Il "Decreto Semplificazioni" e le modifiche al Codice della privacy: conseguenze pratiche della eliminazione dell'obbligo di redazione del Documento Programmatico sulla Sicurezza.

di:
Prof. Avv. Alessandro del Ninno
Studio Legale Tonucci & Partners
adelninno@tonucci.com

Indice

---

§ 1. Introduzione

Il Codice della privacy, dopo le rilevanti modifiche apportate dal c.d. "decreto salva-Italia" dello scorso 6 Dicembre 2011, è stato oggetto di rinnovato interesse da parte del Legislatore. Nell'ambito di un intervento normativo organico del Governo volto a semplificare numerosi adempimenti previsti in vari settori dell'ordinamento giuridico – difatti - il decreto legge 9 Febbraio 2012, n. 5 (pubblicato nella G.U. del 9 Febbraio 2012, n. 33, Supplemento n. 27) – noto come "Decreto Semplificazioni" – ha anche previsto all'articolo 45 la eliminazione dell'obbligo di "*tenuta di un aggiornato documento programmatico sulla sicurezza*" [(prima disposto dall'art. 34, comma 1, lettera (g) del Codice della privacy]. Coerentemente con la eliminazione di tale obbligo normativo generale, il decreto procede altresì sia alla abrogazione delle modalità operative con le quali tale documento doveva essere redatto e aggiornato (previste nell'Allegato B al Codice della privacy – "*Disciplinare Tecnico in materia di misure minime di sicurezza*" - dal punto 19 al punto 19.8 e al punto 26), sia alla abrogazione della diversa norma (l'art. 34, comma 1-*bis* del Codice della privacy) che – mediante un precedente intervento normativo di semplificazione parziale – aveva già sostituito l'obbligo di adottare il Documento Programmatico sulla Sicurezza ("DPS")

con una autocertificazione resa dal titolare del trattamento, in presenza di determinati presupposti, ed avente ad oggetto l'avvenuta adozione delle misure minime di sicurezza che il DPS aveva appunto il compito di certificare e documentare.

Obiettivo di questo articolo è dunque quello di analizzare in primo luogo in cosa consistono le semplificazioni introdotte per poi valutare le conseguenze concrete di tali modifiche, con la finalità di evidenziarne la portata applicativa pratica.

* * * *

§ 2. Inquadramento del DPS nel più generale ambito di obbligo di adozione delle misure di sicurezza nei trattamenti di dati personali.

Prima di analizzare quali siano in concreto gli effetti dell'ultima semplificazione introdotta al Codice della privacy (e dunque comprenderne anche le conseguenze sul piano pratico), appare opportuno ricordare sinteticamente in che cosa consistesse l'obbligo di "*tenuta di un aggiornato documento programmatico sulla sicurezza*". E per far ciò, occorre inquadrare l'obbligo ora abrogato nell'ambito del più generale panorama delle prescrizioni imposte ai titolari dal Codice della privacy di adottare le misure di sicurezza nei trattamenti di dati personali.

Il corollario delle garanzie normative del diritto alla riservatezza è difatti rappresentato dall'obbligo per i titolari o responsabili (se designati) del trattamento di adottare opportune misure di sicurezza nei trattamenti, dal punto di vista logico, organizzativo, fisico e tecnico, per impedire che le garanzie di legge vengano vanificate dall'assenza di misure specifiche in ordine alla sicurezza del trattamento dei dati personali. In particolare, gli articoli 31 e 33 del Codice della privacy prevedono l'obbligo di adottare misure preventive di sicurezza dei trattamenti distinguendo due diversi livelli:

a) le misure di sicurezza "*idonee*", di cui all'articolo 31, co. 1, il cui scopo è quello di ridurre al minimo i rischi per la sicurezza dei dati (pericolo di distruzione o perdita accidentale dei dati, di accesso non autorizzato, etc.);
b) le misure di sicurezza "*minime*", di cui all'articolo 33, come meglio individuate dal Disciplinare Tecnico in materia di misure minime di sicurezza - Allegato B al Codice della privacy.

