogni soluzione può essere valida se opportunamente adattata o, viceversa, inadeguata al problema. Il quadro si complica quando il responsabile del trattamento , individuato dal responsabile dell'ente sia pubblico sia privato, sia

esterno all'ente e adotti soluzioni tecnologiche talmente complesse e poco controllabili (si veda il cloud computing) da far incombere sul titolare una sorta di **responsabilità oggettiva aggravata**, quando non una sorta di colpevolezza presunta nel controllo. La normativa del maggio u.s. (12) va nel senso di "responsabilizzare" il fornitore del servizio ma sicuramente non in quello di esonerare il datore di lavoro , anche quando ha usato tutta la perizia e la diligenza del buon padre di famiglia cui è tenuto.-

ORIENTAMENTI della GIURISPRUDENZA

Come prevedibile, l'evoluzione tecnologica ha avuto un riflesso sull'orientamento giurisprudenziale, nel senso che si è compreso come le nuove tecnologie, cui un soggetto economico non può esimersi dal ricorrere, causano rischi di impresa che si sommano a quelli già esistenti ed aventi origine economico-produttiva.

Dagli anni 2000, e già prima del nuovo testo unico sulla privacy, si sono avute PRONUNCE "A FAVORE" DEL DATORE DI LAVORO : si pensi alla Sentenza di Cass, lav. del 3.4.2002 n. 4746 (8) , già citata , in materia di c.d. controlli difensivi; si pensi alla Sentenza di Cass. Pen. V° Sez. del 18.3.2010 nr. 20722 (10) già citata, inerente l'assoluta esclusione di controlli sull'attività lavorativa dei dipendenti; si pensi alla sentenza di Cass. Civ. sez. lav. del 28.1.2011 n. 2117 inerente riprese audiovisive del lavoratore, addetto

alla vigilanza, che si recava abusivamente in altro contesto produttivo abbandonando la postazione assegnatagli e alla conseguente valutazione di liceità della videoripresa persino al fine del licenziamento del lavoratore, come valutato dalla suprema Corte. (13)

Tra le PRONUNCE "SANZIONATORIE" NEI CONFRONTI DEL DATORE DI LAVORO poiché ritenute in contrasto con l'art. 4 della Legge 300/70 , si consideri la sentenza di Cass. Lav. 17.7.2007 n. 15892 (14) che condanna il datore di lavoro per violazione dell'art. 4 secondo comma Statuto Lavoratori in quanto non ha dato notizia alle R.S.U. delle Organizzazioni sindacali dell'esistenza di sistemi di sorveglianza "a distanza".

La sentenza Cass. Pen. Sez. III° del 24.9.2009 n. 40200 condanna il datore di lavoro ai sensi degli artt. 4 e 38 Statuto dei lavoratori nonché degli artt. 114 e 171 del D.lgs. 196/03 per avere installato in un negozio un impianto di videosorveglianza da cui derivi anche la possibilità di controllo a distanza dell'attività presso i locali ove si svolge l'attività lavorativa , "senza che il personale sia avvisato del funzionamento dell'apparato e del fatto che esso possa riprendere anche l'attività dei lavoratori". La tecnologia si rivela un mezzo che consente un controllo datoriale sempre più idoneo a un impiego penetrante e globale e all'acquisizione delle più varie informazioni e di dati personali.

Ad analoghe conclusioni addiviene la pronuncia di Cass. Civ. sez. lav. del 23.2.2010 n. 4375, negando l'utilizzabilità a fini disciplinari di dati acquisiti

mediante programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi a internet dei dipendenti , sul presupposto che gli stessi strumenti consentono al datore di lavoro di controllare a distanza e in via continuativa l'attività lavorativa durante la prestazione. (15) In sintesi , viene ritenuto che la tecnologia informatico-telematica ha insite tutte le potenzialità per essere considerata sempre, anche alla luce di quanto evidenziato nelle parti precedenti, un mezzo per controllare anche l'attività lavorativa dei dipendenti, ricorrendo dunque i presupposti per l'applicazione dell'art. 4. Affinché si applicabile il 2° comma della norma (e non il 1°, che farebbe scattare il divieto assoluto dell'istallazione dei dispositivi) occorre :

- che l'attività sia indispensabile o comunque assolutamente utile per la gestione d'impresa;
- che non leda l'integrità,la dignità, la libertà di pensiero e di espressione dei lavoratori;
- che siano adempiute le formalità di cui al 2° comma del citato art .4.-

Non si dimentichi, inoltre, che al datore di lavoro che agisce in contrasto con l'art.4 dello Statuto si applica la sanzione prevista dal successivo art. 38.

