PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4415 di Mercoledì 27 febbraio 2019

È possibile assicurarsi a fronte di una violazione di dati personali?

Il livello estremamente elevato delle sanzioni, che possono essere applicate in caso di violazione di dati personali, ha indotto molti titolari, responsabili del trattamento e della protezione dei dati a cercare una copertura assicurativa.

Il nuovo regolamento generale sulla protezione dei dati personali prevede delle sanzioni severe per chi viola alcune specifiche disposizioni. È ben vero che il processo che permette di giungere alla definizione della sanzione è piuttosto articolato, e prevede l'esame di numerosi aspetti, come ad esempio il fatto che il titolare coinvolto abbia adottato misure di protezione, oppure sia stato già coinvolto in violazioni similari, eccetera, ma è possibile che il livello della sanzione, che alla fine viene determinato dall'autorità Garante nazionale, possa essere oltremodo elevato.

Vale la pena di citare un caso recente, che mette in evidenza la gravità potenziale di queste violazioni.

Nell'ottobre 2018, una catena di supermercati del Regno Unito ha perso un ricorso al tribunale britannico, che ha ritenuto che il titolare del trattamento fosse in parte responsabile per una violazione dei dati. In particolare, un auditor interno, che è stato condannato a otto anni di prigione per frode, aveva comunicato dati personali di 100.000 dipendenti a soggetti terzi. 5000 dipendenti coinvolti hanno chiesto al titolare della catena di supermercati un risarcimento. Poiché il titolare ha fatto presente che il totale dei risarcimenti richiesti avrebbe portato al fallimento dell'azienda, egli ha fatto ricorso al tribunale, che tuttavia ha dato torto all'azienda, suggerendo che in futuro l'azienda avrebbe dovuto acquistare una copertura contro questi rischi.

Vediamo quali sono i problemi legati alla costruzione di una possibile copertura assicurativa.

Le caratteristiche principali, che devono essere individuate per costruire una copertura assicurativa, sono evidentemente legate al rischio da assicurare ed al premio conseguente.

Nel caso che abbiamo illustrato in precedenza, si sono verificate due situazioni, tra loro ben diverse:

- da un lato, la catena di supermercati è stata sanzionata perché non avevano protetto in modo idoneo i dati dei dipendenti,
- dall'altro lato, i dipendenti, i cui dati sono stati violati, si sono attivati per chiedere un risarcimento.

Appare evidente che una copertura assicurativa per la prima situazione è ben difficile da trovare, per il semplice fatto che se qualcheduno potesse trovare una copertura assicurativa, in grado di pagare la sanzione affibbiata per essere passati con semaforo rosso, avrebbe ben poco interesse, in futuro, a controllare la condizione del semaforo!

Questa è la ragione per cui, come regola generale, una sanzione amministrativa non è mai assicurabile.

Diversa è la situazione, quando la copertura assicurativa richiesta fa riferimento alla responsabilità civile del titolare, che viene chiamata in causa dagli interessati, i cui dati sono stati violati.

In questo caso, una polizza di responsabilità civile potrebbe coprire questo rischio.

Al proposito, è opportuno citare l'articolo del regolamento che fa riferimento a questo tipo di responsabilità:

Articolo 82 Diritto al risarcimento e responsabilità

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

Omissis

Richiamo in particolare l'attenzione dei lettori sul comma uno, laddove si fa riferimento al diritto di ottenere il risarcimento per un danno materiale o immateriale. Il danno immateriale evidentemente fa riferimento a perdita di immagine, o diffusione di notizie possano in qualche modo compromettere il profilo professionale dell'interessato coinvolto. In questi casi l'importo del risarcimento può essere concordato fra le parti o può essere deciso dal tribunale civile. Non è difficile immaginare importi oltremodo elevate, sia perché potrebbero essere molti interessati coinvolti, sia perché potrebbero essere elevati risarcimenti decisi del tribunale.

Dal momento però che la sanzione massima che potrebbe essere applicata per il primo tipo di violazione può arrivare persino a 20 milioni di euro, appare chiaro che sarebbe oltremodo interessante avere a disposizione una copertura anche per la prima tipologia di rischio.

A questo punto la situazione diventa alquanto complicata, tanto è vero che ad oggi, in Europa, due soli paesi esplicitamente consentono di attivare coperture assicurative per le sanzioni applicate, in caso di violazione della protezione dei dati: questi paesi sono la Finlandia e la Svezia. In altri paesi la situazione è alquanto ambigua. Un esperto assicuratore, operante presso una delle maggiori compagnie europee, ha affermato che ad oggi non esistono ancora esperienze sufficienti per poter costruire un quadro di riferimento legale, circa il fatto che queste sanzioni possano essere o meno coperte da assicurazione.

Andiamo adesso ad esaminare se e come è possibile coprire il rischio di richieste di risarcimento, avanzate da soggetti, i cui dati siano stati coinvolti in una violazione.

Come accennato in precedenza, ci troviamo davanti ad una tipica situazione di responsabilità civile; il problema che occorre adesso prendere considerazione riguarda la determinazione del premio.

