D&O E CYBER: COSA CAMBIA PER LA RESPONSABILITÀ DIRIGENZIALE

L'EVOLUZIONE DEI REGOLAMENTI SULLA SICUREZZA INFORMATICA E LA PRIVACY È UN CAMBIO DI PARADIGMA NELLA GOVERNANCE AZIENDALE CHE PREVEDE PER I VERTICI DELLE AZIENDE UNA MAGGIORE ATTENZIONE, E PER LE COMPAGNIE UNA REVISIONE E UN ARRICCHIMENTO DELLE POLIZZE, COSÌ DA DARE UN VALORE AGGIUNTO

*di **Giorgio Grasso**, senior partner di Btg Legal*

Nel 2025, le polizze D&O devono affrontare un cambiamento epocale. Con l'entrata in vigore di *Dora* (Regolamento Ue 2022/2554) e *Nis 2* (Direttiva Ue 2022/2555 recepita con dlgs 138/2024), senza voler tralasciare altresì le altre norme di settore quali *Gdpr*, *AI Act* e *Cyber resilience act*, il concetto di governance aziendale si amplia enormemente.

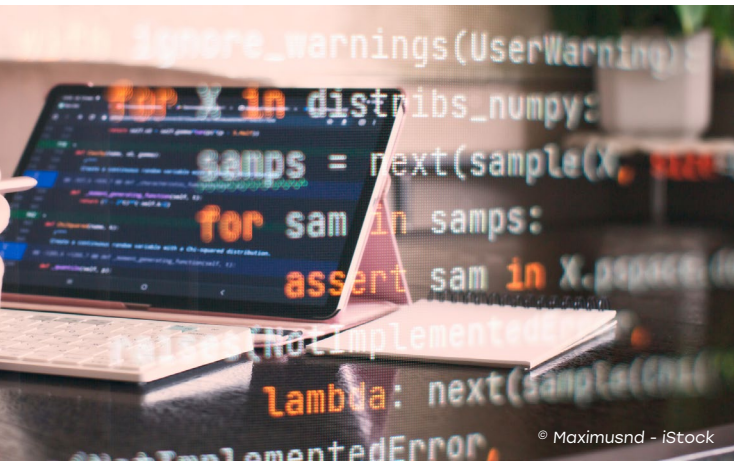
I dirigenti non sono più responsabili solo delle decisioni finanziarie e operative, ma anche della sicurezza informatica, della protezione dei dati e dell'uso etico dell'intelligenza artificiale. Le conseguenze di una mancata conformità possono essere devastanti, sia in termini di sanzioni economiche sia di interdizioni personali per il board. Le compagnie devono rispondere a tale nuova esposizione al rischio, aggiornando le polizze D&O per garantire una protezione adeguata ai dirigenti.

Obblighi di vigilanza e di gestione

L'approccio normativo europeo alla cybersicurezza ha subito un cambiamento radicale con l'introduzione di Dora e Nis 2, che impongono ai vertici aziendali obblighi specifici di vigilanza e di gestione del rischio digitale. Se il regolamento Dora è destinato a disciplinare la resilienza operativa digitale nel settore delle entità finanziarie (bancarie e assicurative *in primis*), la direttiva Nis 2 amplia il perimetro delle imprese obbligate a conformarsi a standard di sicurezza più elevati, includendo settori critici come energia, trasporti, sanità, telecomunicazioni e infrastrutture digitali. L'articolo 5 del Dora attribuisce espressamente ai membri del consiglio di amministrazione una "responsabilità finale per la gestione dei rischi informatici dell'entità finanziaria". Mentre l'articolo 11 impone di integrare la gestione del rischio Ict nella governance aziendale. Il regolamento stabilisce le tempistiche per la segnalazione: una notifica iniziale entro 24 ore dall'identificazione dell'incidente, un report intermedio entro 72 ore con aggiornamenti successivi, e un report finale entro un mese dall'ultimo aggiornamento, pena sanzioni fino a cinque milioni di euro o il 10% del fatturato globale, con la possibilità di interdizione temporanea dei dirigenti responsabili.

