ICT E DIRITTO

Rubrica a cura di

Antonio Piva e David D'Agostini

Scopo di questa rubrica è di illustrare al lettore, in brevi articoli, le tematiche giuridiche più significative del settore ICT: dalla tutela del *domain name* al *copyright* nella rete, dalle licenze software alla *privacy* nell'era digitale. Ogni numero tratterà un argomento, inquadrandolo nel contesto normativo e focalizzandone gli aspetti di informatica giuridica.

La tutela dei dati personali nell'era digitale: il Codice sulla privacy tra vecchi e nuovi adempimenti

1. Introduzione

L'interesse e la sensibilità per la tutela della *privacy*, soprattutto a seguito dello sviluppo e della diffusione degli strumenti informatici e telematici, sono notevolmente aumentati nel corso dell'ultimo decennio, determinando di conseguenza una produttiva attività del Parlamento.

Gli sforzi del legislatore hanno portato, da ultimo, all'emanazione del "Codice in materia di protezione dei dati personali", contenuto nel decreto legislativo 30 giugno 2003 n. 196[1].

A partire dal 1° gennaio 2004, data dell'entrata in vigore del nuovo codice, sono state abrogate numerose fonti normative in materia di tutela della privacy tra cui la legge 31 dicembre 1996, n. 675 (aggiornata ben 10 volte in soli 5 anni) e il decreto del presidente della Repubblica 28 luglio 1999, n. 318 (altrimenti detto "Regolamento sulle misure minime di sicurezza").

Il nuovo testo unico ha l'indiscutibile merito di coordinare le molteplici disposizioni già vigenti, apportando ulteriori integrazioni e modifiche anche in recepimento della direttiva comunitaria 2002/58/CE inerente le comunicazioni elettroniche e compiendo un passo fondamentale, da un lato, per facilitare la conoscenza della normativa e dall'altro per garantire una più ampia e responsabile applicazione della stessa, soprattutto in presenza di trattamento informatizzato dei dati.

Il codice unitario, nel segno della continuità con le scelte legislative passate, riprende la terminologia dei testi precedenti, peraltro ulteriormente affinata sulla scorta dell'esperienza maturata negli ultimi anni, aggiungendo nuove definizioni di matrice tecnica, rese necessarie dall'evoluzione tecnologica degli ultimi anni (per esempio, *comunicazione elettronica, autenticazione informatica* ecc.).

Il "Codice in materia di protezione dei dati personali" si compone di tre parti (si veda, a tal proposito, il riquadro 1), inoltre, viene integrato dall'allegato B contente il disciplinare tecnico in materia di misure minime di sicurezza, dove si trovano, per i trattamenti con strumenti elettronici, le disposizioni e le modalità di autentificazione informatica, i sistemi di autorizzazione

Riquadro 1: Suddivisione del Codice

Prima parte (Disposizioni generali): disciplina sostanziale applicabile a tutti i trattamenti di dati personali, i diritti dell'interessato, gli adempimenti e la sicurezza dei dati e dei sistemi.

Seconda parte (Disposizioni relative a specifici settori): norme relative a specifici trattamenti per esempio, gli ambiti giudiziario, bancario e assicurativo, sanitario, dell'istruzione, del lavoro, del giornalismo ecc..

Terza parte (Tutela dell'interessato e sanzioni): articoli inerenti la difesa dei diritti dell'interessato e il sistema sanzionatorio.

Allegato A: codici di deontologia.

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.

[1] Gazzetta Ufficiale 29 luglio 2003, n.174, S.O. Utile riferimento: *www.garanteprivacy.it*

e sicurezza e, inoltre, la regolamentazione del documento programmatico.

2. I SOGGETTI E GLI ADEMPIMENTI

Le figure principali individuate dal nuovo testo unico, peraltro già identificate dalla precedente normativa, sono l'*interessato* (ossia il soggetto al quale si riferiscono i dati personali), il *titolare* che decide le finalità e le modalità del trattamento di dati personali, il *responsabile* (individuato facoltativamente dal titolare tra soggetti dotati di esperienza in materia), gli *incaricati*, vale a dire le persone fisiche autorizzate a compiere operazioni di trattamento attenendosi alle istruzioni impartite dal titolare o dal responsabile, in relazione alla tipologia di dati trattati (si veda, a tal proposito, il riquadro 2).

Riquadro 2: I dati personali

Identificativi: permettono l'identificazione diretta dell'interessato.
Anonimi: non possono essere associati a un interessato identificato o identificabile.
Giudiziari: idonei a rivelare provvedimenti di natura penale.
Sensibili: 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 o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché lo stato di salute e la vita sessuale.
Quasi sensibili: il loro trattamento presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

