PUBBLICA AMMINISTRAZIONE:
5 PASSI VERSO LA SICUREZZA
(terza tappa)
"GESTIONE DELLE IDENTITÀ, CONTROLLO LOGICO DEGLI ACCESSI E SECURITY AUDITING"

ROMA, 10 GIUGNO 2008 - IBM ROMA TORRINO

"Il trattamento degli accessi nella normativa nazionale: sicurezza Vs Privacy"

A cura di Aldo Agostini
Security Analyst
Presidente di Security Studio System s.r.l. (SSSy)
(www.sssy.it - aagostini@sssy.it)

CODICE PRIVACY

(D. L.vo 196/03)

PRINCIPI FONDAMENTALI

PER IL TRATTAMENTO DEI DATI PERSONALI

- **PRINCIPIO DI LICEITA'**
- **PRINCIPIO DI FINALITA'**
- **PRINCIPIO DI NECESSITA'**
- **PRINCIPIO DI PROPORZIONALITA'**

CAPO III DIVIETO DI CONTROLLO A DISTANZA E TELELAVORO
Art. 114 *Controllo a distanza*
1. Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n.300.

STATUTO DEI LAVORATORI
(Legge 20 maggio 1970, n. 300)

Art. 4 - Impianti audiovisivi

1. E' vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.

2. 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.

…

4. Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale.

PRESIDENZA DEL CONSIGLIO DEI MINISTRI
Dipartimento della Funzione Pubblica
DIRETTIVA 11 febbraio 2005
(pubblicato nella Gazzetta Ufficiale n. 97 del 28 aprile 2005)

MISURE FINALIZZATE ALL'ATTUAZIONE NELLE PUBBLICHE AMMINISTRAZIONI DELLE DISPOSIZIONI CONTENUTE NEL DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196, RECANTE CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, CON PARTICOLARE RIGUARDO ALLA GESTIONE DELLE RISORSE UMANE. (DIRETTIVA N. 1/2005)

… Riguardo al tema del controllo dei lavoratori, occorre rammentare il divieto di controllo a distanza dell'attività lavorativa e le altre garanzie previste in materia di lavoro dall'art. 4 della legge n. 300/1970 richiamato dal Codice. Tali garanzie devono essere rispettate, in particolare, nel caso di installazione nei locali dell'amministrazione di impianti di videosorveglianza per motivi di sicurezza o per esigenze organizzative e dei processi produttivi, tenendo presente l'obbligo di informare, anche con formule sintetiche, i dipendenti ed i visitatori che stanno per accedere o che si trovano in una zona videosorvegliata e dell'eventuale registrazione (art. 13 del Codice).

…

"Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico“

14 giugno 2007 - GU n. 161 del 13-7-2007 - Suppl. Ordinario n.159

2.2. Liceità, pertinenza, trasparenza. Il datore di lavoro pubblico può lecitamente trattare dati personali dei lavoratori nella misura in cui ciò sia necessario per la corretta gestione del rapporto di lavoro, avendo cura di applicare le previsioni che riguardano le proprie funzioni istituzionali o il rapporto di lavoro, contenute in leggi, regolamenti, contratti e in accordi collettivi, in modo da avvalersi di informazioni personali e modalità di trattamento proporzionate ai singoli scopi.

Il Codice in materia di protezione dei dati personali, anche in attuazione di direttive comunitarie (nn. 95/46/Ce e 2002/58/Ce), prescrive che il trattamento di dati personali per la gestione del rapporto di lavoro avvenga, in particolare:

…

- adottando adeguate misure di sicurezza, idonee a preservare i dati da alcuni eventi tra cui accessi ed utilizzazioni indebiti, rispetto ai quali l'amministrazione può essere chiamata a rispondere anche civilmente e penalmente (artt. 15 e 31 e ss. del Codice).

Lavoro: le linee guida del Garante per posta elettronica e internet

1 marzo 2007 - Gazzetta Ufficiale n. 58 del 10 marzo 2007

- 2.3. *Principi del Codice*
- a) il principio di ***necessità***,
- b) il principio di ***correttezza***, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (*art. 11, comma 1, lett. a), del Codice*).
- c) i trattamenti devono essere effettuati per finalità ***determinate, esplicite*** e ***legittime*** osservando il principio di ***pertinenza*** e ***non eccedenza*** (*par. 6*).
- Quindi:
  - 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;*
  - *se pertinente, vale il principio di segretezza della corrispondenza"*

Segue: Lavoro: le linee guida del Garante per posta elettronica e internet

1 marzo 2007 - Gazzetta Ufficiale n. 58 del 10 marzo 2007

3.1. Disciplina interna

Grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, 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. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.

