FABRIZIO DI CROSTA

Ingegnere elettronico, consulente di organizzazione e consulente tecnico del Tribunale di Bologna per l'informatica)

IL NUOVO CODICE DELLA PRIVACY E LA SICUREZZA DELLE INFORMAZIONI

RIASSUNTO

Il D.Lgs 196/2003, noto anche come Testo Unico sulla Privacy, ha introdotto nuove regole per il trattamento dei dati personali effettuato da imprese e professionisti; in particolare sono state definite alcune misure minime di sicurezza da adottare per il trattamento di dati personali, con particolare riguardo all'utilizzo di strumenti elettronici per il trattamento di dati personali e, soprattutto, di dati sensibili e giudiziari. In questo articolo vengono prese in esame le misure di sicurezza contenute nell'allegato B del D.Lgs 196/2003 nell'ottica di implementare non solo le misure minime di sicurezza previste dalla legge, ma quelle realmente idonee e necessarie per garantire in modo efficace ed efficiente la sicurezza delle informazioni trattate da imprese, studi professionali ed ingegneri liberi professionisti.

RIASSUNTO

Testo in inglese da spedire, Testo in inglese da

1. INTRODUZIONE

Il 1° gennaio 2004 è entrato in vigore il Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" che sostituisce la Legge n. 675/1996. Le nuove disposizioni legislative prevedono l'applicazione di procedure più efficaci rispetto al passato per la tutela dei dati personali, soprattutto quelli gestiti su supporto elettronico.
Il D.Lgs 196/2003 richiede, tra l'altro, alcuni adempimenti formali: nomina del Titolare e di un Responsabile del trattamento dei dati personali di capacità tecniche adeguate, la predisposizione e l'aggiornamento annuale del Documento Programmatico sulla Sicurezza, ecc. (per approfondimenti si veda [2] capitoli 3 e 5). Ma le più importanti novità introdotte dal D.Lgs 196/2003 sono senz'altro **le misure minime di sicurezza che ogni organizzazione che tratti dati personali attraverso sistemi informatici deve adottare**, in particolare: autenticazione informatica, adozione di procedure di gestione delle credenziali di autenticazione, protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici, adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi, ecc..
L'allegato B della legge (*Disciplinare tecnico in materia di misure minime di sicurezza*) descrive nel dettaglio quali sono gli accorgimenti tecnici da adottare, ovvero le misure minime necessarie per evitare sanzioni penali.
È opportuno ricordare che la nuova legge sulla privacy si applica a qualunque tipo di organizzazione: aziende di ogni settore, pubblica amministrazione, organizzazioni sanitarie, studi professionali ed anche singoli professionisti che esercitano l'attività con partita d'IVA individuale. In particolare la legge prevede misure ed adempimenti più estesi per coloro che trattano dati sensibili ("*i dati personali 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 od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale*") e giudiziari ("*i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma*

1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale"), soprattutto su supporto elettronico.
Gli adempimenti del D.Lgs 196/2003 coinvolgono quindi direttamente, oltre alle imprese di costruzioni, anche gli studi di ingegneria e gli ingegneri liberi professionisti. Questi ultimi poi, nel caso eseguano perizie per l'Autorità Giudiziaria e/o perizie tecniche di parte, sono soggetti alle prescrizioni previste per coloro i quali trattano dati giudiziari.

2. ANALISI DEL DISCIPLINARE TECNICO

Nel seguito è riportato, in *corsivo*, l'allegato B del Codice della Privacy - DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Artt. da 33 a 36 del codice) - con i commenti e le azioni da intraprendere riportati negli appositi riquadri.

