PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4593 di Lunedì 02 dicembre 2019

GDPR: linee guida per l'applicazione di sanzioni

La raccolta sistematica di dati, afferenti a sanzioni applicate dai Garanti europei a varie tipologie di violazione del regolamento generale sulla protezione dei dati, permette di cominciare ad inquadrare metodi di valutazione e sanzioni relative.

Ricordo innanzitutto ai lettori che le sanzioni, potenzialmente assai salate, previste dal regolamento generale europeo della protezione dei dati personali, devono essere calcolate dopo aver valutato l'evento da sanzionare, sulla base di ben 11 parametri diversi; appare chiaro che una valutazione così personalizzata può portare a situazioni assai diverse, a seconda dei criteri che vengono utilizzati dalle varie autorità garanti europee.

Ecco il motivo per cui in alcuni paesi si stanno cominciando a tracciare delle linee guida, che possono aiutare le autorità Garanti a stabilire il peso da dare agli 11 parametri, giungendo infine alla determinazione della sanzione applicabile. Ricordo, come concetto generale, che il regolamento prevede che una sanzione debba essere **effettiva, proporzionata e dissuasiva**. Gli 11 parametri di valutazione sono elencati all'articolo 83 del regolamento europeo.

È del tutto normale il fatto che, in vari paesi europei, gli 11 parametri possono essere valutati in modo assai diverso e questo fatto va in contrasto con il principio di coerenza, che vuole che le modalità di applicazione del regolamento, e quindi delle sanzioni, siano omogenee in tutta Europa.

L'autorità Garante federale, che coordina l'attività delle autorità garanti dei singoli Stati (Laender) della Germania, si è mossa in questa direzione, mettendo a punto un modello di valutazione dell'entità delle sanzioni, che dovrebbe essere utilizzato dalle singole autorità Garanti dei singoli Stati.

La metodologia è piuttosto complessa, tanto è vero che in un recente caso il calcolo della sanzione, con le dovute spiegazioni, ha portato a sviluppare un documento lungo ben 24 pagine.

Il punto di partenza per il calcolo della sanzione è piuttosto sorprendente, perché parte dalla valutazione del bilancio annuale dell'ente coinvolto, riportato su base quotidiana.

Questa somma viene moltiplicata per dei fattori numerici, che sono appunto calcolati in base al comma 2 dell'articolo 83 del regolamento, come ad esempio la gravità della violazione, la responsabilità oggettiva dell'organizzazione, l'entità del danno causato agli interessati coinvolti, eccetera.

È evidente che una tale approccio può destare un elevato stupore, soprattutto in paesi, come il nostro, in cui il concetto di sanzione correlata al fatturato annuo era completamente sconosciuto.

Per fare un caso concreto, se una azienda, oppure un gruppo di aziende, coinvolte nella violazione, generano vendite per 90 miliardi di euro nell'anno precedente, il rateo giornaliero è 250 milioni di euro, vale a dire 90 miliardi di lire divisi per 360 giorni.

Il passo successivo è una valutazione, effettuata dall'autorità coinvolta, sulla gravità della specifica violazione.

A questo punto si deve prendere in considerazione il comma 4 ed il comma 6 dell'articolo 83 del regolamento, introducendo ovviamente un certo livello di discrezionalità da parte dell'autorità Garanti coinvolte.

Il modello messo a punto in Germania prevede cinque livelli di gravità della violazione, ognuno associato un coefficiente di moltiplicazione. Ecco la tabella:

- violazione minore: moltiplicazione da uno fino a quattro volte
- Violazione media: moltiplicazione da quattro a otto volte,
- violazione grave: moltiplicazione da otto a 12 volte,
- violazione gravissima: moltiplicatore da 12 a 14,4 volte.

Sulla base della valutazione della gravità, si ha a disposizione un fattore moltiplicatore del rateo giornaliero, che può portare a calcolare un valore mediano, che risulta la base per un approfondimento delle modalità di calcolo della sanzione.

Facciamo un esempio:

nel caso la azienda prima menzionata abbia un turnover annuo di 90.000.000.000, i1 rateo giornaliero è 250 milioni di euro; ove essa sia coinvolta in una violazione minore, l'autorità può moltiplicare il rateo giornaliero di 250 milioni di euro per 1 e fino a 4 volte. Ciò porta ad un importo variabile tra 250 milioni ed 1 miliardo di euro, con valore mediano di 625 milioni di euro.

Passiamo adesso a valutare la specifica violazione in esame, analizzando i seguenti parametri:

- durata nel tempo della violazione,
- natura, estensione e finalità di questo trattamento illecito,
- numero di interessati coinvolti nel trattamento violato,
- valutazione del danno subito dagli interessati coinvolti.

L'autorità a questo punto assegnano un punteggio da 0 a 4 ad ognuno di questi criteri e calcola il totale di questi valori. Il punteggio da 0 a 1 viene per solito applicato a fattori che mitigano il rischio, come ad esempio un ridotto numero di interessati coinvolti, modesti danni agli interessati stessi, breve durata della violazione e così via. Il punteggio 2 può essere applicato se non ci sono fattori mitiganti oppure aggravanti; il punteggio da 3 o 4 viene applicato quando vi sono fattori aggravanti, ad esempio come nel caso in cui la violazione sia stata prolungata nel tempo. La somma di questi punteggi produce quindi un numero compreso fra zero e 16.

Questo valore viene inserito in una complessa tabulazione, ancora non diffusa pubblicamente, per vedere se devono essere usati ulteriori moltiplicatori, sia per aumentare sia per diminuire il valore mediano già determinato in precedenza.

Continuiamo con un esempio pratico, seguente a quello precedentemente illustrato.

Se ad esempio le autorità valuta che i quattro criteri sopra menzionati portino ad un punteggio di 2 per ognuno dei quattro criteri, siamo al punteggio totale di otto, senza applicare ulteriori moltiplicatori; pertanto non è necessario aumentare a diminuire il valore mediano già calcolato.

Il valore mediano risulta ancora uguale a 625 milioni di euro.

Indi l'autorità Garante coinvolta passa ad analizzare qualsiasi altro criterio rilevante illustrato al comma 2 dell'articolo 83. Ad esempio, valutando il fattore casuale, doloso o frutto di negligenza, la rapidità con cui la violazione è stata messa sotto controllo, l'esistenza di precedenti violazioni, il livello di cooperazione con l'autorità garante e, se del caso, la presenza di certificazioni applicabili al trattamento.

Infine, l'autorità Garante potrà fare una valutazione globale della situazione e stabilire se vi sono elementi per un aggravamento della sanzione sin qui calcolata.

Alcuni esperimenti pratici, utilizzando questa linea guida, mostrano che le sanzioni che dovrebbero essere applicate dovrebbero essere molto più elevate di quelle fin adesso applicate dall'autorità Garanti statali tedesche. Il metodo di calcolo prevalentemente lineare, che parte dal fatturato annuo, può portare a somme assolutamente straordinarie.

A questo punto ci si chiede se questo schema abbia buone probabilità di essere recepito anche a livello europeo e, in caso di contestazione da parte del titolare coinvolto, bisogna vedere se la magistratura giudicante può ritenere che questo modello sia credibile o non possa essere assoggettato a contestazioni di varia natura, da parte della difesa del titolare.

È comunque apprezzabile il fatto che si sia cercato di mettere a punto una linea guida, che potrà certamente essere migliorata, ma che può rappresentare una guida preziosa per molte autorità nazionali, che ad oggi si muovono con un notevole livello di incertezza, in fase di determinazione di sanzioni applicabili.

Adalberto Biasiotti