NUOVE MISURE
DI SICUREZZA PER LA PRIVACY

•D. Lgs. 30 giugno 2003, n. 196

Dott. Alessandro BRIDI

Dott. Marco BATTISTI

Argomenti trattati

1. Introduzione
2. Il significato di “Sicurezza”
3. Origine dei crimini e della sicurezza informatica
4. Privacy e misure di sicurezza
5. Le definizioni per la sicurezza
6. Obblighi di sicurezza
7. Misure minime di sicurezza
8. Sanzioni e danni
9. Ruolo di CercaSì S.n.c.
10. Assistenza offerta

Introduzione

ENTRO IL 30 GIUGNO 2004 TUTTE LE AZIENDE CHE TRATTANO DATI PERSONALI[1)] DEVONO DOTARSI DI UN DPS

(DOCUMENTO PROGRAMMATICO SULLA SICUREZZA)

[1)]Art 4 (Definizioni) 1. Ai fini del presente codice si intende per:

b) “dato personale”, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

Introduzione

Art. 1 (Diritto alla protezione dei dati personali)

Chiunque, nessuno escluso, ha diritto alla protezione dei dati PERSONALI che lo riguardano.

Le metodologie per ridurre al minimo il rischio della perdita (anche accidentale) di dati sono espresse nell'allegato B del T.U. noto come "Disciplinare tecnico in materia di misure minime di sicurezza".

Il significato di “Sicurezza”

“La sicurezza è l’insieme delle misure atte a garantire la disponibilità, la integrità e la riservatezza delle informazioni gestite.”

Definizione ISO

“Insieme delle misure (di carattere organizzativo e tecnologico) tese ad assicurare a ciascun utente autorizzato (e a nessun altro) tutti e soli i servizi previsti per quell’utente, nei tempi e nelle modalità previste.”

Definizione A.I.P.A.

“Rendere un sistema informativo sicuro non significa solo attuare un insieme di contromisure specifiche (di carattere tecnologico ed organizzativo) che neutralizzi tutti gli attacchi ipotizzabili per quel sistema; significa anche collocare ciascuna contromisura in una politica organica di sicurezza che tenga conto dei vincoli (tecnici, logistici, amministrativi, politici) imposti dalla struttura in cui il sistema informativo opera, e che giustifichi ciascuna contromisura in un quadro complessivo.”

Da “La Sicurezza nei sistemi informativi” di Antonio Leonforte

A.I.P.A. - Aprile 2000

Origine dei crimini e della sicurezza informatica

I rischi e i crimini informatici, da venticinque anni, aumentano costantemente, anche se gli episodi noti sono pochi; e ciò è dovuto soprattutto alle resistenze delle aziende colpite nel denunciare le frodi e i danni subiti, nel timore che la notizia possa innescare fenomeni di pubblicità negativa, rischio di reputazione,e conseguenti ulteriori danni all'immagine ed alla credibilità dell'azienda, con l'effetto probabile di perdere parte della propria clientela e di avvantaggiare le aziende concorrenti.

Origine dei crimini e della sicurezza informatica

L'esigenza di una buona organizzazione della sicurezza interna è dovuta sia alla pervasività e volgarizzazione dell'informatica, sia il fatto che la criminalità, organizzata e non, fa ricorso all'informatica per usare i sistemi telematici come mezzi idonei ad esercitare attività illecite, ma anche come obiettivo del crimine stesso, soprattutto per la sottrazione di informazioni e dati, come nei casi di spionaggio industriale e in tutti gli episodi di infedeltà interna da parte di dipendenti delle imprese.

Origine dei crimini e della sicurezza informatica

A tali pericoli vanno aggiunti altri rischi come quello di distruzione parziale o totale dei dati registrati a causa di incidenti dolosi, colposi, o del tutto automatici come spesso accade a causa dei virus informatici.

Origine dei crimini e della sicurezza informatica

Un’altra variabile che incide pesantemente sulla necessità di tutelare i sistemi informativi, e la cui matrice meriterebbe ampie considerazioni sociologiche, è da ricercare nella crescente moda e nei nuovi atteggiamenti di molti giovani adolescenti che, indipendentemente dalla cultura e dal livello sociale di provenienza, dedicano gran parte del loro tempo libero alle comunicazioni virtuali in rete, all’affiliazione telematica, al tentativo di penetrare nei sistemi informatici altrui e alla ricerca di informazioni registrate nei sistemi.

