Garante per la protezione
dei dati personali

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti e del dott. Giovanni Buttarelli, segretario generale;

VISTO il d.P.R. 28 luglio 1999, n. 318, recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali a norma dell'art. 15, comma 2, della legge 31 dicembre 1996, n. 675;

RITENUTA la necessità di richiamare l'attenzione dei soggetti tenuti all'applicazione di tali misure sulle prescrizioni contenute nel medesimo d.P.R. e sulla prossima scadenza del 29 marzo 2000;

VISTA la documentazione in atti;

VISTE le osservazioni in atti formulate dall'ufficio ai sensi dell'art. 7, comma 2, lett. a), del d.P.R. n. 501/1998, con nota a firma del Segretario generale;

RELATORE l'Ing. Claudio Manganelli;

PREMESSO:

La legge 31 dicembre 1996, n. 675 nell'introdurre una complessa disciplina a tutela del trattamento dei dati personali, ha focalizzato la sua attenzione anche sugli aspetti relativi alla sicurezza nel trattamento dei dati.

Tale esigenza ha trovato attuazione nella Sezione III del Capo III della legge n. 675/1996, significativamente intitolata *"Sicurezza nel trattamento dei dati, limiti alla utilizzabilità dei dati e risarcimento del danno"*.

In detta sezione, all'articolo 15, comma 1, si afferma che "*i dati personali oggetto di trattamento devono essere custoditi e controllati, 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, mediante l'adozione di idonee e preventive misure di sicurezza, 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"*.

Nello stesso articolo, al comma 2, viene stabilito che le

misure minime di sicurezza da adottare in via preventiva sono individuate con regolamento emanato con decreto del Presidente della Repubblica e che esse sono adeguate successivamente, con cadenza almeno biennale, *"in relazione all'evoluzione tecnica del settore e all'esperienza maturata*". Inoltre, all'articolo 18, si prevede che *"chiunque cagioni danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento del danno ai sensi dell'articolo 2050 del codice civile"*.

L'intervenuta emanazione del citato regolamento (D.P.R. n. 318/1999), che va ad aggiungersi alle norme di legge sopra richiamate, ha gettato le basi per una più articolata disciplina della sicurezza specie nell'informatica e nella telematica, la cui importanza emerge anche dalla circostanza che le disposizioni dell'articolo 15 si applicano anche ai trattamenti pubblici in materia di polizia, giustizia, difesa e sicurezza dello Stato ai quali la legge n. 675/1996 si applica solo in parte (art. 4 legge n. 675/1996).

Un richiamo a quanto disposto dall'art. 15, commi 2 e 3, è poi esplicitamente contenuto nell'art. 17, comma 4, del d.lg. n. 135/1999, recante *"Disposizioni integrative della legge 31 dicembre 1996 n. 675, sul trattamento dei dati sensibili da parte di soggetti pubblici"*.

Ponendo attenzione al complessivo impianto normativo emerge con evidenza la finalità di ridurre al minimo i predetti rischi, mediante l'utilizzazione di sistemi di sicurezza costantemente adeguati nel tempo.

Il tipo di tutela che viene assicurato si sviluppa in due diversi aspetti: da un lato l'articolo 18 della legge n. 675/1996 prevede che chiunque (compresi il titolare, il responsabile (se designato) e gli incaricati) debbano risarcire gli eventuali danni ai sensi dell'articolo 2050 del codice civile. Dall'altro, la legge prevede l'individuazione di misure minime di sicurezza la cui mancata adozione comporta anche l'irrogazione di una sanzione penale. L'art. 36 della legge prevede infatti che la responsabilità sussista qualora non siano rispettati, anche in parte, gli standard "minimi" di sicurezza prescritti dal regolamento.

Si è, quindi, in presenza di una diversità sostanziale nella disciplina delle misure di sicurezza, indicata dallo stesso articolo 15 della legge n. 675/1996. Da un lato quelle previste al comma 1, destinate ad operare una costante riduzione del rischio, non individuate, ma individuabili sulla base di soluzioni tecniche concretamente disponibili (la cui

