CORSO DI ALTA FORMAZIONE IN
INFORMATION SECURITY MANAGEMENT

8ª EDIZIONE, ROMA
FEBBRAIO 2011- SETTEMBRE 2011

# Abuso di Internet e posta elettronica in azienda

# Linee guida del Garante per posta elettronica e internet

Michele Crudele
www.crudele.it

2011-03-25

CONSEL
CONSORZIO ELIS
per la formazione professionale superiore

CEFRIEL
FORGING INNOVATION
POLITECNICO DI MILANO

MIP
POLITECNICO DI MILANO
SCHOOL OF MANAGEMENT

# Gazzetta Ufficiale n. 58 del 10 marzo 2007

- Il Garante per la protezione dei dati personali pubblica le Linee guida per definire
  - Principi ispiratori
  - Cosa si può fare
  - Cosa non si può fare
- Un punto di riferimento fondamentale
- Non è un manuale puntuale
- **Non risolve tutte le questioni aperte**
- Richiede adattamento alle nuove tecnologie
- Protagonista è il datore di lavoro

a) Compete ai datori di lavoro assicurare funzionalità e corretto impiego, definendone modalità d'uso
b) Spetta ad essi adottare idonee misure di sicurezza per assicurare disponibilità e integrità di sistemi informativi e di dati
c) Emerge l'esigenza di tutelare i lavoratori interessati
d) L'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione. I servizi **e-mail rischiano di giungere** fino alla conoscenza da parte del datore di lavoro del contenuto della corrispondenza
e) Le informazioni contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili

# 1.2. Tutela del lavoratore

## Utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro

- Le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi**. La linea di confine tra questi ambiti può essere tracciata a volte solo con difficoltà**
- Nel luogo di lavoro va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo una ragionevole protezione di riservatezza nelle relazioni personali e professionali, e della dignità dell'interessato
- Diversi datori di lavoro hanno prefigurato modalità d'uso che assegnano aree di lavoro riservate strettamente personali, ovvero consentono usi moderati di strumenti per finalità private

# 2.1. Principi generali

## Codice in materia di protezione dei dati e discipline di settore

- Il Garante tiene conto del
  - diritto alla protezione dei dati personali
  - della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone
  - dei principi di semplificazione, armonizzazione ed efficacia
- Le prescrizioni **potranno** essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica

# 2.2. Discipline di settore

## Codice in materia di protezione dei dati e discipline di settore

- Alcune disposizioni di settore prevedono specifici divieti o limiti, come quelli posti dallo **Statuto dei lavoratori** sul controllo a distanza
- La disciplina di protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie
  - Codice dell'Amministrazione Digitale

# 2.3. Principi del Codice

## Codice in materia di protezione dei dati e discipline di settore

a) Principio di **necessità**
   - i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite

a) Principio di **correttezza**
   - le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori

a) I trattamenti devono essere effettuati per finalità determinate, esplicite e legittime, osservando il principio di **pertinenza e non eccedenza**
   - trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza”

# 3.1. Disciplina interna
## Controlli e correttezza nel trattamento

- L'eventuale trattamento deve essere ispirato ad un canone di trasparenza
  - esclude la possibilità del controllo informatico "all'insaputa dei lavoratori”
- Grava sul datore di lavoro l'onere di **indicare** in ogni caso, **chiaramente e in modo particolareggiato**
  - modi di uso degli strumenti messi a disposizione ritenuti corretti
  - in che misura e con quali modalità vengano effettuati controlli
- Vari mezzi di informazione tenendo conto delle specificità e dimensioni delle aziende

- **Opportuno** adottare un disciplinare interno senza formule generiche
  - Da pubblicizzare adeguatamente e sottoporre ad aggiornamento periodico
- Specificare
  - comportamenti non tollerati rispetto alla "navigazione" in Internet, oppure alla tenuta di file nella rete interna
  - in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete
    - da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di webmail, indicandone le modalità e l'arco temporale di utilizzo
  - quali informazioni sono memorizzate temporaneamente e chi (anche all'esterno) vi può accedere legittimamente

- Specificare
  - se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno
  - se, e in quale misura, ci 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 e le relative modalità
    - precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni
  - quali **conseguenze**, anche di tipo disciplinare, ci si riserva di trarre se la posta elettronica e la rete Internet sono utilizzate indebitamente

- Specificare
  - le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di **assenza del lavoratore** stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti
  - se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato
  - quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali

- Specificare
  - le prescrizioni interne sulla sicurezza dei dati e dei sistemi secondo l'art. 34 del Codice 196/2003 dei dati personali che dice: *Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti* ***misure minime***:

a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari

# 3.3. Informativa (art. 13 del Codice)

## Controlli e correttezza nel trattamento

- Oltre a pubblicizzare una policy interna rispetto al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare gli interessati ai sensi dell'art. 13 del Codice dei dati personali
- Gli interessati hanno diritto di essere informati **preventivamente** sui controlli, e in modo chiaro sui trattamenti di dati che possono riguardarli
- Le finalità da indicare possono essere connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, quando comportano un trattamento lecito di dati
  - possono anche riguardare l'esercizio di un diritto in sede giudiziaria.
- Devono essere indicate le principali caratteristiche dei trattamenti, il soggetto o l'unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i propri diritti

# 4. Apparecchiature preordinate al controllo a distanza

- **Si può controllare** (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro
- Rispettare la libertà e la dignità dei lavoratori
  - divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori“ tra cui sono comprese strumentazioni hardware e software mirate al controllo dell'utente
    - Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa. Ciò, anche quando i singoli lavoratori ne siano consapevoli
  - In particolare 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 di lavoratori.

# 4. Apparecchiature preordinate al controllo a distanza

- Non si può effettuare
  - lettura e 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
  - riproduzione ed eventuale **memorizzazione sistematica delle pagine web** visualizzate dal lavoratore
  - lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo
  - analisi occulta di computer portatili affidati in uso
- Il controllo a distanza vietato riguarda l'attività lavorativa in senso stretto e altre condotte personali nel luogo di lavoro
  - A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili

# 5.1 Programmi che consentono controlli "indiretti"

- Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (rilevare anomalie o per manutenzioni) o per la sicurezza sul lavoro, **può avvalersi di sistemi che consentono indirettamente un controllo a distanza** e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori
- Il trattamento di dati che ne consegue può risultare lecito. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori

# 5.2 – Principio di necessità

## Programmi che consentono controlli "indiretti"

- 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
- Opportuno che
  - si valuti attentamente l'impatto sui diritti dei lavoratori (prima dell'installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell'eventuale trattamento)
  - si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e l'accesso a Internet
  - si determini quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo.
- Adottare tutte le misure tecnologiche volte a minimizzare l'uso di dati identificativi (privacy enhancing technologies – PETs )
  - Le misure possono essere differenziate a seconda della tecnologia impiegata: mail o Internet

# 5.2 – Principio di necessità

## Programmi che consentono controlli "indiretti"

a) Internet: la navigazione web

- Per ridurre il rischio di usi impropri (siti non pertinenti, up/download, finalità ludiche o estranee all'attività), si **devono** adottare opportune misure per **prevenire controlli successivi** sul lavoratore
  - Tali controlli, leciti o meno, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonee a rivelare idee religiose, filosofiche e politiche, salute o vita sessuale
- Si **possono** adottare misure:
  - individuazione di categorie di siti correlati o meno con la prestazione
  - filtri che prevengano determinate operazioni –non finalizzate al lavoro– con limitazioni di dimensioni o tipo
  - trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni
    - log riferiti al traffico web, su base collettiva o per gruppi
  - eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza

# 5.2 – Principio di necessità

## Programmi che consentono controlli "indiretti"

b) Posta elettronica

- Il contenuto e i metadata e-mail sono tutelati dalla Costituzione
  - Proteggere dignità umana e sviluppo personalità nella società
  - Norme penali a tutela dell'inviolabilità dei segreti
- Dubbio se il lavoratore usa e-mail per l'azienda o per sé
  - Senza policy  si crea aspettativa di privacy nel lavoratore
  - Problemi di liceità dell'analisi del contenuto della posta elettronica
  - Prevenire trattamenti  contro i principi di pertinenza e non eccedenza
- **Opportuno**:
  - Dare indirizzi di posta condivisi tra più lavoratori
  - Dare indirizzi destinati ad uso privato del lavoratore
  - Risposta per assente con altro contatto aziendale
    - attivabile anche dall'amministratore  avvertendo l'interessato
  - Delega a collega, con verbale
  - Avvertimento ai destinatari su natura non personale dei messaggi

# 6.1. Graduazione dei controlli
## Pertinenza e non eccedenza

- Evitare interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori ed esterni
- Controllo lecito se rispettati principi di pertinenza e non eccedenza
- In caso di danni o pericolo **si possono adottare misure** di verifica di comportamenti anomali
- Preferibile un controllo preliminare su dati aggregati per azienda o area
  - Controllo anonimo seguito da avviso generale o limitato ad area su utilizzo anomalo degli strumenti aziendali e invito a rispettare regole.
    - Senza successive anomalie non effettuare controlli individuali
- Non ammessi controlli prolungati, costanti o indiscriminati

