Cifratura dei dati. Storia, tecniche e interazione con la legislazione vigente – Parte III

whynery.com/cifratura-dei-dati-storia-tecniche-e-interazione-con-la-legislazione-vigente-parte-iii

20 settembre 2021

Dietro le Quinte

David Scaffaro – 20 Settembre 2021

Riepilogo parte II

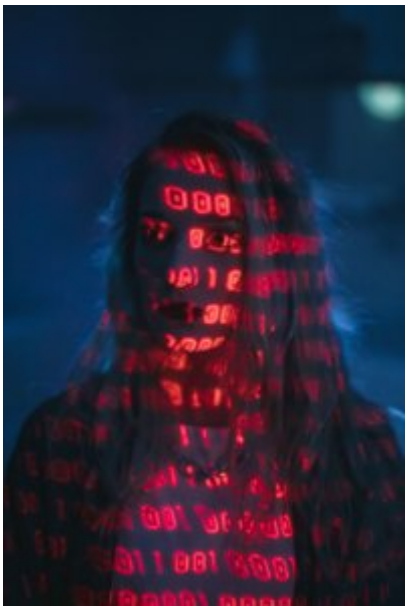
Nella seconda parte, abbiamo visto le differenze tra i tipi di cifratura, nello specifico **simmetrico e asimmetrico**, abbiamo introdotto alcuni **degli algoritmi di cifratura maggiormente noti**, esaminato alcune **tecniche di crittanalisi** e, infine, abbiamo "giocato" con i numeri per dimostrare **l'importanza di una password robusta.**

In questa terza e ultima parte, vedremo **i reati e le sanzioni previste dal D.Lgs. 231/01 e dal GDPR e, poi, come evitarli.**

D.Lgs. 231/01 e i reati informatici

L'introduzione dei reati informatici **nel D.Lgs. 231, è avvenuta nel 2008 in conseguenza della Legge 48/08** la quale ha ratificato la Convenzione di Budapest del Consiglio d'Europa sul cybercrime. Anche **il codice penale e il codice di procedurale penale** hanno subito delle modifiche.

Reati informatici e obblighi legislativi per le Organizzazioni



La sicurezza informatica e i reati ascrivibili a violazioni nel campo informatico, sono richiamati dal **diritto civile e penale** e sono afferenti ad una **pluralità di disposizioni** di varia natura, quindi sono molto articolati e regolano i vari aspetti del settore specifico.

Tra gli obblighi a carico delle Organizzazioni, si segnalano **il D.Lgs. 231/01 e il GDPR.**

Di seguito i principali reati assimilabili a quelli di natura informatica:

Art. 491 bis c.p. falsità in un documento informatico

Art. 615 ter c.p. accesso abusivo ad un sistema informatico o telematico

Art. 615 quater c.p. detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Art. 615 quinquies c.p. diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

Art. 617 quater c.p. intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Art. 635 bis c.p. danneggiamento di informazioni, dati e programmi informatici

Art. 635 ter c.p. danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

Art. 635 quater c.p. danneggiamento di sistemi informatici o telematici

Art. 635 quinquies c.p. danneggiamento di sistemi informatici o telematici di pubblica utilità

Art. 640 quinquies c.p. frode informatica del certificatore di firma elettronica

D.Lgs. 231/01 e sanzioni

L'apparato sanzionatorio è **suddiviso in più tipologie e piuttosto articolato**, infatti sono previste le seguenti tipologie di sanzioni:

– sanzioni amministrative

– sanzioni interdittive

– confisca del prezzo o del profitto del reato

– pubblicazione della sentenza

Sanzioni amministrative.

In particolar modo, per quanto riguarda le sanzioni amministrative, **l'ammontare dell'importo viene determinato dal numero di "quote" relativo al determinato reato, moltiplicato per l'importo assegnato alla quota.**

Il numero delle quote va da 100 a 1000, mentre **l'importo assegnato ad ogni quota va da 258 euro a 1549 euro** e il pagamento in forma ridotta non è ammesso.