La differenza tra misure di sicurezza *idonee* e misure di sicurezza *minime* (entrambi da adottare *preventivamente*, secondo il dettato normativo) sta in quanto segue. Le misure di sicurezza idonee comportano per il titolare il duplice obbligo di custodia e di controllo dei dati personali in modo da ridurre al minimo (dunque non è richiesto – anche perché non sarebbe possibile – di eliminare del tutto) 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. Tuttavia, è il concetto stesso di "idoneità" di tali misure che può variare: l'idoneità, cioè, va rapportata alle conoscenze acquisite in base al progresso tecnico (quindi, se determinate misure di sicurezza possono essere considerate idonee in una certa fase, è possibile che non lo siano più se successivamente il progresso tecnico garantisce più elevati livelli di sicurezza), alla natura dei dati (ad esempio, la necessità di livelli di sicurezza idonei per il trattamento di dati sanitari è sicuramente maggiore rispetto agli standard che sarebbe necessario adottare per il trattamento di dati personali comuni), alle specifiche caratteristiche del trattamento. In conclusione, il concetto giuridico di "idoneità" delle misure di sicurezza va individuato *per relationem* tenendo presente i criteri sopra descritti, che sono per loro natura variabili.

D'altra parte, le misure di sicurezza "minime" individuate dall'articolo 33 del Codice della privacy e – con riferimento alle modalità esecutive – dal Disciplinare Tecnico (che ha assorbito, aggiornato ed abrogato il previgente d.p.r. 28.7.1999 n. 318 recante il regolamento sulle misure minime di sicurezza) rappresentano una base fissa di principi in materia di sicurezza dei trattamenti dei dati personali ai quali i titolari, responsabili (se nominati) ed incaricati del trattamento devono conformarsi essendo ovviamente liberi di adottare – come spesso sarebbe opportuno - anche standard di sicurezza più elevati rispetto a quelli normativi "minimi" richiesti dal Codice della privacy.

La disciplina in materia di misure minime di sicurezza contenuta nel Codice della privacy prevede alcune regole di carattere generale (artt. da 33 a 36) che sono appositamente specificate – anche dal punto di vista tecnico – nel Disciplinare Tecnico. L'adozione delle misure minime di sicurezza è un obbligo che grava in ogni caso su tutti i titolari di trattamenti di dati personali (sia nel caso di trattamenti manuali o cartacei sia nel caso di trattamenti svolti con l'ausilio di strumenti elettronici) e rappresenta una piattaforma per rendere conformi tali trattamenti alle prescrizioni normative volte a garantire un livello minimo di protezione dei dati personali.

L'adozione delle misure minime di sicurezza (definite dall'art. 4, co. 3, lett. a) del Codice della privacy come "*il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il*

livello minimo di protezione richiesto in relazione ai rischi di distruzione o perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta") richiede diversi adempimenti in rapporto alla tipologia di trattamento dei dati effettuato (se manuale o svolto con l'ausilio di strumenti elettronici). Difatti, secondo quanto previsto dall'articolo 34 del Codice della privacy, il trattamento di dati personali effettuato con strumenti elettronici (cioè mediante elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento) è consentito solo se sono adottate, nei modi previsti dal Disciplinare Tecnico contenuto nell'Allegato B) del Codice, le seguenti misure minime:

(a) autenticazione informatica (l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità: cfr. art. 4, co. 3, lett. c) del Codice della privacy);

(b) adozione di procedure di gestione delle credenziali di autenticazione (per "credenziali di autenticazione" l'art. 4, co. 3, lett. d) del Codice della privacy intende " *i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica*");

(c) utilizzazione di un sistema di autorizzazione (per "sistema di autorizzazione" l'art. 4, co. 3, lett. g) del Codice della privacy intende "*l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente*");

(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.

Come già si intuisce dalla mera lettura dell'elenco di misure minime di sicurezza previsto all'art. 34 del Codice della privacy, sarebbe gravemente erroneo ritenere che il Decreto Semplificazioni abbia totalmente eliminato l'obbligo per i titolari di adottare le misure di sicurezza nei trattamenti (sia minime che – soprattutto – idonee): il decreto, con l'abrogazione

della sola lettera (g) del comma 1 dell'art. 34 del Codice della privacy, ha semplicemente eliminato il mero obbligo di documentare l'adozione di quelle minime, adozione che era e resta obbligatoria, come restano in vigore le relative, dettagliate modalità tecniche ed esecutive previste ai punti da 1 a 18, da 20 a 25 e da 27 a 29 del Disciplinate Tecnico – Allegato B al Codice.