E' assai probabile che la giurisprudenza (ed anche l'attività del garante) subiscano oscillazioni di tendenza : tecnologie nuove ed avanzate "rappresentano la nuova sfida rispetto alla quale la Giurisprudenza [….] potrà saggiare la tenuta e la portata della tutela ai diritti dei lavoratori." (15)

L’ATTIVITA’ del GARANTE della PRIVACY

Nel 2007 il Garante della Privacy emanò le “linee guida per posta elettronica e internet in ambito di lavoro”. Le linee rimandano alla necessità del rispetto della normativa a tutela dei lavoratori e in particolare dell’art. 4 dello Statuto. Ribadiscono, inoltre, la necessità del rispetto, da parte del datore di lavoro, dei principi del D. lgs. 196/03 (Codice Privacy) e in particolare dei seguenti :

necessità - il ricorso a dati personali e a dati identificativi va ridotto al minimo ;

correttezza - per cui le caratteristiche essenziali del trattamento devono essere rese note al lavoratore ;

secondo finalità determinate ,esplicite e legittime ,osservando altresì i principi di ;

pertinenza e ;

non eccedenza. I dati vanno trattati nella misura meno invasiva possibile, da parte di soggetti predeterminati circoscritti all’area di rischio aziendale .

Le linee guida, inoltre, distinguono tra controlli sulla navigazione dei dipendenti e controlli sulla posta elettronica aziendale, assoggettati, questi ultimi, ad un’espressa e distinta disciplina che tenga conto, altresì, dell’esistenza del reato di cui all’art. 616 C. p. (violazione, sottrazione e soppressione di corrispondenza).

Pongono l'obbligo di informare i dipendenti sulla "policy" interna sul corretto uso delle risorse tecnologiche e di dare idonea pubblicità alla stessa, le disposizioni interne dovranno essere tali da individuare le mancanze e le relative sanzioni disciplinari.

Il Garante, al n. 5 delle Linee Guida, ammette l'uso di "programmi che consentano controlli indiretti", così rifacendosi al 2° comma dell'art.4 Statuto e nel rispetto delle procedure individuate dalla citata norma, si ammetto i "controlli preterintenzionali". Inoltre, il garante interviene pure sul piano della organizzazione del lavoro, offrendo al datore di lavoro consigli sulle modalità strutturali e operative cui ispirarsi nel predisporre la rete informatica e/o telematica aziendale :

a) prima dell'istallazione di rete se ne valuti l'impatto sui diritti dei lavoratori ;
b) si valuti a quali lavoratori siano consentiti la navigazione e/o l'utilizzo della posta elettronica ;
c) si valuti un'opportuna ubicazione delle postazioni di lavoro per limitarne il rischio di impiego abusivo ;
d) si favorisca l'utilizzo di "privacy enhancing tecnologies " volte a minimizzare il ricorso a dati identificativi .
e) si ricorra a filtri (in positivo o in negativo) per la navigazione o la limitazione rispetto a tipologie di programmi e/o di attività in rete ;

f) si ricorra all'anonimizzazione dei dati oggetto del trattamento necessario per la politica di sicurezza aziendale ;

g) predisposizione di limiti temporali di conservazione dei dati, ovvero limiti temporali onde si addivenga alla identificazione degli utenti, qualora questa sia indispensabile.

