BANCA D'ITALIA
EUROSISTEMA

Sadibaquarantotto

Cyber Risk e Sistema finanziario

Intervento di Giuseppe Siani
Capo del Dipartimento Vigilanza bancaria e finanziaria della Banca d'Italia

28 marzo 2025

Innovazione tecnologica, resilienza operativa e attività di vigilanza

Ringrazio gli organizzatori dell'evento per aver invitato la Banca d'Italia a questa occasione di discussione su temi di grande importanza per la comunità finanziaria, italiana e internazionale.

L'innovazione tecnologica contribuisce a modificare il perimetro e la composizione del sistema finanziario tradizionale, favorisce lo sviluppo di nuovi modelli operativi e l'adeguamento dei processi.

Gli intermediari possono sfruttare le opportunità offerte dalle nuove tecnologie presidiandone i relativi rischi, adeguare le proprie strategie in un mondo che cambia rapidamente, e rafforzare quindi la sostenibilità nel lungo periodo dei propri modelli operativi.

Oggi vorrei riassumere le principali caratteristiche dell'evoluzione dell'innovazione tecnologica nel sistema finanziario negli ultimi anni, le implicazioni per il rischio informatico e la connessa resilienza operativa degli intermediari, tenuto anche conto della recente entrata in vigore del *Digital Operational Resilience Act* ("DORA"). Concluderò descrivendo brevemente la nostra attività di vigilanza in materia.

L'innovazione tecnologia e il sistema finanziario

La Banca d'Italia segue con attenzione la trasformazione digitale degli intermediari anche sulla base di specifiche indagini[1]. Vorrei in particolare segnalare due principali risultati emersi negli ultimi anni. In primo luogo l'eterogeneità dei comportamenti degli intermediari vigilati: se, da un lato, gli investimenti nelle tecnologie innovative

---

[1] L'Indagine Fintech condotta dalla Vigilanza approfondisce dal 2017, con cadenza biennale, lo stato dell'adozione delle innovazioni tecnologiche applicate ai servizi finanziari (Banca d'Italia - Indagine Fintech nel sistema finanziario italiano - 2023). La nuova edizione dell'Indagine è in corso; la scadenza per gli intermediari è fissata al 31 marzo 2025.

– tra effettivi e stimati – sono aumentati di circa quattro volte tra il 2017 e il 2024, dall'altro tale spesa è concentrata in un numero limitato di grandi intermediari (il 90 per cento è riconducibile ai dieci principali operatori)[2]; inoltre, l'intermediazione creditizia e i pagamenti rappresentano le aree operative maggiormente interessate dalla digitalizzazione (ciascuna per circa il 40 per cento del totale).

Un secondo profilo rilevante riguarda il maggiore coinvolgimento delle cosiddette terze parti, tenuto conto dell'aumento sia delle collaborazioni, come emerge dalla crescita di tutte le tradizionali variabili di riferimento[3], sia delle partecipazioni nel capitale di imprese fornitrici di servizi tecnologici.

Tale fenomeno è confermato anche dai risultati della segnalazione di vigilanza relativa all'esternalizzazione di funzioni aziendali[4], che evidenzia ormai la presenza di circa 6.000 contratti relativi a funzioni essenziali, in essere con 1.500 fornitori.

L'innovazione offre sicuramente nuove opportunità operative, ma il maggior utilizzo della leva tecnologica aumenta l'esposizione ai rischi, anche di tipo informatico, degli intermediari. Le evidenze preliminari a disposizione della Vigilanza confermano ad esempio la crescita anche nel 2024 degli incidenti informatici e della rilevanza della *supply chain* del sistema finanziario. In particolare, il numero di incidenti totali e di quelli cyber è aumentato rispettivamente del 45 e dell'8 per cento rispetto all'anno precedente[5]. Risulta inoltre confermata la crescente interconnessione del sistema, evidenziata dall'aumento del numero di intermediari coinvolti in media in singoli eventi e dal crescente coinvolgimento dei fornitori di servizi, rilevabile in circa due terzi degli incidenti (erano meno della metà nel 2023).

Gli impatti economici degli incidenti si mantengono in genere limitati, ma è l'interruzione della disponibilità e della continuità dei servizi a rappresentare la principale conseguenza degli incidenti (in circa il 70 per cento dei casi). È inoltre più che raddoppiato il tempo medio di interruzione dei servizi a causa di un incidente. Risulta infine in significativa crescita il numero degli intermediari che hanno effettuato almeno una segnalazione di incidente. È importante che gli intermediari non temano un "effetto stigma", ma considerino l'importanza di inviare queste informazioni alle Autorità per valutare, se del caso, una risposta coordinata in caso di crisi sistemica.

