



ICT E DIRITTO

Rubrica a cura di

Antonio Piva, David D'Agostini

Scopo di questa rubrica è di illustrare al lettore, in brevi articoli, le tematiche giuridiche più significative del settore ICT: dalla tutela del *domain name* al *copyright* nella rete, dalle licenze software alla *privacy* nell'era digitale. Ogni numero tratterà un argomento, inquadrandolo nel contesto normativo e focalizzandone gli aspetti di informatica giuridica.

Privacy sul posto di lavoro

David D'Agostini, Antonio Piva, Luca Zenarolla

1. INTRODUZIONE

Sempre più numerosi sono i casi di controversie che vengono devolute all'attenzione del Garante Privacy o del Giudice del Lavoro e che sono conseguenti a provvedimenti disciplinari irrogati dal datore di lavoro ai dipendenti e relativi all'uso, da parte degli stessi, di Internet e della posta elettronica. È lo stesso Garante, nelle premesse del suo provvedimento generale dell'1 marzo 2007 ad affermare: *“Dall'esame di diversi reclami, segnalazioni e quesiti è emersa l'esigenza di prescrivere ai datori di lavoro alcune misure, necessarie o opportune, 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”*¹.

Siamo in presenza di un ambito molto delicato perché si tratta di bilanciare due esigenze certamente meritevoli di tutela: da una parte l'interesse del datore di lavoro a controllare che il dipendente non utilizzi le risorse aziendali per finalità personali e in contrasto con l'attività lavorativa, dall'altra quello del lavoratore a che tali controlli non siano invasivi della propria sfera di riservatezza nelle relazioni personali e professionali.

Di seguito due esempi di controversie ispirate a casi reali giunti all'attenzione del Garante Privacy e dell'Autorità Giudiziaria:

1. Tizio, addetto all'accettazione di una casa di cura, è destinatario di un provvedimento disciplinare per accessi a internet non autorizzati effettuati sul posto di lavoro. In particolare il datore di lavoro, controllando la cronologia del browser, ha rilevato che il dipendente ha navigato continuamente in orario di lavoro in siti a carattere politico e pornografico. Tizio ricorre al Garante Privacy contestando che questi controlli costituiscano violazione della propria riservatezza, chiedendo il divieto per il datore di trattare ulteriormente le informazioni assunte illecitamente. Il Garante, pur riconoscendo la ragione sostanziale del datore di lavoro, accoglie il ricorso².

2. L'azienda Alfa per verificare il rispetto delle policy aziendali in tema di corretto utilizzo degli strumenti elettronici dati in uso al personale, installa su tutti i terminali un programma in grado di registrare in maniera sistematica l'attività svolta dal singolo lavoratore. In questa maniera scopre che alcuni dipendenti navigano su siti internet per ragioni non attinenti all'attività lavorativa e li licenzia. La Cassazione, investita in

¹ “Lavoro: le linee guida del Garante per posta elettronica e internet” (Gazzetta Ufficiale n. 58 del 10 marzo 2007) <http://www.garanteprivacy.it/garante/doc.jsp?ID=1387522>

² Decisione su ricorso, “Internet: proporzionalità nei controlli effettuati dal datore di lavoro” - 2 febbraio 2006 <http://www.garanteprivacy.it/garante/doc.jsp?ID=1229854>

ultimo grado della controversia, censura il comportamento del datore di lavoro³.

2. LA PRIVACY SUL LUOGO DI LAVORO

Gli scenari sopra riportati, relativi a vicende realmente accadute, sono solamente alcune delle possibili controversie che riguardano la delicata materia della tutela della privacy del dipendente sul luogo di lavoro. Internet e, più in generale, gli strumenti informatici sono entrati prepotentemente nella nostra vita quotidiana e nella nostra attività lavorativa. Oggigiorno è impensabile riuscire a svolgere la nostra attività rinunciando, ad esempio, alla posta elettronica, al VOIP ecc..

A fronte degli innegabili vantaggi connessi all'uso di questi servizi, però, è necessario rendersi conto di alcuni aspetti di non secondaria importanza: a differenza di altri strumenti tradizionali, essi si prestano ad utilizzi ulteriori e non manifesti. Anche se l'utente non se ne accorge, tutto (o quasi) quello che viene fatto on-line lascia una traccia che può essere utilizzata o controllata più o meno legittimamente.

3. I CONTROLLI

Implementare un sistema informatico in azienda comporta una serie di attività e di costi che non si riducono semplicemente a quelli iniziali per la sua realizzazione e prima configurazione. Di più, non sono nemmeno sufficienti le attività periodiche di manutenzione del sistema.

Nel momento in cui un'azienda decide di utilizzare quelli che il Legislatore definisce genericamente come "strumenti elettronici" sorge in capo ad essa un nuovo obbligo, che è quello di garantire che le operazioni di trattamento delle informazioni effettuate con essi avvenga nel rispetto di precise garanzie anche tecniche. E ciò deve essere inteso in senso ampio. Se esiste una norma che impone di dotarsi di *antivirus* e *firewall*, è evidente che la ratio della stessa vuole che il funzionamento di questi strumenti sia monitorato per prevenire possibili lesioni ai dati e ai sistemi, e che questi controlli devono riguardare non solo i rischi provenienti dall'esterno, ma anche quelli provenienti dall'interno dell'azienda

stessa. Il punto di partenza di questa vicenda è, quindi, che il datore di lavoro non solo può ma addirittura DEVE effettuare controlli sul sistema informatico aziendale.