4. Apparecchiature preordinate al controllo a distanza

Con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b), del Codice), il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 cod. civ.).

Segue: Lavoro: le linee guida del Garante per posta elettronica e internet

1 marzo 2007 - Gazzetta Ufficiale n. 58 del 10 marzo 2007

3.2. Linee guida

Un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente e da sottoporre ad aggiornamento periodico.

Esempi:

- **….**
- **quali informazioni sono memorizzate temporaneamente (ad es., 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);**
- **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, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);**

Segue: Lavoro: le linee guida del Garante per posta elettronica e internet

1 marzo 2007 - Gazzetta Ufficiale n. 58 del 10 marzo 2007

3.2. Linee guida; segue il disciplinare interno:

- **quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente;**
- **quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali;**
- **le prescrizioni interne sulla sicurezza dei dati e dei sistemi (art. 34 del Codice, nonché Allegato B), in**

particolare regole 4, 9, 10).

3.3. Informativa (art. 13 del Codice)

Rispetto a eventuali controlli gli interessati hanno infatti il diritto di essere informati preventivamente, 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.

Segue: Lavoro: le linee guida del Garante per posta elettronica e internet

1 marzo 2007 - Gazzetta Ufficiale n. 58 del 10 marzo 2007

4. Apparecchiature preordinate al controllo a distanza

…. DIVIETO:

- **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;**
- **dell'analisi occulta di computer portatili affidati in uso.**

5. Programmi che consentono controlli "indiretti"

5.1. Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Ciò, anche in presenza di attività di controllo discontinue.

Segue: Lavoro: le linee guida del Garante per posta elettronica e internet

1 marzo 2007 - Gazzetta Ufficiale n. 58 del 10 marzo 2007

5.2. Principio di necessità - INTERNET

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

- **valutazione d'impatto;**
- **chi può avere accesso alla posta elettronica e a Internet;**
- **si determini quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo.**

- Prevenire i controlli successivi sul lavoratore, che possono riguardare dati sensibili.

Misure da adottare:

- **individuazione di categorie di siti;**
- **configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni ;**
- **trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante le loro opportune aggregazioni ;**
- **eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative,produttive e di sicurezza.**

Segue: Lavoro: le linee guida del Garante per posta elettronica e internet

1 marzo 2007 - Gazzetta Ufficiale n. 58 del 10 marzo 2007

5.2. Principio di necessità - Posta elettronica

Impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa:

- **rendere disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, urp@ente.it, etc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente.it), valutando possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato;**
- **mettere a disposizione apposite funzionalità di sistema (risposta automatica);**
- **fiduciario per verifica posta in caso di assenza;**
- **i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi.**

Segue: Lavoro: le linee guida del Garante per posta elettronica e internet

1 marzo 2007 - Gazzetta Ufficiale n. 58 del 10 marzo 2007

6. Pertinenza e non eccedenza

6.2. Conservazione

I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario –e predeterminato– a raggiungerla (v. art. 11, comma 1, lett. e), del Codice).

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- **ad esigenze tecniche o di sicurezza del tutto particolari;**
- **all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;**
- **all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.**

Segue: Lavoro: le linee guida del Garante per posta elettronica e internet

1 marzo 2007 - Gazzetta Ufficiale n. 58 del 10 marzo 2007

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;

- esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti;

- obbligo dei soggetti preposti di svolgere solo operazioni strettamente necessarie senza realizzare attività di controllo a distanza;

- amministratori di sistema o figure analoghe: attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni

MISURE DI SICUREZZA

- **ART. 31 *Obblighi di sicurezza* (Misure Idonee di Sicurezza)**

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

- **ART. 33: MMS (Misure Minime di Sicurezza)**
- **ART. 34: trattamenti con strumenti eletttronici**
- **ART. 35: trattamenti senza l'ausilio di strumenti elettronici;**

ALLEGATO "B" AL CODICE: DISCIPLINARE TECNICO

LE MISURE DI SICUREZZA
(Misure Minime)

Documento programmatico sulla sicurezza

Regola 19, all. B del Codice della Privacy

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

CASE STUDY 1

QUALI DATI "LOGGARE"?