# 6.2. Conservazione

## Pertinenza e non eccedenza

- Rotazione dei log, per **non conservare dati di traffico**
  - Tempo determinato da necessità reali
- Eccezioni solo per:
  - esigenze tecniche o di sicurezza del tutto particolari
  - indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria
  - obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria
- Nelle eccezioni il trattamento dei dati personali deve essere limitato alle sole informazioni indispensabili per la finalità predeterminata

# 7.1. Datori di lavoro privati

## Presupposti di liceità del trattamento: bilanciamento di interessi

- Possono effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili, seguendo i criteri già esposti
  a) se legittimo esercizio di un diritto in sede giudiziaria
  b) in caso di valida manifestazione di un libero consenso
  c) anche in assenza del consenso, ma per effetto del presente provvedimento che individua un legittimo interesse al trattamento in applicazione della disciplina sul bilanciamento di interessi
- Garanzie per il controllo "indiretto" a distanza senza esplicito consenso degli interessati, ma con **accordo sindacale**
- L'eventuale trattamento di dati sensibili è consentito con il consenso degli interessati o, senza il consenso, nei casi previsti
  - Salvaguardia vita o incolumità
  - Ambiti giudiziari

# 7.2. Datori di lavoro pubblici

## Presupposti di liceità del trattamento: bilanciamento di interessi

- Differenti presupposti a seconda della natura dei dati, sensibili o meno
  - Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici
  - Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari
  - Principi applicabili al trattamento di dati sensibili
  - Principi applicabili al trattamento di dati giudiziari
  - Principi applicabili al trattamento di dati sensibili e giudiziari
  - Finalità di rilevante interesse pubblico

- In tutti i casi resta impregiudicata la facoltà del lavoratore di **opporsi al trattamento** per motivi legittimi

# 8. Individuazione dei soggetti preposti

- Designazione **facoltativa** di uno o più responsabili del trattamento cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità
  - Nel caso di interventi per manutenzione del sistema, prevenire l'accesso a dati personali presenti in spazi di memoria assegnati a dipendenti
- Svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa
- **Formare** gli amministratori di sistema sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni

# Prescrizione 1 del Garante

- Ai datori di lavoro privati e pubblici
  - adottare la misura necessaria a garanzia degli interessati, per specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori
    - indicando chiaramente le modalità di uso degli strumenti messi a disposizione
    - in che **misura** e con quali **modalità** vengano effettuati **controlli**

# Prescrizione 2 del Garante

a) Adozione e pubblicizzazione di un **disciplinare interno**
b) Adozione di misure di tipo organizzativo per:
   - valutare l'impatto sui diritti dei lavoratori
   - individuare preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e dell'accesso a Internet
   - individuare quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi

# Prescrizione 2 del Garante

c) Adozione di misure di tipo tecnologico

I. Rispetto alla "navigazione" in Internet:

- individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa
- configurazione di sistemi o l'utilizzo di **filtri** che prevengano determinate operazioni
- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione degli utenti, tramite aggregazioni
- eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza
- graduazione dei controlli

# Prescrizione 2 del Garante

c) Adozione di misure di tipo tecnologico

II. Rispetto all'utilizzo della posta elettronica:

- indirizzi e-mail condivisi
- eventuale e-mail privato
- sistema di risposta per assente
- consentire delega a collega
- **nota in calce** a ogni e-mail su natura non personale del messaggio con specifica se le risposte sono condivise da altri nell'azienda
- graduazione dei controlli

# Prescrizioni 3, 4, 5 del Garante

3) **Vieta** ai datori di lavoro privati e pubblici trattamenti di dati personali hardware e software per controllo a distanza di lavoratori come
   a) lettura e registrazione sistematica di e-mail e metadata, oltre quanto tecnicamente necessario per svolgere il servizio
   b) riproduzione e memorizzazione sistematica delle pagine web visualizzate dal lavoratore
   c) keyboard logging
   d) analisi occulta di computer portatili affidati in uso
3) Individua i casi nei quali il trattamento dei dati personali di natura non sensibile possono essere effettuati per perseguire un legittimo interesse del datore di lavoro anche senza il consenso degli interessati
4) Dispone pubblicazione su Gazzetta Ufficiale del presente provvedimento