Privacy
e misure di sicurezza

Le misure di sicurezza poste a tutela del trattamento dei dati personali diviene obbligatoria con la legge 31 dicembre 1996 n. 675 che, in materia di misure minime di sicurezza, fu completata con il D.P.R. 28 luglio 1999 n. 318.

Privacy
e misure di sicurezza

La direttiva comunitaria 2002/58/Ce del 12 luglio 2002 ha poi reso necessario ulteriori interventi di armonizzazione e la conseguente proroga al 30 giugno 2003 del termine di delega per la compilazione del testo unico.

Privacy
e misure di sicurezza

La scelta di predisporre un testo unico, nel rispondere a esigenze di chiarezza di lettura, di linguaggio e di semplificazione dell'intero quadro legislativo, permette di elevare tutta la materia a un solo rango legislativo, integrato dalla introduzione di un allegato disciplinare tecnico per le misure minime di sicurezza che potrà essere adeguato in relazione all'evoluzione del settore con decreti ministeriali non regolamentari.

Privacy
e misure di sicurezza

Il codice si compone di tre parti che contengono rispettivamente:

1) Le disposizioni generali;
2) Le disposizioni particolari per specifici trattamenti;
3) Le disposizioni relative alle azioni di tutela dell'interessato e al sistema sanzionatorio.

Privacy
e misure di sicurezza

I principi che ispirano la legge mirano a 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.

Privacy
e misure di sicurezza

In caso di motivata richiesta di risarcimento del danno dovuto al trattamento dei dati, il titolare e il responsabile avranno l'onere della prova per dimostrare di aver adottato tutte le misure idonee ad evitare il danno.

Art. 2050 del codice civile
Chiunque cagiona danno ad altri nello svolgimento di una Attività pericolosa per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di aver adottato tutte le misure idonee a evitare il danno

Le definizioni per la sicurezza

Misure minime:

il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

Le definizioni per la sicurezza

Strumenti elettronici:

Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Le definizioni per la sicurezza

Autenticazione informatica:

L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Le definizioni per la sicurezza

Credenziali di autenticazione:

I dati e i dispositivi, in possesso di una persona, da questa conosciuti o da essa univocamente correlati, utilizzati per l'autenticazione informatica.

Le definizioni per la sicurezza

Parola chiave:

Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

Le definizioni per la sicurezza

Profilo di autorizzazione:

L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

Le definizioni per la sicurezza

Sistema di autorizzazione:

L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Obblighi di sicurezza

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.

Obblighi di sicurezza

Nel quadro dei più generali obblighi di sicurezza i titolari del trattamento sono comunque tenuti ad adottare le “misure minime di sicurezza” volte ad assicurare un livello minimo di protezione dei dati personali.

Sanzioni e danni

SANZIONI:

In caso di violazione accertata, sono previste sanzioni di tipo amministrativo fino a 50.000 Euro e la reclusione fino a 3 anni, esclusione dalle gare di appalto e risarcimento di danni ai sensi dell'art. 2050 C.C.

Art. 2050 del codice civile (Responsabilità per l'esercizio di attività pericolose)

"Chiunque cagiona danno agli altri nello svolgimento di un'attività pericolosa, per sua natura o per i mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.

Sanzioni e danni

ISPEZIONI:

E' stato siglato un protocollo d'intesa tra la Guardia di Finanza ed il Garante della Privacy per una sempre più intensa ed efficace attività di controllo sulla raccolta dei dati. La Guardia di Finanza collaborerà alle attività ispettive attraverso la partecipazione del proprio personale ai controlli sulle banche dati, alle verifiche e alle altre rilevazioni nei luoghi ove si svolge il trattamento. Le ispezioni serviranno per cancellare sacche di non applicazione della legge e per evitare disparità di trattamento tra i privati che hanno sopportato spese per adeguarsi e chi non lo ha fatto.