Quindi le sanzioni amministrative, sono comprese in una forbice **tra 25.800 euro e 1.549.000 euro.**

Sanzioni Interdittive.

Le sanzioni interdittive prevedono:

a) **l'interdizione dall'esercizio dell'attività;**

b) **la sospensione o la revoca** delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;

c) **il divieto di contrattare con la pubblica amministrazione**, salvo che per ottenere le prestazioni di un pubblico servizio;

d**) l'esclusione da agevolazioni**, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;

e) **il divieto di pubblicizzare beni o servizi.**

Confisca.

Per quanto riguarda la confisca del prezzo o del profitto del reato, **che viene sempre applicata**, viene fatta salva la parte che può essere restituita al danneggiato.

Nel caso non sia possibile eseguire la confisca, **la stessa può avere ad oggetto somme di denaro, beni o altre utilità, di valore equivalente al prezzo o al profitto del reato.**

Pubblicazione della sentenza di condanna.

La pubblicazione della sentenza di condanna può essere disposta quando nei confronti dell'ente viene applicata **una sanzione interdittiva**.

La sentenza è pubblicata una sola volta, per estratto o per intero, **in uno o più giornali indicati dal giudice nella sentenza**, nonché mediante **l'affissione nel comune ove l'ente ha la sede principale.**

La pubblicazione della sentenza è eseguita, a cura della cancelleria del giudice, **a spese dell'Organizzazione.**

Sanzioni Penali.

La responsabilità penale a carico della persona, o delle persone, che ha, o hanno, **commesso il reato, permane** ed i relativi provvedimenti **sono autonomi e indipendenti rispetto a quelli comminati all'ente giuridico.**

Sostanzialmente, **oltre all'iter giudiziario verso l'azienda**, vi è anche **l'iter giudiziario verso i rei**, con le relative ed eventuali pene previste.

GDPR e sicurezza tecnica

L'ambito dei reati informatici all'interno del GDPR può ricondotto a due punti ben definiti, ovvero:

– **l'art. 25**, il quale definisce "la privacy by design", ovvero le attività di protezione dei dati a partire dalla progettazione stessa del sistema, e la "privacy by default", ovvero la protezione dei dati come attuazione predefinita, e dispone al Titolare del trattamento

“misure tecniche e organizzative adeguate, in modo da attuare efficacemente i principi di protezione dei dati e da garantire nel trattamento i requisiti del Regolamento e la tutela dei diritti degli interessati”

– **l’art. 32**, il quale impone all’Organizzazione di dotarsi di misure di sicurezza tecniche ed organizzative adeguate alla tutela dei dati personali.

GDPR e sanzioni

Le sanzioni previste dal GDPR, sono richiamate all’art. 83 e indicano 2 casistiche:

a) **10 milioni di euro o 2% del fatturato mondiale annuo dell’anno precedente, se superiore**, per

le Organizzazioni nei casi in cui, per esempio, non venga comunicato un data breach, i dati personali degli utenti vengano trattati in maniera non lecita oppure non venga nominato il DPO.

b) **20 milioni di euro o 4% del fatturato del fatturato mondiale annuo dell’anno precedente, se superiore**, per casistiche che riguardino, ad esempio, la mancata osservanza dei diritti degli interessati o il trasferimento illecito di dati personali verso paesi esteri.

Non esiste un valore minimo della sanzione, spetta quindi al Garante determinarla, applicando i principi di **effettività, proporzionalità e dissuasività.**

Ulteriori sanzioni.

Da considerare a fronte di un reato previsto dal GDPR, anche le eventauli ulteriori tipologie di sanzioni:

– penali;

– risarcimento a vario titolo;

– divieto, temporaneo e subordinato alla risoluzione delle difformità, del trattamento dei dati personali.

