

PRIVACY: DANNI COLLATERALI

Il “Codice della privacy” e alcuni aspetti inerenti il mondo B2B

* di Giancarlo Butti

E' da poco entrato in vigore nella sua completezza il Dlgs 196/03, meglio noto come “Codice privacy”.

In realtà la normativa sulla privacy è in vigore in Italia, nella sua prima stesura fin dal lontano maggio 97. Sono quindi ben 9 anni che, in ottemperanza alla Direttiva n. 95/46/CE, l'Italia si è dotata di una norma per la tutela dei dati personali (in prima versione 675/96).

La normativa italiana ha alcune caratteristiche particolari, come quella di aver esteso la tutela dei dati oltre che alle persone fisiche (come prescritto dalla suddetta direttiva), anche alle persone giuridiche, enti, associazioni....

La Direttiva n. 95/46/CE recita infatti:

a) “*dati personali*”: *qualsiasi informazione concernente una persona fisica identificata o identificabile (“persona interessata”); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale;*

nella 196/03 la definizione di dato personale è invece la seguente:

b) “*dato personale*”, *qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indiretta-*

mente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

Questa apparente banale estensione è in realtà uno degli elementi che da sempre rende difficile, se non impossibile, il reale rispetto di una normativa che viene vista, dalla maggior parte dei soggetti tenuti al rispetto della stessa (aziende, professionisti, pubblica amministrazione...), come un'insieme ingiustificato di obblighi e costrizioni, senza nessun ritorno o vantaggio.

Per chi da numerosi anni si occupa quotidianamente di privacy appare evidente come nella realtà italiana, costituita per lo più da piccole o micro aziende, sia estremamente complessa l'applicazione della norma ed il rispetto della stessa, proprio a causa di questa infelice estensione.

Consideriamo il caso di una qualunque normale azienda.

Questa ha una serie di rapporti con enti, pubbliche amministrazioni, aziende clienti, aziende fornitori, qualche consulente e con i propri dipendenti.

Quanti soggetti di questo elenco sono persone fisiche?

Quanti sono invece soggetti di altro tipo?

Se la normativa privacy tutelasse solo i dati personali delle persone fisiche, gli archivi da proteggere, le informative da rilasciare, i consensi da raccogliere, i diritti di accesso

da gestire, si limiterebbero ad un numero estremamente esiguo, e quindi facilmente gestibili.

Le aziende, anche le più piccole non avrebbero alcuna difficoltà a rispettare la norma.

Questa estensione della tutela anche alle persone giuridiche, enti ed associazioni, fa sì invece che il numero dei soggetti da tutelare sia enorme e difficilmente identificabile.

L'applicazione letterale della norma comporta che prima del trattamento dei dati di qualunque soggetto sia necessario informarlo sulla motivazione della raccolta e del successivo trattamento dei suoi dati, oltre che di un'altra serie di elementi per altro assolutamente ragionevoli.

L'aspetto inquietante è che l'identificazione di questi soggetti è in genere difficoltosa e le aziende si limitano, nel migliore dei casi, a considerare dipendenti e clienti.

Ci si dimentica così che i soggetti di cui si trattano i dati sono invece molto più numerosi; ad esempio i fornitori, i potenziali clienti, i potenziali fornitori, i potenziali dipendenti, i soggetti con i quali si hanno rapporti indiretti (ad esempio i vettori delle controparti che non sono anche fornitori dell'azienda), tutte le persone fisiche, dipendenti o collaboratori delle aziende con le quali si interagisce, le società di software dei quali si usano le applicazioni e delle quali si gestiscono i dati in quanto si

ha con loro un vero e proprio contratto chiamato licenza d'uso (chi ha mai rilasciato un'informativa a Microsoft?, a RedHat? a IBM?). L'elenco potrebbe continuare a lungo.

La maggior parte di questi soggetti non sono persone fisiche e la "semplice" necessità di dover rilasciare un'informativa con eventuale richiesta di consenso è in molti casi difficile se non impossibile. Oltretutto tale attività è nella realtà perfettamente inutile per un semplice motivo: la reciprocità dei diritti e dei doveri che esistono, a livello di applicazione della norma, fra due aziende.

Entrambe le aziende (ad esempio un cliente ed un fornitore) sono sia soggetti obbligati a rispettare la norma, sia soggetti tutelati.

Non capiterà quindi mai che un'azienda che abbia un normale rapporto commerciale con un'altra azienda cerchi di far valere i propri diritti ai sensi della normativa privacy; immediatamente la controparte potrebbe fare la stessa cosa. Ben diverso il caso delle persone fisiche, le quali non hanno un obbligo esteso di rispetto della normativa, per cui questa reciprocità di diritti e di doveri non esiste ed il soggetto privato può a ben diritto chiedere di far valere i propri diritti senza che la controparte possa fare altrettanto.

In realtà la normativa, che comporta l'attivazione di una serie notevole di attività di natura formale, tecnica ed organizzativa non deve essere vista come un inutile balzello.

Gli aspetti positivi sono notevoli e superano, se gestiti con intelligenza, le inutili formalità.

L'aspetto più importante è che questa norma costringe qualunque azienda a organizzarsi, a documentare il proprio modo di gestire i processi aziendali, a formalizzare ruoli e responsabilità ed a tutela il patrimonio informativo



aziendale.

La norma è nata per tutelare i dati personali dei soggetti che interagiscono con l'azienda, ma quali altri dati l'azienda gestisce se non "dati personali"?

Guardate la definizione di dato personale per convincervi di questa affermazione.

Un dato personale è "qualunque informazione"; un progetto, un ordine, una fattura, un preventivo, una relazione...; sono tutti insieme di dati personali, e quindi da tutelare per legge.

Obbligando a tutelare i dati di terzi, questa legge obbliga le aziende a tutelare il proprio patrimonio informativo e quindi, ancor prima, a conoscerlo e ad analizzare i rischi che sta correndo.

Praticamente il 100% delle aziende con cui ho interagito mai si era posta il problema di quale danno avrebbe subito nel caso in cui il sistema informativo fosse andato distrutto; mai tale aziende si erano poste il problema di conservare copia dei loro dati in un altro luogo diverso da quello in cui è presente la copia principale, mai si erano poste il problema di quali conseguenze civili e penali avrebbero subito, indipendentemente dall'esistenza della normativa privacy, nel caso in cui ad esempio

andassero distrutte schede cliniche (dentisti...), o giustificati di detrazioni fiscali (commercialisti...), tanto per citare i casi più eclatanti. Ben venga quindi una normativa che ha portato le aziende a ragionare in termini di sicurezza e a tutelare prima di tutto se stesse.

Se, analogamente a quanto accaduto per il casco e la cintura di sicurezza è necessaria una normativa per costringere le aziende a dotarsi di firewall e antivirus ed a fare il backup dei dati, ben venga in ultima analisi, che il legislatore abbia esteso alle persona giuridica, ente od associazione, l'obbligo di tutela, costringendo quindi le aziende a tutelare l'intero patrimonio informativo aziendale e non solo le schede dei dipendenti.

Almeno da questo punto di vista non possiamo che essere concordi con il legislatore, considerando come un "danno collaterale gli inutili adempimenti formali" che questa estensione ha comportato. ■

*



Giancarlo Butti,
Consulente di informatica