Il nuovo Codice sulla Privacy

Il 1gennaio 2004 è entrato in vigore il nuovo Codice sulla Privacy (decreto legislativo 30 giugno 2003, n. 196) che, raccogliendo l'intera materia in un'unica fonte, ha riunito, in un solo testo, le disposizioni in materia di trattamento dei dati personali, dalla Legge 675/96 (sostituita dalla sua entrata in vigore) alla direttiva UE 58/2002 (sulla riservatezza nelle comunicazioni elettroniche).

Il Testo è suddiviso in tre parti fondamentali:

1. La prima parte è dedicata alle disposizioni generali, riordinate in modo tale da trattare tutti gli adempimenti e le regole del trattamento con riferimento ai settori pubblico e privato;
2. La seconda sezione si rivolge ai settori specifici, e, oltre a disciplinare aspetti in parte inediti (informazione giuridica, notificazioni di atti giudiziari, dati sui comportamenti debitori), completa anche la disciplina attesa da tempo per il settore degli organismi sanitari e quella dei controlli sui lavoratori;
3. La terza affronta il tema delle tutele amministrative e giurisdizionali con il consolidamento delle sanzioni amministrative e penali e con le disposizioni relative all'Ufficio del Garante.

L'articolo 1 del nuovo codice recita: "Chiunque ha diritto alla protezione dei dati personali che lo riguardano".

Partendo da questo assunto, il legislatore ha inteso, con questa nuova normativa, garantire a tutti che il trattamento dei dati personali venga svolto "nel rispetto dei cittadini e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale ed al diritto alla protezione dei dati personali" (art. 2).

Sono intesi Dati Personali tutte le informazioni relative a

- Persona fisica
- Persona giuridica
- Ente o associazione

La Legge riguarda quindi tutti i dati (sia quelli gestiti elettronicamente che quelli cartacei) relativi a

a. Sesso, data di nascita, caratteristiche biometriche (quali l'altezza, il colore degli occhi, ma anche la taglia dei vestiti o il numero di scarpe);
b. il nome, il cognome, l'indirizzo, il numero di telefono, il codice fiscale, la partita I.V.A., dati bancari.
c. informazioni circa la composizione del nucleo familiare, la professione esercitata da un determinato soggetto, sia fisico che giuridico, la sua formazione.
d. fotografie, radiografie, video, registrazioni, impronte.
e. informazioni relative al profilo creditizio, alla retribuzione.
f. informazioni relative alla vita sessuale, all'origine razziale od etnica, alle convinzioni religiose, alla partecipazione ad associazioni di categoria, a partiti, sindacati, alla salute di un soggetto, cartelle cliniche;
g. qualunque altra informazione che permetta l'identificazione di una persona (es. un codice).

I dati personali oggetto di trattamento devono essere "custoditi e controllati … in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, …, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta" (art. 31).

Per questi motivi, ai suddetti principi sono tenuti ad adeguarsi tutti coloro che trattano dati personali: aziende (indipendentemente dalle loro dimensioni), liberi professionisti, associazioni, cooperative, amministrazioni ed enti pubblici (comuni, scuole, …), strutture sanitarie e chiunque altro tratti i dati personali di

- Fornitori
- Dipendenti e collaboratori
- Cittadini, Clienti, utenti, pazienti.

Naturalmente gli adempimenti ai quali le diverse organizzazioni devono rispondere sono differenti a seconda delle dimensioni e della tipologia di struttura che effettua il trattamento dei dati, della tipologia dei dati trattati (comuni, sensibili, giudiziari) e della modalità di trattamento, nonché dell'eventuale presenza di una struttura informatica collegata ad Internet.

In linea di massima gli adempimenti riguardano:

- l'inventario dei dati personali;
- l'adozione di misure di sicurezza obbligatorie (fisiche, logiche ed organizzative): allarmi, stabilizzatori di corrente, protezione dei PC dal rischio di intrusione e di virus, armadi chiusi a chiave ed ignifughi, accesso selezionato ai locali;
- la notifica dei trattamenti di dati che si intende effettuare al Garante (art. 37);
- la nomina di figure incaricate della gestione dei dati (responsabile, incaricati, custode delle credenziali, etc);
- l'adozione di procedure scritte che evidenzino i processi gestionali dei dati;
- l'elaborazione del Documento Programmatico sulla Sicurezza (DPS).

Il DPS:

Il Documento Programmatico sulla Sicurezza è l'unico elaborato che attesta l'adeguamento dell'organizzazione alla normativa di riferimento. Esso è un manuale di pianificazione della sicurezza dei dati all'interno dell'azienda. Esso deve avere data certa, quale prova formale dell'adeguamento sostenuto e deve essere aggiornato annualmente (entro il 31 marzo); per il 2004, il temine ultimo è stato prorogato al 30 giugno.

Il DPS deve contenere:

- l'elenco dei trattamenti dei dati personali;
- la suddivisione dei compiti e delle relative responsabilità riguardanti le strutture preposte al trattamento dei dati;
- l'elaborazione di un programma per la formazione e/o aggiornamento degli incaricati del trattamento dei dati;
- l'analisi dei rischi ai quali i dati sono soggetti (rilevazione, identificazione e classificazione);
- le misure minime di sicurezza da adottare al fine di garantire l'integrità e la disponibilità dei dati e la protezione dei locali e delle postazioni ove i dati sono disponibili e/o accessibili;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito ad eventuale distruzione, danneggiamento o perdita.

La violazione delle norme sulla privacy, oltre alla richiesta di risarcimento da parte dei "danneggiati", può portare alla determinazione di sanzioni sia di tipo penale (fino a 36 mesi di reclusione) che amministrativo (fino a 90.000 euro).

Caterina Ledda