PROVVEDIMENTO 17 gennaio 2008

Conservazione dei dati di traffico: misure e accorgimenti a tutela dell'interessato (GU n. 30 del 5-2-2008)

7.1. Sistemi di autenticazione.

Il trattamento dei dati di traffico telefonico e telematico da parte dei fornitori deve essere consentito solo agli incaricati del trattamento e unicamente sulla base del preventivo utilizzo di specifici sistemi di autenticazione informatica basati su tecniche di strong authentication …. … .

Limitatamente a tali addetti tecnici, circostanze legate a indifferibili interventi per malfunzionamenti, guasti, installazioni hardware e software, aggiornamento e riconfigurazione dei sistemi, possono determinare la necessità di accesso informatico a sistemi di elaborazione che trattano dati di traffico in assenza di autenticazione biometrica o di strong-authentication per operazioni che comportano la presenza fisica dell'addetto che procede all'intervento in prossimità del sistema di elaborazione (per esempio, per lo svolgimento di operazioni di amministrazione da console locale che implichino la disabilitazione dei servizi di rete e l'impossibilita' di gestire operazioni di input/output tramite dispositivi accessori come quelli utilizzabili per la strong authentication).

In caso di accesso da parte degli addetti tecnici nei termini anzidetti, fermo restando l'obbligo di assicurare le misure minime in tema di credenziali di autenticazione previste dall'Allegato B) al Codice e, per quanto concerne i trattamenti di dati di traffico telefonico per esclusive finalità di giustizia, quanto specificato al successivo paragrafo 7.3, dovrà essere tenuta preventivamente traccia in un apposito »registro degli accessi» dell'evento, nonché delle motivazioni che lo hanno determinato, con una successiva descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di sistemi elettronici. Tale registro deve essere custodito dal fornitore presso le sedi di elaborazione e messo a disposizione del Garante nel caso di ispezioni o controlli, unitamente a un elenco nominativo dei soggetti abilitati all'accesso ai diversi sistemi di elaborazione con funzioni di amministratore di sistema, che deve essere formato e aggiornato costantemente dal fornitore.

CASE STUDY 1

Segue: QUALI DATI "LOGGARE"?

PROVVEDIMENTO 17 gennaio 2008

Conservazione dei dati di traffico: misure e accorgimenti a tutela dell'interessato (GU n. 30 del 5-2-2008)

7.6. Altre misure.

Audit log

Devono essere adottate soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi database utilizzati.

Tali soluzioni comprendono la registrazione, in un apposito audit log, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici.

I sistemi di audit log devono garantire la completezza, l'immodificabilità e l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad auditing. A tali scopi devono essere adottati, per la registrazione dei dati di auditing, anche in forma centralizzata per ogni impianto di elaborazione o per datacenter, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche.

Le misure di cui al presente paragrafo sono adottate nel rispetto dei principi in materia di controllo dei lavoratori sull'uso di strumenti elettronici, con particolare riguardo all'informativa agli interessati. (NO ARTICOLO 4 STRATUTO LAVORATORI?)

CASE STUDY 1

Segue: QUALI DATI "LOGGARE"?

PROVVEDIMENTO 17 gennaio 2008

Conservazione dei dati di traffico: misure e accorgimenti a tutela dell'interessato (GU n. 30 del 5-2-2008)

Segue: 7.6. Altre misure.

Audit log

7.7. Audit internoRapporti periodici.

La gestione dei dati di traffico per finalità di accertamento e repressione di reati deve essere oggetto, con cadenza almeno annuale, di un'attività di controllo interno da parte dei titolari del trattamento, in modo che sia verificata costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal provvedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati.

L'attività di controllo deve essere demandata a un'unità organizzativa o, comunque, a personale diverso rispetto a quelli cui e' affidato il trattamento dei dati per la finalità di accertamento e repressione dei reati.

I controlli devono comprendere anche verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di Alerting e di Anomaly Detection, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento. Sono svolte, altresì, verifiche periodiche sull'effettiva cancellazione dei dati decorsi i periodi di conservazione.

L'attività di controllo deve essere adeguatamente documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate.

