Documento Programmatico Per La Sicurezza

Luca M. De Grazia

Senza alcuna pretesa di essere l'unico "portatore della verità", vorrei tentare di analizzare brevemente le questioni riportate nel titolo dell'articolo, cogliendo l'occasione per esprimere qualche considerazione c.d. "de jure condendo", ma solamente da un punto di vista – spero – di tecnica di analisi giuridica.

I) D.P.S.

Partendo dal dlgs n.196/2003, vediamo quali sono le premesse che esso pone per quanto concerne l'ambito di applicazione delle misure minime di sicurezza. Infatti, occorre ricordare preliminarmente:

- che le definizioni di legge applicabili sono le seguenti:

a) "*trattamento*", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

b) "*dato personale*", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

d) "*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) "*titolare*", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

f) "*responsabile*", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

g) "*incaricati*", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

h) "*interessato*", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

- che ai fini delle redazione del DPS, previsto dagli artt. 31[1] e 33 – 34 - 35[2] del Dlgs n.196/2003 TU sulla privacy) è necessario, quanto meno, rispettare quanto imposto dagli articoli appena citati.

---

[1] Art. 31 - Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono 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.

[2] Art. 35

Trattamenti senza l'ausilio di strumenti elettronici

1. Il trattamento di dati personali effettuato **senza l'ausilio di strumenti elettronici** 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;

L'articolo sembra porre le basi giuridiche per l'obbligo di adozione delle misure di sicurezza, "*minime*" per evitare la sanzione penale di "omessa adozione", "*adeguate*" per evitare le conseguenze del trattamento dati come parificato all'esercizio di attività pericolosa, ex art. 15 [3] TU

L'articolo 33 [4] del TU chiarisce, al comma primo, che i «titolari» "*sono comunque tenuti ad adottare le misure minime individuate nel presente capo"*, ovvero quelle previste dal Titolo V Capo I; l'art. 34 [5] specifica – a propria volta - le misure di sicurezza da adottare quando il trattamento dati è "***effettuato con strumenti elettronici"…"*** *nei modi previsti dal disciplinare tecnico contenuto nell'allegato B)" …" le seguenti misure minime*".

Orbene, **sia la struttura giuridica** stessa del TU (testo di legge ed allegato tecnico, quindi norma di rango inferiore rispetto al testo di legge, come specificato dall'art.36 del TU il quale testualmente recita: - *Adeguamento - Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore*), **sia la semantica della lingua** utilizzata, non possono avere altro significato che: "*Se il trattamento è effettuato con strumenti elettronici devono essere adottate tutte le misure minime previste dalle lettere da (a) a (g), con le modalità previste dal disciplinare tecnico"*.

Tanto è vero che alla lettera (a), per esempio, si parla di "autenticazione informatica", mentre nel disciplinare viene specificato cosa sia tale procedura, così come per le credenziali di autenticazione, e così via.

La lettera (g) dell'art.34 appare – a parere di chi scrive - molto chiara:
una delle misure minime di sicurezza è la redazione del D.P.S., così come le "ulteriori" misure minime di sicurezza previste dai punti successivi al 19 del disciplinare si applicano "solamente" se

---

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.

d)

[3] Art. 15 - Danni cagionati per effetto del trattamento

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

[4] Art. 33

Misure minime

1. 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.

[5] Art. 34

Trattamenti con strumenti elettronici

1. 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), le seguenti misure minime:

a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

i)

si trattano dati sensibili (a prescindere dalla considerazione che, data l'estensione della definizione di dato sensibile, appare difficile individuare un soggetto che tratti dati personali e neppure "un" dato sensibile, anche se non è una situazione impossibile da realizzare).

Passiamo, a questo punto, all'analisi del disciplinare tecnico.

Il punto 19 del disciplinare medesimo mi sembra che possa essere ricondotto nell'alveo della norma generale, semplicemente leggendo esattamente cosa vi sia scritto: "*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..:"*.

Viene solamente posta una scadenza "fissa" per la redazione del DPS da parte di chi tratti "dati sensibili o giudiziari", mentre per le categorie di soggetti che - eventualmente - non trattino dati di questo tipo – la cadenza rimane annuale ma senza una data fissa per la compilazione.

In pratica persiste di fatto la disciplina esistente in precedenza (L.675/96 e DPR 318/99). Oggettivamente, la norma – di carattere secondario rispetto al?tu?– non mi sembra che possa essere letta in contrasto con quanto scritto negli articoli sopra specificati, ma può utilmente e coerentemente essere letta solamente come:

(a) la specificazione di cosa debba contenere il D.P.S. e come
(b) integrazione della norma generale per quanto concerne la scadenza della redazione (per inciso, la proroga al 30.06.2004 concerne solamente le misure di sicurezza NON previste dal 318/99, e non quelle che dovevano esistere anche prima, e conseguentemente – a stretto rigore – non si dovrebbe applicare alla pura e semplice redazione del D.P.S., anche se si potrebbe obiettare che, essendo mutato il contenuto obbligatorio del DPS, il medesimo possa rientrare nelle misure di sicurezza la cui implementazione possa essere "prorogata" sino al 30.06.2004).

Il documento programmatico sulla sicurezza, come dal punto 19 dell'allegato B, disciplinare tecnico per le misure di sicurezza, deve contenere:

19.1. l'elenco dei trattamenti di dati personali [6];
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.

[6] A mio parere si tratta di indicare esattamente i "trattamenti", e non le tipologie di trattamento, per cui ne consegue che occorra previamente effettuare un analitico censimento dei trattamenti esistenti presso la struttura interessata.

Conseguentemente, l'organizzazione logica e la sequenza delle attività da compiere dovrebbe essere la seguente:

A) Le misure minime di sicurezza devono essere adottate anteriormente all'inizio di un trattamento effettuato con strumenti elettronici (tralascio per ora i trattamenti NON effettuati con strumenti elettronici)
B) Le misure minime devono essere adottate sempre e comunque dal titolare, nella accezione ora meglio specificata dal TU
C) Le misure minime devono essere poste in essere non solamente dal titolare, ma anche dal responsabile e dagli incaricati del trattamento, i soli soggetti - persone fisiche che siano per legge abilitati al trattamento dei dati;
D) Le misure minime sono quelle indicate dagli artt.33, 34 e 35 del TU. Le modalità di implementazione delle misure minime sono descritte nel disciplinare tecnico, che a partire dal punto 20 disciplina le "ulteriori" misure minime da adottare in caso di trattamento di dati sensibili.