A livello europeo, il Regolamento DORA promuove la massima armonizzazione delle informazioni da riportare alle Autorità in caso di incidente. Nell'ambito del G20, il *Financial Stability Board* sta finalizzando la definizione di un formato comune per la segnalazione degli incidenti, il cd FIRE ("*Format for Incident Reporting Exchange*"), con

---

2 Analoga eterogeneità emerge anche in termini di tecnologie sviluppate, tenuto conto che le piattaforme web-mobile, l'intelligenza artificiale (AI) e le *Application Programming Interfaces* (API) costituiscono le tecnologie di riferimento di circa la metà dei progetti.

3 Ad esempio, il numero di accordi e delle imprese coinvolte, la percentuale di intermediari che hanno stretto almeno un rapporto di collaborazione.

4 Cfr. Banca d'Italia - Segnalazione in materia di esternalizzazione di funzioni aziendali per gli intermediari vigilati

5 Il totale delle segnalazioni comprende le controllate estere dei gruppi italiani.

l'obiettivo di favorire la convergenza tra gli schemi di segnalazione degli incidenti e ridurre l'onere segnaletico per gli intermediari, soprattutto nelle prime ore successive all'evento, quando l'intermediario deve concentrare i maggiori sforzi sulla risoluzione dell'incidente[6].

In estrema sintesi, l'evoluzione recente del mercato si caratterizza quindi per: i) il maggiore ricorso a tecnologie innovative; ii) l'eterogeneità delle strategie adottate al riguardo; iii) la maggiore interconnessione con soggetti al di fuori del tradizionale perimetro di supervisione; iv) l'aumento della minaccia cyber e, più in generale, del rischio informatico.

La resilienza operativa

Dopo una lunga negoziazione, il Regolamento DORA è operativo dal 17 gennaio 2025 e, nonostante la complessità della regolamentazione e gli sforzi necessari per la relativa attuazione da parte degli intermediari e delle Autorità, non è previsto un periodo transitorio.

La nuova normativa europea fa riferimento al concetto di resilienza, che presuppone la certezza (anziché una probabilità) del verificarsi dell'evento indesiderato, concentrandosi, quindi, sulle misure da adottare per mitigare il relativo danno e per preservare la capacità dell'intermediario di continuare a fornire i propri servizi anche in momenti di difficoltà.

Oggi vorrei in particolare soffermarmi su alcune implicazioni operative per gli intermediari finanziari: (a) l'importanza della *governance*; (b) il presidio della relazione con i fornitori di servizi; (c) la gestione dei dati.

Con riferimento al primo punto, DORA conferma come nell'ambito della *governance* aziendale i rischi informatici debbano formare oggetto della medesima attenzione riservata ai più tradizionali profili di rischio. Sono quindi ribadite le responsabilità dell'organo di gestione nel definire e approvare la strategia, le politiche, i protocolli e i meccanismi di gestione del rischio ICT, nonché un assetto dei controlli basato sulle tradizionali tre linee di difesa.

Il Regolamento DORA richiede inoltre che i membri dell'organo di gestione mantengano conoscenze e competenze adeguate per comprendere i rischi informatici e valutare il loro impatto sulle attività aziendali, sulla base anche di una formazione specifica. È un requisito importante per preservare un'azione sostanziale e non solo formale per il rispetto dei nuovi requisiti e rafforzare la cultura aziendale in materia di innovazione digitale e di presidio dei rischi informatici.

Al riguardo, la Banca d'Italia ha già emanato alcuni orientamenti di vigilanza, richiamando l'attenzione delle banche di propria competenza affinché, tenuto conto

---

6 Il *Financial Stability Board* ha evidenziato come una banca di importanza sistemica globale (G-SIB), nelle prime 72 ore dalla scoperta dell'incidente, debba contattare verbalmente cinque o più Autorità, emettere tra 7 e 13 relazioni scritte, completare e inviare 12-14 moduli di segnalazione iniziale dell'incidente e inserire i dettagli in 5-9 portali di segnalazione online.

delle proprie caratteristiche operative e organizzative, assicurino la presenza di consiglieri che abbiano competenze nei profili ICT, perseguendo un'adeguata diversificazione delle competenze nel *board*[7].