Ciò anche in ottemperanza del **D.Lgs. 101/18**, che, come il precedente D.Lgs. 196/03, **prevede 6 fattispecie di reato**, per la precisione:

trattamento illecito dei dati (art. 167);

comunicazione e diffusione illecita dei dati personali oggetto di trattamento su larga scala (art. 167-bis);

acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (art. 167-ter);

falsità nelle dichiarazioni al Garante e interruzioni dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante (art. 168);

inosservanza di provvedimenti del Garante (art. 170);

violazione delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori (art. 171).

Le pene previste, a seconda del reato, **vanno da un minimo di 15 giorni ad un massimo di 6 anni.**

Si deve precisare che le pene previste **possono essere difformi nei diversi paesi europei**, infatti l'art. 84 del GDPR, al comma 1, sancisce che "Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive."

Da qui, per l'Italia, le sanzioni contenute nel D.Lgs. 101/18.

Come evitare le sanzioni

L'Organizzazione può evitare le situazioni a rischio sanzioni **attraverso cinque step collegati e interagenti tra loro:**

– **Un sistema documentale** conforme alle disposizioni di legge e procedurizzato in modo da coprire le **più ampie casistiche** e, quindi, **abbattere il rischio di commettere reati**;

– **La formazione** interna dei propri lavoratori;

– **L'attuazione degli incarichi di sorveglianza** previsti dalla legge.

– **Il controllo, la vigilanza e il miglioramento dei processi di lavoro.**

– **L'aggiornamento documentale** a seguito di modifiche e integrazioni legeslative e/o modifiche nei processi di lavoro.

Nel **D.Lgs. 231/01**, in modo esplicito, i termini per dimostrare l'esimenza da parte dell'Organizzazione, sono enunciati **dall'art. 6**, in particolare il comma 1, dove riporta:

"Se il reato è stato commesso dalle persone indicate nell'articolo 5, comma 1, lettera a), **l'ente non risponde se prova che:**

a) l'organo dirigente **ha adottato ed efficacemente attuato**, prima della commissione del fatto, **modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;**

b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento **è stato affidato a un organismo** dell'ente dotato di autonomi poteri di iniziativa e di controllo;"

Nel GDPR, invece, l'Organizzazione **deve predisporre un sistema documentale**, atto al corretto funzionamento e svolgimento delle attività atte a minimizzare il rischio di reati.

Tra **i principali documenti** si ricordano:

– Informativa sulla Privacy

– Politica sulla Protezione dei Dati Personali

– Registro delle Valutazioni d'Impatto sulla Protezione dei Dati

– procedure per i diritti degli interessati

– procedure per la sicurezza tecnica

– procedure per le attività di gestione

– modulistica per la gestione delle procedure

– mudilistica per gli incarichi

– altra documentazione accessoria, pertinente a determinate categorie o dimensioni aziendali

Inoltre **per determinate tipologie di attività è obbligatorio incaricare un DPO** (Data Protection Officer); **dove non vige l'obbligo, è comunque fortemente consigliato l'incarico.**

Considerazioni parte III

La congiuntura attuale, **dove i margini delle Organizzazioni sono sempre più ristretti**, fa si che **nessuna Organizzazione può permettersi finanziariamente sanzioni pesanti**, oltre agli **effetti collaterali**, quali una **caduta di immagine o impedimenti allo svolgimento delle attività**, ricadenti, questi ultimi, nelle sanzioni accessorie.

Quindi, **l'unica via per evitare le sanzioni è strutturare un robusto sistema di gestione documentale e implementare le successive attività di gestione, formazione e controllo.**

Tutto ciò, oggi**, è possibile farlo con impatti pressochè nulli, sotto tutti i punti di vista, per qualsiasi Organizzazione.**

Scopri il nostro online store

Accedi allo store Whynery, registrati per acquistare e profila la tua identità sensoriale.

Vai allo Store

Lascia un commento

Il tuo indirizzo email non sarà pubblicato. I campi obbligatori sono contrassegnati *