" LE MISURE DI SICUREZZA OBBLIGATORIE PER IL TRATTAMENTO DEI DATI "

Prima di iniziare ad analizzare in concreto le singole misure di sicurezza richieste dalla nuova normativa, l'ormai noto testo unico 196 del 2003, meglio conosciuto come codice della privacy, bisogna necessariamente premettere cosa si debba intendere per "sicurezza".

Al di là delle definizioni normative, che poi vedremo, la sicurezza va intesa certamente come un processo ove nessuna soluzione è mai definitiva.

Il "processo sicurezza" è più di un semplice prodotto da acquistare ed installare e comprende sia un fattore materiale, tecnico, sia un fattore umano, che notoriamente costituisce l'anello debole della cd. *security chain*.

Solo partendo da questo necessario presupposto si può capire perché la sicurezza assoluta non esista: è infatti un processo che va gestito continuamente ed esistono solo livelli diversi di sicurezza, più o meno alti, che dovranno essere proporzionali all'importanza del bene da custodire.

Il legislatore, proprio per tali motivi, non può pretendere la sicurezza assoluta dei dati e dei sistemi ma, diversamente, può esigere l'adozione di tutto il complesso di misure tecniche, informatiche, organizzative e logistiche, tale da ridurre al minimo i rischi, graduando le diverse misure di sicurezza da adottare a seconda della tipologia del bene da tutelare.

Dopo queste doverose premesse iniziamo ad addentrarci nell'analisi del testo normativo.

Il Codice inizia a trattare il "problema" sicurezza al titolo V° della parte prima intestandolo "**SICUREZZA DEI DATI E DEI SISTEMI**".

Già da questa prima definizione si intuisce come questi siano i due ambiti entro i quali bisogna operare per ottenere quel livello di sicurezza richiesto dalla legge, che si

orienta appunto non solo verso i dati ma anche verso i sistemi di trattamento e conservazione degli stessi. A questi due ambiti si rivolgono le Misure Di Sicurezza.

La prima, e principale, distinzione operata dal legislatore è quella tra le cd. Misure minime e le cd. Misure idonee.

Le prime, le misure minime, a differenza delle seconde, sono a loro volta differenziate a seconda che il trattamento dei dati sia effettuato con o senza l'ausilio di strumenti elettronici, mentre per le seconde risulta indifferente la tipologia di trattamento.

Si rammenta che la materia è di stringente attualità posto che la mancata adozione delle citate misure di sicurezza può comportare sia una responsabilità penale che una responsabilità civile.

In particolare la mancata adozione delle Misure Minime, disciplinate e previste agli artt. da 33 a 36 del T.U. e, nella pratica, dall'allegato b) del Codice, comporta addirittura una responsabilità penale come espressamente previsto all'art. 169 T.U. .

La mancata adozione delle Misure Idonee, previste all'art. 31 del T.U., può comportare invece una responsabilità civile per danno da attività pericolosa, e conseguentemente il risarcimento dei danni ex. art.2050 c.c. (art.15 T.U.).

Vediamo ora la definizione che il codice dà di **MISURE MINIME DI SICUREZZA**:

Art. 4, c. 3, lett. a) – definizione: "*Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall'art. 31*" e cioè i rischi di distruzione o perdita (anche accidentale) dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

L'art. 33, invece, dispone l'obbligo di adozione delle citate misure da parte dei titolari del trattamento. (Art. 33 Misure minime: "*Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono*

comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali").

Come già detto il codice distingue tra:

- trattamenti con l'ausilio di strumenti elettronici (art.34), e
- trattamenti senza l'ausilio di strumenti elettronici (art.35)

riservando molta più attenzione alle misure di sicurezza relative alla prima delle due ipotesi, non foss'altro per la relativa novità della materia attinente alla sicurezza-informatica in ambito normativo.

Analizziamo pertanto quello che può considerarsi il cuore dell'intero sistema delle misure di sicurezza, quello appunto relativo al **TRATTAMENTO DEI DATI EFFETTUATO TRAMITE L'AUSILIO DI STRUMENTI ELETTRONICI**.

L'art.34 dispone che il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato b), tutte le misure minime ivi previste.

Le misure minime individuate dall'art.34 sono ben 8:

A - L'ADOZIONE DI UN SISTEMA DI AUTENTICAZIONE INFORMATICA

e la predisposizione di adeguate

B - PROCEDURE DI GESTIONE DELLE RELATIVE CREDENZIALI DI AUTENTICAZIONE

La definizione è nuova, ossia sconosciuta alla precedete normativa della L.675/96.

In sostanza si tratta di un sistema che dovrebbe garantire il controllo di chi accede agli elaboratori, verificando e convalidandone l'identità.