D'altro canto, ai sensi del successivo articolo 35 del Codice della privacy, il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, sempre nei modi previsti dal Disciplinare Tecnico, 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.

E anche tali misure di sicurezza non sono state interessate dal Decreto Semplificazioni.

§ 3. Che cosa era il Documento Programmatico sulla Sicurezza.

Va in primo luogo chiarito che la redazione del Documento Programmatico sulla Sicurezza gravava solamente sui titolari che trattano con strumenti elettronici dati sensibili (tassativamente ed esclusivamente 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*") o giudiziari (cioè i dati personali idonei a rivelare situazioni e/o qualità dell'interessato nel solo ambito penale, come i dati dei provvedimenti iscritti nel casellario giudiziale, nella anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato). Dunque tale obbligo non è mai sussistito per i titolari di trattamenti di dati personali diversi da quelli sensibili e/o giudiziari oppure per i titolari che trattano dati sensibili o giudiziari ma non con l'ausilio di strumenti elettronici, ad esempio in modalità manuale e cartacea.

Il DPS doveva descrivere in maniera completa tutte le misure minime di sicurezza poste in essere dal titolare di trattamenti di dati personali sensibili o giudiziari con strumenti elettronici. Tale documento:

(a) doveva essere redatto dal titolare o dal responsabile del trattamento a ciò delegato (se designato) e – solo laddove fossero intervenute modifiche soggettive od oggettive nelle politiche sulla sicurezza dei trattamenti - doveva essere aggiornato ogni anno entro il 31 marzo di ogni anno (punto n. 19 – ora abrogato – del Disciplinare Tecnico – Allegato B al Codice della privacy);

(b) solo in caso ai sensi del codice civile fosse stata richiesta per particolari categorie di titolari del trattamento la redazione della relazione accompagnatoria del bilancio di esercizio, doveva essere riferito in tale relazione dell'avvenuta redazione od eventuale aggiornamento del DPS (punto n. 26 – ora abrogato – del Disciplinare Tecnico – Allegato B al Codice della privacy);

(c) il DPS non doveva essere inviato al Garante, ma trattenuto presso il titolare del trattamento ed esibito in caso di eventuali controlli;

(d) non era richiesto che il DPS avesse data certa (nonostante una vera e propria "leggenda metropolitana" – del tutto infondata - circa l'obbligo di data certa del DPS, a causa di una errata quanto diffusa comprensione degli obblighi posti dall'art. 180, comma 2, del Codice della privacy).

Per quanto riguarda le modalità operative della sua adozione, non era richiesto – ad esempio presso aziende private – che il DPS fosse formalmente adottato con delibera del Consiglio di Amministrazione, anche se poteva comunque apparire opportuno seguire procedure interne di formale adozione (ad esempio, deliberare negli appositi organi l'adozione della versione finale del DPS, sottoscritta per approvazione sia dai rappresentanti legali del titolare del trattamento che da tutti quelli che – a vario titolo – avessero collaborato alla sua stesura).

Con riferimento al contenuto del DPS, esso doveva contenere:

L'elenco dei trattamenti dei dati personali (punto n. 19.1 – ora abrogato – del Disciplinare Tecnico – Allegato B al Codice della privacy). Andavano cioè indicati tutti i trattamenti svolti, inclusa la descrizione degli eventuali database, delle modalità con cui i dati vengono trattati, delle applicazioni utilizzate nei trattamenti, delle modalità di archiviazione e conservazione dei dati, delle finalità dei trattamenti, degli ambiti di comunicazione dei dati personali (cioè i soggetti ai quali vengono messi a disposizione i dati), dei profili di autorizzazione degli incaricati.

La distribuzione dei compiti e delle responsabilità (punto n. 19.2 – ora abrogato – del Disciplinare Tecnico – Allegato B al Codice della privacy). Andava cioè descritto come il titolare provvede alla gestione del sistema di autenticazione, del sistema di autorizzazione, dei sistemi antivirus e di

quelli anti-intrusione, del sistema di *backup/restore*, le procedure di aggiornamento del DPS.

