L'attuazione del Codice in Materia di Protezione dei Dati Personali in ambito sanitario

Ernesto Setti, Riccardo Di Sarcina

2 marzo 2004

Il DLG 196/03 (Codice in Materia di Protezione dei Dati Personali, d'ora in poi il Codice), entrato in vigore il 1 gennaio 2004, sostituisce e abroga diverse leggi, tra cui la Legge 675/96 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali) e il DPR 318/99 (Regolamento recante norme per l'individuazione delle misure di sicurezza minime per il trattamento dei dati personali). È opinione comune che il Codice rappresenti una significativa evoluzione rispetto ai precedenti regolamenti, soprattutto per quanto riguarda l'aderenza alle realtà tecnologiche e operative del trattamento dei dati.
Il trattamento dei dati personali è equiparato ad *attività pericolosa*. Di conseguenza, chi trattando dati personali provoca danni ad altri è tenuto al risarcimento. Oltre ad eventuali sanzioni amministrative che possono arrivare fino a 125.000 Euro, il Codice prevede specifici reati penali con pene fino a tre anni di reclusione.

Come il Codice si applica ai dati sanitari?

I dati atti a rivelare lo stato di salute o la vita sessuale delle persone vengono considerati *sensibili* e sono sottoposti a un regine speciale di trattamento. In particolare:

- devono essere conservati separatamente dai dati non sensibili;
- devono essere protetti dall'accesso non autorizzato, ad esempio per mezzo di tecniche di cifratura;
- non possono essere diffusi.

Quali misure è necessario prendere per rispettare la legge?

Il Codice prevede esplicitamente che i dati debbano essere custoditi e controllati in modo da ridurre al minimo i rischi di perdita (anche accidentale), di accesso non autorizzato o di trattamento non consentito. Le precauzioni da prendere possono variare nel tempo in relazione al progresso tecnico. Premesso ciò, gli art.33 segg. del Codice identificano un insieme di misure minime di sicurezza che devono essere adottate. Tali misure prevedono:

- l'autenticazione informatica e la gestione delle credenziali di autenticazione;
- l'utilizzazione di un sistema di autorizzazione;
- la protezione dei dati nei confronti di accessi non autorizzati e a trattamenti illeciti;
- la protezione da parte di software maligno;
- l'adozione di procedure di back-up e ripristino dei dati;
- la tenuta di un Documento Programmatico di Sicurezza;
- per i dati sensibili (sanitari) l'adozione di tecniche di cifratura o di codici identificativi.

Quali sono le scadenze di legge?

Queste le principali scadenze. Si tenga conto che poichè alcune delle norme sono state ereditate dal precedente DPR 318/99 è possibile essere già inadempienti.

- Entro il 30 marzo 2004 è previsto l'aggiornamento del Documento Programmatico di Sicurezza (da ripetersi annualmente).
- Entro il 30 aprile 2004 occorre effettuare la notifica al Garante (per i casi previsti).
- Le misure minime di sicurezza devono essere adottate entro il 30 giugno 2004. Solo qualora obiettive ragioni tecniche impediscano l'adeguamento è possibile avere una proroga di 6 mesi: in ogni caso occorre prendere ogni possibile misura organizzativa, logistica e procedurale atta a ridurre il rischio e redigere un documento (avente data certa) che motivi la ragione del ritardo.

Come posso garantire la confidenzialità dei dati?

È un argomento complesso che non può configurarsi nella semplice adozione di misure minime di sicurezza tecniche (che sono comunque previste) ma comporta l'adozione di adeguate procedure organizzative e, implicitamente, l'educazione del personale incaricato del trattamento.
Il codice prevede che gli incaricati del trattamento siano dotati di credenziali di autenticazione. Per stabilire cosa un utente sia abilitato a fare è indispensabile identificarlo in modo certo. Le credenziali di autenticazione possono consistere in:

- User id associato a parola chiave riservata (conosciuta solo dall'incaricato medesimo);
- dispositivo di autenticazione ad uso esclusivo dell'incaricato;
- caratteristica biometria dell'incaricato.

Il titolare dovrà fornire agli incaricati precise istruzioni scritte in merito alla individuazione puntuale delle modalità di accesso ai dati, sia in caso di assenza prolungata o impedimento dell'incaricato che per esigenze organizzative e di sicurezza del sistema. Non ha più rilevanza la figura dell'Amministratore di Sistema. Resta la figura del preposto alla custodia delle copie delle credenziali che devono essere individuati per iscritto.
Almeno annualmente deve essere verificata la validità delle condizioni per la conservazione dei profili di autorizzazione: la lista degli incaricati (personale incaricato del trattamento e staff di gestione e manutenzione degli strumenti elettronici), nell'ambito dell'aggiornamento periodico almeno annuale può essere redatta per classi omogenee di incarico e dei relativi profili di autorizzazione.

Come deve essere redatto il documento programmatico di Sicurezza?