C - L'UTILIZZO DI UN SISTEMA DI AUTORIZZAZIONE

che, come vedremo dopo, si rende necessario quando per gli incaricati sono previsti profili di autorizzazione di ambito diverso. Ad esempio, al titolare dello studio sarà consentito il trattamento di tutti i dati archiviati mentre alla segretaria addetta esclusivamente alla contabilità di studio sarà certamente negato accedere ai dati idonei a rivelare lo stato di salute dei clienti dello studio.

In tale caso è quindi necessario predisporre un efficace sistema di autorizzazione differenziata rispetto alle diverse tipologie di dati trattati e, ovviamente, procedere alla corretta

D - INDIVIDUAZIONE DELL'AMBITO DI TRATTAMENTO CONSENTITO AI SINGOLI INCARICATI

e cioè del cd. *profilo di autorizzazione* dei singoli incaricati (e degli addetti alla gestione e manutenzione degli strumenti elettronici),

E AL SUO AGGIORNAMENTO PERIODICO .

Particolarmente significativa è anche l'indicazione contenuta nel successivo punto e) che prescrive la

E - PROTEZIONE DEGLI STRUMENTI ELETTRONICI E DEI DATI

Tale misura tende ad impedire che i dati siano trattati illecitamente, oppure che si verifichino accessi non consentiti o infine si verifichino altri danni ai dati causati dall'azione dei cd. *malware* (virus, worm, trojan horse o script maligni etc.).

Altrettanto importante è anche l'indicazione contenuta nel successivo punto f) che prescrive l'obbligatorietà di effettuare, almeno ogni settimana, delle

F - COPIE DI BACK-UP DEI DATI, PREDISPONENDO ALTRESI' APPOSITE PROCEDURE DI CUSTODIA,

e ciò per procedere al ripristino degli stessi in caso di perdita o danneggiamento.

Sul punto si precisa che, procedendosi negli studi legali al trattamento soprattutto di dati sensibili e giudiziari, è necessario anche adottare una procedura di *disaster recovery* (con la predisposizione di un adeguato *Disaster recovery plan*, e cioè non solo l'effettuazione di periodici *back-up* ma anche la predisposizione di un vero e proprio piano di ripristino dei dati con conseguente possibilità di accesso ed elaborazione degli stessi entro il termine massimo di 7 giorni dall'evento distruttivo.

Ulteriore misura minima prevista dal codice è l'obbligatoria

G - REDAZIONE E AGGIORNAMENTO DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA **(D.P.S.)**

Infine viene prescritta ma solo per organismi sanitari che trattino determinati dati sensibili la

H - ADOZIONE DI **TECNICHE DI CIFRATURA O DI CODICI IDENTIFICATIVI** che permettono di risalire agli interessati solo in caso di necessità.

* * * * *

Come già anticipato, tali 8 misure di sicurezza sono singolarmente analizzate, sotto il profilo delle modalità di attuazione, nel **DISCIPLINARE TECNICO** allegato al codice.

Il D.T. (Disciplinare Tecnico o Allegato B), riserva i primi 11 punti al sistema **di AUTENTICAZIONE INFORMATICA E alla GESTIONE DELLE CREDENZIALI**.

Inizialmente si precisano quali possano essere le credenziali di autenticazione da utilizzare.

Si parte dal classico **codice d'identificazione personale (user id) associato ad una password** passando per un **dispositivo autenticazione esclusivo** (del tipo smart card, token) **eventualmente associato ad un codice identificativo oppure ad una password** finendo poi ad un più sofisticato **dispositivo biometrico esclusivo (sempre eventualmente associato ad un codice identificativo oppure ad una password).**

Si precisa poi che ad ogni singolo incaricato possono essere **assegnate o associate una o piu' credenziali che dovranno essere diligentemente custodite e tenute segrete.**

I punti successivi del D.T. analizzano poi quelle che devono essere le caratteristiche delle credenziali utilizzate:

La password, ad es., deve essere:

1. composta da almeno 8 caratteri alfanumerici;
2. non contenere riferimenti agevolmente riconducibili all'interessato;
3. modificata al 1° utilizzo e poi almeno ogni 6 me si, che si riducono a 3 per il trattamento di dati sensibili o giudiziari.

Il codice per l'identificazione (il nome utente), non può essere riutilizzato dopo una prima assegnazione.

Le credenziali di autenticazione non utilizzate da almeno 6 mesi e quelle di un incaricato che non abbia più tale qualifica o la relativa facoltà, devono essere disattivate.

Si prevede inoltre che devono essere redatte preventivamente, e talune per iscritto, tutta una serie di **istruzioni**:

- per non lasciare incustodito l'elaboratore durante il trattamento (ad es. mediante l'adozione di uno screensaver associato ad una password)

- per consentire l'accesso all'elaboratore e/o ai dati qualora il singolo incaricato sia assente o impedito (ad es. conservando in busta chiusa e protetta copia della password degli incaricati, o il floppy/cd-rom di reimpostazione password o addirittura la copia fisica delle smart-card o dei token).