Come è evidente, qualsiasi compagnia di assicurazione determina il premio sulla base di una valutazione storica della probabilità e dell'importo di sinistri, che si siano verificati in precedenza.

Ad oggi, l'esperienza maturata nel settore è quasi nulla e, peggio ancora, i pochi dati disponibili nei vari paesi europei non sono fra loro confrontabili, perché le modalità con cui vengono applicate le sanzioni o vengono attivate le procedure di rivendicazione, sulla base di una responsabilità civile, sono assai diverse da paese a paese.

L'assicuratore si trova pertanto dove determinare un premio sulla base di dati storici poco affidabili e poco confrontabili.

Chi scrive ricorda assai bene una conversazione che ebbe una ventina di anni fa con uno dei maggiori sottoscrittori dei Lloyd's, che aveva emesso la prima polizza a copertura del lancio di un satellite. Non vi era nessuna esperienza precedente, non vi era nessun dato statistico; in altre parole non vi era nulla di nulla su cui basare il premio. Questo sottoscrittore mi disse che il premio venne determinato su parametri, in cui il fattore "fortuna o sfortuna", era dominante!

Nonostante il tentativo apprezzabile, costituito dall'introduzione di un regolamento europeo, ancora oggi sono presenti differenze nei vari paesi europei, a fronte della possibilità di presentare richieste di indennizzo, nel caso un interessato abbia visto violati i propri dati personali; gli approcci dei vari dispositivi legislativi e l'atteggiamento delle varie autorità Garanti sono molto diversi.

Questo fatto deve essere preso in considerazione dagli assicuratori, che con ogni probabilità dovranno stabilire premi non più armonizzati a livello europeo, ma adattati alla specifica realtà di ogni singolo paese.

Un altro aspetto da prendere considerazione riguarda il tipo di trattamento coinvolto.

Il tipo di trattamento può avere un impatto determinante sulla probabilità di violazione dei dati, come pure la natura dei dati trattati può avere un impatto determinante sulla probabilità che, in caso di violazione, venga avanzata una richiesta di risarcimento, da parte degli interessati coinvolti.

Prendendo ad esempio un campo in cui dispongo di un'esperienza diretta, si prenda in considerazione il caso di un'associazione di donatori di sangue, che detiene solo i dati relativi al profilo del socio donatore, laddove gli unici dati particolari sono il gruppo sanguigno e l'eventuale temporanea sospensione dalle donazioni, senza ovviamente conoscere la ragione.

In altri casi, un'associazione di donatori di sangue può provvedere in proprio al prelievo del sangue, acquisendo una gigantesca quantità di dati personali, di natura particolare, che richiedono un livello di protezione molto più elevato, in ragione del fatto che un'eventuale violazione di questi dati potrebbe avere un impatto ben più grave sull'interessato coinvolto, rispetto alla ipotesi più semplice illustrata in precedenza.

Infine, un aspetto determinante, nel valutare l'applicabilità di una copertura assicurativa, è legato al fatto che nessun sottoscrittore dei Lloyd's, o più in generale nessun assicuratore, offre una copertura su un rischio di questo genere, senza aver affidato ad uno specialista, un security Surveyor, una indagine sul campo, verificando i livelli di protezione dei dati, attuati dall'aspirante assicurato. In molti casi, al termine della security Survey, il Surveyor elenca tutta una serie di raccomandazioni, che devono essere attuate in un lasso di tempo relativamente breve. Alcuni assicuratori sospendono la copertura sino a che tutte le raccomandazioni non siano state attuate, mentre altri assicuratori, alla caccia di clienti, garantiscono l'immediata attivazione della copertura, a condizione che tutte le raccomandazioni vengano attuate nei tempi stabiliti.

In questo, una eventuale copertura contro responsabilità connesse alla violazione dei dati assomiglia molto alle vigenti coperture Computer Crime, che prevedono una sequenza di assunzione del rischio, assai simile a quella illustrata.

Infine, vorrei spendere una parola di conforto per i responsabili della protezione dei dati.

Le responsabilità cui possono andare incontro questi profili professionali sono ben diverse, rispetto a quelle cui può andare incontro il titolare ed il responsabile del trattamento. È bene ricordare che il responsabile della protezione non è un organo di *line*, ma un organo di *staff*; ciò significa che questo professionista ha l'obbligo di evidenziare situazioni anomale, dare saggi consigli per metterle sotto controllo, ma non ha una responsabilità diretta, se il titolare o responsabile non attuano i suoi consigli.

Una sua responsabilità professionale potrà essere chiamata in causa solo se, operando in violazione degli obblighi di diligenza e perizia, egli non abbia individuato una situazione di rischio, che successivamente abbia portato ad una violazione.

Per questa ragione, ritengo che la copertura assicurativa, a fronte di responsabilità civili connesse a violazione di dati personali, costituisca un argomento, che sono certo verrà approfondito a tempi brevi.

Nel contempo, dovrà essere approfondito anche l'argomento afferente alla possibilità che la copertura assicurativa si estenda anche alle sanzioni applicate, secondo le disposizioni del regolamento.

Adalberto Biasiotti