Nella prassi il responsabile dei sistemi informativi aziendali viene spesso nominato quale responsabile del trattamento dei dati, costituendo, inoltre, un punto di riferimento per amministratori dei sistemi e incaricati alla custodia delle *password*. Pertanto, è essenziale che questi professionisti prendano conoscenza dei dettami riguardanti i trattamenti informatizzati, contenuti nel menzionato disciplinare tecnico in materia di misure minime di sicurezza, i cui temi vengono illustrati nel prossimo paragrafo.
Oltre agli atti di nomina del responsabile e degli incaricati (che devono essere effettuati per iscritto), vengono posti a carico del titolare del trattamento una serie di adempimenti: in primo luogo, ai sensi dell'art. 13 (che ricalca l'art. 10 L. 675/96), l'interessato deve essere preventivamente *informato*, oralmente o per iscritto, in merito alle finalità e modalità del trattamento, all'obbligatorietà o meno del conferimento dei dati e alle conseguenze di un eventuale rifiuto; egli dovrà, inoltre, sapere quali soggetti potranno venire a conoscenza delle informazioni raccolte e quale la logica viene applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici (si pensi alla comunicazione via *e-mail* o alla diffusione dei dati anche a mezzo di Internet).
L'interessato ha sempre il diritto di ottenere, oltre alle indicazioni presenti nell'informativa, la conferma dell'esistenza di dati che lo riguardano, l'aggiornamento, la modifica, la cancellazione, l'anonimizzazione dei dati medesimi, potendo opporsi per motivi legittimi al trattamento (come nel caso di invio di materiale pubblicitario non richiesto via Internet, tramite posta elettronica, pratica comunemente detta *spamming*).
In secondo luogo, l'art. 23 (sulla falsa riga dell'art. 11 L. 675/96) conferma che il trattamento è ammesso solo se l'interessato abbia prestato in maniera valida il proprio consenso. Il *consenso*, che deve essere espresso in forma specifica per ogni trattamento chiaramente individuato, va documentato per iscritto, e comunque preceduto dall'informativa. Qualora siano trattati dati sensibili, oltre al consenso manifestato in forma scritta da parte dell'interessato, è necessaria l'autorizzazione del Garante il quale può prescrivere misure e accorgimenti anche tecnici a garanzia dell'interessato stesso, che il titolare è tenuto ad adottare.
Le disposizioni sopra elencate devono essere rispettate anche in caso di trattamento elettronico delle informazioni e sistemi informativi automatizzati (si pensi alla raccolta dati per telefono da parte di un *call center*), eventualmente impiegando gli strumenti innovativi resi disponibili dalle moderne tecnologie, vale a dire anche, per esempio, tramite e-mail o *web*.
In particolare, nell'ipotesi non infrequente di trattamento dei dati mediante un sito Internet, l'informativa deve essere posizionata in calce alla pagina in cui vengono raccolte le informazioni personali (ovvero, in un'apposita finestra *pop-up*, o in altra maniera equivalente) e il consenso, se richiesto, può essere espresso tramite la compilazione di un *form* e successivamente registrato nelle memorie del

sistema, in ottemperanza all'obbligo di documentazione.
Quanto al trattamento dei dati sensibili, per il quale è richiesta la forma scritta, il consenso dovrà essere manifestato in maniera conforme alle normative vigenti in materia di firme elettroniche.

3. Le misure di sicurezza

Gli adempimenti inerenti la sicurezza dei dati e dei sistemi informatici sono finalizzati a ridurre al minimo i rischi di distruzione o perdita dei medesimi, ovvero di accesso non autorizzato o di trattamento non consentito, in relazione al tipo di dati trattati.
Il già menzionato Allegato B (Disciplinare tecnico in materia di misure minime di sicurezza) prevede, tra le modalità tecniche da adottare in caso di trattamento con l'ausilio di strumenti elettronici, il ricorso a sistemi di autenticazione informatica e di autorizzazione degli incaricati, mediante codice di identificazione personale (*username*) e parola chiave riservata (*password*), ovvero tramite dispositivi di autenticazione in possesso a uso esclusivo dell'incaricato (per esempio, *token*, *smart card*).
A tale scopo viene suggerito anche l'impiego delle tecnologie biometriche che trovano sempre maggiore applicazione per la loro elevata capacità di verificare in maniera sicura l'identità di un soggetto riconoscendone l'impronta digitale, l'iride, il timbro vocale e perfino i tratti somatici del volto.
I dati personali, inoltre, devono essere protetti contro il rischio di intrusione (per esempio, mediante *firewall* e programmi denominati *Intrusion Detection System*, IDS) e dall'azione di virus tramite idonei strumenti elettronici da aggiornare con cadenza almeno semestrale; vengono anche previsti l'aggiornamento periodico dei programmi finalizzati a prevenire la vulnerabilità dei sistemi e a correggerne i difetti (per esempio, *Patch* e nuove versioni) da effettuarsi almeno annualmente e il salvataggio periodico dei dati (*back-up*) con frequenza almeno settimanale.
Tra le misure di sicurezza, soprattutto nel caso di trattamento di dati sensibili, viene indicato anche l'utilizzo della cifratura, il che lascia pensare all'impiego su larga scala della crittografia basata sull'infrastruttura a chiave pubblica (PKI, *Public Key Infrastructure*).
Un tassello fondamentale nel mosaico della sicurezza informatica è costituito dal documento programmatico, da adottarsi entro il 31 marzo di ogni anno (ma per il 2004 il termine scadrà il 30 giugno!), obbligatoriamente nel caso di trattamento di dati sensibili[2].
Si tratta di un manuale, redatto anche in collaborazione con il responsabile, sulle politiche per la sicurezza delle informazioni e dei sistemi e sulle procedure e modalità di registrazione delle attività degli incaricati.
In particolare, il documento programmatico sulla sicurezza deve contenere l'elenco dei trattamenti, la distribuzione dei compiti e delle responsabilità, l'analisi dei rischi sui dati, le misure di sicurezza da adottare per l'integrità e disponibilità dei dati, la protezione delle aree e dei locali, la modalità di ripristino (si pensi al *disaster recovery*), il piano di formazione del personale incaricato al trattamento e inoltre, per i dati personali idonei a rilevare lo stato di salute e la vita sessuale, le modalità di cifratura e di separazione dei dati dalle altre informazioni personali dell'interessato.
Un'assoluta novità sul tema è l'obbligo di riferire in merito all'avvenuta redazione o aggiornamento del documento programmatico nella relazione accompagnatoria del bilancio d'esercizio. Con questa disposizione viene riconosciuto alla tutela dei dati personali un rango di importanza primaria nell'ambito della gestione aziendale di una società.

