Data breach: prevenire è meglio che curare

Aspetti penali relativi ai reati informatici e collegamenti al GDPR

a cura del Referente del TdL congiunto «Protezione dei dati personali – GDPR»
Ordine degli Avvocati di Torino

Avv. Claudio Strata

TaxLawPlanet™

Torino, 14 maggio 2021

CAUSE DEL DATA - BREACH

INTERNE:

DISATTENZIONE – VIOLAZIONE DA PARTE DEL TITOLARE DEL TRATTAMENTO

ESTERNA:

ACCESSO ABUSIVO – INTRUSIONE – VIOLAZIONE DA PARTE DI TERZI

Comportamenti che provocano il data - breach

Data breach = «violazione di sicurezza che comporta – accidentalmente o in modo illecito – la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati».

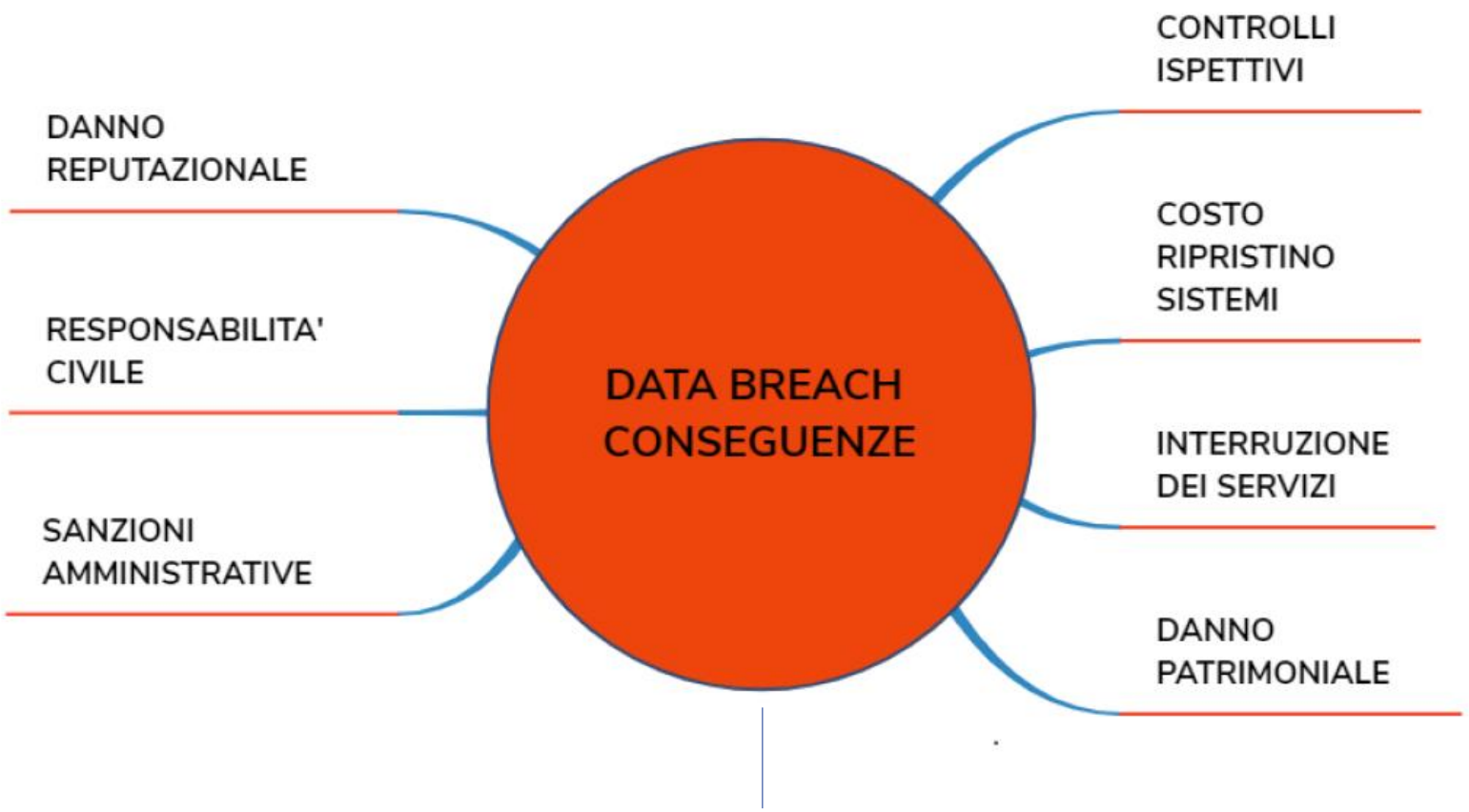
Il titolare del trattamento:

