

# **Il nuovo Testo Unico in materia di protezione dei dati personali.**

di Mariangela Fagnani\*

Come ormai noto, la Legge n.675 del 31.12.1996 è nata con l'obiettivo di definire gli adempimenti formali e strutturali da adottare nel trattamento dei dati personali al fine di garantire la tutela della privacy dell'individuo. Con un successivo regolamento attuativo, il DPR n.318 del 1999, il Legislatore richiedeva alle aziende di adottare anche specifiche misure minime di sicurezza per la protezione dei dati. Ad essi si sono uniti, nel tempo, numerosi decreti e autorizzazioni atti a gestire la specificità e la complessità della materia e la difficile interpretazione delle norme.

Per semplificare l'operatività delle aziende ed, in generale, dei titolari dei trattamenti, il Legislatore ha in questi ultimi anni operato per definire un Testo Unico finalizzato a riorganizzare la materia relativa alla privacy e a raccoglierla, razionalizzandola, in un unico codice di riferimento.

Il 30 giugno 2003, con il Decreto Legge n.196/03, è stato approvato il "Codice in materia di protezione dei dati personali". Conseguentemente dal 1 gennaio 2004 tutta la precedente normativa, compresa la "675" e il "DPR 318", non hanno più validità.

Il nuovo Testo Unico, tuttavia, non si limita a recepire le normative precedenti ma le modifica richiedendo nuovi adempimenti ed eliminandone altri: si compone di tre parti e di tre allegati:

**Parte 1:** disposizioni generali, riordinate per gestire tutti gli adempimenti e le regole del trattamento con riferimento ai settori pubblico e privato.

**Parte 2:** disciplina del trattamento in specifici settori (es. organismi sanitari e controlli sui lavoratori, e con l'aggiunta di aspetti inediti – es. informazione giuridica, notificazioni di atti giudiziari, comportamenti debitori, ..).

**Parte 3:** tutele amministrative e giurisdizionali, consolidamento delle sanzioni amministrative e penali e disposizioni relative all'Ufficio del Garante.

**Allegato A-** Codici deontologici.

**Allegato B-** Disciplinare tecnico in materia di misure minime di sicurezza.

**Allegato C-** Trattamenti non occasionali effettuati in ambito giudiziario o per fini di Polizia.

Prima di passare in rassegna le modifiche intervenute nel Nuovo Codice riprendiamo brevemente quelle che sono le sue caratteristiche e gli adempimenti principali richiesti alle aziende, alle pubbliche amministrazioni, agli enti locali e alle associazioni.

Ricordiamo che la legislazione italiana ha come obiettivo quello di regolamentare le modalità di gestione e custodia dei dati che riguardano sia le caratteristiche della persona (dati personali) che le abitudini, scelte ed opinioni (dati sensibili) per proteggere la sfera privata e la dignità delle persone fisiche e di quelle giuridiche: per il raggiungimento di tale obiettivo richiede una serie di adempimenti formali (assegnazione delle responsabilità, informativa, consenso, autorizzazione al trattamento, notificazione) e strutturali (inventario banche dati, analisi del rischio, misure di sicurezza idonee, procedure di risposta agli interessati).

Nella figura sottostante e' riportato uno schema di sintesi della normativa :

Il mancato adempimento ai requisiti e alle scadenze di legge comporta sanzioni sia di tipo amministrativo che di tipo penale.

Le recenti proroghe concesse dal Garante lasciano tempo fino al 31 dicembre 2004 per adeguarsi alle misure minime di sicurezza, ed ulteriori tre mesi (fino al 31 Marzo 2005) per eventuali adeguamenti tecnologici necessari per realizzare le misure minime di sicurezza.

### **Come e' cambiata la legge ?**

L'obiettivo che il legislatore si e' posto con l'introduzione del Nuovo Testo Unico e' quello di riunire, razionalizzare e semplificare la normativa esistente introducendo nuove garanzie per gli interessati. Il Codice intende garantire agli interessati il più ampio diritto alla protezione dei loro dati personali, associando alla tutela della riservatezza, già prevista, la tutela dell'integrità e della disponibilità.