4. Le sanzioni e le responsabilità

La mancata ottemperanza alle disposizioni indicate nel nuovo codice della privacy comporta conseguenze sotto diversi profili.
Innanzitutto, possono configurarsi violazioni punite con sanzioni amministrative fino a 60.000 euro o addirittura sussistere illeciti pe-

[2] [N.d.A.] Vivamente consigliata anche in presenza di meri dati comuni, in quanto questa documentazione servirà da supporto al piano organizzativo interno nell'adempiere alle disposizioni legislative in materia di sicurezza, nonché come elemento probatorio nelle eventuali procedure ispettive: ovvero, in contenziosi di natura giudiziaria.

Riquadro 3: Le sanzioni

Omessa o inidonea informativa all'interessato: sanzione amministrativa da 3.000 a 18.000 euro (da 5.000 a 30.000 euro se si tratta di dati sensibili) aumentabile fino al triplo.
Omessa o incompleta notificazione al Garante: sanzione amministrativa da 10.000 a 60.000 euro.
Omessa informazione o esibizione al Garante: sanzione amministrativa da 4.000 a 24.000 euro.
Omessa adozione delle misure minime di sicurezza: arresto fino a 2 anni o ammenda da 10.000 a 50.000 euro.
Falsità nelle dichiarazioni e notificazioni al Garante: reclusione da 6 mesi a 3 anni.
Inosservanza dei provvedimenti del Garante: reclusione da 3 mesi a 2 anni.
Trattamento illecito di dati: reclusione da 6 a 18 mesi (da 6 a 24 mesi se consiste in comunicazione o diffusione, ovvero da 1 a 3 anni se dal fatto deriva nocumento).

nalmente rilevanti per i quali sono previste sanzioni detentive fino a 3 anni (si veda a tal proposito il riquadro 3).
In secondo luogo, alla responsabilità amministrativa e/o penale si affianca quella civile: il danno causato dal trattamento di dati personali deve essere risarcito, a meno che non si dimostri di aver adottato tutte le misure idonee a evitarlo, prova estremamente difficile da fornire in concreto. La giurisprudenza, pronunciandosi sul punto, ha già riconosciuto tale diritto, spesso liquidando poste di danno molto elevate; si ricorda che in materia di privacy può essere oggetto di risarcimento anche il danno non patrimoniale (si pensi al danno morale causato a una persona) in base all'art. 15 e all'art. 2059 c.c..
Concludendo, notoriamente l'ordinamento italiano non ammette l'ignoranza e a maggior ragione, come nel caso della privacy, dopo l'introduzione di uno specifico codice; pertanto, l'adeguamento alla normativa in esame da parte dei titolari del trattamento non può essere ulteriormente dilazionata.
Le responsabilità in gioco e l'inasprimento delle sanzioni, in particolare quelle pecuniarie, devono far riflettere chi già non l'abbia fatto, su tale necessità, soprattutto ora che l'Ufficio del Garante, dopo anni di rodaggio e grazie al recente aumento del proprio organico, sembra deciso ad applicare la legge senza deroghe di sorta.

Antonio Piva laureato in Scienze dell'Informazione, Presidente, per il Friuli - Venezia Giulia, dell'ALSI (*Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica*) e direttore responsabile della Rivista di Informatica Giuridica.
Docente a contratto di Informatica giuridica all'Università di Udine.
Consulente sistemi informatici, valutatore di sistemi di qualità ISO9000 e ispettore AICA per ECDL base e advanced.
E-mail: antonio_piva@libero.it

David D'Agostini avvocato, ha conseguito il master in informatica giuridica e diritto delle nuove tecnologie, fornisce consulenza e assistenza giudiziale e stragiudiziale in materia di software, privacy e sicurezza, contratti informatici, e-commerce, nomi a dominio, computer crime, firma digitale. Ha rapporti di partnership con società del settore ITC nel Triveneto.
Collabora all'attività di ricerca scientifica dell'Università di Udine e di associazioni culturali.
E-mail: david.dagostini@adriacom.it