L'analisi dei rischi che incombono sui dati (punto n. 19.3 – ora abrogato – del Disciplinare Tecnico – Allegato B al Codice della privacy). In tale importante parte del DPS il titolare doveva descrivere in dettaglio un elenco dei rischi inerenti la sicurezza dei dati preventivamente individuati e delle possibili conseguenze in termini di: 1) distruzione o perdita dei dati; 2) accesso non autorizzato alle informazioni o esecuzione di trattamenti non autorizzati; 3) indisponibilità dei sistemi; 4) presenza di informazioni errate.

Dopo aver descritto i rischi il titolare doveva procedere ad elencare le contromisure che, per ogni rischio individuato, erano poste in essere come misura di protezione, tenendo conto che le misure possono essere graduate per classi di dati, e che la medesima misura può avere effetto su rischi diversi.

Le misure da adottare per garantire l'integrità e la disponibilità dei dati e la protezione delle aree e dei locali rilevanti ai fini della loro custodia ed accessibilità (punto n. 19.4 – ora abrogato – del Disciplinare Tecnico – Allegato B al Codice della privacy). In tale parte del DPS andavano descritti ad opera del titolare i criteri adottati per garantire integrità e disponibilità dei dati, quali sistemi di autenticazione ed autorizzazione sono implementati presso l'organizzazione, quali sistemi antivirus e anti-intrusione informatica sono in uso, quali sono le procedure di sviluppo e avviamento di nuove applicazioni software, come avviene la gestione degli aggiornamenti dei programmi, come sono organizzati gli archivi degli utenti, quali misure sono poste in essere per la protezione delle aree e dei locali (generali o relative ai locali informatici, es i centri di elaborazione dei dati), quali procedura di vigilanza e controllo accessi ai locali sono in essere, quali misure antiincendio sono adottate dal titolare.

La descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati (punto n. 19.5 – ora abrogato – del Disciplinare Tecnico – Allegato B al Codice della privacy). In tale parte del DPS andavano descritti quali sistemi di *back-up* dei dati sono in uso presso l'organizzazione, che tipo di dispositivi per le copie di sicurezza sono adottati, come sono protetti gli archivi, come operano i sistemi per il ripristino della disponibilità dei dati, quale è la frequenza delle relative procedure di *back-up* e ripristino dei dati, con quali modalità il titolare o responsabile verificano le relative procedure ed attività, quali strumenti per la segnalazione di errori sono in uso presso la struttura del titolare, quali sistemi assicurano la continuità dell'alimentazione degli apparati, quali piani di *disaster recovery* sono eventualmente previsti dall'azienda in caso di "*crashdown*" dei sistemi.

La previsione degli interventi formativi (punto n. 19.6 – ora abrogato – del Disciplinare Tecnico – Allegato B al Codice della privacy). Il Disciplinare tecnico prevedeva appositi interventi formativi organizzati dal titolare o responsabile (se designato) del trattamento per gli incaricati del trattamen-

to, al fine di 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 doveva essere programmata già al momento dell'ingresso in servizio del singolo incaricato, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali. In tale ottica, il relativo paragrafo del DPS doveva contenere una descrizione delle iniziative formative – appositamente documentate - al riguardo previste all'interno dell'organizzazione aziendale.

La descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza dei dati affidati all'esterno della struttura del titolare (punto n. 19.7 – ora abrogato – del Disciplinare Tecnico – Allegato B al Codice della privacy). Tale parte del DPS poteva contenere, a titolo esemplificativo: 1) una descrizione delle specifiche finalità, modalità, ed ambiti di comunicazione autorizzati per il trattamento ad opera di soggetti esterni alla struttura del titolare cui i dati sono affidati; 2) una dichiarazione dell'ente esterno a cui vengono affidati i dati di adozione delle misure di sicurezza; 3) copia del Documento Programmatico del soggetto esterno, se dovuto o comunque disponibile; 4) piani di controllo, se disponibili, relativi alla vigilanza sulle attività del soggetto esterno.