Le pronunce del garante sono state più penalizzanti rispetto a quelle giurisprudenziali nei confronti del datore di lavoro, considerato in qualità di titolare/responsabile del trattamento ; quasi sempre la prosecuzione del trattamento è stata vietata e il trattamento ha dovuto subire una modifica da parte del responsabile. Esemplificativa è la pronuncia del Garante datata 7.4.2011 (16) avente ad oggetto il trattamento di dati personali del dipendente ricavati da files acquisiti nell'ambito di operazioni di back up effettuate sul server aziendale. Il garante ha censurato il trattamento e ne ha vietato la prosecuzione in base alle seguenti considerazioni :

- non erano sufficientemente rese note ai lavoratori le caratteristiche essenziali del trattamento , anche se connesso a possibili controlli periodici sul server (violazione del principio di correttezza e del principio di finalità) ;
- in conseguenza del divieto incombente sul lavoratore di "detenere" e trattare dati personali sui computer aziendali –come adombrato nel regolamento interno dell'azienda- al fine della dimostrazione della violazione di tale divieto, sarebbe stato sufficiente rilevare la presenza

- di una cartella denominata “xy-personali”, anziché aprirla e prendere completa conoscenza del suo contenuto.

CONCLUSIONI

In capo al datore di lavoro incombe l’onere di essere in grado di valutare l’adeguatezza del proprio sistema informativo in funzione degli obbiettivi che si desidera raggiungere, valutando inoltre se e come le soluzioni ICT disponibili possono fornire un vantaggio competitivo e significativo. La predisposizione di **policy aziendali di sicurezza** e di corretto uso della rete predisposte in modo da selezionare soggetti e privilegi , in ossequio ad un principio di responsabilità e corretto utilizzo delle risorse, permetterà di capire e valutare come funziona la “struttura aziendale”, sia essa privata sia pubblica : quali trattamenti effettua, quanto investe per difendere i suoi clienti, come si organizza per tutelare la privacy dei suoi dipendenti, conseguendo altresì l’obbiettivo di preservare l’immagine e la missione istituzionale. Ci si chiede se una **policy di sicurezza della rete** corretta e lungimirante possa mai essere in grado di tutelare l’azienda (pubblica o privata che dir si voglia) da sanzioni penali e, target ancor più difficile, da pretestuose richieste di risarcimento di danni, o se gli articoli di legge citati siano forieri di una sorta di responsabilità oggettiva, in capo al datore di

lavoro – titolare/responsabile del trattamento che “lo stato dell’arte”, ovvero le ultime tecnologie telematiche, non fanno che rendere inevitabile.

Diviene sempre più urgente una modifica normativa che limiti in modo più radicale rispetto all’attuale il disposto di cui ai commi 4 e 5 dell’art.13 del d.lgs. 196/03, il diritto alla trasparenza del soggetto interessato laddove il rispetto del medesimo pregiudichi la raccolta dei dati per fini difensivi. (17)

Certo è che, nonostante non vi sia più un obbligo giuridico di redigere il documento programmatico per la sicurezza e di aggiornarlo annualmente, la policy aziendale non potrà essere un documento statico ma seguirà pedissequamente, pena la sua inefficacia, le modifiche tecnologiche della rete aziendale. Si è di fronte ad un problema complesso in cui gli aspetti giuridici, quelli organizzativi sono rilevanti tanto quanto quelli tecnologici e la necessità di continuità della “Informazione” diventa a tal punto importante da dover definire un “piano metodologico di sicurezza” all’interno di tutte le strutture informatizzate.

Si omette in questa sede di affrontare il problema dei controlli del datore di lavoro alla/e casella/e di posta elettronica aziendale assegnata/e al lavoratore in quanto la tematica è peculiare, e meritevole di un approfondimento a sè stante.-

[1] White paper – Rete "Rete di prossima generazione: sicurezza per il presente e il futuro" edito da Cisco Systems www.cisco.com

[2] Sul sito www.garanteprivacy.it dal titolo: "Cloud computing-proteggere i dati per non cadere dalle nuvole"

[3] D.L.9.2.2012 n.5 di modifica al D.Lgs. 196/03

[4] Art.11 Legge 196/3

[5] "Lavoro:le line guida del Garante per posta elettronica e internet" in G.U. n. 58 del 10.3.2007

[6] Pareri del Gruppo di lavoro nr.8/2001 (13.9.2001) e documento 29.5.2002 (working document on the surveillance of the electronic comunication in the work place)

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

[8] Cass.lav. 3.4.2002 nr.4746 in Or.Giur.Lav.2002. 221

[9] Cass.V – 18.3.2010 n.20722 in Foro it 2010 II 439 Cass.Lav.17.7.2007 nr.15892 in Lav. e Prev.oggi 2007, 1678

[10] Giur.Cass.V 18.3.2010 nr.90722

[11] "Squid il server Proxy" di Lorenzo Lazzari su Linux 8c nr.14-

[12] D. Legislativo 28.5.2012 nr.69 in materia di protezione di dati personali, di reti e servizi di comunicazione elettronica e di cooperazione tra le autorità nazionali a tutela dei consumatori.