Resilienza digitale e governance d'impresa

Parallelamente, la direttiva Nis 2 amplia ulteriormente il regime di responsabilità estendendolo agli operatori essenzia-



li e importanti, imponendo, tra l'altro, ai vertici apicali l'obbligo di approvare e supervisionare direttamente le strategie di cybersecurity (ex articolo 20), non limitandosi a delegarle ai responsabili IT. Infine, entrambe le normative (come per il Gdpr) prevedono una tempistica estremamente rigida per la segnalazione degli incidenti (pena sanzioni particolarmente severe) e questo significa aver attuato un preventivo piano di comunicazioni della crisi. In tale contesto, la responsabilità degli amministratori non si limita più alla gestione finanziaria e operativa dell'impresa, ma si estende alla cybersicurezza e alla gestione del rischio informatico. Questo principio trova fondamento giuridico nell'articolo 2086 del Codice civile che, nella sua nuova formulazione, impone agli amministratori l'adozione di "un assetto organizzativo, amministrativo e contabile adeguato alla natura e alle dimensioni dell'impresa". Un'interpretazione attuale della norma impone di considerare la resilienza digitale come parte integrante della governance d'impresa.

La mancata adozione di misure adeguate di protezione dei dati, sicurezza informatica e gestione dell'AI può compromettere la stabilità dell'impresa, esponendo gli amministratori non solo a sanzioni regolatorie, ma altresì ad azioni di responsabilità da parte di azionisti, creditori e clienti.

Nuove estensioni per le polizze

Questa convergenza normativa ha indubbiamente una conseguenza diretta sulle polizze D&O, che non possono più essere considerate uno strumento statico e generalista: il rischio cyber è diventato un elemento strutturale della responsabilità manageriale e deve essere trattato come tale anche in ambito assicurativo. Le tradizionali polizze D&O erano state concepite per proteggere i dirigenti da azioni legali derivanti da errori di gestione, negligenza e violazioni normative di carattere generale. Tuttavia, l'introduzione di sanzioni sempre più severe e la responsabilizzazione diretta del board sulla cybersecurity impongono una revisione della struttura delle coperture, che devono essere adattate per rispondere alle nuove tipologie di rischio. Le compagnie stanno già pensando a modifiche nei contratti D&O, introducendo nuove esclusioni, nuove condizioni di sottoscrizione e una maggiore interconnessione tra polizze D&O e cyber.

Un tema, ad esempio, è rappresentato dalle sanzioni amministrative e dalle interdizioni (le polizze escludono la copertura per le sanzioni regolatorie, ma maggiore attenzione potrebbe essere dedicata alle spese legali e ai costi di compliance sostenuti per contestare le sanzioni imposte da autorità regolatorie in caso di violazioni Nis 2 o Dora). Si potrebbero altresì prevedere delle estensioni/sezioni di copertura per cyber governance, failure to prevent risk e data breach. Dall'altro, occorrerebbe pensare a esclusioni specifiche (ad esempio, chiarendo l'esclusione degli atti intenzionali – vi ricade la deliberata omissione di una notifica di data breach per evitare danni reputazionali – ovvero inserendo l'esclusione per mancata adozione di *compliance cyber* prevista dalla normativa).

Un valore aggiunto per le aziende

Per evitare una maggiore esposizione al rischio, le compagnie potrebbero introdurre parametri di valutazione della compliance aziendale, da richiedere in sede assuntiva (cybersecurity risk assessment; obbligo di reporting degli incidenti; presenza di piani di continuità operativa).

Un ulteriore sviluppo tecnico della polizza D&O potrebbe essere l'integrazione con la copertura cyber risk, prevedendo una sinergia tra le due polizze. Le polizze cyber più avanzate, inoltre, potrebbero fornire copertura finanziaria in caso di eventi come il cosiddetto system failure del fornitore terzo di servizi IT, nel caso in cui questi determinino un'interruzione del funzionamento dei sistemi IT aziendali (con conseguente interruzione delle attività, ulteriori costi straordinari per il ripristino dell'operatività, nonché perdita di dati e spese legali).

In chiusura, l'evoluzione normativa cyber non è solo un aggiornamento regolatorio, ma un vero e proprio cambio di paradigma nella governance aziendale, che impone ai vertici aziendali una maggiore attenzione alle tematiche di sicurezza informatica e alle compagnie un cambio di rotta sulle polizze D&O che, ora più che mai, possono costituire un valore aggiunto per le aziende del Paese.