I criteri di cifratura o separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale (punto n. 19.8 – ora abrogato – del Disciplinare Tecnico – Allegato B al Codice della privacy). Il Disciplinare Tecnico prevedeva infine che il DPS, per i soli dati personali idonei a rivelare lo stato di salute e la vita sessuale (dunque non per tutti i dati sensibili, nella cui categoria tali dati pure rientrano) trattati da organismi sanitari o dagli esercenti le professioni sanitarie (dunque solo da queste categorie di titolari) e contenuti in elenchi, registri o banche di dati elettroniche, individuasse i criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato. In sostanza, con la cifratura i dati sono archiviati utilizzando criteri di criptazione che ne rendono impossibile la lettura ai soggetti non autorizzati, mentre con la separazione i dati sensibili sono memorizzati unicamente in archivi ad accesso limitato a cui – utilizzando i profili di autorizzazione – possono avere accesso solo i soggetti abilitati. Il DPS doveva dunque descrivere, in tale parte, i relativi adempimenti.

§ 4. Cosa cambia con il Decreto Semplificazioni e l'abolizione dell'obbligo di adozione del Documento Programmatico sulla Sicurezza.

A questo punto, occorre analizzare e valutare l'impatto pratico derivante dalla eliminazione dell'obbligo di adottare, conservare ed eventual-

mente aggiornare il DPS nell'ottica dei titolari del trattamento e delle loro scelte in materia di politiche del trattamento dei dati.

La formulazione delle norme di cui all'art. 45 del Decreto Semplificazioni non lascia d'altra parte spazio ad alcun esercizio interpretativo: l'obbligo è semplicemente eliminato. Tale scelta del Legislatore (nel corso degli anni più volte auspicata da molte categorie di titolari, che da sempre hanno ravvisato nel DPS un adempimento burocratico e costoso, tanto che alcune stime economiche degli effetti dell'abrogazione parlano di un risparmio di circa 500 milioni di Euro per i titolari del trattamento) comporta però una serie di rischi a livello di percezione presso le categorie interessate di cosa effettivamente comporti l'eliminazione del DPS.

E' su tali rischi che si intende nel prosieguo soffermare la nostra riflessione.

Un primo aspetto, come già segnalato, riguarda il rischio che la semplificazione introdotta sia percepita come comportante la totale eliminazione degli obblighi normativi che – invece – impongono anche dopo il Decreto Semplificazioni di adottare scrupolosamente le misure di sicurezza (sia minime che idonee) previste agli articoli da 31 a 35 del Codice della privacy.

Ciascun titolare del trattamento dovrebbe poi ricordare che l'omessa adozione delle misure di sicurezza nei trattamenti (pur essendo venuto meno l'obbligo specifico di documentare quelle minime) resta pesantemente sanzionata dal Codice della privacy, sia in sede amministrativa che penale:

a) all'art. 162, comma 2-*bis*, che prevede che in caso di trattamento di dati personali effettuato in violazione delle misure indicate nell'articolo 33 è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da diecimila euro a centoventimila euro, essendo in tali ipotesi è escluso il pagamento in misura ridotta;
b) all'art. 164-*bis*, che prevede che in caso di più violazioni di un'unica o di più disposizioni (ad esempio prescritte in materia di misure minime di sicurezza dall'art. 33 come richiamato dall'art. 162 del Codice della privacy), commesse anche in tempi diversi in relazione a banche di dati di particolare rilevanza o dimensioni, si applica la sanzione amministrativa del pagamento di una somma da cinquantamila euro a trecentomila euro, non essendo ammesso in tali casi il pagamento in misura ridotta (tra l'altro, lo stesso articolo prevede che in altri casi di maggiore gravità e, in particolare, di maggiore ri-

levanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi interessati, i limiti minimo e massimo delle sanzioni sono applicati in misura pari al doppio e possono essere aumentate fino al quadruplo quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore);

c) all'art. 169, che prevede che chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni (salvo il meccanismo di oblazione previsto al secondo comma dell'art. 169).