- per organizzare la custodia delle copie delle credenziali e individuare i relativi incaricati (ad es. in cassetti muniti di luchetto o, preferibilmente, nella cassaforte di studio).

Il D.T. riserva i successivi punti 12, 13 e 14 al **sistema di autorizzazione**.

Come già anticipato tale procedura si rende necessaria allorquando per gli incaricati (o per classi omogenee di incaricati) siano individuati profili di autorizzazione di ambito diverso in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento così come peraltro prevede il *principio di necessità* di cui all'art. 3 T.U. la cui ratio lascia intuire che ciascun incaricato abbia accesso solo ai dati allo stesso strettamente necessari.

Si prevede espressamente che almeno annualmente sia verificata la necessità di conservazione dei profili di autorizzazione e redatta la lista degli incaricati e addetti.

Il D.T. nei successivi punti 15, 16, 17 e 18 dà alcune specificazioni in merito all'applicazione delle **altre misure di sicurezza** dettate all'art.34.

E' stabilito principalmente un 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, prevedendo che la lista

degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

E' stabilita inoltre la **installazione di sistemi antivirus e firewall con aggiornamento periodico** almeno semestrale.

Tale misura appare francamente non tenere conto di quella che è la realtà: circa dodici nuovi virus vengono scoperti ogni giorno e oltre 50.000 virus sono già in circolazione. E allora che senso ha "consigliare" un aggiornamento dell'antivirus ogni sei mesi quando anche un puntualissimo aggiornamento quotidiano potrebbe non essere sufficiente?

Si sollecita pertanto un aggiornamento automatico del software o quantomeno quotidiano.

Sono previsti poi i necessari **aggiornamenti periodici dei software (patch) atti a correggere difetti o vulnerabilità dei software** con cadenza annuale o, in caso di dati sensibili e giudiziari, semestrale.

Anche tale misura appare poco legata alla realtà. Se si considera che per il più diffuso sistema operativo le patch rilasciate negli ultimi sei mesi sono decine (e la maggior parte per porre rimedio a gravissime falle di sicurezza) si può intuire come anche in tal caso sia necessario predisporre un aggiornamento automatico con verifica manuale almeno bisettimanale.

Si prevede, infine, **l'adozione di una procedura di back-up per il salvataggio dei dati** settimanale.

Il D.T. successivamente, al punto 19, affronta la problematica circa la **redazione e l'aggiornamento del documento programmatico sulla sicurezza.**

si stabilisce espressamente l'obbligo per il titolare di un trattamento di dati sensibili o di dati giudiziari di redigere un documento programmatico sulla sicurezza contenente informazioni circa:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte 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, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- 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;
- 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;
- 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;
- 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 D.T. successivamente, ai punti 20, 21, 22, 23 e 24 analizza le **ulteriori misure per il trattamento di dati sensibili e giudiziari**, prescrivendo in tale ipotesi l'utilizzo di un firewall o di altri **strumenti elettronici contro l'accesso abusivo**, la predisposizione di

istruzioni organizzative e tecniche per la custodia e l'uso di supporti rimovibili (floppy disk, cd-rom - memory card - hd estraibili - memorie zip) e per la **cancellazione** "sicura" dei dati dopo l'uso o, diversamente, per la loro **distruzione**; l'adozione, infine, di un **sistema di disaster recovery** per il recupero dei dati "*in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni*".

Infine, al punto 25 del D.T. il legislatore si occupa delle **misure di tutela e garanzia** prevedendo che **il titolare del trattamento dati, qualora adotti le misure minime di sicurezza avvalendosi di soggetti esterni,** dovrà tutelarsi anche nei confronti dell'installatore che è tenuto a rilasciare una descrizione scritta con la dichiarazione dell'intervento effettuato che ne attesti la conformità alle disposizioni del disciplinare.

*** * * * ***

Dopo tutti gli incombenti appena elencati, a taluni potrebbe sorgere il dubbio circa l'effettiva convenienza nell'utilizzo di sistemi elettronici per il trattamento dei dati.

Tale dubbio comunque non può che svanire rammentando come l'intera società si stia muovendo versa una informatizzazione dei trattamenti, con l'introduzione di talune procedure obbligatorie di comunicazione o notificazione digitale alla P.A. e con l'introduzione a breve (o almeno si spera) del processo telematico. Tali circostanze, ma non solo queste, impongono al professionista di sviluppare maggiormente le sue conoscenze informatiche e non certo di allontanarsene.

* * * * *

Analizziamo ora quali siano Misure di Sicurezza da predisporre per i **TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI**.

