

I diritti del cittadino : una opportunità per crescere e per migliorare in azienda

# TESTO UNICO SULLA PRIVACY

Sarebbe un grave errore considerare questa nuova Legge un ennesimo intoppo burocratico posto sulla testa delle nostre imprese. E' un'innovazione indispensabile

Di Oscar Lambrughi\*

Il Dlgs 196 promulgato nel giugno 2003 ed entrato in vigore il primo gennaio scorso, riunisce in unico contesto la precedente legge 675/96 e gli altri decreti legislativi, regolamenti e codici deontologici che si sono succeduti in questi anni, e contiene anche importanti innovazioni tenendo conto della "giurisprudenza" del Garante e della direttiva Ue 2000/58 sulla riservatezza nelle comunicazioni elettroniche.

Con questa nuova norma il legislatore si è preoccupato di garantire un principio fondamentale per tutti i cittadini, quindi per tutti noi: il diritto alla riservatezza delle informazioni che ci riguardano. Un diritto fondamentale, specialmente oggi che con il proliferare dei sistemi informatici è sempre più semplice gestire ed utilizzare grandi archivi di dati, un diritto da far ben valere quando siamo noi dall'altra parte della barricata. Questo principio viene esplicitato nel primo dei 186 articoli di legge " *Art. 1: Chiunque ha diritto alla protezione dei dati personali che lo riguardano*".

La legge va poi ad identificare cosa si intenda per dati personali, e cioè qualsiasi informazione che riguardi persone, società, enti, associazioni. Tutte le aziende, per loro stessa funzione vitale, trattano dati. La pura gestione delle informazioni anagrafiche di clienti e fornitori è un trattamento di dati, per non parlare di tutto quanto riguarda la gestione dei dipendenti.

Per capire meglio cosa intende la legge come trattamento dei dati citiamo testuale l'articolo 4:

*"qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti 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"*

Ci rendiamo ben conto che il legislatore non lascia spazi di interpretazione, tutte, ma proprio tutte le operazioni che si possono compiere nel gestire dati personali ricadono all'interno di questa legge. E cosa prevede la norma? Prevede essenzialmente l'obbligo da parte del Titolare del trattamento dei dati (riconducibile nella maggioranza dei casi all'Amministratore Delegato) di applicare e verificare che siano rispettate tutte le misure idonee a far sì che i dati siano trattati in "sicurezza".

Cosa si intenda con "sicurezza" viene ben riassunto nell'articolo 31 che è un pò "il cuore della Legge" :

## **Art. 31**

***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.***

## **Decreto Legislativo 196/03 "Codice in materia di protezione dei dati personali"**

### **Che cosa è ?**

E' la normativa, in vigore dal primo gennaio 2004, in materia di tutela dei dati personali meglio nota come TESTO UNICO SULLA PRIVACY. Amplia il percorso legislativo compiuto dall'Italia in materia di dati personali a partire dalla legge 675/96.

### **Chi è interessato**

Tutti i soggetti ( aziende, enti, associazioni, ecc..) privati e pubblici, che trattano dati personali sensibili e non (fornitori, clienti, associati, dipendenti, ecc).

### **Cosa sono i dati personali**

Sono qualsiasi informazione relativa a persona fisica, persona giuridica, ente od associazione, identificabili, anche indirettamente attraverso codici.

### **Cosa prevede**

Prevede che ciascun soggetto tratti i dati personali con specifici canoni di riservatezza e liceità. Prevede altresì che debbano essere adottate misure tecniche ed obblighi garantiti di sicurezza minimi. Inoltre entro il 31 marzo di ciascun anno (di cui il primo è il 2004) deve essere redatto il DPSS (Documento Programmatico sulla Sicurezza) e successivamente allegato alla relazione accompagnatoria del bilancio di esercizio d'azienda.

### **Le sanzioni**

Chiunque, essendovi tenuto, omette

Certo il periodo è un poco lungo e complicato, ma viene ben esplicitato che i dati devono essere "custoditi" quindi va regolamentata la loro presa visione (password, permessi ecc) e negata la possibilità di accesso a chi volesse introdursi nel sistema o non fosse autorizzato... Vanno inoltre "controllati" cioè va verificato se nel tempo le misure messe in atto siano ancora efficaci, anche in considerazione dell'evoluzione della tecnologia (un sistema antivirus per computer se non aggiornato è inefficace solo dopo pochi giorni dalla sua installazione !!). Inoltre grande attenzione deve essere riservata a quei dati, che essendo per loro natura di tipo particolare (dati Sensibili) necessitano di procedure, sistemi e misure di sicurezza diversi. Sempre l'articolo 31 indica l'adozione di misure "idonee" (sia tecniche che comportamentali) e "preventive" (quindi da attuare subito), per evitare al minimo i rischi di "distruzione" (volontaria) o di "perdita" (computer privi di sistemi per effettuare copie aggiornate dei dati). Misure da attuare anche allo scopo di evitare l'accesso non autorizzato ai dati, sia esterno (attraverso internet) oppure dall'interno, da personale non autorizzato. Inoltre lo stesso articolo indica che i dati possono essere trattati solo e solo se si è stati autorizzati a farlo. In pratica si possono avere archivi, anagrafiche ecc, solo se si è stati esplicitamente autorizzati a farlo, clienti e fornitori compresi. Così come si possono "utilizzare" questi dati solo per gli scopi leciti per i quali si è ottenuta l'autorizzazione.

