RESILIENZA OPERATIVA DIGITALE - L'ITALIA SI ADEGUA AL REGOLAMENTO DORA

Con il Decreto Legislativo n. 23/2025, che rappresenta un importante passo avanti nel percorso di modernizzazione del quadro normativo italiano in materia di sicurezza digitale nel settore finanziario, l'Italia si adegua pienamente al Regolamento (UE) 2022/2554 (*DORA - Digital Operational Resilience Act*), che introduce un approccio omogeneo a livello europeo per rafforzare la resilienza delle infrastrutture digitali in ambito finanziario.

Di seguito un'analisi dei principali elementi del decreto, con alcune sintetiche considerazioni.

1. Gestione del rischio ICT

Le istituzioni finanziarie devono dotarsi di un sistema di gestione del rischio ICT (rischio informatico) che sia integrato nella governance aziendale e aggiornato rispetto all'evoluzione delle minacce. L'obbligo non si limita alla protezione da attacchi informatici, ma impone un cambiamento culturale, richiedendo che la sicurezza digitale sia considerata parte integrante della strategia d'impresa, con il coinvolgimento diretto del management e degli organi di controllo. L'obbligo si basa su un principio di proporzionalità, prevedendo che sia commisurato alle dimensioni e alla complessità dei soggetti interessati.

2. Segnalazione degli incidenti significativi

Il decreto impone la comunicazione tempestiva alle autorità competenti nonché al CSIRT Italia (*Computer Security Incident Response Team*, organo dell'Agenzia per la Cybersicurezza Nazionale) di ogni incidente ICT che abbia impatti rilevanti su servizi, clienti o sistemi, con ciò rafforzando la trasparenza e la reattività del sistema finanziario. L'obbligo di segnalazione contribuisce anche a costruire un database centralizzato di minacce e vulnerabilità che può essere utile a livello sistemico per prevenire attacchi futuri.

3. Test di resilienza operativa digitale

Le entità devono effettuare regolarmente verifiche e simulazioni, tra cui i TLPT (Threat-Led Penetration Testing), particolarmente per le infrastrutture critiche. Si tratta di un approccio proattivo, non reattivo: l'obiettivo non è solo reagire agli attacchi, ma prevederli, simularli e anticiparli. Un cambio di paradigma nell'approccio alla cybersecurity nel settore finanziario.

4. Gestione dei rischi legati a fornitori terzi ICT

Il decreto impone obblighi specifici per la gestione dei rapporti con terze parti fornitrici di servizi tecnologici, inclusi cloud, software, e piattaforme. In un contesto in cui sempre più istituzioni esternalizzano componenti fondamentali della propria infrastruttura, il legislatore riconosce che la catena della sicurezza è forte quanto il suo anello più debole, e introduce misure per rafforzarla.

5. Rafforzamento delle autorità di vigilanza

Banca d'Italia, Consob e IVASS ottengono nuovi poteri ispettivi e sanzionatori per garantire il rispetto delle nuove norme DORA. L'armonizzazione europea richiede che anche le autorità nazionali siano adeguatamente attrezzate, al fine di garantire una vigilanza più efficace, con strumenti adeguati a intervenire anche in situazioni complesse o transfrontaliere.

6. Ambito di applicazione

Le regole si applicano a una gamma molto ampia di soggetti, dalle banche tradizionali alle società di criptovalute, riflettendo l'evoluzione dell'ecosistema finanziario, che oggi include molti attori cc.dd. digitali nativi. Il decreto evita così il rischio di "zone grigie" normative, assicurando che tutti gli operatori siano soggetti a standard minimi di resilienza.

7. Sanzioni e misure correttive

Il decreto prevede sanzioni amministrative, anche pecuniarie, graduate in base alla gravità della violazione e ai danni prodotti. Il nuovo sistema sanzionatorio, chiaro e proporzionato, garantisce l'effettività delle nuove disposizioni. Le sanzioni sono anche un incentivo per le imprese a investire in sicurezza e prevenzione, piuttosto che rischiare danni economici e reputazionali.

8. Conclusioni

In conclusione, il decreto non si limita a costituire un adeguamento formale al diritto europeo: esso introduce un vero e proprio cambio di passo nella gestione della sicurezza digitale nel settore finanziario italiano. In un contesto caratterizzato da crescente digitalizzazione e sofisticazione degli attacchi informatici, la resilienza operativa non è più una scelta ma una necessità. Le nuove norme mirano non solo a proteggere singole imprese, ma a tutelare la stabilità dell'intero sistema finanziario, rafforzando al contempo la fiducia degli utenti nei servizi digitali.

Paolo Iemma, Partner
Email: *paolo.iemma@grplex.com*