Particolare attenzione viene infatti posta dalla norma al trattamento dei dati sensibili, cioè ai dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Il trattamento e' da intendersi come qualunque operazione, effettuata anche senza l'ausilio di strumenti elettronici, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Relativamente alla 675/'96, numerosi sono gli adempimenti modificati dal nuovo codice che apporta, in sintesi, variazioni per le seguenti attività:

- informativa e consenso;
- incarico ai dipendenti;
- notificazione del trattamento al Garante;
- misure di sicurezza;
- trattamento all'esterno della struttura titolare;
- formazione degli incaricati;
- continuità del servizio;
- trattamento di dati sanitari e genetici.

### **1) Informativa (art. 13) e Consenso (art. 23)**

L'informativa è la comunicazione con cui il Titolare dichiara all'interessato le caratteristiche del trattamento cui saranno sottoposti i suoi dati personali: per essa rimane fermo l'adempimento agli interessati preventivamente al trattamento dei dati. All'interno dell'informativa devono essere riportati:

- gli estremi del titolare e, se designati, del rappresentante nel territorio dello Stato e del responsabile (almeno uno);

il sito della rete di comunicazione o le modalità per conoscere l'elenco aggiornato dei responsabili;

le tipologie di incaricati del trattamento autorizzati;

le categorie di dati trattati (se dati raccolti c/o terzi).

Il Garante si è impegnato ad individuare modalità semplificate per la gestione dell' informativa per ambiti specifici (es. call center).

Il consenso è la dichiarazione tramite cui l'interessato dichiara al Titolare il proprio bene- stare relativamente al trattamento di cui è stato informato e deve essere:

espreso - per tutti i trattamenti eseguiti da soggetti privati;

modulabile - può riguardare l'intero trattamento ovvero una o più operazioni dello stesso;

espreso liberamente;

documentato per iscritto (solo per i dati sensibili deve essere scritto);

successivo all'informativa;

vincolato ad un trattamento "chiaramente individuato".

Non viene più richiesto il consenso per i dati relativi all'adesione ai sindacati e per i dati sensibili per la gestione del rapporto di lavoro.

## **2) Incarico ai dipendenti (art. 30)**

Le operazioni di trattamento possono essere effettuate solo da dipendenti (o esterni) inca- ricati del trattamento che operano sotto la diretta autorità del titolare o del responsabile, atte- nendosi alle istruzioni impartite.

Il Nuovo Codice richiede che la designazione sia effettuata per iscritto e individui pun- tualmente l'ambito del trattamento consentito: operativamente questo si può gestire anche do- cumentando l'assegnazione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima e definendo un "mansionario" aziendale cui si individuano, per gli uffici o le unità organizzative, gli ambiti del trattamento consentiti.

## **3) Notificazione del trattamento al Garante (art. 37)**

La notificazione è l'atto con cui l'impresa, il professionista o la pubblica amministrazione segnala all'Autorità Garante i trattamenti di dati che si intendono effettuare.

A differenza della vecchia legislazione in cui era richiesto a tutti i soggetti, se non esplici- tamente esentati, di effettuare la notifica, ora devono notificare solo i soggetti esplicitamente individuati ed inoltre non esiste più l'obbligo di effettuare una specifica notifica dei dati desti- nati all'estero.

La notificazione è richiesta nei seguenti casi, che devono essere comunque valutati alla luce dei vari Comunicati rilasciati dall'Ufficio Garante nei mesi passati al fine di chiarire e specificare con maggior precisione quali fossero gli ambiti per i quali è richiesta la Notifica- zione:

dati genetici, biometrici o dati sull'ubicazione di persone od oggetti;

dati idonei a rivelare lo stato di salute e la vita sessuale o la sfera psichica;

dati trattati con l'ausilio di strumenti elettronici per definire il profilo o la personalità

dell'interessato, o ad analizzare abitudini o scelte di consumo ovvero a monitorare l' utilizzo di servizi di comunicazione elettronica;

dati sensibili registrati in banche di dati a fini di selezione del personale conto terzi per sondaggi di opinione e simili;

dati relativi al rischio sulla solvibilità economica e simili (centrali rischi").