- Dimentica un fascicolo/una chiavetta usb/un dispositivo informatico in un luogo pubblico
- Divulga accidentalmente un dato di un proprio cliente
- Divulga accidentalmente le proprie password di accesso a pc/mail

Il titolare del trattamento:

- Subisce un furto di dispositivi
- Subisce un attacco informatico ed un furto «virtuale» di dati
- È vittima di *ransomware* con relativa richiesta di riscatto
- È vittima di una divulgazione dei dati da parte di un dipendente «infedele»

CONSEGUENZE



Primo caso: data-breach con causa «interna» → SE IL DATA BREACH E' PROVOCATO DA UNA VIOLAZIONE DA PARTE DEL TITOLARE DEL TRATTAMENTO

→ IL GARANTE PUO' IRROGARE SANZIONI AMMINISTRATIVE (AFFLITTIVE E CORRETTIVE) – Art. 83 G.D.P.R.

Elementi utilizzati per la valutazione, ai fini dell'irrogazione della sanzione:

- Natura, gravità e durata, carattere doloso o colposo della violazione
- Misure adottate per attenuare il danno subito dagli interessati
- Grado di responsabilità di titolare e responsabile del trattamento, tenendo conto delle misure tecniche e organizzative messe in atto ai sensi degli artt. 25 e 32, adesione a codici di condotta o meccanismi di certificazione
- Eventuali violazioni precedenti, pertinenti, commesse da titolare o responsabile, rispetto di eventuali prescrizioni precedenti
- Grado di cooperazione con Autorità di controllo al fine di porre rimedio alla violazione e attenuare possibili effetti negativi
- Categorie di dati interessati dalla violazione e notificazione
- Eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, come benefici finanziari conseguiti o perdite evitate quale conseguenza della violazione

Sanzioni afflittive

Fino a 10 milioni di Euro, o per le imprese, fino al 2% del fatturato annuo globale dell'esercizio precedente, nei casi di:

- inosservanza degli obblighi del titolare e del responsabile del trattamento;
- inosservanza degli obblighi dell'organismo di certificazione;
- inosservanza degli obblighi dell'organismo di controllo.

Fino a 20 milioni di Euro, o per le imprese, fino al 4% del fatturato annuo globale dell'esercizio precedente, nei casi di:

- inosservanza dei principi base del trattamento; inosservanza dei diritti degli interessati;
- inosservanza delle disposizioni sul trasferimento dei dati personali in paesi terzi o verso organizzazioni internazionali;
- inosservanza di un ordine, limitazione provvisoria o definitiva o di un ordine di sospensione dei flussi da parte dell'autorità di controllo. Inosservanza di un ordine correttivo dell'autorità di controllo.

Sanzioni correttive

L'Autorità di controllo può:

- rivolgere avvertimenti/ammonimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono violare il GDPR o l'abbiano violato;
- ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i relativi diritti, nonché di conformare i trattamenti alle disposizioni del GDPR, anche specificando in che modo ed entro quale termine;
- ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
- imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
- Ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali;
- Revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;
- Infliggere una sanzione amministrativa pecuniaria in aggiunta alle presenti misure;
- Ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

Sanzioni penali

Art. 167 Codice Privacy - Trattamento illecito dei dati

Viene punito chi, al fine di trarre un profitto per sé o per altri, arrechi un danno al proprietario dei dati. Ciò avviene anche quando le informazioni personali vengono trasferite verso un paese terzo o a un'organizzazione internazionale, recando dei danni all'interessato.