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
È necessario che tutti gli incaricati al trattamento siano dotati di un codice utente e di una parola chiave per accedere ai dati memorizzati su supporto informatico. Ogni incaricato che accede a sistemi informatici contenenti dati personali deve avere un codice identificativo utente (comunemente denominato *user name*) abbinato ad una *password* di accesso; quest'ultima deve essere segreta e conosciuta soltanto dall'incaricato. Alternativamente il codice identificativo può essere sostituito da un *badge* o una *smartcard*, mentre le veci della parola chiave possono essere fatte da un'impronta digitale o altra caratteristica biometrica che consenta di individuare univocamente l'individuo.
Ogni incaricato può avere anche più di una coppia di *username - password* per effettuare accessi con profili diversi.
Windows 98 è un sistema operativo non adeguato se i dati personali vengono registrati sul disco fisso del medesimo PC in quanto è possibile superare la procedura di autenticazione lasciando il campo *password* vuoto. Viceversa tale sistema operativo può essere utilizzato su un *client* che accede ad un *server* con sistema operativo di rete adeguato (WIndows NT o superiore) ove sono contenuti i dati personali. In tal caso, infatti, è necessario fornire la *password* per accedere ai dati sul server. Naturalmente sul disco fisso del PC *client* non possono essere memorizzati dati personali.
Non è possibile derogare alla coppia codice utente – parola chiave, solamente chi gestisce autonomamente dati personali registrati su un unico PC stand alone (non collegato in rete con altri) può accontentarsi della sola password del BIOS. E comunque in caso di furto del PC e dei relativi dati contenuti dovrà dimostrare di aver intrapreso misure di sicurezza adeguate.
Dunque anche un singolo libero professionista è invitato a dotare il proprio PC di un sistema operativo adeguato con gestione dell'autenticazione.
Occorre poi fare attenzione alla posta elettronica, protetta da propria password che generalmente non viene richiesta, in quanto in talune configurazioni la posta risiede nel PC *client*.
Per approfondimenti si veda [1] (capitoli 3 e 4).

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
È necessario istruire gli incaricati al trattamento - fornendo istruzioni scritte ed una adeguata formazione - circa la gestione delle *password* e di eventuali dispositivi per l'autenticazione (smartcard, ecc.).
Tra gli incaricati al trattamento vi sono sempre dipendenti e collaboratori, ma spesso anche i professionisti esterni a cui sono affidate attività specifiche di progettazione e consulenza (commercialisti, legali, consulenti del lavoro, ecc.)

5. La parola chiave, quando è prevista dal sistema di autenticazione, è 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 non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
Le parole chiavi (password) devono essere di almeno 8 caratteri alfanumerici e non devono essere riconducibili

facilmente alla persona (ad es. data di nascita, nome della moglie/marito, del figlio, ecc.). Esse devono essere modificate dall'incaricato al primo accesso al sistema e quindi almeno ogni 6 mesi (3 mesi se sono trattati dati sensibili o giudiziari).

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
Lo stesso nome utente non può essere successivamente assegnato ad altre persone a seguito di dimissioni o disattivazioni dell'utente originario.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
Se un incaricato si assenta per oltre 6 mesi, nome utente e password devono essere disattivati e modificati.
È importante monitorare le credenziali di accesso concesse a collaboratori esterni – eventualmente anche per permettere connessioni remote - che possono rimanere inutilizzate per molto tempo.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
Lo stesso discorso del comma 7 vale se un incaricato si dimette oppure la sua password viene resa nota ad altri.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
Devono essere fornite istruzioni scritte ed adeguata formazione agli incaricati per evitare che essi lascino incustodito il proprio PC/Terminale con la sessione aperta. Si suggerisce di disconnettere i terminali durante le pause e di utilizzare screen-saver con password.
Tale situazione è particolarmente critica nelle imprese di costruzioni e negli studi di ingegneria dove c'è un continuo andirivieni di persone, non tutte autorizzate a vedere certi dati.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
È necessario predisporre istruzioni scritte per assicurare la disponibilità di dati personali il cui accesso è riservato ad un incaricato il quale potrebbe assentarsi per un periodo prolungato (sicuramente per più di 7 giorni). Ad esempio potrebbero essere mantenute in cassaforte le credenziali di autenticazione di particolari utenti oppure si potrebbe consentire l'accesso a qualsiasi tipo di dato agli utenti di tipo amministratore di sistema. In caso di accesso ai dati utilizzando la password riservata dell'operatore da parte di altri soggetti autorizzati è necessario avvertire l'incaricato che, quindi, provvederà a cambiare la propria password.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.
Tutte le regole dei punti 1 ÷ 10 non si applicano se i dati gestiti sono destinati alla diffusione (comunicazione a soggetti indiscriminati).
Naturalmente imprese di costruzioni, studi di ingegneria, architetti ed ingegneri liberi professionisti trattano molti dati personali che sono pubblici (ad es. dati relativi ad appalti pubblici, concessioni, ecc.): per essi non sono necessarie le cautele di cui sopra, ma è difficile pensare che tali dati siano registrati su sistemi distinti da quelli che trattano dati di altra natura.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
Il sistema di autorizzazione è necessario quando gli incaricati possono avere diversi profili di autorizzazione per l'accesso a diverse tipologie di dati. Questo significa che se alcuni incaricati hanno accesso alle anagrafiche del personale, ma non ai dati relativi alla contabilità del personale (paghe, malattie, ecc.) a cui sono autorizzati solo gli incaricati dell'ufficio personale, occorre predisporre un sistema di autorizzazione configurato in modo tale che ogni utente - dotato di proprio nome utente e password - possa accedere a determinati dati ma non ad altri.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
I profili utente devono essere configurati ed attivati, ovviamente prima di iniziare un determinato trattamento dati, in modo tale da consentire ad ogni utente - o gruppo di utenti con le medesime autorizzazioni - di accedere solo ai dati di cui necessita per espletare la propria attività e non a dati personali, sensibili o giudiziari aggiuntivi. Questa regola, interpretata alla lettera, è molto impegnativa da rispettare e coinvolge direttamente gli sviluppatori di sistemi informatici, in quanto oggi molti programmi software consentono la consultazione di dati di tipo personale in modo molto meno selettivo.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
La verifica della congruenza dei profili di autorizzazione deve essere fatta almeno annualmente, ma questa è solo

