

# QUANDO IL RISPETTO DELLA PRIVACY DIVENTA UN BUSINESS

**T**utte le novità del codice sul trattamento dei dati personali. Le interpretazioni controverse e le zone d'ombra delle disposizioni. Di particolare importanza il capitolo dedicato al Documento Programmatico sulla Sicurezza e l'individuazione dei

soggetti abilitati alla sua redazione. Si tratta di un obbligo che si rinnova anno dopo anno...

Come oramai tutti sanno, dal primo gennaio 2004 è entrato in vigore il nuovo Codice sulla Privacy (D.Lgs. n. 196/2003, pubblicato sulla Gazzetta Ufficiale del 29 luglio 2003) ma forse non tutti hanno seguito, passo dopo passo, le reazioni a tale "innovazione", che è nota molto di più a chi fa di tutto perché se ne venga a conoscenza e si provveda ad adeguarsi, piuttosto che ai diretti interessati.

Afferma correttamente l'avvocato Andrea Lisi: "...dagli istituti bancari alle strutture alberghiere, dalle case di cura ai produttori



di automobili, dagli operatori dell'e-commerce ai gestori della telefonia nessuno può ritenersi più esentato dall'osservare la normativa, nazionale ed europea, dettata a tutela dei dati personali. Ma una cosa è la formale constatazione di quel che si deve fare (magari con uno sba-

diglio o un gesto inconsueto di stizza!), altra cosa è recepire sostanzialmente la normativa, assorbendone culturalmente il cambiamento, sentendo come utili e manifestando nella propria quotidianità i numerosi adempimenti che la normativa ci richiede..."

Il Codice in materia di trattamento dei dati personali rappresenta indubbiamente una miglioria rispetto alla precedente normativa (legge 675/1996 e successive modifiche ed integrazioni) ma, al contempo, ha dato adito ad una serie di interpretazioni controverse e, di fatto, permangono non poche zone d'ombra. Una delle questioni che maggiormente ha "infuocato" i dibattiti è stata quella relativa al "famoso" DPS, ovve-

**Dalle banche agli alberghi, tutti dovranno adeguarsi alle indicazioni contenute nel nuovo codice che regola il trattamento dei dati personali. Però il testo, pur presentando dei miglioramenti rispetto alla situazione precedente, contiene non poche zone d'ombra. E, soprattutto, può costituire un'occasione di business per particolari categorie professionali. Vediamo perché**

ro il Documento Programmatico sulla Sicurezza, ed in particolare modo sull'individuazione esatta della cerchia dei soggetti tenuti alla redazione di tale documento. Su questo punto è molto chiaro Lisi: *"Il DPS, in realtà, altro non è che un resoconto delle misure di sicurezza adottate da chiunque sia titolare (imprese, singoli ed istituzioni) di un trattamento di dati personali altrui per evitare (o meglio per ridurre al minimo il verificarsi di) qualsiasi tipo di evento dannoso o pericoloso a carico degli stessi dati personali. In definitiva, il DPS serve a fotografare la politica aziendale in tema di sicurezza dei dati personali e, una volta redatto, esso deve essere custodito in un luogo*

*preciso (e ovviamente sicuro!) – solitamente all'interno dell'azienda stessa – per gli eventuali possibili controlli. "*

V'è stato un grande dibattere, nei mesi scorsi, su coloro che dovevano provvedere alla redazione del DPS, con il conseguente formarsi di due opposte fazioni: chi riteneva che dovesse essere redatto da tutti coloro che trattano dati personali, anche solo comuni, e chi, al contrario, riteneva dovesse essere redatto solo da coloro che trattano dati sensibili e giudiziari. Il parere del Garante del 22 marzo u.s. ha sciolto ogni dubbio: il DPS va redatto solo da parte di coloro che trattano dati sensibili e giudiziari. Il Documento Programmatico per le misure di

sicurezza diventa, dunque, obbligatorio per tutti i titolari che trattino dati sensibili e giudiziari tramite elaboratori, a differenza di prima quando era necessario solo per i trattamenti svolti mediante una rete disponibile al pubblico (art. 34 e allegato B).