Sono state inoltre snellite le modalità di notificazione che deve essere fatta solo per via telematica, seguendo le indicazioni del Garante quanto all'utilizzo della firma digitale.

#### **4) Misure di sicurezza (art. 31 – 36)**

Il legislatore pone la sicurezza come condizione fondamentale al trattamento dei dati personali.

Per misure di sicurezza si intende l'insieme delle misure tecniche, informatiche, organizzative, logistiche e procedurali che configurano il livello di protezione necessario a ridurre al minimo 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.

Le misure di sicurezza richieste dalla Norma sono orientate al raggiungimento di precisi obiettivi finalizzati alla protezione dei dati personali e dei trattamenti ad essi correlati, quali:

- disponibilità;
- integrità;
- riservatezza;
- continuità;
- verificabilità;

e devono essere preventive, obbligatorie, correlate al mezzo utilizzato per il trattamento, e crescenti in funzione della criticità dei dati stessi.

La Norma distingue inoltre fra misure di sicurezza:

- idonee (è l'obiettivo di sicurezza della legge), ovvero tutte le misure di sicurezza necessarie a minimizzare i rischi in funzione delle caratteristiche organizzative e tecniche dell'azienda nonché dell'evoluzione tecnologica;
- minime (è il livello minimo delle misure idonee), che devono essere adottate indipendentemente dalle caratteristiche dell'azienda. Esse rappresentano il livello "minimale" e non sono sufficienti a rappresentare l'obiettivo voluto dalla legge, che rimane quello delle "Misure Idonee" ; si tratta di un elenco pre-definito e identificate nel "Disciplinare Tecnico" (allegato B).

Ogni azienda o ente pubblico dovrà quindi, per realizzare le misure minime di sicurezza dei dati personali, verificarne lo stato attuale, il conseguente livello di rischio e individuare le adeguate contromisure dal punto di vista organizzativo e tecnologico: per quanto riguarda l'aspetto tecnologico deve essere presa in considerazione la sicurezza della rete, la sicurezza logica dei sistemi/applicazioni, PC e workstation, la continuità e la disponibilità dei dati, nonché la sicurezza fisica delle aree e dei locali in cui i dati sono trattati e custoditi.

Nel Nuovo Codice sono state ridefinite, in parte, le misure minime di sicurezza che tutte le aziende, ed i loro dipendenti, sono tenute ad adottare sia per il trattamento informatico sia per quello cartaceo. Tali misure, individuate nell'allegato B denominato "Disciplinare Tecnico in Materia di Misure Minime di Sicurezza", modificano e integrano quanto previsto dal precedente DPR n. 318/99. Le principali variazioni sono da attribuire alla semplificazione dei ruoli (es.: non è più necessario identificare l'Amministratore di Sistema) introdotta nell'Allegato B, nonché degli strumenti (elettronici o non elettronici) ed una particolare attenzione alla protezione dei dati sulla salute.

Le principali novità introdotte nel Disciplinare Tecnico possono essere così sintetizzate: doppio controllo per l'accesso ai dati, basato su autenticazione e autorizzazione. L'autenticazione informatica prevede che il trattamento dei dati sia consentito solo mediante l'utilizzo di una credenziale di autenticazione (utenza più password riservata; dispositivo di autenticazione – es. smartcard,.. - eventualmente associato a utenza o password; caratteristica biometrica eventualmente associata a utenza o password) e che tutti gli incaricati siano dotati di credenziale di autenticazione. L'utenza deve essere individuale e non riutilizzabile, e disattivata in caso di mancato utilizzo (6 mesi, eccetto che per le utenze tecniche) o di perdita della qualità.

