NEWSLETTER

DATA PROTECTION AND CYBERSECURITY; WHITE COLLAR CRIME & INVESTIGATION

Legge sulla cybersecurity

Introduzione

Il cosiddetto "DDL Cyber" è stato pubblicato sulla Gazzetta Ufficiale come legge 90/2024 e contiene "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*" ("**Legge Cybersecurity**").

I Disposizioni in materia di cybersecurity

Il primo ambito di intervento del legislatore è nel contesto degli **obblighi di notifica**. Nello specifico, le pubbliche amministrazioni, le società *in house* e i soggetti inclusi nel cosiddetto "perimetro di sicurezza nazionale cibernetica" saranno tenuti a segnalare determinati incidenti informatici **entro 24 ore** e, **entro le 48 ore** successive, dovranno inviare una notifica completa di tutti gli elementi necessari.

Dunque, con la Legge Cybersecurity vengono modificate le tempistiche della comunicazione per i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica: ora dovranno effettuare una prima segnalazione degli incidenti che di verifichino su asset diversi dai beni ICT entro 24 ore. Rimane in ogni caso fermo l'obbligo di procedere con la notifica entro 72 ore.

È importante sottolineare che in caso di reiterata inosservanza di tali disposizioni nell'arco di 5 anni consegue una **sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000**.

Un'altra novità è costituita dall'obbligo per le pubbliche amministrazioni, gli enti inclusi nel perimetro di sicurezza nazionale cibernetica, quelli soggetti alla Direttiva NIS, i fornitori e i soggetti Tel.Co di adottare **entro 15 giorni gli**

interventi risolutivi indicati dall'Agenzia per la Cybersicurezza Nazionale (ACN), laddove quest'ultima dovesse segnalare una **vulnerabilità** a cui potrebbero essere esposti.

Un'altra interessante area di intervento è quella in materia di contratti pubblici con i *provider* tecnologici.

Nello specifico, la Legge Cybersecurity prevede che, nel caso di approvvigionamento di specifiche categorie di beni e servizi informatici impiegati in contesti connessi alla tutela degli interessi strategici nazionali, le Pubbliche Amministrazioni, le società pubbliche e i soggetti privati compresi nel Perimetro di Sicurezza Nazionale Cibernetica dovranno **tenere in considerazione alcuni elementi di cybersecurity** che saranno definiti da un apposito decreto del Presidente del Consiglio dei ministri. Inoltre, sempre nell'ambito delle procedure di affidamento di beni e servizi ICT, dovranno essere previsti dei **criteri di premialità** in caso di offerte che prevedano l'utilizzo di tecnologie nazionali, europee, di paesi appartenenti alla NATO o che abbiano accordi di collaborazione con quest'ultima.

II Disposizioni per la prevenzione e il contrasto dei reati informatici

II.I Modifiche al Codice penale e al Codice di procedura penale

La Legge Cybersecurity ha apportato modifiche significative al Codice penale, sia in termini di **inasprimento sanzionatorio**, che con riferimento all'**estensione dell'ambito di applicazione** di alcune fattispecie di reato.

In particolare, l'articolo 16 della Legge Cybersecurity ha introdotto numerose modifiche che hanno toccato, fra l'altro, alcuni reati già esistenti e le relative circostanze aggravanti.

Tra le novità più rilevanti, si segnalano:

(i) l'inasprimento delle pene per i reati di accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.) e di danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* c.p.);

(ii) l'estensione delle fattispecie aggravate per i medesimi reati, includendovi anche l'uso di minaccia, la sottrazione o l'inaccessibilità dei dati e il caso di abuso da parte di pubblici ufficiali, incaricati di pubblico servizio o investigatori privati;

(iii) l'introduzione del reato di estorsione mediante reati informatici (art. 629, co. 3, c.p.), con previsione di pene elevate;
(iv) l'introduzione di una circostanza aggravante per il reato di truffa commesso a distanza con strumenti informatici o telematici (art. 640, co. 2, n. 2-*ter*, c.p.), con applicazione della confisca;
(v) l'introduzione di due circostanze attenuanti per taluni reati informatici, in relazione alla lieve entità del fatto o all'azione del reo per evitare conseguenze ulteriori (artt. 623-*quater* e 639-*ter* c.p.);
(vi) la modifica di altre fattispecie di reati informatici, tra cui la detenzione, diffusione e installazione abusiva di dispositivi informatici (art. 635-*quater*.1 c.p.), il danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-*quinquies* c.p.) e le intercettazioni illecite (artt. 617-*bis ss.* c.p.).