4. IL QUADRO NORMATIVO

Acclarata, quindi, la necessità di effettuare controlli, è necessario stabilire una sorta di linea guida affinché tale attività rimanga nell'alveo della legittimità. Dal punto di vista tecnico, infatti, esistono diversi strumenti, anche *open source*, che consentono di monitorare in maniera pressoché totale l'attività del lavoratore. Il nocciolo della questione, invece, è stabilire quali di questi strumenti siano utilizzabili senza incorrere in violazioni di legge che rischiano non solo di rendere inutilizzabili le informazioni così acquisite, ma anche di ricevere una sanzione.

Le normative che bisogna tenere in considerazione sono essenzialmente due:

- lo Statuto dei Lavoratori (Legge 300/1970);
- il Codice in materia di protezione dei dati personali (D.Lgs. 196/2003).

5. I CONTROLLI A DISTANZA

Recita l'articolo 4 dello SdL: "È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori". Questa prescrizione, nata in un preciso momento storico e con una ben specifica motivazione, trova ai giorni nostri nuovi ambiti di applicazione. Per pacifica interpretazione giurisprudenziale, infatti, rientrano nel divieto tutti quegli strumenti che consentono di controllare "a distanza" le attività compiute dal lavoratore sul proprio computer.

L'art. 4 in questione disciplina in modo diverso due ipotesi:

- apparecchiature finalizzate specificatamente al controllo a distanza dell'attività dei lavoratori, che sono assolutamente proibite;
- apparecchiature installate per esigenze organizzative e produttive ovvero della sicurezza del lavoro, ma tali comunque da poter essere utilizzate anche per il controllo a distanza del dipendente, consentite soltanto a condizione del previo accordo sindacale ovvero, in assenza di questo, del provvedimento autorizzativo della direzione provinciale del lavoro territorialmente competente.

³ Corte di Cassazione, Sezione Lavoro, Sentenza n. 4375/2010.

Resta da dire dei c.d. **controlli difensivi**, categoria di controlli che non si trova nel dettato normativo ma di genesi giurisprudenziale. La Cassazione, con la sentenza n. 4746 del 3 aprile 2002, infatti, ha affermato il seguente principio *“Ai fini dell’operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell’attività dei lavoratori previsto dall’articolo 4 della legge n. 300 del 1970, è necessario che il controllo riguardi (direttamente o indirettamente) l’attività lavorativa, mentre devono ritenersi certamente fuori dell’ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (c.d. controlli difensivi), quali, per esempio, i sistemi di controllo dell’accesso ad aree riservate, od, appunto, gli apparecchi di rilevazione di telefonate ingiustificate”*.

Alla luce di questa sentenza, quindi, si devono escludere dall’ambito di applicazione dell’art. 4 dello Statuto dei Lavoratori quei controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi) che, quindi, sono ammessi senza dover sottostare ai limiti e alle regole sopraindicate.

È necessaria, però un’ultima precisazione: una recente sentenza della Cassazione⁴, nel censurare l’operato di un datore di lavoro che utilizzava un software (Super Scout) per monitorare in maniera continuativa e senza avvertire i lavoratori la navigazione in internet dei dipendenti, ha di fatto ristretto il concetto di controllo difensivo. Per poter rientrare in questa categoria, detti controlli devono essere occasionali e non continuativi oltre che indispensabili ai fini della tutela del patrimonio aziendale o per l’accertamento di aspetti della prestazione lavorativa che potrebbero essere altrimenti conoscibili solo attraverso un controllo palese ma continuativo e, quindi, oppressivo e invasivo, oltre che oneroso.

6. LE LINEE GUIDA DEL GARANTE PRIVACY

Il primo marzo 2007 il Garante Privacy ha emanato delle importanti linee guida per posta elettronica e internet sul posto di lavoro. È un testo fondamentale per riuscire a capire, in pratica, in che

modo porre in essere i controlli sull’utilizzo da parte dei lavoratori di questi strumenti. Si tratta, ad ogni buon conto, di un insieme di regole che integra il disposto dello Statuto dei Lavoratori ma che, ovviamente, non si sostituisce ad esso. Punto di partenza è la considerazione che una qualsiasi attività di controllo costituisce, ai sensi del D.Lgs. 196/03, un’attività di trattamento di dati personali: di conseguenza ai controlli devono essere applicati tutti i principi e le regole contenute nel Codice Privacy.

In primo luogo il controllo deve essere ispirato al principio di necessità, in base a cui i sistemi informativi e i programmi informatici devono essere configurati, già in origine, in modo da ridurre al minimo l’utilizzo di dati personali, e a quello di proporzionalità rispetto alle finalità perseguite.

