Direttiva NIS2: prendono forma le nuove norme europee sulla sicurezza informatica e delle reti

Il Consiglio Europeo ed il Parlamento europeo hanno recentemente raggiunto un'intesa politica sulle nuove misure per un livello comune elevato di cibersicurezza in tutta l'Unione, al fine di migliorare ulteriormente la resilienza e le capacità di risposta agli incidenti del settore pubblico e privato e dell'UE nel suo insieme.

Si tratta della nuova Direttiva denominata "NIS2" che, una volta definitivamente adottata, andrà a sostituirà l'attuale Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi (NIS), primo strutturato atto legislativo a livello europeo sulla sicurezza informatica, ancora in corso di vigenza.

Adottata nel lontano maggio 2016 la e recepita in Italia con il D.lgs. 18 maggio 2018, n. 65 (anche detto "decreto legislativo NIS"), la NIS ha risposto alla progressiva esposizione dell'Europa alle minacce informatiche che nel corso degli anni sono diventate sempre più frequenti e pervasive, per via di un aumento esponenziale della superficie esposta nell'ecosistema digitale, ormai sempre più eterogeneamente interconnesso.

La direttiva NIS2 mira a fronteggiare ulteriormente questo trend di escalation cyber, rispondendo all'esigenza di protezione, in modo omogeneo nel lungo termine, a livello europeo, dei servizi e presidi essenziali e strategici di ciascuno Stato membro, includendo adesso anche Organizzazioni di medie e grandi dimensioni di più settori critici per

l’economia e la società, compresi i fornitori di servizi pubblici di comunicazione elettronica, servizi digitali, acque reflue e gestione dei rifiuti, produzione di prodotti critici, servizi postali e di corriere e pubblica amministrazione, sia a livello centrale che regionale.
Il requisito dimensionale rappresenta peraltro una delle novità maggiormente significative dell’intesa politica perché i soggetti inclusi nell’alveo applicativo della nuova Direttiva verranno espressamente indicati dal Legislatore europeo, che ne circoscriverà l’ambito sulla base dei criteri di proporzionalità, un livello di gestione del rischio e criticità.
A tal riguardo vale la pena di evidenziare che la NIS2 si applicherà agli enti della pubblica amministrazione a livello centrale e regionale, riservandosi ai singoli Stati membri l’opportunità di estenderne l’applicazione a livello più periferico.

La NIS2 includerà anche l’adozione di misure di gestione del rischio di cibersicurezza per il settore sanitario, con particolare riferimento ai produttori di dispositivi medicali, proprio per rispondere alle crescenti minacce alla sicurezza rilevate durante la pandemia di COVID-19.
Dunque, la nuova direttiva intende rafforzare i requisiti di sicurezza informatica imposti alle aziende, attraverso l’introduzione di un quadro normativo che preveda un meccanismo più omogeneo ed efficace sia in termini di requisiti sia di misure di sicurezza, per la cooperazione nella gestione del rischio, degli incidenti nonché per lo snellimento degli obblighi di segnalazione in tutti i settori che rientrano nel perimetro dalla direttiva, nell’ambito di EU-CyCLONe, ossia dell’organizzata rete europea di collegamento per le crisi informatiche, che sosterrà la gestione coordinata degli incidenti di sicurezza informatica su larga scala e favorirà la condivisione di best practices a livello nazionale ed europeo.
A tal riguardo, la NIS2 nell’aggiornare l’elenco dei settori e

delle attività soggetti agli obblighi di sicurezza informatica andrà anche a prevedere una serie di rimedi e sanzioni per garantirne l’effettiva applicazione.

A tal proposito, di fondamentale importanza è il tema della sicurezza delle catene di approvvigionamento e delle relazioni con i fornitori che vede introdurre adesso la responsabilità del top management nel caso di mancata osservanza degli obblighi di sicurezza informatica, introducendo altresì misure di vigilanza più rigorose per le autorità nazionali.

L’accordo provvisorio raggiunto, nel caso di definitiva approvazione da parte del Consiglio europeo e del Parlamento europeo prevederà a carico degli Stati membri un generale obbligo di recepimento della nuova Direttiva negli ordinamenti giuridici nazionali nel termine dilatorio di 21 mesi dalla sua entrata in vigore.