Paolo Giardini
Consulente per la sicurezza delle Informazioni
Eucip Certified Informatics Professional
AIP – OPSI – AIPSI – CLUSIT - ISSA - FORMEZ

La gestione della Privacy
e della Sicurezza in Azienda

I controlli difensivi fra diritti del datore e privacy dei lavoratori

Congresso AIP Umbria

Orvieto
27/04/2007

OPSI - AIP

- OPSI - Osservatorio Privacy e Sicurezza Informatica nasce in seno all'Associazione Informatici Professionisti.
- Ha come scopo lo studio delle problematiche relative alla Sicurezza informatica ed ai rischi legati alla tutela dei dati personali e confidenziali.
- Promuove la cultura della Sicurezza Informatica.
- Si propone come centro di concertazione e di confronto tra e varie associazioni, gruppi e aziende pubbliche e private che si occupano di sicurezza.
- Rappresenta AIP presso il Garante Privacy al tavolo per la redazione del Codice Deontologico per i servizi di telecomunicazione.

La situazione

L'utilizzo degli strumenti elettronici e soprattutto di Internet ha creato nelle aziende una situazione del tutto particolare:

- Da una parte il diritto alla privacy dei lavoratori, intesa come diritto alla riservatezza ed alla espressione della propria individualità e personalità;
- Dall'altra il diritto (ma anche il dovere) del datore di lavoro di mettere in atto misure di atte a garantire la continuità lavorativa e la sicurezza dei dati personali;

Dal punto di vista del Datore

- Il datore di lavoro ha un potere di vigilanza e controllo sancito dal Codice Civile art. 2086:
  - L'imprenditore è il capo dell'impresa (Cost. 41) e da lui dipendono gerarchicamente i suoi collaboratori.
- Il Dipendente ha dei doveri nei confronti del Datore sanciti dal Codice Civile:
  - Art. 2094: Lavoro subordinato;
  - Art. 2104: Diligenza del prestatore di lavoro;
  - Art. 2105: Obbligo di fedeltà.

Dal punto di vista del Dipendente

- I diritti dei cittadini sono indicati nella Costituzione Italiana (diritti della persona, Art. 2, 3, 4; diritti relativi a libertà e riservatezza art. 13, 14, 15);
- Lo statuto dei lavoratori (L.300/70) art. 4 vieta i controlli a distanza dell'attività dei lavoratori mentre l'art.8 vieta le indagini sulle opinioni;
- Anche la legge 626/94 (sicurezza nei luoghi di lavoro) vieta l'utilizzo di sistemi di controllo all'insaputa del lavoratore (all.VII punto 3b);
- La legge 196/2003 stabilisce i principi per la protezione dei dati personali.

la pratica:

Vediamo adesso quali sono i reati collegati con l'uso del computer in azienda, i rischi connessi e quali sono gli strumenti che il datore di lavoro può utilizzare per esercitare il proprio diritto di vigilanza e controllo.

I reati in azienda

Accesso abusivo (c.p. art.615 ter);
Detenzione o diffusione dei codici di accesso (c.p. art.615 quater);
Diffusione di programmi dannosi (c.p. art.615 quinques);
Intercettazione, impedimento, interruzione di comunicazioni telematiche (c.p. art. 617 quater);
Installazione di apparati per intercettazione (c.p. art. 617 quinques);
Falsificazione, alterazione di comunicazioni telematiche (c.p. art. 617 sexties);
Frode, phishing, spam;
Pedopornografia;
Download di prodotti multimediali protetti da copyright;
Download di software protetti da copyright;
Scambio di file illegali;
Reati di calunnia, diffamazione;
Utilizzo non autorizzato degli strumenti;
Duplicazione abusiva di software od altro materiale;
Furto di informazioni;
Accesso non autorizzato ai dati;
Trattamento non conforme;
Diffusione dei dati;
Mancata applicazione delle misure di sicurezza;
...

La responsabilità del Datore

- Responsabilità del Datore di lavoro in caso di reato commesso dal Dipendente (Art.40 C.P.);
- Ricadono sul titolare tutte le responsabilità per errato trattamento o danno da esso derivato;
- Il trattamento di dati personali è equiparato ad attività pericolosa (art. 15 Cod. Privacy);
- Inversione dell'onere della prova in caso di danno derivato da attività pericolosa (art. 2050 C.C.);
- Punibilità per inosservanza dei provvedimenti dell'Autorità (art. 650 C.P., art. 170 Cod. Privacy);

I controlli difensivi

Il Datore di lavoro ha diritto a mettere in atto le azioni che ritenga necessarie per la salvaguardia della sua attività: sono i cosiddetti Controlli Difensivi.