la misura minima! Una misura idonea deve comprendere una procedura che preveda la verifica delle autorizzazioni ogniqualvolta un utente del sistema informatico cambia incarico o lascia l'organizzazione. Tale attività è generalmente demandata al responsabile dei sistemi informativi in imprese di certe dimensioni e nelle grandi società di ingegneria, deve invece essere gestita con cura nelle piccole imprese e negli studi di progettazione non dotati di un vero responsabile del CED.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
Almeno una volta all'anno bisogna rivedere i profili di autorizzazione, ovvero "chi" ha accesso a "quali" dati, compresi i profili di System Administrator per coloro che sono addetti alla manutenzione dei sistemi informatici.
La lista degli incaricati - che dovrebbe essere documentata su supporto cartaceo o elettronico - può comprendere anche classi omogenee di incaricati - ad esempio Ufficio Personale, Ufficio Commerciale o altro - senza dettagliare i nominativi degli appartenenti all'ufficio/reparto, anche se tali nominativi dovrebbero comparire in qualche altro documento aziendale aggiornato (organigramma o lettere di incarico).
Questi aspetti vanno gestiti non solo a livello di sistema operativo di rete, ma anche per ogni singolo programma software (gestionale o applicativi specifici) che gestisce profili di autorizzazione.
Come per il comma 14 l'attività può essere più critica nelle piccole imprese e studi di ingegneria.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
L'Art. 615 - quinquies del C.P.P. - (Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico) cita: "*Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi un esso contenuti o a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire 20 milioni.* "
Dunque bisogna proteggersi da qualunque programma software che potrebbe danneggiare il nostro sistema informatico, ovvero dobbiamo dotarci di tutti i programmi anti-*malware* (dove *malware* è l'acronimo di "*malicious software*", termine denigrativo applicato al software che produce effetti nocivi, sia per dolo che per colpa dell'autore) che sono ritenuti necessari ed idonei. In questa categoria di programmi sono compresi non solo gli antivirus, ma anche i *firewall* (è un prodottohardware e software in grado di controllare lo scambio di comunicazioni tra una rete ad esso esterna, la zona non protetta, ed una rete ad esso interna, la zona protetta, in ambiente Internet) ed i programmi che rilevano ed eliminano altre forme di codice dannoso od in grado di alterare il corretto funzionamento dei sistemi informatici, quali *worm*, *trojans*, *data miner*, *spyware* (è un applicativo utilizzato per tenere sotto controllo le attività informatiche svolte dagli utenti del sistema informatico, in particolare via Internet).
In altre parole è possibile scaricare da internet - spesso involontariamente o, meglio, incoscientemente - codice software che ha lo scopo di raccogliere alcuni dati presenti sul nostro PC (numeri di carta di credito, altri dati personali, indirizzi di posta elettronica, siti consultati) per finalità spesso poco lecite, che vanno dalla vera e propria truffa all'invio di documenti a carattere pubblicitario "personalizzati" in base ai nostri gusti personali.
In altri casi tale codice software potrebbe giungere su nostro disco fisso a seguito di un vero e proprio attacco da parte di *hacker* che hanno sfruttato alcune vulnerabilità presenti nel nostro sistema.
Per evitare, o per lo meno limitare, ciò occorre installare ed utilizzare costantemente apposti programmi anti *spyware* e *firewall* (hardware o software). Mentre a mio giudizio la legge non obbliga l'utilizzo di programmi anti-*spamming*, vista anche l'efficacia, spesso non ottimale, di tali programmi; piuttosto è necessario avere comportamenti prudenti nell'attività legata ad internet (navigazione siti web e posta elettronica).
Ma se da un lato esistono applicativi *freeware* o *sharewa-re* che soddisfano discretamente la maggior parte delle esigenze, è altresì vero che tali programmi, se mal configurati, non ci proteggono da eventuali attacchi. Dunque è opportuno che vengano installati e configurati da personale esperto in materia: le piccole imprese e gli studi di ingegneria che non dispongono di personale qualificato al proprio interno farebbero bene a rivolgersi a consulenti qualificati.
È indispensabile prestare attenzione anche alla gestione dei cosiddetti "*cookie*" (piccole stringhe di testo che vengono scaricate sul PC e permettono al sito web di riconoscerci nelle navigazioni successive): molti di essi possono essere dannose per la privacy, ma altri invece sono necessari per usufruire di servizi utili presso alcuni siti web (ad es. internet/home banking). Sia i principali browser (Internet Explorer ed altri), sia appositi programmi di terze parti sono in grado di gestire lo scaricamento e la presenza dei *cookie* sul proprio PC, ma anche in questo caso occorre un briciolo di conoscenza della materia per impostare un livello di sicurezza adeguato alle nostre necessità e soprattutto efficace ed efficiente.
Riguardo all'aggiornamento di software antivirus ed anti-*malware*, la frequenza prevista dalla misura minima prevista dalla legge è da considerarsi non idonea alla maggior parte degli utenti professionali. In caso di danni provocati a terzi l'aggiornamento semestrale dell'antivirus non