Sanzioni e danni

RISARCIMENTO DANNI:

E' tenuto al risarcimento, chi non prova di avere adottato tutte le misure idonee al trattamento della sicurezza dei dati. Chiunque cagiona danno è tenuto al risarcimento ai sensi dell'art. 2050 C.C.

Ruolo di CercaSì S.n.c.

- Verifica sullo stato di attuazione degli adempimenti previsti dalla normativa. Questa prima analisi consentirà di chiarire eventuali rischi e possibili conseguenze derivanti da omissione negli adempimenti;
- Censimento dei dati trattati con relative finalità, categorie di interessati ed ambito di comunicazione e diffusione;
- Creazione di un gruppo privacy all'interno dell'azienda. Ne faranno parte i Responsabili dell'area gestione risorse umane, amministrativa, legale ed informatica;

Ruolo di CercaSì S.n.c.

- Analisi strutturata dei rischi.

  Questa fase riveste un'importanza fondamentale sia per la redazione del "Documento programmatico sulla sicurezza" sia per la realizzazione del "Piano di assistenza recovery", divenuto obbligatorio con l'introduzione del Decreto Legislativo 30 giungo 2003, n. 196 e di cui all'Allegato B in caso di trattamenti di dati sensibili e giudiziari effettuati con strumenti elettronici.

Ruolo di CercaSì S.n.c.

Per la stesura del Documento programmatico sulla sicurezza, dovranno essere definiti i compiti e le responsabilità in materia di sicurezza al fine di adottare un piano di intervento per la tutela e la protezione delle aree e dei locali, dell'integrità dei dati e delle trasmissioni delle stesse.

Ruolo di CercaSì S.n.c.

- Collaborazione con i componenti del gruppo privacy;
- Assistenza alla compilazione e aggiornamento della notificazione al Garante (se necessaria come previsto dall'articolo 37)
- Predisposizione delle informative di cui all'articolo 13: clienti, fornitori, dipendenti, utenti, agenti, etc.
- Definizione delle nomine con predisposizione della modulistica (lettere di incarico per i Responsabili del trattamento interni ed esterni, Preposti alla custodia delle copie delle credenziali, Incaricati del trattamento, etc.

Ruolo di CercaSì S.n.c.

- Indicazione delle clausole contrattuali per trattamenti effettuati con società esterne;
- Corsi di formazione, specifici per categorie di incaricati al trattamento dei dati, con consegna ai partecipanti di documentazione per l'esatta applicazione della normativa;
- Predisposizione di un'adeguata policy privacy relativa al sito internet;
- Attivazione di eventuali misure di sicurezza idonee per la protezione dei dati;

Ruolo di CercaSì S.n.c.

- Predisposizione di informative ed ulteriore documentazione per i trattamenti dati effettuati con strumenti quali videosorveglianza, dispositivi biometrici, etc.
- Risposte a quesiti che dovessero insorgere per l'esatta applicazione della normativa;
- Consegna e aggiornamento della documentazione pubblicata dal Garante (newsletter, comunicati stampa, pareri, etc.)

Per mettersi in regola…

Ruolo di CercaSì S.n.c.

È necessario:

- compilare e stampare la documentazione per le figure previste dalla normativa (lettere d'incarico per Responsabile della Sicurezza Dati Personali, Incaricati per i trattamenti, ecc...);
- proteggere tutte le banche dati (di qualsiasi tipologia) da intrusioni o utilizzi non autorizzati;
- adottare le misure minime di sicurezza previste dalla normativa (password, sistemi antintrusione, antivirus, copie di backup, ecc...);

Per mettersi in regola…

Ruolo di CercaSì S.n.c.

È necessario:

- compilare e stampare il DPS (Documento Programmatico Sulla Sicurezza) con cadenza annuale apportando di anno in anno le opportune modifiche (solo il DPS fa prova dell'avvenuto adeguamento alla norma);
- adottare le misure fisiche di protezione (allarmi, stabilizzatori di corrente, armadi chiusi a chiave ed ignifughi, accesso selezionato ai locali...);
- inventariare i dati personali, adottare le misure di sicurezza obbligatorie (fisiche, logiche ed organizzative), adeguandosi agli obblighi di informativa, consenso, nomina figure.