In secondo luogo è necessario che queste particolari ipotesi di trattamenti di dati personali siano ispirate ad un canone di trasparenza, per cui è da escludere la possibilità di un controllo informatico “all’insaputa dei lavoratori”. Il datore di lavoro ha quindi il dovere di indicare preventivamente e in modo particolareggiato (anche integrando le esistenti informative ex articolo 13 D.Lgs. 196/03), quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli.

In questo quadro è indispensabile adottare un **disciplinare interno** da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall’art. 7 dello Statuto dei lavoratori) e che contenga disposizioni chiare in merito a ciò che è consentito o è vietato fare con gli strumenti e i servizi aziendali indicando:

- se determinati comportamenti sono tollerati rispetto alla “navigazione” in Internet (per esempio, il *download* di software o di file musicali), oppure alla tenuta di file nella rete interna;
- quali informazioni sono memorizzate temporaneamente (per esempio, le componenti di file di *log* eventualmente registrati) e chi (anche all’esterno) vi può accedere legittimamente;
- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di *back up*, della gestione tecnica della rete o di file di *log*);

⁴ Corte di Cassazione, Sezione Lavoro, Sentenza n. 4375/2010.

- se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime - specifiche e non generiche - per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengano inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constatati che la posta elettronica e la rete Internet sono utilizzate indebitamente;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi (art. 34 del Codice, nonché Allegato B), in particolare regole 4, 9, 10.

7. APPARECCHIATURE PREORDINATE AL CONTROLLO A DISTANZA

Il provvedimento ribadisce, poi, che a prescindere dal fatto che il lavoratore ne sia informato non può ritenersi consentito il trattamento effettuato mediante sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire - a volte anche minuziosamente - l'attività dei lavoratori. È il caso, per esempio:

- della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- della riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo (*keylogger*);
- dell'analisi occulta di computer portatili affidati in uso.

8. SISTEMI CHE CONSENTONO CONTROLLI "INDIRETTI"

Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o di sicurezza (per esempio, per rilevare anomalie, per manutenzioni o per verificare il regolare funzionamento degli strumenti) può avvalersi legittimamente di sistemi che consentono indirettamente un


controllo a distanza (c.d. controllo preterintenzionale). In questo caso, però, il datore di lavoro è chiamato a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri (da preferire rispetto all'adozione di misure "repressive") e, comunque, a "minimizzare" l'uso di dati riferibili ai lavoratori.

Per esempio, per quanto attiene alla navigazione su Internet è fondamentale che in azienda la navigazione non sia "libera" ma che, attraverso *proxy* o altri sistemi:

- siano individuate categorie di siti considerati correlati o meno con la prestazione lavorativa o, comunque, sia impedita la navigazione su siti che sicuramente non concernono l'attività lavorativa;
- siano configurati sistemi o filtri che prevenano determinate operazioni - reputate interferenti con l'attività lavorativa - quali l'*upload* e/o il *download* di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato). In tema di posta elettronica, invece è opportuno che:
 - il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (per esempio, *info@alfa.it*, *ufficiovendite@alfa.it*, ecc.);
 - il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (per esempio, per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura;
 - i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.

9. CONCLUSIONI: L'IMPORTANZA DI UN SISTEMA INFORMATICO BEN CONFIGURATO

Il Garante Privacy, in conclusione, sottolinea l'importanza di queste attività preventive: con un sistema informatico configurato correttamente, infatti, vengono a mancare i presupposti affinché possano nascere controversie tra datori e lavoratori.



Tornando, infatti ai due esempi visti prima, se fossero state impostate le restrizioni sulla navigazione internet non ci sarebbe stata la neces-

sità di procedere disciplinarmente nei confronti del lavoratore e, conseguentemente, si sarebbe evitato il contenzioso.

DAVID D'AGOSTINI avvocato, master in informatica giuridica e diritto delle nuove tecnologie, collabora all'attività di ricerca scientifica dell'Università degli studi di Udine e ha fondato l'associazione "*Centro Innovazione & Diritto*". È componente della Commissione Informatica dei Consigli dell'Ordine del Triveneto, responsabile dell'area "*Diritto & informatica*" della rivista "*Il foro friulano*", membro dell'organo di Audit Interno di Autovie Venete SpA.

E-mail: studio@avvocatodagostini.it

ANTONIO PIVA, laureato in Scienze dell'Informazione, *Vice Presidente dell'ALSI* (Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica) e Presidente della commissione di informatica giuridica. Docente a contratto di *diritto dell'ICT e qualità* all'Università di Udine. Consulente sistemi informatici e Governo Elettronico nella PA locale, valutatore di sistemi di qualità ISO9000 ed ispettore AICA.

E-mail: antonio@piva.mobi

LUCA ZENAROLLA, avvocato, esperto di informatica giuridica e diritto delle nuove tecnologie. Autore di articoli per riviste e portali di settore, relatore in numerosi convegni e seminari su diritto e informatica. Presidente dell'associazione culturale CINDI, Centro Innovazione & Diritto. www.cindi.it

E-mail: info@cindi.it