PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4189 di Lunedì 05 marzo 2018

Come si applicano le sanzioni del regolamento europeo sui dati personali?

Il regolamento generale europeo in materia di protezione dei dati si applica nello stesso modo in tutti i paesi europei. I criteri che le varie autorità garanti potrebbero adottare, in caso di applicazione di sanzioni, possono essere diversi?

Le istituzioni europee, che hanno elaborato il nuovo regolamento 679/2016, ormai avevano imparato la lezione: per convincere i cittadini europei ad obbedire alle leggi, il bastone è molto più efficace della carota! Basandosi su questa filosofia, il nuovo regolamento generale ha stabilito delle sanzioni estremamente elevate, che aggiungono 1 o 2 zeri alle sanzioni che finora sono state applicate dai vari Garanti, con modalità completamente diverse da paese a paese. Era legittimo quindi il timore delle autorità europee che una situazione del genere potesse portare ad una differenza di atteggiamento e comportamento dei vari titolari del trattamento, a seconda del paese in cui essi operano.

Anche se il regolamento ha stabilito i livelli delle sanzioni, i criteri con le quali esse devono essere applicate potrebbero variare da paese a paese ed ecco perché un'interpretazione autentica è stata da varie parti capeggiata ed è stata adesso pubblicata.

Ricordo ai lettori quali sono i principi fondamentali che regolano la applicazione e determinazione di sanzioni per violazioni di disposizioni del regolamento, in materia di dati personali:

- la violazione del regolamento deve portare all'applicazione di "sanzioni equivalenti",
- le sanzioni amministrative debbono essere effettive, proporzionate e dissuasive,
- le sanzioni da applicare devono essere determinate caso per caso, senza automatismi.

Sono questi i tre principi fondamentali che guidano le autorità Garanti dei vari paesi nell'applicazione di sanzioni.

Tralascio, almeno per il momento, il fatto che il regolamento concede alle autorità Garanti nazionali di applicare anche sanzioni di natura penale, che non sono previste nel regolamento generale.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[USBGDPR] ?#>

Il concetto di "sanzioni equivalenti" fa evidentemente riferimento al fatto che per una analoga violazione le sanzioni applicate in un paese devono essere uguali a quella applicate in un altro paese.

Per quanto riguarda il primo punto, ricordo ai lettori che con il nuovo regolamento è entrato in vigore il cosiddetto one stop shop, vale a dire le decisioni assunte da un'autorità Garante si applicano allo stesso modo anche in altri paesi. Ove vi sia

disuniformità di vedute fra il Garante di un paese che quello di un altro paese, si ricorre al comitato europeo per la protezione dati personali, che garantisce la funzione di congruità e coerenza.

Il concetto di completa indipendenza, che è sottolineato nel regolamento, nei confronti dell'autorità Garante nazionale, vale quindi nei confronti dei legislatori, e non nei confronti di autorità Garanti di altri paesi.

Per quanto riguarda il secondo principio, al momento non sono disponibili nelle regole generali, e quindi bisognerà attendere alcune pronunzie, per poter capire quando una sanzione sia realmente conforme al principio elencato in questo punto.

Ciò che mi interessa sottolineare, e che il regolamento ben evidenzia, è il valore dissuasivo. In Italia sappiamo tutti benissimo che molti titolari di trattamento pagano senza battere ciglio le sanzioni applicate dall'autorità Garante, perché la violazione, cui le sanzioni si riferiscono, ha portato ad incassi di un paio di ordini di grandezza superiori all'importo della sanzione! È questa una situazione inaccettabile ed ecco perché in alcuni casi il regolamento non prevede neppure un limite assoluto alla sanzione, ma la esprime come percentuale del fatturato annuo del titolare coinvolto.

Infine, esaminiamo le modalità con cui l'autorità garante nazionale determina se e quale sanzione deve essere applicata.

Viene sottolineato il fatto che ogni applicazione di sanzioni deve essere determinata alla fine di uno specifico ed individuale processo di valutazione, senza adottare modelli standardizzati.

Ad esempio, il nostro codice della strada prevede che il divieto di sosta venga sanzionato con un certo importo. Facendo un parallelo con una situazione simile, nel mondo della protezione dati personali, l'autorità Garante dovrà non solo costatare se è stato un parcheggio in zona proibita, ma anche tutte le altre circostanze al contorno, come ad esempio il fatto che il parcheggio potesse costituire un pericolo per le altre autovetture, che potesse intralciare il movimento di altri mezzi, che il mezzo non fosse ben visibile di notte, che il mezzo avesse un colore chiaro che lo rendeva comunque visibile, oppure un colore scuro che lo rendeva meno visibile e via dicendo.

E' bene tenere presente che non sempre, in caso di violazione, è indispensabile applicare una sanzione: il regolamento prevede anche numerosi altri schemi correttivi, che possono indurre il titolare ad un comportamento più appropriato. Ecco perché una reprimenda è, in certi casi, accettabile, invece dell'applicazione pura e semplice della sanzione.

Appare evidente l'intento delle autorità europee di utilizzare le sanzioni come strumento non solo punitivo, ma educativo, ed ecco perché potrebbe essere possibile che la sanzione si articoli in una parte economica ed in una parte basata su indicazioni specifiche, che il titolare del trattamento dovrà adottare, in tempi e modi indicati dall'autorità Garante.

Ho già accennato in precedenza alla armonizzazione delle sanzioni, che potrà essere raggiunta scambiando informazioni tra le varie autorità Garanti e, in caso di contenzioso, rivolgendosi al comitato europeo per la protezione dei dati, che potrà dare un parere vincolante, almeno nel caso specifico, per tutti i paesi coinvolti.

Un altro aspetto molto interessante, che riguarda l'analisi delle violazioni caso per caso, è esplorato nei cosiddetti "considerando", che costituiscono premessa al regolamento.

È evidente che il comportamento delle autorità Garanti, nel valutare una violazione causata da un virus ignoto, che improvvisamente è apparso sullo scenario mondiale, oppure quella causata da una protratta negligenza del titolare, magari già messo in guardia in precedenza dai suoi collaboratori, dovrà essere completamente diverso.

Un altro elemento che influenza in maniera significativa la gravità della violazione, e quindi la gravità della sanzione, è il numero degli interessati coinvolti.

Violazioni sistematiche evidentemente vanno valutate in modo diverso, rispetto a violazioni occasionali.

Un altro elemento che l'autorità Garante deve prendere considerazione riguarda la durata della violazione. Se la durata si è prolungata per il fatto che il titolare non ha adottato tempestivamente misure correttive, appare evidente che la situazione merita una sanzione più elevata, come pure la merita una situazione nella quale erano già noti gli strumenti, che potevano mettere sotto controllo una potenziale violazione, e il titolare non aveva ancora adottati

Conclusioni

Sulla base delle considerazioni offerte in precedenza, appare evidente che l'autorità Garante dovrà sviluppare dei processi di valutazione molto più articolati ed approfonditi, rispetto a quelli attuali, per giungere alla determinazione di applicare una sanzione amministrativa o altre misure, meno rilevanti sul piano economico, ma altrettanto efficaci per mettere sotto controllo le conseguenze di una possibile violazione.

Tra l'altro, nulla impedisce che le misure correttive possono essere multiple, abbinando sanzioni economiche a prescrizioni procedurali ed amministrative.

Resta del tutto aperto un aspetto afferente a eventuali sanzioni penali, per l'applicazione delle quali ogni paese potrà decidere in autonomia.

Adalberto Biasiotti

WP 253 (pdf, 0.4 MB)

Questo articolo è pubblicato sotto una Licenza Creative Commons.