Digitalizzazione, Regolamentazione

Cybersicurezza ***senza illusioni regolatorie***

21.01.2026

A colpo d'occhio

- Dopo anni di crescente regolamentazione, l'UE punta sempre più su semplificazione, armonizzazione e sicurezza degli investimenti, anziché introdurre continuamente nuove norme dettagliate.
- Misure guidate dal mercato, standard internazionali e competenza tecnologica contribuiscono maggiormente alla resilienza rispetto a requisiti statali sempre più frammentati.
- La Svizzera ha finora adottato un approccio equilibrato nel settore della cybersicurezza: ora risulta fondamentale non abbandonarlo e non riprendere regolamentazioni che l'UE stessa sta già iniziando a correggere.

L’Unione europea apre un nuovo capitolo nella politica digitale. Dopo anni di crescente regolamentazione, si moltiplicano i segnali di una correzione di rotta. Il Digital Omnibus, il previsto Digital Networks Act, la revisione del Cyber Security Act e l’attuale Digital Fitnesscheck si riassumono in una tendenza chiara: semplificazione, armonizzazione e maggiore attenzione agli investimenti e all’attuazione, anziché all’introduzione continua di nuove norme dettagliate.

Cosa riconosce ora l’UE – e da cosa dovrebbe imparare la Svizzera

Un pregiudizio centrale continua a influenzare molti dibattiti: la cybersicurezza si realizzerebbe solo se lo Stato obbliga le imprese ad agire. Si ritiene che misure volontarie e meccanismi di mercato non siano sufficienti. La pratica mostra invece un quadro diverso.

La cybersicurezza, per le imprese, non è un “nice-to-have”, ma un fattore esistenziale. Perdite di dati, interruzioni della produzione o danni alla reputazione hanno conseguenze economiche dirette. Ma l’entità e la tempestività degli investimenti nella cybersicurezza variano significativamente in base alla dimensione dell’impresa.

Le piccole e medie imprese (PMI) sono già sottoposte a notevoli oneri economici e burocratici. Spesso mancano dei margini finanziari per implementare per tempo complesse disposizioni regolatorie in materia di cybersicurezza. Ulteriori norme dettagliate aiutano poco. Sono maggiormente efficaci la sensibilizzazione, l’orientamento e informazioni facilmente accessibili, che permettano di gestire i rischi in modo proporzionato e graduale. Inoltre, standard internazionali e certificazioni come l’ISO 27001 o i framework NIST vanno spesso ben oltre i requisiti minimi di legge.

Va anche considerato che i fornitori moderni di servizi cloud e di sicurezza operano Security Operation Center globali e investono miliardi in rilevamento delle minacce, ridondanza e automazione. Questo livello di sicurezza deriva dalla vicinanza alla tecnologia e dalla capacità di adattamento rapido – non da direttive amministrative.

Ciò non significa che lo Stato non abbia un ruolo. Interviene laddove i meccanismi di mercato mostrano i loro limiti: per standard minimi nelle infrastrutture critiche, per responsabilità chiaramente definite e per trasparenza. Ciò che però non può fornire è la cybersicurezza operativa nella quotidianità. Le minacce evolvono più rapidamente della regolamentazione.

Ed è proprio questo che considera il cambio di rotta europeo. Il Cyber Resilience Act illustra in modo chiaro la curva di apprendimento dell'UE. Come intervento complesso e burocratico sul ciclo di vita dei prodotti, era stato duramente criticato dal mondo economico. Il fatto che l'UE ora accolga queste obiezioni non è tanto un successo dello strumento quanto un riconoscimento che una regolamentazione eccessiva diventa uno svantaggio competitivo.

Un vero e proprio cambio di paradigma

Non si tratta di deregolamentazione, ma di politica economica. La sicurezza nasce dalla certezza, non dall'introduzione continua di nuovi obblighi. Gli investimenti in cybersicurezza avvengono lì dove le imprese sanno cosa aspettarsi.

Il ripensamento dell'UE sulla regolamentazione nel settore digitale rappresenta un segnale di allarme – non per una possibile azione unilaterale della Svizzera oggi, ma come promemoria per non abbandonare la rotta attuale. Nel settore della cybersicurezza, la Svizzera ha fatto bene a non correre avanti e a implementare le disposizioni europee con equilibrio. Ora è fondamentale non recepire quei residui regolatori che l'UE stessa ha riconosciuto come troppo complessi e ha iniziato a correggere.

Una cybersicurezza sostenibile si realizza dove le imprese assumono responsabilità – supportate, ma non sostituite, da linee guida statali chiare e semplici. L'UE sta iniziando a mettere in pratica questa consapevolezza. La Svizzera dovrebbe osservare con attenzione.

Angela Anthamatten

Responsabile supplente del dipartimento concorrenza e regolamentazione

David Stauffacher

Responsabile di progetto infrastrutture e digitale