Legge Cyber-security, n. 90/2024, e 231: la responsabilità dell'Ente alla luce della nuova disciplina dei reati informatici

Dopo l'approvazione dello scorso 19 giugno, da parte del Senato, del nuovo DDL n. 1717 in materia di *rafforzamento della cybersicurezza nazionale e di reati informatici*, è stata pubblicata oggi in Gazzetta Ufficiale la **Legge n. 90/2024** che entrerà in vigore dal prossimo 17 luglio.
Con il provvedimento, si assiste all'introduzione di un nuovo tassello che funge da *trait d'union* tra la normativa sempre più attuale e il D. Lgs. 231/2001.
In particolare, la novella, si dedica nella prima parte al rafforzamento della sicurezza cibernetica nazionale e al contrasto del *cyber crime,* agli attacchi a sistemi telematici e banche dati in uso presso gli uffici giudiziari; nella seconda, invece, si concentra sul trattamento sanzionatorio dei reati informatici, sulle modifiche di carattere processuale e sulle innovazioni in tema di responsabilità amministrativa degli enti.

In particolare, quali sono le nuove implicazioni per la Responsabilità degli Enti (D. Lgs. 231/2001) con tale novella?

Le modifiche sostanziali apportate dalla Legge *Cybersecurity* (in particolare, Cfr. art. 16) si riflettono e modificano diverse fattispecie rientranti all'intero del novero dei reati c.d. presupposto del D. Lgs. 231/2001.
Segnatamente, la norma, all'art. 20, modifica l'art. *24bis* del D. Lgs. 231/2001 su i "*Delitti informatici e trattamento illecito di dati*" nei seguenti termini:

- aumento **delle sanzioni** previste al **comma 1** che passano dalla cornice edittale compresa tra cento e cinquecento quote, a quella compresa tra duecento e settecento;
- introdotto nell'art. 24*bis* il nuovo **comma 1-bis**: si applicherà all'ente la sanzione pecuniaria da trecento a ottocento euro in relazione alla commissione della **nuova fattispecie di estorsione informatica** di cui all'art. 629, terzo comma, c.p.;
- modificato il **comma 2** dell'art. 24*bis***,** elevando la sanzione pecuniaria sino a quattrocento euro, e sostituendo tra i reati presupposto per i quali è prevista l'applicazione all'ente della sanzione pecuniaria suddetta il riferimento all'art. 615-quinquies c.p. (abrogato dall'art. 16, lettera d. della Legge), con il richiamo al **nuovo delitto di detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico,** di cui all'art. 635-quater.1;
- viene integrato il **comma 4** dell'art. 24*bis*: nei casi di condanna per il delitto indicato nel comma 1-bis si **applicheranno le sanzioni interdittive previste dall'art. 9, comma 2**, per una durata non inferiore a due anni.

Ebbene vista l'attenzione sempre più alta posta dal legislatore nazionale e sovranazionale sui

reati informatici, è doveroso chiedersi come le Società possano contrastare tali illeciti e porre in essere azioni preventive.

Dirimente, per le Aziende, è l'adozione ed efficace attuazione del Modello di Organizzazione e Gestione ai sensi del D.Lgs. 231/2001 e, conseguentemente, la nomina di un Organismo di Vigilanza, avente il compito di vigilare sul MOG stesso.
Infatti, costruendo un sistema di procedure e regole chiare da un lato e avendo nominato un soggetto con reali poteri di controllo dall'altro, si impedirà, o quantomeno si ridurrà al minimo, la commissione di reati.
Come noto, nel caso in cui l'Ente implementi e rispetti tali regole potrà andare esente da responsabilità.
Allo stesso modo, con l'introduzione del MOG, l'Azienda non solo potrà, con l'aiuto dei professionisti, valutare da vicino quali fattispecie di reato siano astrattamente configurabili all'interno della propria realtà, ma anche cogliere quali siano le attività sensibili e le possibili criticità.
Ciò consentirà all'Ente di attuare tutti gli interventi preventivi e/o correttivi più opportuni, valutare la corretta gestione dei rischi per la sicurezza delle informazioni e, forse il punto più importante, rivedere i regolamenti aziendali informatici, nonché realizzare una campagna di sensibilizzazione alla sicurezza informatica.

In conclusione

Il legislatore, specie nell'ultimo periodo, visto anche l'avvento dell'intelligenza artificiale, nel presumibile intento di colmare tutti i vuoti normativi, sta avanzando nel tentativo di "ringiovanire" la normativa in tema di reati presupposti e responsabilità amministrativa degli enti (D. Lgs. 231/2001).
Si ricorda, infatti, che, sebbene la norma risalga al 2001, ad oggi, il numero di Aziende che ha effettivamente adottato un Modello di Organizzazione e Gestione è limitato e, soprattutto, non omogeneo.
Si ritiene quindi che quest'ultima svolta in materia di Cybersicurezza potrebbe, una volta per tutte, indirizzare la maggior parte delle imprese italiane verso la *compliance* legislativa, da raggiungersi con il connubio tra l'implementazione di procedure e misure di prevenzione e sicurezza e la formalizzazione di un sistema di gestione su misura tramite il MOG 231/2001.

Studio Legale Mosetti Compagnone