mancata predisposizione comporta responsabilità civile in caso di danno). Dall'altro, le misure "minime" previste al comma 2, specificamente individuate all'interno di un ulteriore atto (il regolamento), che contiene i vari precetti della norma contenuta nell'articolo 36, la cui violazione, come si è detto, comporta una sanzione di carattere penale.
Pertanto, il regolamento non è destinato a contenere tutte le regole tecniche da adottare in ogni caso per la sicurezza dei dati personali, in riferimento alle diverse modalità di trattamento utilizzate, e individua unicamente quei requisiti minimi il cui mancato rispetto comporta una maggiore esposizione a rischio del bene giuridico che la norma vuole tutelare.
Tale strumento è stato impostato in chiave di flessibilità, essendo destinato ad un aggiornamento avente cadenza biennale, all'evidente fine di evitare una sua oggettiva "staticità" a fronte di un evoluzione tecnologica per sua natura "dinamica". Il regolamento non intende quindi individuare le "migliori" misure evidenziate dalla scienza tecnica in un dato momento, mirando più semplicemente ad enucleare un minimo denominatore comune delle misure di sicurezza disponibili, tale da poter definire le stesse come "minime".
In ciò può essere pertanto meglio compresa la diversità esistente tra l'obbligo di "massima" riduzione del rischio previsto dal comma 1 (che impone un costante aggiornamento verso la migliore tecnica) e la diversa previsione di misure "minime" comuni a varie metodologie di trattamento dei dati (misure che sono anzitutto la condizione necessaria per l'applicazione dello strumento sanzionatorio avente natura penale).
In coerenza con la legge da cui promana, il regolamento previsto dalla legge n. 675/1996 si rivolge a tutti i soggetti - pubblici e privati - che nell'ambito delle loro attività pongono in essere un trattamento di dati personali.
Il Governo ha ritenuto pertanto necessario individuare categorie omogenee di modalità di trattamento di dati, al fine di correlare la soglia minima di sicurezza da un lato alla tipologia dei dati e, dall'altro, allo strumento tecnico utilizzato per l'elaborazione. Si è ritenuto peraltro di non poter prescindere dalla distinzione già operata dalla norma generale tra dati "comuni" e "sensibili" dovendosi tenere in debito conto la diversa valenza di questi ultimi nel quadro di una differente intensità del grado di tutela per essi previsto.

Una prima grande distinzione operata dal regolamento ha avuto riguardo alle modalità delle operazioni svolte per effettuare il trattamento: da una parte quelle effettuate in sostanza con l'ausilio di supporti cartacei, dall'altra quelle poste in essere anche in parte mediante strumenti elettronici o comunque automatizzati.

Tale ultima modalità è stata a sua volta distinta in ulteriori tre categorie:

a) trattamenti di dati personali mediante elaboratori non accessibili da altri elaboratori o terminali (art. 2 D.P.R. n. 318/1999);

b) trattamenti di dati personali effettuati mediante elaboratori accessibili in rete (artt. 3 e 7 D.P.R. n. 318/1999), categoria a sua volta distinta in:

- elaboratori accessibili da altri elaboratori solo attraverso reti non disponibili al pubblico (art. 3, comma 1, lett. a), D.P.R. n. 318/1999);
- elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico (art. 3, comma 1, lett. b), D.P.R. n. 318/1999);

c) trattamenti di dati personali effettuati per fini esclusivamente personali (ai sensi dell'articolo 3 della legge 675/1996) mediante elaboratori stabilmente accessibili da altri elaboratori.

Poiché l'ottica con cui sono state previste le singole misure di sicurezza è collegata non solo alla protezione dei sistemi o delle trasmissioni in quanto tali, ma, più direttamente nella protezione dei dati personali, il livello di sicurezza si modifica di conseguenza in relazione alla presenza o meno dei dati stessi. Così pure, nel caso siano contestualmente presenti dati "comuni e "sensibili", è necessario osservare le misure previste per la categoria più elevata.

Va evidenziato, inoltre, come nel regolamento il Governo abbia preferito non individuare per ogni singola misura di sicurezza i soggetti tenuti ad adottarla. Tale individuazione dipende quindi dalle attribuzioni del titolare del trattamento e dai ruoli e degli incarichi conferiti in concreto all'interno della relativa struttura.

Quanto alle definizioni, il regolamento, oltre ad utilizzare quelle già contenute nella legge 675/1996, prevede all'art. 1 quelle di:

"misure minime" intendendo per esse il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi a cui fa riferimento

l'articolo 15, comma 1, della legge (misure che possono ad esempio comportare, nei casi previsti nei successivi articoli: l'identificazione dell'utente, l'autorizzazione all'accesso alle funzioni, ai servizi, ai locali, ai dati e la registrazione degli ingressi, nonché limiti al riutilizzo di supporti per l'archiviazione elettronica o automatizzata o cartacea);
"strumenti", intendendo per essi i mezzi elettronici o comunque automatizzati con cui si effettua il trattamento;
"amministratori di sistema", riferendosi ai soggetti cui è conferito il compito di sovraintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

Quanto agli effetti che il regolamento spiega sui trattamenti effettuati a fini esclusivamente personali, l'articolo 3 della legge li eccettua, anzitutto, dall'osservanza di diversi obblighi normativi fissati dalla medesima legge, a condizione che i *"dati non siano destinati ad una comunicazione sistematica o alla diffusione"*. Nella seconda parte, però, la citata disposizione limita la portata di detta statuizione, disponendo che sono comunque applicabili gli articoli 15, comma 1, 18 e 36 della legge stessa, anche per ciò che riguarda, quindi, le misure minime di sicurezza.