### Ma chi può dire di non trattare alcun dato sensibile?

Si legge, correttamente, in un approfondimento della tematica a cura dell'avvocato Cassazionista L.M. De Grazia: *"La lettera (g) dell'art.34 appare – a parere di chi scrive - molto chiara: una delle misure minime di sicurezza è la redazione del D.P.S., così come le "ulteriori" misure minime di sicurezza previste dai pun-*



**G** ESTIONE



**E** LETTRONICA



**D** OCUMENTALE

La Gallo Pomi vi offre soluzioni per massimizzare gli investimenti di ieri e anticipare le esigenze di domani, che aiutano a realizzare i processi di lavoro e che catturano le informazioni e i documenti per un'accesso rapido ed una archiviazione a basso costo. Risultati concreti per problemi concreti.





**Optical Docu System**





**NOVITÀ!**  
**PER PICCOLI E**  
**GRANDI FORMATI**

Gallo Pomi Group®

Direzione: via R. Sanzio, 34 - Milano  
 tel. 02.46.765.400 - fax. 02.46.765.302  
 e-mail: sede\_milano@gallopomi.it • www.gallopomi.it  
 Ufficio di Roma: tel. 06.37.01.441 • Ufficio di Padova: tel. 049.86.47.659

*ti successivi al 19 del disciplinare si applicano “solamente” se si trattano dati sensibili (a prescindere dalla considerazione che, data l’estensione della definizione di dato sensibile, appare difficile individuare un soggetto che tratti dati personali e neppure “un” dato sensibile, anche se non è una situazione impossibile da realizzare).”*

Inoltre, il punto 19 del Disciplinare tecnico (“Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo...”) pone una scadenza “fissa” per la redazione del DPS da parte di chi tratti “dati sensibili o giudiziari”.

### **Per una preda allettante (la Privacy) tanti lupi in agguato...**

E’ un business, quello del “perenne adeguamento/aggiornamento” ai dettami della normativa sulla Privacy, che si perpetuerà di anno in anno in quanto occorrerà, come visto più sopra, che il titolare del trattamento dei dati, entro il 31 marzo di ogni anno, stabilisca delle puntuali politiche di sicurezza in base allo stato dell’arte e all’evoluzione tecnologica. Tali politiche dovranno essere multidisciplinari e pertanto dovranno prevedere l’implementazione di nuove tecnologie (gli strumenti elettronici migliori sul mercato, allo scopo di ridurre al minimo qual-

siasi rischio sul dato personale), la definizione dei ruoli chiave necessari e la predisposizione delle procedure di sicurezza richieste dal Testo Unico sulla Privacy.

Il nuovo Codice ripropone la distinzione tra misure di sicurezza idonee e misure di sicurezza minime con le medesime conseguenze previste dalla previgente legge 675/1996. Responsabilità civile in caso di violazione delle misure idonee; responsabilità penale nel caso delle minime (art. 169). Il legislatore si attende una maggior sicurezza e per questo chiarisce che occorre un livello minimo di sicurezza che può essere garantito solo mediante l’applicazione delle misure minime che sono esplicitate in un allegato del Codice (il disciplinare tecnico ovvero l’ Allegato B).

Tra le righe del nuovo Codice si intravede a chiare lettere la necessità non solo di rispettare dei meri oneri burocratici, ma principalmente di creare una pregnante “cultura della privacy” (secondo il ben noto adagio “privacy is not a solution, is a process”) attraverso strumenti più complessi delle semplici informative e richieste di consenso.

Nasce così l’esigenza di allestire delle strutture dedicate (uffici di sicurezza, nomine di responsabili interni ed esterni); di predisporre procedure e manuali di sicurezza efficaci; di elaborare contratti di *outsourcing* che prevedano la nomina del fornitore responsabile ed apposite clausole a tutela delle informazioni; di preve-

dere nuovi obblighi di dichiarazione di conformità da parte dei fornitori di servizi informatici; sino ai più stringenti obblighi di formazione e all’obbligo di allegare ai bilanci delle società di capitale l’avvenuta predisposizione del Documento Programmatico per la Sicurezza.