Anche il Meccanismo di Vigilanza Unico (MVU) ha pubblicato aspettative di vigilanza specifiche[8], volte a rafforzare le competenze ed esperienze in materia ICT nei *board* bancari. Ad esempio, nel valutare la propria idoneità collettiva (cd "*collective suitability*"), l'organo di gestione deve verificare che ci sia almeno un membro non esecutivo con conoscenze ed esperienze in materia.

Con riferimento al secondo punto, il Regolamento DORA ribadisce il principio secondo il quale rimane in capo agli intermediari la piena responsabilità degli obblighi regolamentari, anche in caso di ricorso a fornitori terzi. In particolare, l'organo di gestione deve esaminare periodicamente i rischi connessi con gli accordi contrattuali per l'utilizzo di servizi ICT a supporto di funzioni essenziali o importanti. Inoltre, qualora questi accordi prevedano la possibilità di subappalto a fornitori terzi di servizi ICT, rimane sempre responsabilità dell'intermediario valutare in che misura 'catene di fornitura' potenzialmente lunghe e complesse possano incidere sulla propria capacità di monitorare pienamente le funzioni appaltate.

Siamo consapevoli che questo requisito può indurre qualche preoccupazione da parte degli operatori, ma è importante valutare la propria operatività con tutti i fornitori, tenuto anche conto del citato crescente coinvolgimento delle terze parti in molti incidenti informatici.

Il Regolamento DORA introduce, infine, talune previsioni normative che sembrano generare alcuni dubbi applicativi (ad esempio per quanto riguarda l'individuazione dei servizi ICT da considerare nel regolamento e gli altri dati da inserire nel Registro delle Informazioni[9]). Rimaniamo ovviamente disponibili ad approfondire, nell'ambito della consueta interazione con gli intermediari, le possibili incertezze interpretative e le difficoltà attuative.

Con riferimento al terzo aspetto, il Regolamento DORA conferma l'esigenza per l'organo di gestione di disporre di informazioni adeguate, aggiornate e aggregate per gestire efficacemente il profilo di rischio degli intermediari e assumere pertanto decisioni consapevoli[10]. Nel 2023 la Banca d'Italia ha condotto sulle banche italiane uno specifico approfondimento in materia[11], dal quale sono emerse aree di possibile miglioramento, ad esempio, nella progettazione dell'infrastruttura IT e dell'architettura dei dati, ovvero nei processi di aggregazione e reporting. Tra le prassi di *governance* meno diffuse figurano la

---

7 Orientamenti della Banca d'Italia sulla composizione e sul funzionamento dei consigli di amministrazione delle LSI

8 *New policy for more bank board expertise on ICT and security risks*

9 Il Regolamento prevede che le entità finanziarie mantengano un registro di informazioni su tutti gli accordi contrattuali per l'utilizzo di servizi ICT prestati da fornitori terzi.

10 Cfr. anche i principi di Basilea in materia di *Risk Data Aggregation and Risk Reporting* (cd "BCBS 239").

11 Indagine su Risk Data Aggregation e Risk Reporting

valutazione delle implicazioni sulla gestione e sul *reporting* dei dati in caso di importanti eventi aziendali. Inoltre, la maggior parte delle banche ha procedure strutturate per il controllo della qualità dei dati e la successiva aggregazione; risultano peraltro margini di miglioramento nell'automazione della riconciliazione dei dati gestionali, contabili e normativi. È inoltre necessario attuare i relativi investimenti con continuità, al fine di garantire una solida gestione del rischio.

Attività di vigilanza

Il rapporto fiduciario che lega la clientela agli intermediari del mercato finanziario è cambiato in misura significativa nel corso degli ultimi anni: dalla custodia di beni materiali (ad esempio, oro, contanti, titoli), alla registrazione di moneta a corso forzoso e di strumenti finanziari anche in formato elettronico, alla capacità di proteggere e mantenere integro il complesso di informazioni che riguardano la nostra sfera privata, garantendo nel contempo l'accessibilità e la continuità dei servizi.

Il sistema finanziario svolge quindi un ulteriore importante ruolo nell'ecosistema tecnologico, tenuto conto che rappresenta il depositario del complesso patrimonio informativo della clientela. Gli intermediari sono ormai esposti anche al rischio reputazionale connesso con la percezione di sicurezza e affidabilità circa la tutela dell'integrità dei dati personali. Il rischio tecnologico rappresenta quindi un profilo di rischio autonomo, che permea tutta l'operatività aziendale e richiede efficaci processi di valutazione e presidi di controllo, unitamente alla disponibilità di competenze adeguate.