Un secondo aspetto attiene invece alla più generale domanda circa la convenienza effettiva della eliminazione del Documento Programmatico sulla Sicurezza. L'obbligo di redazione del DPS fin dall'inizio è stato valutato solo come appesantimento burocratico, invenzione tutta italiana non prevista né nella Direttiva comunitaria del 1995 né nelle legislazioni *privacy* nazionali dei principali Paesi UE. Ciò ha impedito però di scorgere gli effettivi benefici pratici che da un tale documento derivano, pur se vissuto come oneroso adempimento. Si intende cioè dire che fin dall'inizio l'obbligo di redazione del DPS non avrebbe dovuto essere vissuto dai titolari di trattamenti di dati personali come un adempimento relativo (solo) alla *privacy*, adempimento da evitare - ove possibile – per risparmiare inutili costi. In questo approccio miope si è sempre dimenticato da parte di molti che la tematica della "sicurezza delle informazioni" non è una tematica solo *privacy*, ma attiene alle esigenze ben più ampie della sicurezza di impresa, inclusa la sicurezza delle informazioni e dei dati, irrinunciabili beni primari della Società dell'Informazione e dei mercati globalizzati.

Avere cioè un documento che – pur previsto da una normativa specifica come il Codice della privacy - consentiva comunque una sorta di "fotografia" complessiva sempre aggiornata delle *security policies* applicate da ciascun titolare del trattamento alle informazioni e dati aziendali, una sorta di "*check-list*" dei rischi per la sicurezza delle informazioni e delle correlative soluzioni implementate, non doveva apparire affatto come inutile appesantimento burocratico, ma piuttosto come efficace strumento di gestione e tutela presso ogni struttura privata o pubblica di beni immateriali fondamentali (anche dal punto di vista economico) come i dati e le informazioni.

In sostanza, i titolari del trattamento avrebbero dovuto correttamente ritenere il DPS uno strumento da adottare nel loro stesso interesse, da sviluppare a far crescere nel tempo a livello di completezza di struttura e contenuti. E ciò prima ancora che come adempimento richiesto da una normativa ritenuta burocratica e generatrice di costi.

Dal 9 Febbraio 2012, invece, l'obbligo di redazione del DPS (o della autocertificazione sostitutiva) non esiste più e molti ancora plaudono ad una sorta di "liberazione" da lacci e lacciuoli burocratici ed al risparmio di costi inutili.

Ma quanto potrà effettivamente costare ai titolari del trattamento l'assenza di una organizzazione documentale interna contenente linee-guida sulla sicurezza delle proprie informazioni, sui rischi, sulle contromisure?

Quali costi per la sicurezza comporterà, ad esempio, affidare i trattamenti elettronici di dati sensibili o giudiziari ad incaricati privi di ogni formazione, se ad oggi non è più vigente il relativo obbligo prima previsto dal punto 19.6 del Disciplinare Tecnico come da documentare nel DPS?

Che responsabilizzazione dei fornitori esterni si ottiene (e quali garanzie sui dati) con questa ultima semplificazione quando non c'è più l'obbligo per il titolare del trattamento di documentare – come prevedeva il punto 19.7 - i criteri per garantire l'adozione delle misure minime di sicurezza dei dati affidati all'esterno della struttura del titolare?

E ancora, come reagiranno quegli stessi titolari quando in sede di accertamento ispettivo da parte del Garante per la privacy la verifica sulla adozione delle misure minime di sicurezza nei trattamenti (verifica resa prima facilitata e a volte anche più spedita dalla mera consegna in copia del DPS per quei soggetti tenuti a redigerlo) passerà attraverso lunghe e approfondite analisi ed accessi tecnici a sistemi e infrastrutture?

Sono solo alcune delle molteplici domande che sorgono solo se ci si avvicina senza impostazioni preconcette e con completezza di prospettive alla semplificazione che è stata oggetto di analisi in questo articolo. Forse, sono le stesse domande che si sono posti avveduti titolari del trattamento che - indipendentemente dall'art. 45 del Decreto Semplificazioni – si stanno sempre più numerosi rispondendo in maniera lungimirante con la scelta di continuare comunque ad adottare (magari chiamandolo in un altro modo) un documento non più obbligatorio ma di indubbia utilità per la gestione delle proprie politiche di sicurezza a garanzia dei loro dati e informazioni.