potrà essere considerato, in sede giudiziaria, misura preventiva idonea, soprattutto se supportata da una perizia tecnica informatica della controparte. Il consiglio è comunque quello di aggiornare settimanalmente gli antivirus e ogniqualvolta vengono rilasciati gli aggiornamenti degli *antispyware* e dei *firewall* provvedere senza ulteriori indugi ad installarli.
La cadenza fissata dalla legge comunque riguarda essenzialmente l'aggiornamento delle definizioni dei virus e dell'elenco di altri codici software dannosi, non necessariamente *l'upgrade* alla *release* più recente del programma.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
Il suddetto comma si riferisce agli aggiornamenti del sistema operativo e dell'altro software di base finalizzati ad eliminare le nuove vulnerabilità scoperte ed in generale a correggere "bachi" nel funzionamento del software di base.
Anche qui non ci si riferisce all'aggiornamento delle versioni del sistema operativo (in realtà PC con Windows 98 sono ammissibili, con le limitazioni esposte in precedenza relativamente alle procedure di autenticazione), ma solo alle cosiddette "*patch*" rilasciate dal produttore per migliorare la sicurezza del sistema. Nel caso di Windows e di Microsoft è necessario usufruire del servizio di *Windows Update* ed installare tutti gli aggiornamenti critici per la sicurezza del sistema entro sei mesi dal rilascio (un anno se non si trattano dati sensibili o giudiziari). Questo significa che il recente *Service Pack 2* di Windows XP va scaricato (o meglio ordinato alla Microsoft per chi non possiede la banda larga) ed installato entro i prossimi sei mesi.
Come per altri adempimenti tecnici non tutto è così semplice: spesso gli aggiornamenti dei sistemi operativi presentano dei conflitti con altri programmi di utilità ed anche con i software utilizzati per la progettazione ingegneristica (CAD, programmi di calcolo strutturale, ecc.), occorrerà quindi possedere conoscenze adeguate ed un po' di tempo a disposizione per riuscire a cavarsela.
Pure in questo caso le "misure minime" potrebbero non essere quelle "idonee": nel lasso di tempo previsto dalla legge possiamo prenderci con una certa facilità virus come i famosi *Sasser* e *Blaster*, devastanti in termini di blocco dell'attività lavorativa e non solo… (pare infatti che possa essere stata opera di Blaster il grande blackput verificatosi negli Stati Unito lo scorso anno [3]). Infatti l'antivirus non sempre è sufficiente a proteggerci da programmi dannosi e spesso se ci siamo presi l'infezione occorre curarla con "terapie" diverse da quelle utili per prevenirla.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.
Le istruzioni per il backup dei dati devono essere descritte in una apposita istruzione scritta. La frequenza di backup è opportuno ridurla all'intervallo minimo che ci permetta di salvaguardare adeguatamente le attività lavorative svolte.
A parte gli adempimenti di legge, è opportuno valutare attentamente modalità, tecniche e frequenze di backup ([4]) per non subire lunghi tempi di blocco delle attività in caso di perdita di dati, con conseguenti costi e disservizi nei confronti dei clienti. Questo suggerimento vale per tutti, ma in particolare per chi – come un ingegnere progettista - mantiene il risultato di numerose ore di lavoro su di un unico PC.