Ogni utente può comunque disporre di più credenziali di autenticazione.

La password deve rispondere a precisi requisiti, quali la lunghezza minima di 8 caratteri, o il massimo consentito dal sistema, deve essere modificata al primo utilizzo e comunque ogni 6 mesi (ogni 3 mesi se utilizzata per accedere a dati sensibili o giudiziari) e non deve contenere riferimenti riconducibili all'incaricato.

Per quanto riguarda la gestione, il Titolare ha la responsabilità di fornire istruzioni agli incaricati in merito alla gestione e conservazione delle credenziali di autenticazione, alla custodia degli eventuali dispositivi di autenticazione, alla gestione e custodia dello strumento elettronico durante le sessioni di trattamento ed infine alla modalità di accesso ai dati, in caso di assenza prolungata o impedimento dell'incaricato, per esigenze organizzative e di sicurezza aziendale.

Il sistema di autorizzazione è 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. Il profilo di autorizzazione, invece, ha le seguenti caratteristiche:

- ✓ E' l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa con sentiti.
- ✓ E' assegnato al singolo incaricato o per classi omogenee.
- ✓ I criteri del profilo sono individuati preventivamente.
- ✓ Esistono criteri di revoca del profilo stesso.
- ✓ Sono svolte verifiche periodiche sui profili assegnati.
- ✓ Il Documento Programmatico Sulla Sicurezza (DPS) è il documento "principe" con cui il Titolare dichiara come intende gestire e tutelare la sicurezza dei dati trattati e conseguentemente quali sono le misure di sicurezza, organizzative, normative o tecniche, adottate o da adottarsi. In pratica, sintetizza la Policy di sicurezza adottata e costituisce prerequisito per le misure "idonee".

In precedenza era richiesto solo per i dati sensibili elaborati tramite strumento elettronico accessibile al pubblico. Nel Nuovo Codice invece, riguarda tutti i trattamenti di dati personali trattati elettronicamente (per il trattamento di dati sensibili comporta sanzioni penali e sono definiti i contenuti minimi).

Va aggiornato annualmente entro il 31 marzo e deve essere allegato (o comunque citato nella sua redazione o aggiornamento) nella relazione accompagnatoria del bilancio d'esercizio, se dovuta.

Il DPS deve includere:

- ✓ elenco dei trattamenti
- ✓ distribuzione compiti e responsabilità
- ✓ analisi dei rischi che incombono sui dati
- ✓ misure adottate per garantire:
  - ✓ l'integrità e la disponibilità dei dati;
  - ✓ la protezione delle aree e dei locali, rilevanti ai fini della custodia e accessibilità dei dati;
- ✓ criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento
- ✓ education degli incaricati
- ✓ misure minime di sicurezza per i trattamenti affidati all'esterno della struttura
- ✓ criteri per cifrare o separare i dati, idonei a rivelare lo stato di salute o l'attività sessuale, dagli altri dati personali

Ulteriori misure di sicurezza:

Ambito di trattamento - aggiornamento periodico e verifiche (almeno annuali)

dell'ambito di trattamento consentito agli incaricati e redazione della lista degli incaricati

- ✓ Antivirus - installazione e aggiornamento (almeno ogni 6 mesi)
- ✓ Patch di sicurezza - aggiornamenti periodici dei software volti a prevenire la vulnerabilità di strumenti elettronici e a correggere difetti (almeno annualmente; ogni 6 mesi in caso di trattamento di dati sensibili)
- ✓ Backup - Istruzioni tecniche e organizzative per il salvataggio dei dati (almeno ogni settimana)
- ✓ Misure specifiche per i dati sensibili:
  - ✓ supporti rimovibili (anche cartacei) - istruzioni organizzative e tecniche per la loro custodia, il loro uso, la loro distruzione e per la cancellazione delle informazioni con tenute;
  - ✓ ripristino dei dati - adozione di idonee misure per il ripristino in caso di danneggiamento dei dati e/o degli strumenti (entro 7 giorni);
  - ✓ firewall – attivazione di idonei strumenti elettronici contro l'accesso abusivo;
  - ✓ accesso agli archivi – accesso autorizzato, controllato e registrato dopo l'orario di ufficio.