Il Documento Programmatico di Sicurezza è un manuale che deve essere redatto dal titolare del trattamento e descrive sia la situazione attuale (analisi dei rischi, distribuzione dei compiti, contromisure di sicurezza in atto, distribuzione delle responsabilità) che il percorso di adeguamento prescelto dall'organizzazione per adeguarsi alla normativa. Il Codice impone come data ultima per la redazione e l'aggiornamento il 31 marzo di ogni anno. Una copia del D.P.S deve essere custodito presso la sede per essere consultabile e deve essere esibita in caso di controlli. Dal 2005 il D.P.S. dovrà trovare posto nella relazione di accompagnamento del bilancio di esercizio.
Nel D.P.S. devono essere descritti:

- le banche dati (elenco dei trattamenti);
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento;
- analisi dei rischi che incombono sui dati;
- le misure da adottare per salvaguardare la sicurezza (integrità, riservatezza, disponibilità) dei dati (sicurezza logica e sicurezza fisica delle aree e locali);
- la descrizione dei criteri e modalità di disaster recovery (ripristino disponibilità dei dati in caso di distruzione o danni);
- la programmazione di interventi formativi differenziati per il personale (la formazione va programmata sin dal momento dell'ingresso in servizio, quando si cambiano mansioni e si introducono nuovi importanti strumenti utilizzati per il trattamento dei dati);
- i contenuti degli interventi formativi;
- descrizione dei criteri adottati per garantire l'adozione delle misure di sicurezza in caso di utilizzo di società esterne per il trattamento di dati personali;
- la descrizione dei criteri adottati, per le organizzazioni che trattano dati sanitari e dati inerenti la vita sessuale, per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

App.1 - Termini usati dal legislatore e loro significato

Trattamento: qualunque operazione o insieme di operazioni, eseguite o meno per mezzo di un computer, relative alla raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.

Dati personali: tutte le informazioni relative a una persona (fisica, giuridica, ente o associazione) che la rendano identificabile. (Es. Nome, cognome, indirizzo, numeri telefonici, n. Patente, P. IVA...)

Dati sensibili: dati relativi a razza o etnia, tendenza politica, fede religiosa, nonchè dati personali idonei a rilevare lo *stato di salute* e la vita sessuale dell'individuo.

Dati anonimi: dati che in origine, o a seguito di trattamento, non possono più essere associati ad un individuo identificato o identificabile.

Banca dati: qualsiasi raccolta di dati personali.

Interessato: la persona (fisica, giuridica, ente o associazione) a cui si riferiscono i dati personali trattati.

Titolare del trattamento: la persona (fisica, giuridica, pubblica amministrazione o qualsiasi altro ente, associazione od organismo) che ha la competenza a decidere in ordine alle finalità, alle modalità del trattamento di dati personali ed alla loro sicurezza.

Responsabile del trattamento dei dati: la persona (fisica, giuridica, pubblica amministrazione o qualsiasi altro ente, associazione od organismo) che il titolare prepone al trattamento di dati personali. Titolare e responsabile possono essere la stessa persona. I compiti affidati al responsabile devono essere dettagliati per iscritto.

Incaricato: colui (o coloro) che elabora i dati personali sulla base delle istruzioni scritte fornite dal titolare o dal responsabile

Misure di sicurezza: accorgimenti fisici o logici atti a proteggere i documenti (armadi chiusi a chiave, firewall, wiping, accesso selezionato ai dati...)

Autenticazione informatica: insieme degli strumenti elettronici e delle procedure atte a verificare l'identit/'a personale. Può essere effettuata tramite User ID e Password, con dispositivi fisici (Token, Smart Card,...) o per mezzo di un rivelatore biometrico (impronte digitali, retina,...).

User ID: codice identificativo personale formato da lettere e numeri. Viene sempre abbinato alla password (segreta).

Password: parola chiave. Una sequenza di lettere, numeri e segni di punteggiatura atta a verificare l'User ID. Deve essere sufficientemente complessa da non poter essere indovinata facilmente, deve essere cambiata frequentemente e non deve essere riutilizzabile.

Amministratore di sistema: colui che si occupa del sistema informatico e delle risorse operative.

Riferimenti bibliografici

[1] `www.garanteprivacy.it` il sito del Garante della Privacy, contiene il testo del D.Lgs 196/2003.

[2] `www.interlex.it` InterLex è un periodico plurisettimanale di carattere informativo, scientifico e culturale giuridico, dedicato al diritto sulla Rete.

Gli autori

Riccardo Di Sarcina è diplomato in Ingegneria Elettronica presso l'Università di Genova e ha accumulato una esperienza decennale nel campo della consulenza informatica. Nel 1999 fonda ICT Consult, azienda che si contraddistingue per la caratura dei suoi clienti (Banca Popolare di Milano, SIA spa, Lotus/IBM , Deutsche Bank, TelecomItalia, Lloyd Italico). Nel 2003 ha conseguito il Master in Sicurezza delle Tecnologie dell'Informazione e della Comunicazione presso l'Università degli Studi di Milano. Attualmente si occupa di adeguamenti alla normativa sulla Privacy (D.Lgs. 196/2003)
È contattabile all'indirizzo `disa@writeme.com`

Ernesto Setti è laureato in Ingegneria Elettronica presso il Politecnico di Milano. Si occupa da diversi anni di ICT in ambito sanitario e specificatamente radiologico, con particolare interesse per gli aspetti più innovativi, la ricerca e l'insegnamento. È professore a contratto presso l'Università degli Studi di Milano. Nel 2003 ha conseguito il Master in Sicurezza delle Tecnologie dell'Informazione e della Comunicazione presso l'Università degli Studi di Milano .
È contattabile all'indirizzo `setti@istitutotumori.mi.it`