IL FOGLIO – 14 MARZO 2025

Oltre Musk. Ciò che l'Ue non deve fare per vincere la sfida sul cyberspazio

di Stefano Firpo e Valeria Falce

L'Europa ha appena proposto un Piano per il cyberspazio con l'obiettivo di definire e auspicabilmente uniformare strategia e tattica da seguire per gestire incidenti e crisi su larga scala attraverso una risposta coordinata da parte di tutti gli attori coinvolti, civili e militari.

E' questa una raccomandazione non vincolante che, nel promuovere un ecosistema europeo di eccellenza e "fiducia" nei dati, interviene sui rapporti tra Stati membri all'insegna di un nuovo modello di collaborazione integrata.

Nell'attuale contesto di crescente digitalizzazione e diffuse tensioni geopolitiche, infatti, l'intera catena del valore - incluse le imprese di ogni dimensione e settore - è esposta a nuovi rischi, dalla perdita di controllo e condivisione inconsapevole di dati sensibili, ai furti di proprietà intellettuale, alle interruzioni di attività, con conseguenze disastrose sia sul piano economico e legale, che in termini reputazionali. Il cybercrime rimane la principale fonte degli attacchi, tuttavia, si è registra un ritorno dell'hacktivism, con attacchi motivati da ragioni politiche per non dire di vera e propria "guerra cyber".

Secondo il "Cost of a Data Breach Report 2024" il costo medio di una violazione dei dati derivante da attacchi cyber, è passato, a livello globale da 4,45 milioni a 4,88 milioni di dollari nel 2024. L'Italia è il quinto Paese al mondo per esposizione a questo tipo di minacce avendo raggiunto 4,73 milioni di euro nel 2024, con un incremento del 23% rispetto al 2023, a fronte di violazioni sempre più aggressive, che colpiscono innanzitutto il settore tecnologico seguito da quello industriale, sanitario e farmaceutico.

Per rispondere, dunque, ai nuovi rischi cyber, l'Europa si è attrezzata sul fronte delle imprese con la Direttiva Nis2 (recepita in Italia dal D.Lgs. n. 138/2024). Questa allarga il perimetro dei soggetti e dei settori sottoposti ad obblighi di cybersicurezza, regolando il tema della sicurezza delle catene di approvvigionamento e dei rapporti con i fornitori e responsabilizzando gli organi di amministrazione anche attraverso misure di vigilanza più rigorose e un sistema sanzionatorio più severo.

Così facendo, l'Unione spinge le imprese verso la "disruption" della gestione della cybersecurity, da non relegare più a questione di stretta sicurezza IT, ma da elevare a tema strategico e di sviluppo aziendale per le ricadute notevolissime sulla stabilità finanziaria, la produttività e la reputazione d'impresa.

Gli stessi organi di corporate governance sono chiamati a partecipare attivamente e costantemente al processo decisionale attraverso una relazione diretta e un flusso continuo di informazioni con chi è chiamato a gestire i rischi cyber all'interno dell'impresa.
La cybersicurezza esprime perciò una nuova dimensione su cui esercitare la business judgment rule, richiedendo agli organi di governo societario di valutare l'adeguatezza degli investimenti, i piani di risposta agli incidenti e la solidità delle misure da introdurre a garanzia (firewall, sistemi di backup, sistemi crittografici). A tali organi spetta inoltre il compito di promuovere una cultura aziendale incentrata su alfabetizzazione ed "igiene" digitale, per favorire un uso consapevole e responsabile delle nuove tecnologie (come l'intelligenza artificiale) all'interno dell'azienda, con importanti ricadute sull'equilibrio da trovare fra esternalizzazione su infrastrutture cloud as a service e controllo sul patrimonio informativo strategico su infrastrutture di calcolo on premises.
Per passare, secondo gli auspici europei, ad un modello di governo e gestione dei dati, che sia tanto integrato e sicuro, da consentirne la valorizzazione e lo sfruttamento, si tratta pertanto di incoraggiare un salto culturale e uno spostamento di baricentro. Non basta cioè interpretare ed applicare cautele ed obblighi sulla sicurezza cyber in modo formale, ma occorre far proprio un nuovo approccio (oggetto dei lavori della Giunta di Assonime) che ponga i dati, in termini di governo, condivisione, gestione e valorizzazione, tra le priorità strategiche d'impresa.