Pubblica amministrazione - Schema di regolamento in materia di individuazione delle misure di sicurezza minime per il trattamento dei dati person...

[doc. web n. 1106380]

Pubblica amministrazione - Schema di regolamento in materia di individuazione delle misure di sicurezza minime per il trattamento dei dati personali - 12 ottobre 1998

Il Garante ha rilasciato al Ministero di grazia e giustizia il parere richiesto dall´art. 15, comma 2 della legge n. 675/1996, sul regolamento per l´adozione delle misure minime di sicurezza, previste allo stesso art. 15.

Roma li, 12 ottobre 1998

Ministero di grazia e giustizia
Ufficio legislativo
Via Arenula, 71
00185 - *ROMA*

Oggetto: Schema di regolamento recante norme in materia di "Individuazione delle misure di sicurezza minime per il trattamento dei dati personali ai sensi dell´articolo 15, comma 2, della legge 31 dicembre 1996, n. 675"

Con la nota indicata a margine, il Ministero di grazia e giustizia ha trasmesso lo schema di regolamento in oggetto, chiedendo a questa Autorità di esprimere il parere previsto dall´art. 15, comma 2, della legge n. 75/1996.

Al riguardo, il Garante ritiene di formulare alcune osservazioni di ordine prevalentemente formale. 1. Il regolamento in esame attua la disciplina sulla sicurezza dei dati personali prevista dall´art. 15 della legge n. 675/1996, individuando modalità e misure "minime" che tutti i soggetti, pubblici e privati, devono rispettare quando raccolgono ed utilizzano tali informazioni.

L´individuazione di *standard* minimi per la sicurezza dei dati personali richiede una valutazione dei diversi aspetti del trattamento (finalità, tipologia dei dati, logiche di elaborazione, strumenti utilizzati, dimensioni della banca dati, ecc.) ed un attento bilanciamento tra la necessità di garantire una protezione minima delle informazioni personali e l´esigenza di calibrare le responsabilità penali che possono derivare dalla mancata adozione degli accorgimenti da prescrivere.

Le misure individuate dallo schema sono il risultato di una prima ricognizione normativa delle cautele basilari da seguire nel trattamento dei dati, che è soggetta ad adeguamenti

apportati con cadenza almeno biennale, in relazione "*all´evoluzione tecnica del settore e all´esperienza maturata*" (art. 15, comma 3, legge n. 675/1996). In una prospettiva di gradualità, si potrà quindi affrontare in maniera più analitica, nei successivi adeguamenti, il rapporto tra le misure minime di sicurezza e le dimensioni, le caratteristiche e la vulnerabilità delle banche dati.

Come precisato nella relazione illustrativa dello schema, resta ferma la netta distinzione tra il piano della responsabilità penale (cui è legato il regolamento in esame) e quello della responsabilità civile. Le misure di sicurezza rilevanti sotto quest´ultimo profilo non sono, infatti, quelle "minime" individuate nel regolamento, ma quelle più efficaci che in relazione alle conoscenze acquisite devono garantire la riduzione al minimo del rischio di una distruzione o perdita accidentale dei dati, di un accesso non autorizzato o di un trattamento non consentito o non conforme alle finalità della raccolta.

Deve poi osservarsi preliminarmente che:

lo schema individua le misure minime senza indicare i soggetti tenuti ad adottarle. La soluzione è stata probabilmente prescelta per semplificare l´articolato sul piano della tecnica normativa, e può essere condivisa apparendo chiaro che i diversi soggetti che trattano i dati (titolare, responsabile e incaricati del trattamento) saranno tenuti ad adottare e ad esigere il rispetto delle misure minime a seconda della loro sfera di attribuzioni e di compiti nell´ambito della struttura presso la quale operano. Questa circostanza potrebbe essere oggetto di una breve precisazione nella relazione illustrativa;

