Cyber Resilience Act e intelligenza artificiale: le implicazioni per il settore finanziario

Da **Redazione BitMAT** - 17/11/2026

Per banche e intermediari, il nuovo quadro normativo rafforza dunque l'importanza di verificare la sicurezza delle soluzioni tecnologiche adottate



La sicurezza informatica dei sistemi di intelligenza artificiale assume crescente rilevanza nel quadro normativo europeo, soprattutto nei settori, come quello bancario e finanziario, caratterizzati da un utilizzo sempre più diffuso di soluzioni tecnologiche avanzate.

In questo contesto si inserisce il **Regolamento (UE) 2024/2847**, noto come *Cyber Resilience Act* (CRA), che introduce requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali, con l'obiettivo di garantirne la sicurezza durante l'intero ciclo di vita.

Il regolamento, la cui applicazione generale è prevista dall'11 dicembre 2027, ha già iniziato a produrre effetti: dall'11 settembre 2026 sono infatti applicabili gli obblighi di segnalazione delle vulnerabilità attivamente sfruttate e degli incidenti gravi previsti dall'articolo 14.

Il coordinamento tra Cyber Resilience Act e AI Act

Particolarmente significativo è il rapporto tra il CRA e il Regolamento (UE) 2024/1689 (*AI Act*), espressamente disciplinato dall'articolo 12 del CRA.

La disposizione prevede che i prodotti con elementi digitali qualificati anche come sistemi di intelligenza artificiale ad alto rischio possano essere considerati conformi ai requisiti di cibersicurezza dell'articolo 15 dell'AI Act, purché soddisfino le condizioni stabilite dal CRA, anche sotto il profilo della documentazione di conformità.

Il considerando 51 richiama, inoltre, le vulnerabilità specifiche dei sistemi di IA, quali gli attacchi volti ad alterare i dati utilizzati dagli algoritmi (*data poisoning*) o a manipolarne le prestazioni (*adversarial attacks*).

Ne emerge un modello regolatorio nel quale la sicurezza dell'intelligenza artificiale non riguarda soltanto l'affidabilità dei risultati prodotti, ma anche la protezione delle infrastrutture software e dei componenti digitali che ne consentono il funzionamento.

Le ricadute sul sistema finanziario e il rapporto con DORA

Le disposizioni assumono particolare interesse per gli operatori finanziari che utilizzano sistemi di IA nell'analisi dei dati, nella prevenzione delle frodi e nella valutazione del merito creditizio.

In tale ambito, il CRA si affianca al **Regolamento (UE) 2022/2554 (*Digital Operational Resilience Act* – DORA)**, applicabile dal 17 gennaio 2025, che impone alle entità finanziarie specifici presidi di gestione dei rischi informatici e di controllo dei fornitori terzi di servizi ICT.

Le due discipline operano su piani distinti ma complementari: mentre il CRA pone requisiti di sicurezza principalmente a carico dei fabbricanti di prodotti digitali, DORA disciplina la resilienza operativa degli intermediari e la gestione dei rischi connessi alle dipendenze tecnologiche.

Il considerando 125 del CRA riconosce espressamente tale complementarità, evidenziando come i requisiti di sicurezza dei prodotti digitali possano agevolare il rispetto degli obblighi relativi alla catena di approvvigionamento previsti da DORA.

Per banche e intermediari, il nuovo quadro normativo rafforza dunque l'importanza di verificare la sicurezza delle soluzioni tecnologiche adottate, senza che la conformità dei prodotti al CRA esaurisca gli autonomi obblighi di gestione del rischio previsti dalla disciplina finanziaria.

La progressiva applicazione del Cyber Resilience Act contribuisce così a delineare un sistema europeo nel quale **sicurezza informatica, affidabilità dell'intelligenza**

artificiale e resilienza operativa finanziaria costituiscono dimensioni strettamente interconnesse.

Di Antonio Ferraguto e Elisa Varisco, Partner di La Scala Società tra Avvocati

Redazione BitMAT

https://www.bitmat.it/

BitMAT Edizioni è una casa editrice che ha sede a Milano con una copertura a 360° per quanto riguarda la comunicazione rivolta agli specialisti dell'Information & Communication Technology.