È per questo motivo che la Banca d'Italia dedica da tempo una grande attenzione ai temi della digitalizzazione, del rischio informatico e della crescente interconnessione del mercato. Lo strumentario di vigilanza a disposizione delle Autorità si è nel tempo arricchito su questo fronte: analisi a distanza, ispettive, *benchmarking* orizzontale, incidenti, *cyber stress test* rappresentano strumenti in grado di restituire prospettive diverse, da integrare nella valutazione complessiva del profilo di rischio specifico dei soggetti vigilati.

Le analisi condotte hanno evidenziato alcuni punti di attenzione, sui quali occorre che gli operatori continuino a investire, come le funzioni operative e di controllo che si occupano di tecnologia, la gestione dei rapporti con le terze parti, i profili di sicurezza e accesso ai dati.

Il Regolamento DORA aumenta la tipologia di strumenti a disposizione della vigilanza. In primo luogo verranno rafforzate le basi informative esistenti, quali ad esempio quella degli incidenti informatici, grazie all'ampliamento dei soggetti segnalanti (non solo banche, Istituti di Pagamento e IMEL come nel precedente schema segnaletico, ma tutte le entità nell'ambito di applicazione di DORA)[12] e della tipologia di evento oggetto delle segnalazioni (quali le minacce informatiche, finora escluse)[13].

---

12 Ad esempio imprese di investimento, gestori, emittenti di *token* collegati ad attività, prestatori di servizi per le cripto-attività, fornitori di servizi di *crowdfunding*, etc.

13 Verranno rese note alla Vigilanza anche le segnalazioni di incidenti avvenuti in altro Paese europeo, ma con potenziale impatto in Italia.

Verrà inoltre introdotto il Registro delle Informazioni (RoI), che rappresenta un'importante nuova fonte informativa per valutare il rischio di concentrazione e di interconnessione e che aiuterà a formare un quadro più completo delle interrelazioni tra soggetti vigilati e non.

Il Regolamento DORA include infine i *Threat Led Penetration Test* (TLPT) tra gli strumenti ordinari di supervisione. Tale strumento, già adottato su base volontaria dagli intermediari, diventerà quindi obbligatorio e contribuirà all'identificazione – in tempi di "pace" e attraverso simulazioni specifiche – delle debolezze nei meccanismi di difesa e all'adeguata preparazione degli attacchi reali di attori malevoli. La messa a fattor comune delle informazioni derivanti dagli incidenti cyber e le risultanze dei TLPT contribuiranno a comporre un quadro più ampio per la cybersicurezza nel sistema finanziario italiano.

Nello scorso mese di dicembre abbiamo chiesto ai soggetti direttamente vigilati le proprie autovalutazioni sul grado di preparazione rispetto alle nuove regole[14]. Attendiamo l'esito di questo esercizio entro la fine del prossimo mese di aprile, unitamente alle valutazioni degli organi di amministrazione e delle funzioni di controllo, per integrare le analisi a nostra disposizione e valutare il grado di preparazione a DORA e il relativo percorso di aggiustamento.

Va comunque considerato che il legislatore europeo ha volutamente mantenuto il Regolamento DORA "*principle-based*" attraverso requisiti adattabili a più soluzioni specifiche, secondo il principio della "*technology-neutrality*", al fine di preservarne l'efficacia nel tempo ("*future-proof*"). L'attività di vigilanza deve in ogni caso basarsi sull'analisi dei rischi effettivi insiti in tecnologie specifiche, per affrontarne adeguatamente i riflessi e gestirne i presidi.

Conclusioni

La gestione dell'innovazione tecnologica e dei relativi rischi consente di rendere sostenibili i modelli operativi nel lungo periodo. Un ruolo centrale nel governo dell'innovazione e dei relativi rischi è affidato all'alta *governance* degli intermediari, che deve preservare la sana (quindi redditizia) e prudente (quindi con un'adeguata gestione dei relativi rischi) gestione degli intermediari e la stabilità finanziaria nel suo complesso.

Il Regolamento DORA offre strumenti utili – agli intermediari e alle Autorità – per rafforzare la resilienza operativa del sistema finanziario. Una piena e sostanziale attuazione della DORA non dovrebbe quindi essere considerata un mero esercizio obbligatorio imposto dall'Autorità, ma un percorso che sia il più efficace possibile per gli intermediari stessi, affinché rafforzino la "*risk culture*" in materia tecnologica e migliorino la propria resilienza operativa.

---

14 Sono state anche pubblicate istruzioni operative che stabiliscono i principi di compilazione dell'autovalutazione richiesta.

Grafica a cura della Divisione Editoria e stampa della Banca d'Italia