Le peculiari caratteristiche ed i limiti di questo particolare tipo di trattamento, che la stessa norma generale considera come categoria a sé stante, hanno però reso opportuno prevedere misure di sicurezza che tenessero conto in misura adeguata il minore rischio insito in tale attività.

Considerato poi che anche alcune osservazioni formulate nella fase di predisposizione del regolamento sia dal Consiglio di Stato, sia dal Garante andavano nella direzione di limitare per quanto possibile l'ambito di applicazione della norma penale in materia di sicurezza, con l'intuibile intento di evitare un'applicazione irragionevole delle sanzioni, il Governo ha previsto la sua applicazione soltanto ai trattamenti effettuati mediante elaboratori accessibili da altri elaboratori, escludendo in tal modo vari computer e, in particolare quelli "*stand alone*". Per quelli caratterizzati invece dalla predetta accessibilità la misura minima di sicurezza è stata individuata nel solo obbligo per il soggetto titolare di utilizzare una parola chiave che inibisca l'accesso al sistema o anche solamente ai dati.

L'ultima parte del regolamento è dedicata al trattamento di dati effettuato mediante strumenti diversi da quelli elettronici o comunque automatizzati (artt. 9 e 10). Si tratta

di situazioni diffuse in cui la tenuta di dati è operata per mezzo di supporti cartacei come avviene, ad esempio, presso gli archivi (sia di privati, sia di pubbliche amministrazioni).

Anche in questo caso, nell'individuare le misure minime di sicurezza, il D.P.R. fa riferimento a cautele spesso già adottate di fatto. In proposito, sebbene la tenuta di archivi e l'individuazione dei soggetti che possono prendere conoscenza delle informazioni sia già disciplinata per alcuni uffici pubblici, il regolamento non ha portato ad estendere necessariamente quel tipo di misure, peraltro tipiche degli attuali modelli organizzativi del lavoro delle istituzioni pubbliche, anche ai privati.

E' stato previsto piuttosto che debbano essere osservate le seguenti modalità:

- nel designare per iscritto gli incaricati del trattamento e nell'impartire le istruzioni, il titolare o, se designato, il responsabile devono prescrivere che i soggetti designati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati (art. 9, comma 1, lett. a));
- gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni eseguite (art. 9, comma 1, lett. b)).

Nel caso invece l'attività riguardi dati di tipo "sensibile" o di natura giudiziaria, in aggiunta alle misure sopra descritte occorre prevedere che:

- se affidati agli incaricati, gli atti e i documenti concernenti i dati siano conservati, sino alla restituzione, in contenitori muniti di serratura;
- l'accesso agli archivi sia controllato e siano identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi.

Con queste modalità devono essere conservati anche i supporti cartacei contenenti la riproduzione di informazioni relative al trattamento dei dati di cui all'art. 22 e all'art. 24 della legge.

Con riferimento all'obbligo di predisporre le misure minime di sicurezza anteriormente all'inizio del trattamento, appare quindi opportuno richiamare l'attenzione degli operatori sulla circostanza che l'articolo 41, comma 3, della legge

675/1996 prevede, per l'effettiva e concreta adozione delle misure stesse, un termine di sei mesi decorrente dalla data di entrata in vigore del regolamento (29 settembre 1999) e che è pertanto fissato al 29 marzo 2000.

CIO' PREMESSO, IL GARANTE:

richiama l'attenzione di tutti i soggetti pubblici e privati tenuti al rispetto del d.P.R. n. 318/1999 sulle prescrizioni in esso contenute e sulle connesse sanzioni, nonché sulla prevista scadenza del 29 marzo 2000 prevista per l'applicazione delle misure minime di sicurezza.

Roma, li 29 febbraio 2000

IL PRESIDENTE

F.to Rodotà

IL RELATORE

F.to Manganelli

IL SEGRETARIO GENERALE

F.to Buttarelli