L'esito dell'attività di controllo deve essere:

- comunicato alle persone e agli organi legittimati ad adottare decisioni e a esprimere, a vari livelli in base al proprio ordinamento interno, la volontà della società;

- richiamato nell'ambito del documento programmatico sulla sicurezza nel quale devono essere indicati gli interventi eventualmente necessari per adeguare le misure di sicurezza;

- messo, a richiesta, a disposizione del Garante o dell'autorità giudiziaria.

CASE STUDY 2

QUALI DATI "LOGGARE"?

Il CED P.S.: Provvedimento del 17 novembre 2005

4.8 Auditing di sicurezza

Profili esaminati in tema di security auditing (intendendosi per tale la registrazione, l'esame e la verifica di attività rilevanti ai fini della sicurezza che abbiano luogo in un sistema informatico protetto), il C.e.d. prevede la tenuta dei log degli accessi e delle transazioni, anche di sola lettura, che vengono attualmente conservati nel patrimonio informativo del Centro contribuendo a successivi accertamenti su certe operazioni effettuate. Sono tuttavia assenti meccanismi di auditing di ausilio alla verifica di anomalie o del superamento di soglie predefinite per alcuni indici di prestazione.

Prescrizioni

-individuare termini congrui di conservazione dei log;

- strumenti e funzionalità di auditing;

  - moduli software nel sistema informativo per il monitoraggio delle performance sistema e della disponibilità dei dati;

  - potenziare la funzione organizzativa responsabile dell'attività di auditing per la sicurezza e la disponibilità dei dati, (security manager interno);.

4.9 Rapporti statistici

- elaborazione periodica di rapporti retrospettivi;

4.10 Sicurezza e integrità dei dati di log e di auditing

- classificati come riservati;

-elevate garanzie sull'integrità e sull'autenticità dei log;

- dotati di marche temporali e di controlli di integrità (firma digitale e certified logging);

-consultazione dei log file permessa ai soli soggetti dotati di specifici profili di autorizzazione.

LE SANZIONI PENALI

(Artt. 615 ter, quater e quinquies – Convenzione di Budapest -)

Art. 615 ter Accesso abusivo ad un sistema informatico o telematico
Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volonta' espressa o tacita di chi ha il diritto di escluderlo, e' punito con la reclusione fino a tre anni.

…

Art. 615 quater Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
Chiunque, al fine di procurare a se' o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, e' punito con la reclusione sino ad un anno e con la multa sino a lire dieci milioni..

….

Art. 615-*quinquies*. – *(Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)*. – Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

LE SANZIONI PENALI

(Artt. 635 bis, ter, quater e quinquies – Convenzione di Budapest -)

Art. 635-*bis*. – *(Danneggiamento di informazioni, dati e programmi informatici)*. – Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio».

Art. 635-*ter*. – *(Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità)*. – Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

…

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

LE SANZIONI PENALI

(Artt. 635 bis, ter, quater e quinquies – Convenzione di Budapest -)

Art. 635-*quater*. – *(Danneggiamento di sistemi informatici o telematici)*. – Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-*bis*, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

Art. 635-*quinquies*. – *(Danneggiamento di sistemi informatici o telematici di pubblica utilità)*. – Se il fatto di cui all'articolo 635-*quater* è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata».

LA PEDOPORNOGRAFIA

LEGGE 6 febbraio 2006, n.38 (GU n. 38 del 15-2-2006)
Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet

MODIFICHE AL CODICE PENALE

Art. 600-bis (Prostituzione minorile). – Chiunque Induce alla prostituzione una persona di eta' inferiore agli anni diciotto ovvero ne favorisce o sfrutta la prostituzione e' punito con la reclusione da sei a dodici anni e con la multa da lire trenta milioni a lire trecento milioni.

Salvo che il fatto costituisca piu' grave reato, chiunque compie atti sessuali con un minore di eta' compresa tra i quattordici e i diciotto anni, in cambio di denaro o di altra utilita' economica, e‘ punito con la reclusione da sei mesi a tre anni e con la multa non inferiore a curo 5.164…

«Art. 600-ter (Pornografia minorile). - Chiunque, utilizzando minori degli anni diciotto, realizza esibizioni pornografiche o produce materiale pornografico ovvero induce minori di anni diciotto a partecipare ad esibizioni pornografiche e' punito con la reclusione… …

Art. 600-quater. - (Detenzione di materiale pornografico) Chiunque, …. consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto, e' punito con la reclusione fino a tre anni e con la multa non inferiore a euro 1.549…

Art. 600-quater. I. (Pornografia virtuale). Le disposizioni di cui agli articoli 600-ter e 600-quater si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena e' diminuita di un terzo.

Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualita' di rappresentazione fa apparire

come vere situazioni non reali.

LE NORME ANTITERRORISMO

(Il D.L. 144/05, convertito con modificazioni dalle Legge 155/05)

CALL CENTER - INTERNET POINT – SICUREZZA TELEMATICA

Art. 7.

Integrazione della disciplina amministrativa degli esercizi pubblici di telefonia e internet

.. chiunque intende aprire un pubblico esercizio o un circolo privato di qualsiasi specie, nel quale sono posti a disposizione del pubblico, dei clienti o dei soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, deve chiederne la licenza al questore. La licenza non e' richiesta nel caso di sola installazione di telefoni pubblici a pagamento, abilitati esclusivamente alla telefonia vocale.

materia.))

4. Con decreto del Ministro dell'interno di concerto con il Ministro delle comunicazioni e con il Ministro per l'innovazione tecnologica, … il titolare o il gestore di un … e' tenuto ad osservare per il monitoraggio delle operazioni dell'utente e per l'archiviazione dei relativi dati, nonchè le misure di preventiva acquisizione di dati anagrafici riportati su un documento di identità

Art. 7-bis

Sicurezza telematica

1. Ferme restando le competenze dei Servizi informativi e di sicurezza, … l'organo del Ministero dell'interno – POLIZIA POSTALE - per la sicurezza e per la regolarità dei servizi di telecomunicazione assicura i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'interno, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate.

2.

LE NORME ANTITERRORISMO

(DECRETO 16 agosto 2005 - Pubblicato sulla G.U. n.190 del 17.08.2005)

CALL CENTER - INTERNET POINT

Art. 1. Obblighi dei titolari e dei gestori

1. I titolari o gestori di un esercizio pubblico o di un circolo privato di qualsiasi specie nel quale sono poste a disposizione del pubblico, dei clienti o dei soci, apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale, sono tenuti a:

   a) adottare le misure fisiche o tecnologiche occorrenti per impedire l'accesso agli apparecchi terminali a persone che non siano preventivamente identificate con le modalita' di cui alla lettera b);

   b) identificare chi accede ai servizi telefonici e telematici offerti, prima dell'accesso stesso o dell'offerta di credenziali di accesso, acquisendo i dati anagrafici riportati su un documento di identita', nonche' il tipo, il numero e la riproduzione del documento presentato dall'utente;

   c) adottare le misure di cui all'art. 2, occorrenti per il monitoraggio delle attivita';

4. I dati acquisiti a norma del comma 1, lettere b) e c), sono raccolti e conservati con modalita' informatiche.

Art. 2.

Monitoraggio delle attivita'

1. I soggetti di cui all'art. 1 adottano le misure necessarie a memorizzare e mantenere i dati relativi alla data ed ora della comunicazione e alla tipologia del servizio utilizzato, abbinabili univocamente al terminale utilizzato dall'utente, esclusi comunque i contenuti delle comunicazioni.

SCADENZA AL 31 DICEMBRE 2008

MA PER QUALE PERIODO?

Caso dei tabulati:

- **La Direttiva 2006/24/CE prevede due anni per i dati telefonici, ergo non è dissimile il periodo di conservazione dei log;**

Caso dei call center:

- **Il tempo stabilito dalla Legge;**

PUBBLICA AMMINISTRAZIONE:

5 PASSI VERSO LA SICUREZZA

(terza tappa)

"GESTIONE DELLE IDENTITÀ, CONTROLLO LOGICO DEGLI ACCESSI E SECURITY AUDITING"

ROMA, 10 GIUGNO 2008 - IBM ROMA TORRINO

"Il trattamento degli accessi nella normativa nazionale: sicurezza Vs Privacy"

GRAZIE PER LA VOSTRA ATTENZIONE

A cura di Aldo Agostini
Security Analyst
Presidente di Security Studio System s.r.l. (SSSy)
(www.sssy.it - aagostini@sssy.it)