GDPR

Privacy e tutela penale: evoluzione od occasione o persa?Luci ed ombre della nuova disciplina penale sul trattamento dei dati personali

Commento a cura degli Avv. Maria Roberta Perugini: https://www.mrperugini.it/it/

Avv. Francesco Rubino, Responsabile White Collar Crime Dept. – Morri Rossetti: http://morrirossetti.it/professionisti/francesco-rubino.html

ABSTRACT: Il D.Lgs. n. 101 del 10 agosto scorso ha dato esecuzione al Regolamento (UE) 2016/679 (GDPR). Il Legislatore nazionale era autorizzato a reintrodurre il sistema di tutela penale rivolto alla protezione dei dati personali delle persone fisiche e della libera circolazione dei dati. Il presente contributo analizza le novità introdotte dalla novella normativa e le opportunità di tutela penale non colte dal Legislatore che avrebbero potuto garantire una maggiore tutela per la riservatezza e della circolazione dei dati e, dall'altra parte, una maggiore responsabilizzazione dei soggetti che ne effettuano il trattamento.

Il 19 settembre scorso è entrato in vigore il D.Lgs. n. 101/2018, che prevede l'adeguamento della normativa nazionale al Regolamento Generale sulla Protezione dei Dati Personali (GDPR), nel contesto del quale il legislatore italiano ha dato attuazione alla facoltà – concessa dal GDPR a tutti gli Stati membri – di prevedere anche sanzioni penali per alcune violazioni della nuova normativa sulla privacy.

Il decreto, oltre ad avere confermato, arricchito e meglio specificato le fattispecie di reato già previste nella precedente disciplina (artt. 167, 168, 170 e 171) ha introdotto ipotesi delittuose del tutto nuove.

Si tratta del reato di comunicazione e diffusione illecita (art. 167bis) e acquisizione fraudolenta (art. 167ter) di dati personali oggetto di trattamento "su larga scala" – ossia quei trattamenti che "mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato" (considerando n. 91 GDPR).

Pene sensibilmente (più) elevate dunque – da uno a sei anni – nei confronti di quei soggetti che, trattando big data, espongono i dati personali– e di conseguenza tutti i diritti e libertà fondamentali coinvolti anche indirettamente dallo specifico trattamento – degli interessati ad un potenziale rischio estremamente esteso e diffuso.

Se dunque da un lato il sistema sanzionatorio di natura penale si rafforza nella salvaguardia del diritto alla protezione dei dati personali - concentrando l'attenzione soprattutto sul fenomeno, attualissimo e di grande rilevanza, del trattamento di grandi masse di dati,

dall'altro non è stato pienamente utilizzato per in ambiti che presentano significativa rilevanza.

Non si è infatti concretizzata l'integrazione dei delitti in commento all'interno dei reati-presupposto in tema di responsabilità amministrativa degli enti a norma del D.Lgs. 231/01. Dopo il fallito tentativo, nel 2013, di introdurre tutti i reati previsti dal previgente Codice privacy all'interno della normativa 231, l'adeguamento della normativa italiana al GDPR avrebbe potuto rappresentare una "seconda possibilità". Il sistema di gestione del trattamento dei dati dunque rimane, nel sistema penale, un fatto ristretto alla responsabilità delle persone fisiche e non degli enti. Al contrario, il coordinamento di questo sistema con gli altri sistemi di gestione aziendali avrebbe certamente potuto contribuire fortemente a responsabilizzare gli enti, anche in un'ottica di accelerazione del processo di attuazione delle disposizioni di cui al GDPR.

A ciò si aggiunga il fatto che le condotte fraudolente sopra indicate, qualora commesse mediante attività informatica, lascerebbero il passo alle fattispecie del codice penale (cybercrime) mantenendo quindi una natura prettamente residuale.

Da ultimo, l'ambito della rilevanza penale rimane circoscritto alle fattispecie di natura dolosa, escludendo in tal modo le condotte colpose – rimaste censurabili sotto il profilo amministrativo - caratterizzate da negligenza, imperizia o imprudenza nell'esecuzione del trattamento. È forse mancato un po' di coraggio nell'affidare al sistema sanzionatorio penale i comportamenti colposi, alla luce del fatto che sono di certo più frequenti – ma non meno dannose - le violazioni indipendenti dalla volontà dell'agente ma dettata da una "colpa organizzativa" del soggetto titolare del trattamento. A questo proposito, è utile sottolineare che il vero cuore del GDPR è proprio la richiesta al titolare del trattamento di mantenere costantemente sotto controllo i trattamenti che effettua: dunque, una richiesta "aperta", dal contenuto eminentemente organizzativo, che lascia spazio.

Certamente, l'importanza delle sanzioni amministrative pecuniarie previste (fino a 20 milioni di euro o il 4% del fatturato di gruppo per il primo scaglione di violazioni e fino a 10 milioni di euro o il 2% del fatturato di gruppo per il secondo) teoricamente ha un importante effetto deterrente, ma l'effettiva efficacia in tale senso potrà essere valutata solo a seguito della concreta applicazione di tali criteri da parte dell'Autorità Garante.

Avuto riguardo però alla delicatezza che caratterizza l'oggetto della materia relativa alla protezione dei dati (che vede come oggetto di tutela non solo il diritto alla protezione dei dati personali ma anche tutti i diritti e le libertà fondamentali dell'individuo), l'innalzamento del livello di tutela penalistica anche alle fattispecie colpose – prevedendo al contempo la possibilità di estinguere il reato a seguito della realizzazione di condotte riparatorie - avrebbe di certo inciso in maniera più decisiva sulla loro prevenzione e repressione, soprattutto all'interno di contesti aziendali in cui più o meno consapevolmente non viene applicato un sistema di trattamento dei dati sensibile (formalmente, ma soprattutto sostanzialmente) alle previsioni del GDPR.