

# RISCHI AMBIENTALI E CYBER: AEC AL FIANCO DI PMI ED ENTI LOCALI

LE EVOLUZIONI NORMATIVE IN TEMA DI INQUINAMENTO E DI CYBER RISK APRONO NUOVI SCENARI E OPPORTUNITÀ. CHE IL GRUPPO VUOLE COGLIERE, PUNTANDO SU UN APPROCCIO SPECIALISTICO PER PMI ED ENTI PUBBLICI

Le nuove norme sui reati ambientali sono operative: dopo la pubblicazione in Gazzetta Ufficiale della legge 68/2015, che interviene sugli ecoreati a tutto campo, vengono inserite, nel codice penale, nuovi delitti che portano novità rilevanti, come quelle che aggravano la posizione di chi commette il reato, ma anche la possibilità di una potenziale riduzione della pena inflitta, grazie a soluzioni assicurative *ad hoc* che rispondono alle misure concrete di mitigazione del danno indicate dal legislatore.

“L’introduzione di questi ecoreati – spiega **Federico Capuzzo**, responsabile dell’intermediazione di **Aec Underwriting** – farà sì che sempre più aziende si adopereranno per attivare programmi assicurativi. Il mercato sta rispondendo nell’ottica di soluzioni semplificate, compatibili con le esigenze e le dimensioni di quelle realtà aziendali non molto grandi e più diffuse nel settore produttivo italiano, nonché degli enti locali”.

## CYBER: POCHE LE COPERTURE E SOLO PER LE GRANDI AZIENDE

Novità anche sul fronte del cyber risk, in particolare con il *Data breach notification* che espone l’azienda, in mancanza di elementi che dimostrino che il sistema è stato bucato nonostante fosse protetto, a conseguenze su un triplice profilo: penale, civile e amministrativo.

Nonostante questo nuovo scenario, però, solo le grandi imprese, in particolare dei settori bancario, telecomunicazioni, IT, si sono dotate di coperture cyber risk. “Per questo motivo - conferma Capuzzo – il gruppo Aec, in linea con la solida partnership con **Chubb**, ha deciso di estendere anche al cyber quell’approccio specialistico

## IL VOLANO ARRIVA DALL’EUROPA

Uno dei *driver* più forti in tema IT security è rappresentato dall’evoluzione normativa che la Ue imporrà sul tema, in particolare, con il Reg. 679/2016. Fra tutte le implicazioni di compliance, di particolare rilievo è il *Data breach notification*, che impone alle imprese di informare le autorità di controllo non oltre 72 ore dopo essere venuti a conoscenza dell’attacco informatico. Senza un sistema efficace e sicuro, infatti, è difficile anche solamente accorgersi di un attacco. Quindi sarà nell’interesse dell’azienda attivarsi con soluzioni assicurative che possano andare a coprire quelle aree IT più esposte a questo tipo di rischi.

che lo contraddistingue e lo rende in grado di anticipare rischi e sensibilità che si posizioneranno a breve ai primi posti fra le priorità delle aziende italiane. L’obiettivo è sviluppare lo small/middle market per consentire alle Pmi e ai professionisti interessati da questi rischi di avere una buona copertura. Vista la scarsa sensibilità su entrambi i temi, più aumenta la cultura del rischio e più si assisterà a un progressivo ingrandimento del mercato, sia in termini di soluzioni offerte che di premi complessivamente raggiunti. Le sfide del presente e del futuro prossimo, impongono così a tutti i player del mercato: imprese, professionisti, enti pubblici e, ovviamente, intermediari di assicurazione”.