Questo può integrare il controllo a distanza del lavoratore e deve essere bilanciato con i diritti dei lavoratori.

Il provvedimento del Garante del 1° marzo consolida alcune prassi ed introduce alcune novità.

Regola generale

I controlli che abbiano come scopo fini organizzativi, di sicurezza o di contrasto di comportamenti illegittimi non sono compresi nel divieto dell'art. 4 comma 1 L.300/1970, se questi sono organizzati in modo tale che da essi non possa derivare controllo dei lavoratori durante l'attività; in caso contrario possono essere utilizzati solo dopo accordo con la rappresentanza sindacale. (art.4 comma 2, come richiamato in artt. 114, 171 Cod. Privacy).

Il provvedimento del Garante

- Il Datore di lavoro deve assicurare funzionalità e corretto impiego dei mezzi messi a disposizione dei Lavoratori, adottando adeguate misure di sicurezza (disponibilità ed integrità, prevenzione di utilizzi indebiti - art. 15,31,167,169 del Codice).
- E' necessario tutelare i Lavoratori in quanto l'utilizzo di Internet e della posta comporta la possibilità di analisi di log, proxy, cache, cookie, messaggi di posta ... Da questi dati si possono trarre informazioni anche sensibili relative al Lavoratore o terzi identificati o identificabili.
- Tutte le misure attivate devono rispettare i Principi di Necessità, Correttezza, Finalità determinate, esplicite, legittime, Pertinenza e non eccedenza prescritte dagli artt. 3 e 11 del Codice Privacy.

Principio di necessità

- In applicazione del principio di necessità il Datore deve porre in essere ogni misura atta prevenire il rischio di utilizzi impropri piuttosto che preferire misure “repressive”.
- Si dovranno quindi:
  - Effettuare valutazioni sull'impatto di apparecchiature di controllo sui diritti dei lavoratori;
  - Individuare preventivamente chi sia autorizzato all'utilizzo di Internet;
  - Valutare il posizionamento delle postazioni in modo da evitare utilizzo abusivo;

Pertinenza e non eccedenza

- I controlli sono leciti solo se rispettati i principi di pertinenza e non eccedenza.
- In caso di evento dannoso il Datore può porre in atto misure che consentano verifiche supplementari;
- I dati trattati debbono essere aggregati in forma anonima;
- In caso di violazione dovrà essere emesso un primo avviso generalizzato; in caso di reiterazione il controllo può avvenire su base individuale, se previsto dal regolamento;
- Il controllo non può mai essere prolungato, costante, indiscriminato.

Liceità e bilanciamento

Il trattamento di dati non sensibili può essere effettuato se:

- Necessario per legittimo esercizio di diritto in sede giudiziaria;
- È stato acquisito un legittimo consenso;
- In assenza di consenso è necessario per difendere un legittimo interesse valutandone il bilanciamento. (art. 24 Codice). In tale caso si applica la disciplina prevista dall'art. 4 L.300/1970

Il trattamento di dati sensibili può essere effettuato se:

- È stato acquisito un legittimo consenso;
- È necessario per l'esercizio di un diritto in sede giudiziaria, salvaguardia della vita, incolumità fisica, obblighi di legge, indagine giudiziaria (art. 26 Codice).

Come ottemperare?

Sia lo statuto dei lavoratori art. 4 L. 300/1970 sia il D.lgs 626/1994 allegato 7 punto 3 stabiliscono la necessità di indicare chiaramente e preventivamente strumenti e metodi di controllo che possono avere ad oggetto il Lavoratore.

Il Garante indica due obblighi indispensabili:

- Linee guida o regolamento interno per l'utilizzo degli strumenti Internet.
- Informativa ex art. 13 Codice Privacy.

Regolamento interno (1)

- Deve stabilire in modo chiaro, senza formule generiche quale utilizzo è consentito di Internet, definendo anche come la e-mail sia uno strumento aziendale;
- Se ed in che misura è consentito l'uso personale;
- Quali informazioni sono memorizzate sui sistemi, anche temporaneamente e chi vi può accedere;
- Per quanto tempo vengono conservate, come ad esempio backup e log;
- Se il Datore si riserva di compiere controlli , indicando scopi e modalità;
- Definire le modalità di avviso graduale in caso di violazioni;

Regolamento interno (2)

- Eventuali sanzioni irrorate;
- Modalità di accesso ai dati in caso di assenza dell'incaricato;
- Se sono possibili modalità di utilizzo degli strumenti con pagamento a carico del lavoratore;
- Modalità relative alla riservatezza per particolari categorie di lavoratori;
- Misure di sicurezza adottate a norma del disciplinare allegato B del Codice.

