STUDIO ASSOCIATO TRIBUTARIO E LEGALE
CIMMINO LO MAGLIO COLNAGO GIACOSA

SETTORE TRIBUTARIO
AVVOCATO FRANCESCO CIMMINO
RAG. COMM. PIERANGELO LO MAGLIO
DOTT. COMM. GIAN PAOLO COLNAGO
DOTT. COMM. STEFANO GIACOSA
DOTT. COMM. ANDREA MAGNONI
DOTT. COMM. STEFANO MASSAROTTO
DOTT. COMM. GIAN LUCA MILANESI
DOTT.SSA KATIA MARCHIORO
DOTT.SSA ELISA BOCCACCINI

SETTORE LEGALE
AVVOCATO STEFANO MAGNONI
AVVOCATO ENRICO CIMMINO
AVVOCATO CLAUDIA MESIRCA
AVVOCATO LUCA SANDRI
AVVOCATO ALVAREZ DE CIENFUEGOS
DOTT.SSA ROBERTA CAZZANIGA

CORPORATE FINANCE
DOTT. PAOLO VAILETTI
DOTT. LUCA BOSI

CONSULENTI
AVVOCATO GIUSEPPE DE ANGELIS
DOTT. COMM. PAOLO SFAMENI
AVVOCATO GIUSTINA ANGELILLO
AVVOCATO ROBERT VIA

Milano, 27 febbraio 2004

NEWSLETTER

Oggetto: Il D.Lgs. 30 giugno 2003 n. 196 "Codice sulla privacy"

Con il 1 gennaio 2004 è entrato in vigore il D. Lgs.vo 30 giugno 2003 n. 196, meglio noto come "Codice sulla privacy" (denominato di seguito "Codice").

Si tratta di un provvedimento assai ponderoso (ben 186 articoli) al quale si aggiungono due "Disciplinari tecnici": l'allegato A relativo al trattamento dei dati nell'attività giornalistica e l'allegato B relativo al codice di deontologia e di buona condotta per il trattamento dei dati personali a scopi statistici e di ricerca scientifica.

Il nuovo Codice incide in maniera significativa sull'impianto normativo preesistente, quello, per intenderci, tracciato dalla L. 675/96 e dal D.P.R. 318/99 ora non più validi. Di seguito evidenzieremo i principali elementi di novità rispetto alla disciplina previgente.

Il nostro Studio ha maturato una particolare esperienza sulla materia ed è pertanto in grado di prestare una completa assistenza per l'applicazione delle nuove norme e/o per una revisione delle misure sulla privacy in concreto già adottate dalle aziende.

1. Principali scadenze previste dal Codice

Preme anzitutto mettere in evidenza due scadenze che il Codice prevede a carico delle aziende in tema di sicurezza e di misure di sicurezza.

a) L'adozione di un sistema di misure di sicurezza minime obbligatorie previste dal Codice deve essere adottato *entro il 30 giugno 2004*, fatti salvi i casi di impossibilità tecnica dovuta al sistema informatico. Questi ultimi, se debitamente evidenziati in un

documento di data certa da conservare presso l'azienda, consentono lo slittamento del termine al *1 gennaio 2005*. Le misure minime di sicurezza vengono dettagliatamente descritte nel disciplinare tecnico contenuto nell'allegato B. La loro inosservanza costituisce reato punito con l'arresto sino a due anni, ovvero con una ammenda da 10.000 a 50.000 euro

b) Qualora il trattamento contenga dati sensibili o giudiziari e sia effettuato con strumenti elettronici, il titolare deve redigere *entro il 31 marzo di ogni anno* (prima scadenza *31 marzo 2004*) il Documento Programmatico sulla Sicurezza.

2. Obbligo di redazione del Documento Programmatico sulla Sicurezza

Come si è accennato il Documento Programmatico sulla Sicurezza (DPS) deve essere predisposto in tutti i casi in cui si trattino dati sensibili o giudiziari con l'utilizzo di strumenti elettronici, anche nell'ipotesi in cui tali strumenti non siano in rete.

Il DPS deve contenere dettagliate informazioni riguardo alle seguenti materie:

- l'elenco dei trattamenti personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture proposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati;
- la descrizione dei criteri per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati a terzi;
- l'individuazione dei criteri da adottare per la cifratura o per la separazione di dati relativi allo stato di salute dagli altri dati personali dell'interessato.

Per espressa disposizione di legge la relazione accompagnatoria del bilancio d'esercizio deve riferire dell'avvenuta redazione o aggiornamento del DPS.

3. Obbligo di notifica e di informativa

L'obbligo generale di comunicare al Garante della privacy la tipologia e le modalità di trattamento dei dati personali che si intende effettuare (*obbligo di notifica*) non concerne più, come nella precedente disciplina, qualunque tipologia di trattamento dei dati personali comuni, ma viene ristretto a specifici e determinati casi di trattamento dei dati.

Il Titolare (ovvero l'azienda, il professionista o la P.A) dovrà notificare al Garante della privacy la sua intenzione di trattare dati personali comuni, vale a dire nome, cognome,

indirizzo, luogo di lavoro dell'interessato ecc..) solo ove il trattamento che si intende effettuare abbia ad oggetto:

- la raccolta di dati biometrici (identificano le persone sulla base delle rispettive caratteristiche fisiche: volto, impronte digitali ecc..);
- prestazione di servizi sanitari per via telematica;
- la gestione di dati sensibili da parte di agenzie di ricerca personale per conto terzi e di marketing;
- l'analisi delle caratteristiche di potenziali consumatori;
- indagini sulla solvibilità di soggetti con cui si intrattengono relazioni commerciali (banche dati sulla solvibilità del creditori o antifrode);
- videosorveglianza (strumenti di localizzazione della posizione geografica delle persone)

La notifica dei dati suddetti dovrà essere effettuata per via telematica e a mezzo firma digitale. L'omessa, incompleta o tradiva notifica è punita con una sanzione amministrativa da euro 10.000 a euro 60.000.