Documento programmatico sulla sicurezza

19. 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:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. 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 e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, 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. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.
Il documento programmatico per la sicurezza, ormai comunemente denominato D.P.S. deve contenere - nel corpo dello stesso o nei suoi allegati - tutti gli argomenti sopra esposti. Il Garante ha reso disponibile sul suo sito (www.garanteprivacy.it) una Guida per la stesura del D.P.S., specialmente in realtà di piccole dimensioni.

Il suggerimento che qui si può dare è quello di strutturare il documento rendendone anche agevole il successivo aggiornamento (obbligatorio entro marzo di ogni anno), per esempio demandando ad appositi allegati le parti più frequentemente soggette a revisioni (ad es. l'elenco dei trattamenti di dati e la configurazioni dei sistemi informatici).
Occorre diffidare di facsimile di D.P.S "preconfezionati", esso non è solo un modulo da compilare con alcune informazioni, è un documento da costruire essendo ben consci della realtà in cui ci si trova. Esso deve contenere un'analisi dei rischi che sia non solo utile internamente all'organizzazione, ma anche che ci cauteli adeguatamente di fronte alla legge e nei confronti di chi eventualmente ci ha denunciato per presunti danni subiti.
Un D.P.S. che non sia stato redatto essendo ben consci di questi aspetti è facilmente attaccabile e sgretolabile da un buon Avvocato della controparte supportato da un bravo perito informatico.
Particolare cura nel garantire il rispetto del comma 19.7 deve essere portata da quelle organizzazioni che fanno un uso frequente di professionisti esterni per svolgere parte dell'attività principale della società, mi riferisco in particolare a studi di ingegneria ed organismi di ispezione nel settore costruzioni.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
Art. 615-ter C.P.P. - Accesso abusivo a un sistema informatico o telematico: «*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni….(omissis)*»
Per chi non lo avesse capito si parla esplicitamente di *hacker*.
Per i dati sensibili o giudiziari in particolare è necessario provvedere a dotare gli strumenti elettronici di adeguati sistemi di protezione. La presenza di *firewall* ben configurati potrebbe non essere sufficiente a garantire l'idoneità delle misure di sicurezza previste: un test di vulnerabilità eseguito e certificato secondo standard internazionali riconosciuti potrebbe fornirci la prova evidente che i dati sensibili e giudiziari sono adeguatamente protetti, soprattutto se l'organizzazione del titolare svolge attività critiche su grandi moli di dati sensibili o giudiziari.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
Occorre predisporre istruzioni scritte - ed illustrarle agli addetti al trattamento - circa l'utilizzo e la conservazione dei supporti rimovibili quali hard-disk esterni, CD-R/RW, DVD, Floppy Disk, chiavi USB, ecc..

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
Per i supporti rimovibili che hanno contenuto dati sensibili o giudiziari, se sono passati ad incaricati che non hanno le autorizzazioni all'accesso a tali dati occorre prevedere procedure di cancellazioni sicure attraverso appositi programmi. Infatti non è sufficiente cancellare i file attraverso il sistema operativo (ovvero svuotare il "cestino" di Windows) per renderli irrecuperabili. A maggior ragione chi utilizza frequentemente supporti rimovibili per trasferire file su altri PC, anche di altre organizzazioni, deve prestare grande attenzione a non lasciare incustoditi tali supporti anche se hanno contenuto, solo in passato, dati riservati. Per approfondimenti si veda [1] (capitolo 12).