Art. 167bis Codice Privacy - Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala

Si tratta di una nuova tipologia di reato, che va a colpire chi comunica e diffonde i dati personali di un soggetto su larga scala, per trarne profitto. Si pensi ad esempio agli archivi automatizzati che raccolgono i dati.

Art. 167ter Codice Privacy – Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala

Riprende il reato precedente con l'aggravante del metodo fraudolento.

Art. 168 Codice Privacy - Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante

Viene punito chiunque, durante gli accertamenti di fronte al Garante, dichiari il falso o presenti documenti non veri. Ma, anche chi intenzionalmente interrompa o impedisca il corretto svolgimento di un procedimento presso il Garante può subire una sanzione.

Art. 170 Codice Privacy - Inosservanza di provvedimenti del Garante

Se non vengono rispettare le decisioni del Garante, è sempre prevista come sanzione la pena detentiva

Art. 171 Codice Privacy - Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori

Continua ad essere punito **l'utilizzo di impianti audiovisivi utilizzati per controllare a distanza i propri dipendenti,** se non è stato prima concordato con le parti in questione. E' vietato, inoltre, **svolgere indagini** per conoscere le opinioni politiche, religiose e le appartenenze sindacali di un lavoratore, prima di decidere se assumerlo o meno.

Art. 172 Codice Privacy - Pene accessorie

La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza.

Nel secondo caso, e dunque nei confronti dell'AUTORE del data breach avente causa «esterna» → previsione di ulteriori fattispecie di reato → sanzioni penali

- **Accesso abusivo ad un sistema informatico o telematico** (art. 615-ter c.p.): si configura quando un soggetto si introduce in un sistema informatico protetto da misure di sicurezza o vi si mantiene senza il consenso del titolare. La norma intende tutelare la riservatezza del c.d. domicilio informatico.

- **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici** (art. 615-quater c.p.): si configura quando, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente taluno si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza. In questo caso viene anticipata notevolmente la soglia della tutela penale, andando a proteggere già i codici di accesso.

- **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico** (art. 615-quinquies c.p.): la norma tutela il corretto funzionamento delle tecnologie informatiche e la loro salvaguardia, ad esempio, dai programmi-virus.

- **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche** (art. 617-quater c.p.): viene tutelata la riservatezza delle comunicazioni informatiche e la sicurezza stessa del sistema informatico o telematico, in modo che non venga violato il rapporto fiduciario con il gestore della rete.

- **Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche** (art. 617-quinquies c.p.): la norma tutela la riservatezza, la segretezza e la libertà delle comunicazioni, informazioni o notizie trasmesse per via telematica o elaborate da sistemi informatici.

- **Reati di danneggiamento informatico**, previsti dagli artt. 635-bis, 635-ter, 635-quater e 635-quinquies c.p.. Essi presentano alcuni elementi costitutivi comuni: tutti questi reati sono posti a tutela della integrità dei beni informatici, come dati, informazioni e programmi, e del domicilio informatico e vanno ad individuare diverse condotte penalmente sanzionate, come la distruzione, il deterioramento, alterazione o soppressione di informazioni, dati, programmi informatici o sistemi informatici.

- **Documenti informatici** (art. 491-bis c.p.). Qualora le condotte previste in materia di "*Falsità in atti*" riguardino un documento informatico, pubblico o privato, avente efficacia probatoria, si applicano le disposizioni concernenti il falso in atti pubblici e in scritture private. Occorre inoltre precisare che per "documento informatico" deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

- **Frode informatica del soggetto che presta servizi di certificazione di firma elettronica** (art. 640 quinquies c.p.)

ATTENZIONE!

Spesso questi reati vengono denunciati e, in seguito, contestati, unitamente ad ulteriori fattispecie di reato, ad essi connesse.

→ Art. 494 c.p.: sostituzione di persona

→ Art. 629 c.p.: estorsione

→ Art. 640 c.p.: truffa

→ Art. 648 c.p.: ricettazione

→ Art. 648bis c.p.: riciclaggio

→ Art. 648ter c.p.: autoriciclaggio