PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4186 di Mercoledì 28 febbraio 2018

Un prezioso aiuto per i responsabili del trattamento dati

Una norma per aiutare i professionisti della sicurezza e della protezione dei dati nello sviluppare la valutazione d'impatto sulla protezione dei dati: la ISO/IEC 29134:2017.

Ricordo ai lettori che chiunque tratta dati personali deve effettuare delle valutazioni sulle modalità con cui gli applicativi informatici trattano i dati stessi. Queste valutazioni si articolano in due fasi:

- una fase obbligatoria, prevista per qualsiasi tipo di trattamento, descritta all'articolo 25 del regolamento generale europeo, dal titolo "protezione dei dati fin dalla progettazione e protezione per impostazione predefinita",
- una fase, che è invece obbligatoria solo in relazione a determinati trattamenti, descritta l'articolo 35 del regolamento generale europeo dal titolo "valutazione d'impatto sulla protezione dei dati".

Orbene, in Italia nessuno mai ha fatto nessuna di queste due tipologie di valutazione del trattamento e ciò indubbiamente pone i nostri responsabili del trattamento in una posizione relativamente difficile, rispetto ai vari colleghi, che operano in altri paesi europei, dove queste due tipologie di valutazione di rischio sono state effettuate già da molti anni.

Non per nulla, i pochi responsabili del trattamento italiani che hanno già affrontato questo tema hanno dovuto far riferimento a documentazioni disponibili all'estero, in assenza di qualsiasi studio specifico disponibile in Italia, ed in lingua italiana!

Tralascio l'esame della valutazione del trattamento, di cui all'articolo 25 del regolamento, e concentro la mia attenzione e quella dei lettori sulla valutazione di impatto, prevista dall'articolo 35.

Come accennato, questa valutazione deve essere sviluppata soltanto quando il tipo di trattamento, per varie ragioni, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Ad esempio, quando si usano nuove tecnologie, si vogliono sviluppare nuove finalità di trattamento ed altro, è obbligatorio sviluppare questa valutazione di impatto.

Un prezioso documento dell'articolo 29 Working party ancora una volta ha studiato a fondo questo argomento ed ha offerto preziose indicazioni su quali siano i tipi di trattamento per i quali è obbligatorio sviluppare una valutazione di impatto. Tra quelli che sono più diffusi in Italia e per i quali occorre sviluppare una valutazione di impatto, si trova la sorveglianza sistematica su larga scala di una zona accessibile al pubblico. Ciò significa che i grandi centri commerciali, i comuni dotati di impianti di videosorveglianza, aeroporti, stazioni ferroviarie, porti, autostrade ed altri contesti in cui sono presenti impianti di videosorveglianza di dimensioni significative, debbono necessariamente sviluppare una valutazione di impatto.

Un fattore di democrazia che mi ha colpito positivamente è illustrato poi nel comma 8, laddove si richiede che il responsabile o il titolare del trattamento interpellino perfino gli incaricati coinvolti, per sapere se a loro giudizio il trattamento che si intende attivare possa essere troppo invasivo.

Ricordo ancora brevemente che, ove si abbiano dubbi circa il fatto che sia obbligatorio o meno sviluppare una valutazione di impatto, in corrispondenza di uno specifico trattamento, il titolare può rivolgersi all'autorità garante, secondo le modalità illustrate nell'articolo 36-consultazione preventiva.

Supponiamo quindi di essere giunti alla determinazione che la valutazione di impatto debba essere sviluppata.

Come accennato, una sintesi dei punti principali che devono essere presenti a valutazione di impatto è già illustrata nel regolamento, ma evidentemente si tratta solo di un punto di partenza che deve essere approfondito dal titolare e dal responsabile del trattamento.

Il responsabile della protezione dei dati, se designato, provvederà poi a effettuare una accurata analisi della valutazione di impatto sviluppata dai due soggetti appena menzionati ed avanzerà eventuali proposte migliorative.

Esaminiamo adesso il contenuto di questa norma, che risulta praticamente indispensabile per i professionisti della protezione dei dati, in Italia, proprio per la loro assoluta mancanza di esperienza specifica, maturata negli anni precedenti.

Tanto per cominciare, la norma come di consueto introduce le norme di riferimento ed un glossario, nonché un elenco di termini abbreviati, purtroppo sempre più frequenti in contesti anglosassoni.

La norma quindi prende per mano chi dovrà sviluppare una valutazione di impatto, illustrandogli quali sono i benefici di questo studio, come deve essere impostato il rapporto finale e a chi vanno attribuite le responsabilità nello sviluppare questa valutazione di impatto.

È bene ricordare, a proposito, che anche se il regolamento dà delle prescrizioni, arricchite dal parere dell'articolo 29 Working party, sui trattamenti per i quali è indispensabile sviluppare una valutazione di impatto, atteggiamenti prudenziali possono consigliare di svilupparla comunque, anche se non strettamente necessaria. Non v'è dubbio che una valutazione di impatto costituisca sempre un elemento prezioso di riferimento, per tutti coloro che sono coinvolti nel trattamento di dati piuttosto critici.

Tanto per cominciare, gli estensori della norma raccomandano che la valutazione non sia sviluppata da una persona sola, ma venga costituita una squadra in cui ogni componente può dare il proprio contributo.

Successivamente si deve presentare al titolare del trattamento un piano con costi e tempistica, in modo da avere un punto di riferimento approvato prima di procedere.

Si passano quindi a descrivere le aree critiche da esaminare, si esamina il profilo di tutti i soggetti coinvolti, in particolare gli interessati, si identificano i dati personali coinvolti, si analizza l'implicazione del trattamento di questi dati, si determinano i requisiti primari di salvaguardia dei dati, si effettua una valutazione del rischio legato al trattamento e si prepara un programma di messa sotto controllo dei rischi.

A questo punto sono disponibili tutti gli elementi per preparare una bozza di rapporto che, se approvato, permette di passare alla seconda fase, vale a dire all'attuazione delle misure di messa sotto controllo proposte. Come al solito, si tratta di un processo iterativo che deve essere costantemente aggiornato.

Vediamo adesso come è composto il rapporto di valutazione di impatto.

Dopo una introduzione generale, si illustra la struttura del rapporto, illustrando l'obiettivo della valutazione di impatto, elencando i processi che sono stati valutati, i criteri adottati per valutare i rischi, le risorse ed i profili professionali coinvolti, nonchè i risultati della consultazione di altri soggetti coinvolti, come ad esempio gli interessati.

Si passa quindi alla valutazione di rischio vera e propria, elencando i rischi, sia in termini di natura del rischio, sia in termini di probabilità e di conseguenze, in modo da attribuire una classificazione ad ogni singolo rischio. A questo punto si illustrano le modalità con cui il rischio viene messo sotto controllo (ben 114 misure di sicurezza, elencate nella norma ISO/IEC 27100) e si tirano le decisioni finali.

Di particolare interesse sono gli annessi, che aiutano ad inquadrare correttamente i rischi, secondo quanto previsto dalla norma ISO 31000. Per ogni rischio viene indicata la frequenza e l'impatto, in modo da attribuire un livello specifico. Sono identificati 50 rischi, ma la scala di valutazione si ferma a 4 livelli, anziché i 5 della norma ISO 31000 (si toglie il livello catastrofico-livello 5).

Un secondo annesso prende in considerazione alcune tipologie di minacce e, ancora più importante, nel quarto annesso viene offerta una traccia di come dovrebbe essere impostato l'intero rapporto.

In sintesi, siamo davanti ad una norma che è preziosa per molti ed indispensabile per i professionisti italiani!

Adalberto Biasiotti