analoga precisazione potrebbe essere fatta rispetto alle diverse espressioni tecniche utilizzate nello schema e non definite nell´art. 1 (si pensi, in particolare, alle espressioni: *risorse del sistema operativo di un elaboratore, sistema di base dati, applicazione, codice di identificazione personale, parola chiave, incaricati della manutenzione*, ecc.; si pensi, inoltre, alla nozione di *elaboratore*, particolarmente rilevante ai fini dell´applicazione dell´art. 8 dello schema regolamentare). Si potrebbe dare atto nella relazione che tali espressioni devono ritenersi utilizzate e interpretabili nel senso ormai pacifico nella disciplina dell´informatica;

appare opportuno evidenziare nella relazione illustrativa che le diverse disposizioni del regolamento relative agli incaricati del trattamento richiamano in maniera più precisa l´attenzione del titolare e del responsabile sulla necessità di rispettare l´obbligo, già insito nella legge n. 675/1996 (art. 19), di permettere l´accesso "interno" ai dati alle sole persone fisiche incaricate del relativo trattamento. In difetto dell´incarico scritto di cui agli artt. 8, comma 5 e 19 della legge n. 675/1996, infatti, tali persone dovrebbero essere considerate come soggetti estranei ("terzi") ai fini dell´applicazione della legge stessa e, in particolare, delle disposizioni sulla comunicazione dei dati.

Art. 1

Nel comma 1, lettera a), si suggerisce di inserire le parole: "*di cui ai successivi articoli del presente regolamento*" dopo le parole: "procedurali di sicurezza", eliminando le ulteriori parole che figurano dopo: "*rischi previsti dall´art. 15, comma 1, della legge*,". La variazione appare opportuna in quanto l´attuale elenco delle modalità di attuazione delle misure potrebbe risultare poco chiaro (quando si parla di "*accesso alle funzioni, ai servizi*, ... ") ed incompleto (manca, ad esempio, un riferimento all´utilizzo della parola chiave e ad altre misure specifiche).

Si suggerisce poi:

di sostituire nella lettera b) (e in altri parti dello schema) la parola "*strumenti*" con la parola "mezzi", che è utilizzata nella legge n. 675;

di utilizzare al plurale la definizione di "*amministratore di sistema*", per simmetria con le altre

definizioni e con l´art. 4.

Art. 2

È condivisibile la scelta - armonica con la legge n. 675- di accomunare da un lato i trattamenti svolti anche in parte con mezzi elettronici o automatizzati (artt. da 2 a 7) e, dall´altro, quelli eseguiti con mezzi non elettronici o non automatizzati (artt. 9 e 10). Va però constatato che gli artt. da 2 a 7, malgrado l´intitolazione del Capo II menzioni sia i mezzi elettronici, sia quelli automatizzati, si riferisce in concreto solo ai primi, in quanto gli articoli riguardano soltanto i trattamenti attraverso "elaboratori" . Mantenendo nella sostanza l´attuale ripartizione dei capi e delle sezioni, appare quindi necessario integrare il capo II con disposizioni specifiche o generali applicabili anche ai trattamenti con mezzi elettrici o automatizzati per i quali, altrimenti, non sarebbero previste "misure minime".

La prima parte del comma 1 dell´art. 2 prescrive che le misure ivi previste siano adottate " *anteriormente all´inizio del trattamento*". E´ opportuno, al riguardo, precisare nella relazione illustrativa che resta implicito il termine transitorio di sei mesi previsto dall´art. 41, comma 4, della legge n. 675.

Alla lettera a), occorre aggiungere dopo le parole: "*l´accesso ai dati*" le seguenti: "*o al sistema*", per uniformare la disposizione all´art. 8.

Va infine valutata l´opportunità di prevedere una o più misure aggiuntive per i dati sensibili, selezionandone alcune nell´ambito di quelle che gli articoli 5, 6 e 7 prevedono per gli elaboratori accessibili in rete.

Art. 4

Nel comma 1, appare opportuno spostare l´inciso "*oltre a quanto previsto dall´art. 2*" dopo le parole: "*di cui all´articolo 3*". Si potrebbe inoltre sostituire nel titolo la parola "strumenti" con " *elaboratori*".

