Che cosa si intende per rivoluzione normativa?

FOCUS:

1. La rivoluzione normativa ‘cyber’

2. L’impatto concreto sulle aziende: contratti, organizzazione, responsabilità

Perché una rivoluzione normativa?

Il trend dei cyber attacchi è in **costante ed esponenziale crescita**.

Quali rimedi?

Creazione a livello europeo e nazionale di un **sistema di regole** cogenti e articolate, di **sanzioni**, di **apparati**, rivolti a **tutelare l'architettura economica, sociale ed industriale** dei singoli Stati membri e di conseguenza dell'UE, **riducendo il rischio cyber.**

Quali regole?

a. obblighi di adozione di misure di sicurezza tecniche e organizzative
b. obblighi di comunicazione/notifica da parte dei soggetti interessati in caso di incidenti informatici
c. sanzioni, in caso di inosservanza delle regole.

Cybersecurity: focus normativo

Il contesto normativo è in costante evoluzione e crescita.

Direttiva NIS

Dir UE 2016/1148

Cyber Security Act

Reg UE 2019/881

Perimetro di Sicurezza Nazionale Cibernetica

L. 133/2019

In lavorazione:

Direttiva NIS 2

Cyber Resilient Act

La sicurezza delle catene di approvvigionamento

In una prospettiva di **supply chain "sicura"** la normativa cyber deve essere conosciuta e applicata non solo dai destinatari diretti e qualificati e da tutti i loro fornitori, con particolare riferimento a quei fornitori che hanno a che fare - a diverso titolo - con asset digitali ed informatici.

A tale riguardo, nella NIS2 è stata introdotta una previsione di la **responsabilità del top management** nel caso di mancata osservanza degli obblighi di sicurezza informatica, introducendo anche misure di vigilanza più rigorose per le autorità nazionali.

Per le aziende che rappresentano i singoli anelli della catena di fornitura, questa rivoluzione normativa rappresenta una **opportunità di business**, per confermarsi o entrare in un determinato mercato.

Il settore dei trasporti e della logistica

L'esigenza di cyber sicurezza è maggiormente avvertita per il **settore dei trasporti e della logistica** data la rilevanza strategica del settore e per le peculiarità della supply chain.

L'introduzione di nuovi sistemi di regole previsti da nuove normative obbligatorie richiede la **modifica dell'organizzazione aziendale** (i.e. ruoli, processi).

Tali trasformazioni sono obbligatorie per i soggetti qualificati ma anche fortemente raccomandate per i singoli operatori della catena di approvvigionamento dal momento che un incidente di cybersecurity può creare **danni all'azienda** in termini di:

- **sanzioni amministrative, in caso di violazione di norme di cybersecurity e di data privacy**
- *business continuity*
- **divulgazione di informazioni riservate e danno reputazionale**
- **perdita di avviamento**

L’impatto concreto della normativa di Cybersecurity

Funzione	Attività
▪ **Commerciale/acquisti**	*Test CVCN* *Impatto sui contratti commerciali*
▪ **HR**	*Policy, manuali di condotta, regolamenti sull’utilizzo degli strumenti di lavoro in azienda, piani di formazione e prevenzione sul tema cybersicurezza*
▪ **Operazioni straordinarie e di M&A**	*Cyber due diligence*
▪ **Governance**	*Dotazione di adeguato assetto organizzativo, amministrativo e contabile (nuovo art. 2086 Cod. Civ.)*

Grazie

Avv. Francesco Maria Gavotti

Studio Legale Associato B-right Lawyers

Genova

www.b-rightlawyers.eu