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
A seguito di guasti del sistema, entro 7 giorni devo essere in grado di accedere ai dati personali. Sarebbe opportuno predisporre un buon piano di emergenza che descriva non solo "cosa" fare in caso di guasti, ma anche "come" farlo, ovvero con quale sequenza e quali responsabilità.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.
Per le organizzazioni che operano nel campo della sanità sono prescritte misure più restrittive per la protezione fisica e logica di dati sanitari, tra cui l'utilizzo di sistemi di crittografia in caso di trasferimento dati in formato elettronico.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

Le organizzazioni che adottano misure minime di sicurezza con il supporto di consulenti esterni (informatici e non solo) devono pretendere dal fornitore una dichiarazione di conformità alle disposizioni previste dal Codice per la protezione dei dati personali prima di attuare tali misure (cfr. [1] capitolo 15).
Sono comprese sia le attività di installazione e configurazione di software per la sicurezza (*antivirus*, *firewall*, ecc.) e hardware (sistemi di backup/recovery, firewall hardware, reti, ecc.), sia le consulenze organizzative sull'argomento.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.
La legge richiede che la redazione o l'aggiornamento del D.P.S. sia citata nella relazione che accompagna il bilancio di esercizio, ad ulteriore testimonianza dell'attività svolta ed assunzione di responsabilità da parte degli Amministratori della Società sull'argomento.
Anche se di semplice attuazione, il comma 26, rischia di essere spesso dimenticato se la privacy non viene gestita con consapevolezza in tutte le aree aziendali di competenza.
Circa il primo bilancio di riferimento in cui citare il D.P.S., dopo le ultime proroghe, è chiaramente quello del 2004 la cui approvazione avverrà nel 2005.
Ovviamente tale comma non si applica agli studi associati ed ai liberi professionisti che operano con partita IVA individuale che non sono tenuti alla redazione della relazione accompagnatoria del bilancio.

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
Per il trattamento dati su supporto non elettronico devono essere predisposte istruzioni scritte da distribuire agli incaricati riguardo al controllo ed alla custodia dei documenti contenenti dati personali.
Con frequenza annuale va revisionata la lista degli incaricati al trattamento e dei relativi profili di autorizzazione.
Le prescrizioni si applicano anche ai collaboratori esterni che trattano dati personali.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
È necessario evitare che personale diverso dagli incaricati autorizzati acceda a documenti contenenti dati personali sensibili o giudiziari attraverso una diligente custodia dei medesimi documenti da parte degli incaricati, interni ed esterni alla società o allo studio professionale.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.
Gli archivi contenenti dati sensibili o giudiziari devono essere ad accesso controllato, ovvero devono essere chiusi a chiave o comunque protetti da personale incaricato della loro vigilanza. Le persone che vi accedono devono essere preventivamente autorizzate dal responsabile della custodia dell'archivio e gli accessi devono essere registrati.
Per le imprese di costruzioni – ad esempio – il registro infortuni ed i dati relativi allo stato di salute del personale, nonché informazioni relative al casellario giudiziario, devono essere mantenute in armadi chiusi quando non sono direttamente sorvegliate dal personale incaricato del relativo trattamento.

3. CONCLUSIONI

È dunque necessario adeguarsi alle prescrizioni di legge non solo per evitare le pesanti sanzioni previste (in alcuni casi anche penali), ma anche per essere veramente tranquilli a fronte di perdita di dati accidentale o dovuta a fattori esterni (hacker, virus, ecc.) o interni (dipendenti o collaboratori disonesti che cancellano dati importanti e/o li sottraggono per scopi personali).

4. BIBLIOGRAFIA

[1] A. Biasiotti, "Codice della privacy e misure minime di sicurezza", II edizione, D.Lgs 196/2003 (Ed. EPC Libri S.r.l.– Roma, 2004)
[2] D. Tumietto, E. Garlaschelli, G. Ciancia, "Privacy – Un'opportunità per i professionisti" (Ed. Euroconference – Verona, 2004).
[3] A. Faenza, "Quando il virus esce dal computer spegne la rete e complica la vita" (ABC - Supplemento scientifico manageriale de "Il Domani di Bologna" del 26/10/2004, pag. 16)
[4] G.J. Cossu, "La gestione dei backup: piccole precauzioni…grandi vantaggi" (Rivista ICT Security n. 28, novembre 2004, pagg. 26 – 30)