Il Titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del Disciplinare Tecnico.

Misure per dati trattati da organismi o esercenti sanitari (dati idonei a rivelare lo stato di salute o la vita sessuale): sono previste misure di sicurezza aggiuntive, quali il trattamento disgiunto dei dati personali dagli altri dati presenti nelle banche dati [all.B 24] e l'adozione di tecniche di cifratura o di codici identificativi (o altro) che li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità (es. tramite una tabella di conversione separata tra nominativi e codici identificativi) [art.34.h; art.22.6; all.B 24].

Misure per i dati genetici: tali dati devono essere trattati all'interno di locali protetti, accessibili solo agli incaricati specificatamente autorizzati [all.B 24], il trasporto all'esterno dei locali deve avvenire solo in contenitori muniti di serratura o equivalente [all.B 24] ed il trasferimento in formato elettronico solo previa cifratura [all.B 24].

### **Cosa devono fare le aziende?**

Anche le aziende già in regola con la Legge n.675/'96 devono intraprendere specifiche attività per allinearsi al Nuovo Testo Unico, in particolare:

Mappatura dei nuovi trattamenti e/o banche dati

Aggiornamento dell'inventario

Mappatura di eventuali nuove tecnologie utilizzate nel trattamento

Aggiornamento dell'organizzazione aziendale

Redistribuzione delle responsabilità organizzative e di sicurezza

Confronto tra modalità di trattamento vs. requisiti imposti dal Nuovo Testo Unico

Individuazione dei gap da colmare

Aggiornamento dell'Analisi dei Rischi

Aggiornamento dei requisiti formali (es. notifica, aggiornamento riferimenti legislativi, informative, consensi, etc..).

Predisposizione del piano degli interventi (es adeguamento lunghezza password, crittografia dati, predisposizione del sistema di autorizzazione, etc..).

Predisposizione delle attività necessarie per la gestione adempimenti posticipati o non implementabili entro i termini di legge.

Aggiornamento del DPS e suo inserimento/richiamo nella relazione di bilancio

Revisione del package di formazione

Formazione e sensibilizzazione dei Responsabili e degli Incaricati del Trattamento (dati sensibili)

### **Solo oneri o anche vantaggi ?**

L'adeguamento alla norma di tutela dei dati personali rappresenta certamente per le aziende, amministrazioni pubbliche ed enti locali un costo ed uno sforzo organizzativo non trascurabili, ma comporta anche qualche vantaggio costituito dalla maggiore trasparenza e consapevolezza dei flussi operativi e dei dati trattati. Inoltre, nell'applicazione delle misure di sicurezza, si può estendere l'ambito non solo alla protezione dei dati personali, ma anche a quelli critici e vitali per il business e la mission aziendale, raggiungendo in questo modo anche l'obiettivo di rafforzare il livello generale di sicurezza del sistema informativo dell'azienda.

\* *Mariangela Fagnani*.- Laureata in Matematica presso l'Università degli Studi di Milano, dal 1981 lavora in IBM dove ha ricoperto diversi ruoli, nell'area dello sviluppo applicativo e delle Operations.

Si è occupata di Sicurezza Informatica, (Strategic Outsourcing e Business Consulting Services), punto di riferimento per le Funzioni interne e per i clienti.

Dal 2001 ha assunto la responsabilità di Security & Privacy Practice Leader ed ha maturato significative esperienze, nella definizione degli aspetti organizzativi e normativi, in particolare nell'applicazione della legge e regolamenti successivi inerenti la Data Privacy. E' Socia Onoraria ItaSForum.