Awareness, compliance, security by design: come faranno a sopravvivere le PMI?

Iniziamo il 2020 con una riflessione sul cambio di paradigma della *compliance* (osservanza) delle norme e delle direttive internazionali per la tutela dai rischi (informatici, ambientali, alimentari, ecc), che risulta oggi indirizzata verso criteri di "consapevolezza" e di "responsabilizzazione" e non più all'esecuzione acritica di prescrizioni autoritarie.
Come sottolinea Corrado Giustozzi nell'**intervista a essecome**: *"Si è passati in modo abbastanza repentino da un approccio interamente prescrittivo, basato su una logica che potremmo definire "dell'adempimento", ad un approccio finalizzato ai risultati e basato su una logica "della responsabilizzazione".*
Esaminando le disposizioni più recenti che interessano a vario titolo il mondo della sicurezza, si osserva che norme relative ad ambiti tra loro diversi - come GDPR e Direttiva NIS per la sicurezza delle informazioni, ISO 31030 per la tutela dei lavoratori in missione, Direttiva (UE) 2018/843 sull'antiriciaggio - condividano in realtà lo stesso approccio impostato su procedure di "analisi dei rischi", "analisi d'impatto" e "progettazione autonoma delle misure di sicurezza" che, almeno in Italia, sono ancora piuttosto sconosciute.
Si starebbe dunque delineando un intrigante salto culturale per l'intero Sistema Paese (aziende pubbliche e private, consulenti, organi di controllo), ma non si possono sottovalutare le conseguenze sul piano pratico, in particolare per le piccole/medie imprese.
Secondo molti osservatori, se le grandi organizzazioni industriali e finanziarie sono già orientate verso questi nuovi approcci o, quanto meno, sono in grado di investire per adeguarsi, le **PMI** possono trovarsi in difficoltà non solo nell'attuare le procedure richieste (magari per un banale motivo di costi) ma, in molti casi, perfino nel sapere dell'esistenza di norme che le riguardano e che devono rispettare.
Sicurezza delle reti e dei dati (per tutti), gestione delle trasferte dei dipendenti (per chiunque lavori all'estero) e procedure antiriciclaggio (per chiunque maneggi denaro contante) potrebbero quindi diventare altrettante occasioni di inadempimento per la galassia delle PMI che, ricordiamo, nel 2017 contava 5,3 milioni di imprese con oltre 15 milioni di addetti **(Prometeia - Sole 24 Ore)**.
Inadempimenti che possono comportare non solo alti rischi economici per sanzioni ed eventuali risarcimenti, ma anche danni reputazionali e conseguenze penali per gli amministratori nei casi più gravi.
Per attenuare questi rischi, sarebbe necessario che governo, parti sociali (associazioni di categoria, sindacati dei lavoratori) e gli operatori dell'info/formazione si facessero carico, ognuno per la propria parte, della diffusione della conoscenza delle norme e dei percorsi per la compliance. Purtroppo, il primo problema è il loro livello di informazione e di consapevolezza su questi temi...
In questa situazione, la filiera della sicurezza, per quanto costituita principalmente da PMI esposte agli stessi rischi, potrebbe cogliere l'opportunità di proporsi come *problem* solver per gli ambiti di competenza, offrendo soluzioni efficaci e, soprattutto, sostenibili all'enorme bacino di soggetti che devono mettersi in regola, ma non possono farlo da soli.
In fondo, non sarebbe anche questo un modo per "fare sicurezza"?