Accanto alla necessità della redazione del DPS e del suo aggiornamento con cadenza annuale, quasi unanime vista l’estensione della definizione di dato sensibile, v’è quella della formazione periodica degli incaricati (Allegato B, 19.6), “*per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.*”

Sulla scorta di quanto detto sinora è agevole constatare come siano “comparsi”, d’un tratto e con tempistica eccellente, una serie di società e di “consulenti” che di questa normativa sulla Privacy ne hanno fatto un vero e proprio business. C’è la società di software che ha “sfornato” un prodotto per la redazione del DPS e lo vende sia al singolo utente finale sia a parti terze (rivenditori) che lo utilizzano per produrre, in quantità industriale, DPS per i propri clienti (ovviamente proponendo una propria “soluzione chiavi in mano”); c’è l’esperto di informa-

tica che si reinventa “consulente sulla sicurezza”; ci sono società che sino all’altro ieri si occupavano di altri settori merceologici e che da poco dopo il primo gennaio 2004 offrono “pacchetti Privacy” a go-go.

Va bene il business, ma con prudenza sia da parte dei fornitori che dei fruitori del servizio...

### Alcuni spunti per pretendere un servizio “a regola d’arte”

La società o la persona alla quale vi affidate per l’adeguamento al Codice Privacy dovrebbe garantirvi (e dovrete pretenderli!) i seguenti servizi:

- puntuale analisi della vostra struttura: analisi, si badi bene, che va compiuta tramite accurato check-up in loco di un incaricato con interviste al titolare, al/ai responsabile/i ed agli incaricati del trattamento dei dati e non tramite semplici questionari inviati via e-mail;
- il check-up è volto ad individuare ed approfondire, con il vostro ausilio, “l’elenco dei trattamenti dei dati personali”, “la distribuzione dei compiti e delle responsabilità nell’ambito delle strutture preposte al trattamento dei dati”, “i rischi che incombono sui dati” e “le misure da adottare per garantire l’integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia ed accessibilità”, “i criteri e le modalità per il ripristino della disponibilità

*dei dati in seguito a distruzione o danneggiamento”;*

- analisi personalizzata dei rischi che incombono sui dati trattati, ossia verifica “ad hoc” delle dotazioni di sicurezza presenti e mancanti; pertanto, non deve trattarsi di una mera fornitura di software antivirus, firewall (sia esso software o hardware) ed apparecchiature per il back-up ma di una “consulenza sartoriale”, tarata sulle reali necessità della vostra struttura;

La struttura alla quale vi affidate, dunque, deve avvalersi di professionalità composite ovvero di un esperto sulla normativa che sappia guidarvi nel “comprendere” come la vostra realtà debba relazionarsi con il dettato del nuovo Codice Privacy (non tralasciando gli aspetti relativi all’informativa da fornire agli interessati, la notifica da inviare al Garante quando prevista, la stesura e consegna delle lettere di incarico, ...) e di un esperto di sicurezza logica e fisica che sappia orientarvi nella scelta delle soluzioni più consone e confacenti alle vostre concrete necessità.

Un discorso a parte merita la formazione periodica di tutti coloro che, all’interno della vostra struttura, trattano i dati personali: questa formazione non deve essere né solo teorica né solo pratica ma andrebbe erogata attraverso moduli, ben equilibrati, che abbiano ad oggetto nozioni didattico/normative e nozioni pratico/operative.

Un buon corso, a ben vedere, si

avvale delle due stesse professionalità viste prima: un esperto sulla normativa (che non sia a digiuno di conoscenze informatiche) ed un esperto di sicurezza logica e fisica (che ben padroneggi i 186 articoli ed i tre allegati del Codice in materia di protezione dei dati personali).

Infine, non dimenticate di pretendere da coloro che vi redigono il DPS, vi erogano la formazione sulle tematiche della Privacy, vi installano le misure minime di sicurezza o intervengono in qualsiasi maniera sulle vostre banche dati, una certificazione di conformità (Allegato B, 25) di tali loro attività alle disposizioni del disciplinare tecnico allegato al Codice Privacy (D.Lgs. n. 196/2003).

### PER SAPERNE DI PIÙ

*I lettori che desiderano approfondire l’argomento possono consultare i seguenti articoli pubblicati su Bancamatica, o farne richiesta alla redazione della rivista scrivendo a: [bancamatica@epcperiodici.it](mailto:bancamatica@epcperiodici.it)*

#### **Bancamatica 5/2004 – pag. 4**

Newsletter del Garante – Arriva il codice della privacy: cosa cambia dal 30 giugno prossimo

#### **Bancamatica 4/2004 – pag. 11**

F. Egidi – Cominciano i dibattiti sul nuovo codice della privacy

#### **Bancamatica 3/2004 – pag. 5**

C. Giannotti – Privacy, che cosa cambia con l’arrivo del nuovo codice