Di questi principi generali la norma traccia indicazioni dettagliate e specifiche che per ampiezza e opportunità non è possibile qui riportare.

Il Dlgs. 196/03 è pienamente vigente al pari di ogni altra legge dello Stato Italiano e gli adeguamenti previsti sono obbligatori e dipendenti da molti parametri (dimensioni della struttura, della tipologia di trattamento dati, della modalità di trattamento, dei sistemi utilizzati ecc). Per inosservanza anche parziale delle norme si rischiano sanzioni molte dure: multe e reclusione, risarcimento del danno patrimoniale e morale ex art. 2050. Gli accertamenti a differenza della scorsa normativa vengono effettuati dalla Guardia di Finanza. Inoltre deve essere indicata nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, l'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza DPSS.

**Ma come può essere un'opportunità di crescita e di miglioramento per le aziende una legge che obbliga ad attuare procedure, installare sistemi, compilare documenti e svolgere dei corsi di formazione ?**

Per diversi motivi.

Gli archivi e la gestione dei dati oggi a differenza solo di pochi anni fa è completamente affidata ai computer, spesso se non sempre collegati in rete locale tra loro e connessi ad internet.

Ma i sistemi informatici se non ben utilizzati e regolamentati possono creare dei guai tali da essere peggiori dei vantaggi che procurano.

Immaginate di tornare a 30 anni fa. Tutto o quasi era su carta. Immaginatevi di prendere il contenuto dei vostri armadi, delle vostre scrivanie e di portare per assurdo tutto in strada e di lasciarli lì abbandonati, o peggio di bruciarli, tutti !

Ecco questo è esattamente quello che oggi potrebbe succedere se non si adottano procedure e non si prendono misure adatte a garantire la sicurezza dei computer che ci sono in azienda. Un cassetto chiuso a chiave si vede, si tocca, si ha esattamente la sensazione che sia ben chiuso, un computer invece no. La realtà attuale di molte aziende in Italia è quella di non comprendere i rischi a cui sono esposte.

Rischi di subire danni assai maggiori di quanto costerebbe oggi

di adottare le misure minime di sicurezza è punito con l'arresto fino a due anni o con l'ammenda da 10.000,00 a 50.000,00 euro.

**Le scadenze principali**

*31 marzo 2004*

Analisi dei rischi e stesura del DPSS (Documento Programmatico Sulla Sicurezza).

*30 giugno 2004*

Adozione misure minime di sicurezza.

**Come ci si mette in regola ?**

- **Nominando** le figure richieste dalla legge relative al trattamento dei dati personali:
  - Titolare
  - Responsabile (non obbligatoria)
  - Incaricati
- **Proteggendo** gli elaboratori contro il rischio di intrusione e di virus.
- **Adottando** le misure fisiche di protezione (allarmi, stabilizzatori di corrente, accesso selezionato ai locali...).
- **Stabilendo** (per iscritto) le procedure comportamentali da seguire.
- **Stilando** il DPSS (documento programmatico sulla sicurezza), che descrive quanto fatto ed individua quanto ancora resta da fare. Solo il DPSS fa prova dell'avvenuto adeguamento alla normativa.
- **Partecipando** ai corsi di formazione specifici (la fase di formazione è obbligatoria per i Titolari, i Responsabili e gli Incaricati del trattamento dei dati).

**Il trattamento dei dati :  
"ATTIVITA'PERICOLOSA"**

Il Dlgs. 196/03 oltre alle sanzioni penali previste a causa del mancato adeguamento rilevato durante le ispezioni della **Guardia di Finanza**, prevede all'articolo n° 15 che i danni cagionati per manchevolezze nel trattamento dei dati, siano risarciti secondo l' Art. 2050 del Codice Civile. (Attività pericolosa).

*Da notare che in questo specifico caso a differenza della normalità non è il*

mettersi in regola. Per le aziende ad oggi prive di misure minime di sicurezza (più numerose di quanto si immagini). L'esempio più banale è quello dell'azzeramento di tutti i dati, di tutti i computer per un virus informatico. Immaginatevi di arrivare un mattino in azienda e di avere i vostri computer "vuoti" e magari le copie di backup (se ci sono) sono di 3 mesi prima, perchè come sempre non si aveva avuto tempo ..... Prospettiva drammatica vero ?

Per le aziende che già oggi adottano le misure di sicurezza idonee, questa potrebbe invece essere un'ottima occasione per un momento di verifica dell'attualità delle stesse e di pianificazione delle procedure e degli interventi atti a garantire non solo una sempre più efficace protezione dei dati per loro vitali, ma al loro utilizzo strategico. Tutto ciò non significa necessariamente complicare le procedure, al contrario prevedere di semplificarle, ad esempio con l'adozione di un'infrastruttura di SSO (Single Sign On) questo per favorire di focalizzarsi sul proprio business.

**Articolo pubblicato su  
"Corriere delle Opere" Maggio 2004**

*querelante interessato a dover provare il danno ma è il Titolare del trattamento dei dati che l'ha provocato a dover dare prova documentata (DPSS) di aver adottato tutte le misure idonee di sicurezza. Per evitare la responsabilità civile non è sufficiente l'adeguamento alle misure minime .*

*\* Amm. Del. Educom Srl*