Nella lettera b), si suggerisce di sostituire le parole: "in caso di perdita della qualità che ne consentiva l´accesso all´elaboratore" con le parole: "*in caso di perdita della qualità soggettiva che consentiva l´accesso all´elaboratore*".

Infine, al comma 2, occorre inserire dopo le parole: "si applicano ai" le seguenti: "*trattamenti dei*" .

Art. 5

Occorre perfezionare sul piano formale il collegamento tra la prima parte del comma 1 ("... *l´accesso... è determinato sulla base di autorizzazioni assegnate... agli incaricati*... ") e la seconda (... "*nonché... agli strumenti*... "). Si potrebbe mettere un punto dopo la parola "manutenzione", riformulando il secondo periodo come segue: "*Se il trattamento è effettuato ai sensi dell´articolo 3, comma 1, lettera b), l´autorizzazione è riferita anche agli strumenti che possono essere utilizzati per l´interconnessione mediante reti disponibili al pubblico*".

Nel comma 6, è opportuno inserire dopo le parole: "codice identificativo personale" le parole: "di cui all´articolo 4".

Il comma 7 dovrebbe essere modificato come il comma 2 dell´art. 4, mettendo poi in cifra ("1") la parola "uno".

Art. 6

Andrebbe valutata la possibilità di estendere l´obbligo di redazione del documento informatico anche alle realtà più complesse che ricadono nella previsione di cui all´art. 3, comma 1, lett. a), che si avvicinano, per natura dei rischi, a quelle indicate alla lett. b) del medesimo articolo.

Nella prima parte del comma 1, appare opportuno sostituire la parola "*con*" con "*mediante*" e la parola "*periodicità* " con "*cadenza*" (per simmetria con il comma 2), inserendo una virgola dopo la parola "*aggiornato*".

Nella lettera a), sarebbe opportuno sostituire le parole: "*rilevanti ai fini delle*" con "*interessate dalle* ".

Nella lettera c), potrebbero poi eliminarsi le parole "*per via telematica*" che figurano alla fine della lettera, in quanto ripetitive del concetto espresso nella medesima lettera.

Art. 8

L´art. 8 si applica ai soli trattamenti per fini personali effettuati con elaboratori non accessibili da altri elaboratori e, quindi, già contiene un´opportuna selezione, nell´ambito di tali trattamenti, di quelli che sono soggetti all´obbligo, sanzionato penalmente, dell´adozione di misure minime di sicurezza (sono esclusi dall´applicazione della disposizione gli indirizzari e gli elenchi telefonici ad uso personale tenuti in forma cartacea o nelle c.d. agendine elettroniche). Tuttavia, proprio al fine di ridurre al minimo le possibilità di applicare sanzioni penali nei confronti di trattamenti che non presentano particolari rischi per i diritti degli interessati, si propone di rendere obbligatorio l´utilizzo della parola chiave per i soli trattamenti riguardanti dati sensibili organizzati in banche dati. A tal fine, è opportuno inserire: dopo le parole "*esclusivamente personali*" le seguenti "*dei dati di cui agli articoli 22 e 24 della legge*" e dopo le parole "*non accessibili*" la seguente "*stabilmente*", nonché, alla fine, aggiungere dopo "*parola chiave*" e prima del punto il seguente inciso:, "*qualora i dati siano organizzati in banche di dati*".

Art. 9

Nella lettera a) del comma 1, dopo la parola "*titolare*", si dovrebbe infine sostituire la "*e*" con "*o*".

Nella lettera a) del comma 2, aggiungere dopo le parole "*altri dispositivi equipollenti*" la seguente frase: "*salvo che ciò non sia tecnicamente possibile per le speciali modalità dell´attività cui è legato il trattamento, indicate preventivamente per iscritto dal titolare o, se designato, dal responsabile*".

Il Garante resta a disposizione per ogni ulteriore chiarimento o contributo utile.

IL PRESIDENTE