[13] Cass.Civ.Sez.Lav.28.1.2011 n.2117

[14] In "Lavoro e Previdenza Oggi" 2007, 1678 – Cass.Civ.Sez.Lav.23.2.2010 nr.4375

[15] Articolo di Silvio Barone "il controllo datoriale a distanza: disciplina vigente e nuove frontiere tecnologiche in altalex 15.10.2010

[16] Doc.Web. n.1812154

[17] Eulalia Olimpia Policella "privacy e diritto di difesa – Dipendenti infedeli: è legittimo il controllo dei files di back up? " ne: Il quotidiano Ipsoa 11.8.2011-
Guido Pietrosanti "privacy lesa, il mandante nel mirino del garante" in Italia Oggi 5.9.2011.

BIBLIO E SITOGRAFIA

- CISCO White Paper : reti di prossima generazione:sicurezza per il presente e il futuro;
- Gruppo di Lavoro sulla protezione dei dati-art.29.Parere 8/2001 sul trattamento di dati personali nell'ambito dei rapporti di lavoro adottato il 13.9.2001 in www.europa.eu.int ;
- "Cloud Computing:proteggere i dati per non cadere dalle nuvole" in www.garanteprivacy.it;
- "Privacy lesa, il mandante nel mirino del garante" a cura di Guido Pietrosanti ne :Italia Oggi 5.9.2011 ;
- E.O.Policella :"Dipendenti infedeli :è legittimo il controllo dei files di back - up?" in Il quotidiano IPSOA, 11.8.2011;
- C. Pecorella – R. Da Ponti: "Impiego dell'elaboratore sul luogo di lavoro e tutela penale della privacy" ;
- S.Barone : "Il controllo datoriale a distanza:disciplina vigente e nuove frontiere tecnologiche – Cass. Civ. sez. lav. sent. 23.2.2010 n. 4375 in Altalex 15.7.2010 ;

GIURISPRUDENZA CASSAZIONE – Sentenze:

Cass. Lav. 3.4.2002 n. 4746 in Or. Giur. Lav. 2002, 221;
Cass. Lav. 17.7.2007 n. 15892 in Lav. e Prev. Oggi 2007, 1678;
Cass. Pen. Sez. III° del 24.9.2009 n. 40200;
Cass. Civ. Lav. 23.2.2010 n. 4375;
Cass. V° 18.3.2010 n.20722 in Foro it. 2010,II,439;
Cass. Civ. Lav. 28.1.2011 n. 2117 ;
Cass.Civ. sez. lav. 23.2.2012 n. 2722.

DELIBERAZIONI GARANTE Provvedimenti :

del. n. 13 del 1.3.2007. "Lavoro:le linee guida del garante per Posta elettronica e internet";
Boll. N. 113/febbraio 2010 [doc. web. n. 1712856] ;
" " 118/giugno 2010 [" " 1736780] ;
" " 129/luglio 2011 [" " 1829641] ;
Provv. Gar. In Reg. Provv. N. 139 del 7.4.2011 [Doc. web. n.1812154]

SI RINGRAZIANO :
F. Bernabei, candidato – relatore prof. V. Lo Storto “Nuove tecnologie e tutela della riservatezza nei rapporti di lavoro “ Libera Un. M. Ass. anno accademico 2009-2010 ;
G. Quagliato, candidato – relatore prof. F.Caldarelli “ Documento programmatico sulla sicurezza informatica per le Pubbliche Amministrazioni” Master in Diritto Economia e Tecnologie Informatiche Università di Camerino anno accademico 2002-2003.