Quanto, invece, alle modifiche al Codice di procedura penale, si evidenziano:
(i) l'attribuzione della competenza alla procura distrettuale per i reati di detenzione, diffusione e installazione abusiva di dispositivi informatici (art. 635-*quater*.1 c.p.), danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-*quinquies* c.p.) e comunicazione di informazioni, dati o elementi di fatto non rispondenti al vero (art. 1, co. 11, d.lgs. n. 105/2019, conv. con l. n. 133/2019) (art. 51, co. 3-*quinquies*, c.p.p.);
(ii) l'estensione del termine di durata massima delle indagini preliminari a 2 anni per taluni reati informatici commessi in danno di sistemi informatici o telematici di interesse pubblico (art. 407, co. 2, lett. a), n. 7-*ter*, c.p.p.);
(iii) l'estensione del regime semplificato per la concessione della proroga del termine per la conclusione delle indagini preliminari anche ai reati informatici di cui al sopra citato art. 407, co. 2, lett. a), n. 7-*ter*, c.p.p. (art. 406, co. 5-*bis*, c.p.p.).

II.II Modifiche al d. lgs. n. 231/2001

La Legge Cybersecurity è intervenuta anche sul d.lgs. n. 231/2001 in materia di responsabilità amministrativa da reato degli enti, attraverso la previsione di un nuovo reato presupposto e l'innalzamento delle sanzioni pecuniarie. Si segnalano, in particolare:
(i) l'aumento delle sanzioni pecuniarie per gli enti in relazione ai reati informatici di cui all'art. 24-*bis*, co. 1, d.lgs. n. 231/2001;
(ii) l'introduzione di una nuova sanzione pecuniaria per gli enti in relazione al reato di estorsione informatica di cui all'art. 629, co. 3, c.p., con

applicazione delle sanzioni interdittive per una durata non inferiore a 2 anni;

(iii) l'innalzamento della sanzione pecuniaria per gli enti in relazione ai reati informatici di cui all'art. 24-*bis*, co. 2, d.lgs. n. 231/2001 e sostituzione del riferimento all'art. 615-*quinquies* c.p. con quello all'art. 635-*quater*.1 c.p.

III Conclusioni e suggerimenti

Le novità introdotte dalla Legge Cybersecurity ribadiscono la crescente centralità del tema della cybersecurity per le aziende. Pertanto, le seguenti azioni diventano di fondamentale importanza:

- Predisposizione o revisione delle procedure di classificazione degli incidenti
- Revisione delle procedure interne di notifica
- Strutturazione di processi di *vulnerability management*
- Revisione dei processi di procurement ovvero, laddove la società sia un fornitore, *assessment* sulle misure di cybersecurity in essere e predisposizione della documentazione necessaria a darne atto
- Revisione e aggiornamento dei modelli di organizzazione, gestione e controllo, in modo da includere le nuove fattispecie di reato e le relative procedure di prevenzione e di reazione
- Formazione e sensibilizzazione del personale e dei collaboratori sulle norme e le best practice in materia di sicurezza informatica e di rispetto della normativa in materia di protezione dei dati personali
- Verifica e potenziamento delle misure tecniche e organizzative di protezione dei sistemi informatici o telematici aziendali, in particolare quelli di interesse pubblico o che trattano categorie particolari di dati personali
- Costante collaborazione – anche attraverso gli opportuni flussi informativi – tra Organismo di Vigilanza e Responsabile della protezione dei dati (Data Protection Officer, "DPO"), che si pongono come figure fondamentali nell'attività di monitoraggio e prevenzione dei rischi connessi alla commissione di reati informatici, in ottica di rafforzamento e valorizzazione di un sistema di compliance integrata
- Collaborazione con le autorità competenti in ipotesi di violazione o sospetto di violazione dei sistemi informatici o telematici aziendali, al fine di limitare i danni e beneficiare di eventuali attenuanti

Contatti

Francesco D'Alessandro
Partner – Chiomenti
White Collar Crime & Investigation
T. +39 02 72157676
francesco.dalessandro@chiomenti.net

Alain Maria Dell'Osso
Partner – Chiomenti
White Collar Crime & Investigation
T. +39 02 72157673
alain.dellosso@chiomenti.net

Marilena Hyeraci
Of Counsel – Chiomenti
Data Protection and Cybersecurity
T. +39 02 721571
marilena.hyeraci@chiomenti.net

Stefano Manacorda
Of Counsel – Chiomenti
White Collar Crime & Investigation
T. +39 06 46622243
stefano.manacorda@chiomenti.net

Pierluigi Perri
Of Counsel – Chiomenti
Data Protection and Cybersecurity
T. +39 02 721571
pierluigi.perri@chiomenti.net

Ennio Alagia
Managing Associate – Chiomenti
White Collar Crime & Investigation
T. +39 02 72157828
ennio.alagia@chiomenti.net

Lucrezia Falciai
Associate – Chiomenti
Data Protection and Cybersecurity
T. +39 02 721571
lucrezia.falciai@chiomenti.net

Virginia Putortì
Associate – Chiomenti
Data Protection and Cybersecurity
T. +39 02 721571
virginia.putorti@chiomenti.net