In tutti gli altri casi, non sarà necessario dare corso alla notifica. Tuttavia, ove il trattamento abbia ad oggetto dati sensibili quali razza ed etnia, adesione ad associazioni politiche o sindacali, salute, religione ecc…, il trattamento dovrà essere sempre previamente autorizzato dal Garante della privacy.

Quanto all'obbligo di informare il soggetto interessato al trattamento dei dati, questo rimane invariato. Il Codice sottolinea però che nell'informativa devono essere indicati tutti i soggetti ai quali i dati saranno comunicati, anche in outsourcing.

Per alcune materie particolarmente importanti per le imprese (rapporti di lavoro, informazione commerciale, direct marketing e pubblicità, videosorveglianza, centrale rischi e banche dati sul comportamento debitorio) le *future* regole di trattamento verranno fissate dalle categorie interessate con il meccanismo di autoregolamentazione proprio dei "codici di deontologia e di buona condotta", il cui rispetto costituirà condizione essenziale per la liceità del trattamento.

4. Misure di sicurezza in azienda

All'interno del Codice viene prestata molta attenzione al tema della sicurezza, il quale notoriamente costituisce anche una delle maggiori preoccupazioni per le aziende che gestiscono il flusso dei dati personali, soprattutto qualora vi sia anche una presenza in Internet.

Due, in particolare, i tipi di misure di sicurezza che vengono in rilievo: quelle c.d. minime e quelle c.d. idonee.

4.1 Le misure minime

Le misure minime previste dal Codice, sono in concreto individuate dal disciplinare tecnico allegato B, e sono volte ad assicurare un livello (appunto) minimo di protezione dei dati personali. Un livello al di sotto del quale non si può scendere in quanto, come si è detto, il mancato rispetto di dette misure costituisce reato.

In riferimento alle misure minime, il Codice riserva una particolare attenzione alla nozione di "autenticazione informatica": la definizione è nuova (ossia sconosciuta alla L.675/96) e comprende i mezzi – siano essi programmi informatici o componenti hardware – deputati alla verifica ed alla convalidazione dell'identità di un dato soggetto.

Con particolare puntigliosità vengono specificate le caratteristiche che deve avere una password per essere considerata realmente tale. A norma del Disciplinare Tecnico, infatti, la parola-chiave dovrà essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Essa, inoltre, non dovrà contenere riferimenti agevolmente riconducibili all'interessato (ad es.: nome della moglie, marca dell'autovettura, squadra di calcio della quale si è tifosi, ecc.) e dovrà essere per legge modificata almeno ogni sei mesi.

Un'ulteriore disposizione riguarda l'obbligatorietà di effettuare, almeno ogni settimana, copie di *back-up* dei dati contenuti nei propri sistemi informatici.

4.2 Le misure idonee

Il Codice impone al titolare del trattamento dei dati personali di predisporre tutte le misure di sicurezza idonee 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".

Si tratta in sostanza di adottare tutte quelle misure che permettono la migliore custodia e il massimo controllo dei dati oggetto di trattamento sulla base delle conoscenze acquisite in base al progresso tecnico.

Se l'adeguamento alle "misure minime" implica l'assenza di responsabilità penali, tale adeguamento non è tuttavia sufficiente per affrancarsi dalla responsabilità civile. Qualora infatti gli accorgimenti presi non soddisfino le misure dichiarate "idonee" può trovare applicazione l'art. 2050 c.c. espressamente richiamato dal Codice. In base a tale norma è tenuto al risarcimento di ogni danno eventualmente cagionato a terzi chiunque non riesca a dar prova di aver adottato "tutte le misure" idonee ad evitare il danno stesso.

5. La videosorveglianza

Una nuova disciplina legale è dedicata dal Codice alla "videosorveglianza", la quale come noto consiste nell'installazione di sistemi, reti ed apparecchiature che permettono la ripresa e l'eventuale registrazione di immagini in particolare ai fini di sicurezza.

Al riguardo, il Codice deferisce al Garante il compito di emanare un codice di deontologia volto a disciplinare il fenomeno, prevedendo specifiche modalità di trattamento e forme semplificate di disciplina.

Allo stato, le indicazioni più interessanti in materia sono contenute nel "provvedimento generale del 29 novembre 2000" (facilmente reperibile al sito www.garanteprivacy.it), che prevede una sorta "decalogo di regole" per non violare la privacy nell'effettuare la videosorveglianza.

6. Invio di messaggi commerciali per via interattiva e terrestre

Il Codice ha infine recepito parte dei contenuti della Direttiva n. 2002/58/CE sul "*trattamento dei dati personali e sulla tutela della vita privata nel settore delle comunicazioni elettroniche"*. In particolar modo il dettato legislativo ha confermato il meccanismo del c.d. *opt-in* nell'invio di messaggi commerciali per via telematica. In base alla nuova norma chiunque abbia intenzione di inviare messaggi commerciali a

mezzo *posta elettronica, fax, telefono o telefonino* (Sms e Mms) o altro strumento telematico deve avere acquisito preventivamente il consenso del destinatario a tale invio.

Il meccanismo dell'opt-in (consenso preventivo) si applica all'invio di materiale pubblicitario, alla vendita diretta e al compimento di ricerche di mercato per le via terrestre (posta ordinaria).

* * *

Restiamo a disposizione per qualsiasi necessità e, con l'occasione, porgiamo cordiali saluti.