Informativa

- Oltre alle informazioni specificate nell'art. 13 del Codice è fatto obbligo al Titolare specificare nell'informativa l'esistenza di una policy interna e dell'esistenza, dei fini, dei metodi di possibili controlli anche ai fini di un esercizio di un diritto in sede giudiziaria.
- Dovranno altresì essere indicate le principali caratteristiche dei trattamenti effettuati oltre ai soggetti incaricati ed il nominativo del responsabili a cui rivolgersi per eventualmente esercitare il proprio diritto (Art. 7 Codice).

Controlli vietati

- Anche se il Datore può lecitamente controllare l'effettivo adempimento della prestazione lavorativa e se necessario il corretto utilizzo degli strumenti di lavoro (cfr. c.c.), sono vietati ogni e qualunque tipologia di controllo a distanza dell'attività del lavoratore, anche se il lavoratore è informato.
- Sono dunque vietati strumenti HW e SW tramite i quali sia possibile ricostruire l'attività dei lavoratori come: lettura sistematica delle e-mail, riproduzione delle pagine web visitate, registrazione dei dati immessi da tastiera, analisi occulta dei computer.

Controlli permessi

- Il divieto di controllo riguarda l'attività lavorativa in senso stretto e le condotte poste in essere sul luogo di lavoro.
- Eventuali strumenti posti in essere per fini produttivi, organizzativi, di sicurezza che per le loro caratteristiche possano consentire un controllo indiretto (controllo preterintenzionale) non contrastano la norma, fermo restando le obbligazioni di informativa e consultazione dei lavoratori.

Conservazione

- I sistemi devono essere configurati per una cancellazione automatica mediante sovrascrittura dei dati e dei log dei quali non sia necessaria la conservazione;
- La durata della conservazione temporanea deve essere predeterminata e giustificata;
- Un eventuale prolungamento dei tempi può essere giustificato solo se indispensabile per l'esercizio di un diritto in sede giudiziaria, esigenze tecniche particolari, richiesta dell'autorità.
- In questi casi, informazioni conservate, fini, modalità, devono essere predeterminate.

Incaricati e formazione

- Il titolare può nominare un responsabile a norma dell'art 29 Codice, impartendo opportune e specifiche istruzioni sul tipo di controllo ammesso e sulle modalità.
- Gli amministratori di sistema ed i manutentori dovranno essere formati sulla policy, misure di sicurezza, normative, ecc.

Misure per la navigazione

- Individuazione delle categorie di siti considerati correlati o meno con la prestazione lavorativa;
- Configurazione di sistemi o filtri che impediscano le operazioni non consentite (download di determinati file o navigazione di siti vietati);
- Trattamento in forma anonima dei dati relativi a log di navigazione o comunque su una base che renda non immediatamente identificabile l'utente;
- Definizione del tempo di conservazione dei log.

Misure per la e-mail

- La mancata definizione a priori della qualità di strumento aziendale dell'indirizzo e-mail può comportare un illecito comportamento del Datore altrimenti perfettamente lecito.
- Utilizzo di indirizzi condivisi (info@, amministrazione@...)
- Attribuzione di indirizzi privati al lavoratore;
- Risponditori automatici in caso di assenza;
- Delega ad un “fiduciario” per la lettura della posta in caso assenza improvvisa, con redazione di verbale;
- Disclaimer automatico nei messaggi in uscita.

Conclusioni

- Data la delicatezza del tema, è necessario stabilire un giusto bilanciamento degli interessi fra Datore di Lavoro e Dipendenti, definendo a priori diritti e doveri.
- Questo è possibile solo tramite la redazione di una policy chiara e completa, a conoscenza di tutti i lavoratori e da questi approvata, a beneficio non solo del Datore ma anche del Lavoratore che godrà di maggiore tutela sul posto di lavoro.

Per finire...

Si potrebbe dire:

PATTI CHIARI, AMICIZIA LUNGA!

Domande?

Grazie per l'attenzione

paolo.giardini@aipnet.it

opsilist@aipnet.it - http://opsi.aipnet.it - http://www.solution.it