L'art. 35 T.U. dispone che tale trattamento è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

A) **AGGIORNAMENTO PERIODICO DELL'INDIVIDUAZIONE DELL'AMBITO DEL TRATTAMENTO** consentito ai singoli incaricati o alle unità organizzative;

B) previsione di **PROCEDURE PER UN'IDONEA CUSTODIA DI ATTI E DOCUMENTI AFFIDATI AGLI INCARICATI** per lo svolgimento dei relativi compiti;

C) previsione di **PROCEDURE PER LA CONSERVAZIONE DI DETERMINATI ATTI IN ARCHIVI AD ACCESSO SELEZIONATO** e disciplina delle **MODALITÀ DI ACCESSO** finalizzata all'identificazione degli incaricati.

Nel D.T. agli punti 27, 28 e 29 sono infine previste le istruzioni tecniche anche per tale modalità di trattamento.

Inizialmente si stabilisce che agli incaricati debbono essere impartite **istruzioni scritte finalizzate al controllo ed alla continua custodia degli atti e dei documenti** contenenti dati personali.

Similmente a quanto previsto per il trattamento effettuato con l'ausilio di elaboratori elettronici, anche in questo caso è previsto che la **lista degli incaricati** può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione e che va predisposto un documento con **l'individuazione dell'ambito del trattamento consentito** ai singoli incaricati, documento da aggiornarsi periodicamente con cadenza almeno annuale.

Si precisa poi che quando gli atti e i **documenti contenenti dati personali sensibili** o giudiziari vengono affidati agli incaricati per i relativi compiti, gli stessi debbono essere **controllati e custoditi fino alla restituzione** in maniera che ad essi non accedano persone prive di autorizzazione, e devono essere restituiti subito al termine delle operazioni affidate.

Si prevedono, infine, delle cautele anche circa i luoghi ove gli archivi sono localizzati. **l'accesso agli archivi contenenti dati sensibili o giudiziari dev'essere controllato**.

Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, debbono essere 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 devono essere state preventivamente autorizzate.

* * * * *

MISURE IDONEE DI SICUREZZA - ART.31 T.U.

In conclusione, come già detto all'inizio, oltre alle misure minime di sicurezza fin qui analizzate, il legislatore ha richiesto l'adozione delle cd. Misure Idonee di sicurezza, genericamente previste all'art. 31 T.U. che sono quelle misure, non analiticamente indicate dal legislatore, che devono, caso per caso, essere individuate dal titolare e/o responsabile del trattamento, anche in relazione alle conoscenze acquisite in base al progresso tecnico alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo i rischi per i dati (distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta). Si rammenta che la mancata adozione di tali ulteriori misure può comportare, in caso di danno all'interessato, una responsabilità civile ex art. 2050 c.c. con conseguente risarcimento dei danni, anche non patrimoniali stante l'espressa previsione operata dall'art.15 T.U. .

SCADENZE	
ENTRATA IN VIGORE CODICE	**01.01.2004**
MISURE MINIME NUOVE	**30.06.2004**
DPS	**31.03.2004** **30.06.2004 ***
ADEGUAMENTO TECNOLOGICO	**31.12.2004**

*** E' applicabile tale termine solo qualora tale misura sia da considerarsi a tutti gli effetti una misura di sicurezza "nuova" ex art. 180 T.U. .**
Sul punto vedasi, comunque, il Parere del Garante del 22/3/2004 al link http://www.interlex.it/675/tutela/p040322.htm e il relativo Comunicato stampa - 23/3/2004 http://www.interlex.it/675/tutela/c040323.htm .

MISURE DA ADOTTARE

1. Identificazione del titolare del trattamento
2. Nomina dei soggetti coinvolti nel trattamento:
   - Responsabile/i del trattamento (facoltativo)
   - Incaricato/i al trattamento
3. Individuazione ambito trattamento consentito ai singoli incaricati (o per classi omogenee).
4. Autorizzazione preventiva agli incaricati per accesso a locali archivio.

TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI

1. Utilizzo di un sistema autenticazione informatica;
2. Adozione di idonee credenziali di autenticazione;
3. Eventuale utilizzo di un sistema di autorizzazione;
4. Aggiornamento periodico dell'ambito di trattamento consentito;
5. Utilizzo di strumenti di protezione dei sistemi elettronici e dei dati;
6. Adozione di procedure per la custodia di copie di sicurezza;
7. Redazione del D.P.S.;
8. Adozione di tecniche di cifratura o di codici identificativi per trattamento dati idonei a rivelare stato di salute o vita sessuale.

TRATTAMENTI SENZA AUSILIO DI STRUMENTI ELETTRONICI

1. Aggiornamento periodico dell'ambito di trattamento consentito;
2. Adozione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
3. Adozione di procedure per accesso selezionato e identificazione degli incaricati negli archivi per la conservazione di determinati atti.