DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Governare l'intelligenza artificiale nell'era della vulnerabilità

Quando il rischio cyber diventa responsabilità degli organi sociali

11 Giugno 2026

Silvia Migliavacca, Head of Demand, Supply Chain e Coordinamento progetti strategici, Banca Mediolanum

Oreste Pollicino, Professore Ordinario di Diritto Costituzionale e della Regolamentazione dell'Intelligenza Artificiale, Università Bocconi

DB non solo diritto bancario

Silvia Migliavacca, Head of Demand, Supply Chain e Coordinamento progetti strategici, Banca Mediolanum

Oreste Pollicino, Professore Ordinario di Diritto Costituzionale e della Regolamentazione dell'Intelligenza Artificiale, Università Bocconi

Silvia Migliavacca

Silvia Migliavacca, laureata con lode in Economia Aziendale presso l'Università Bocconi nel 1997, inizia la carriera in primarie società multinazionali consulenza strategico-organizzativa seguendo progetti nel settore dei servizi finanziari.

Oreste Pollicino

Oreste Pollicino è Professore Ordinario di Diritto Costituzionale e AI Law presso l'Università Bocconi, dove dirige il Master di secondo livello LLM in Law of Technology and Automated Systems (LATAS). Presidente di DICOPO – Centre for Digital Constitutionalism and Policy (Bruxelles).

1. Introduzione

Vi è un momento, nei processi di innovazione tecnologica, in cui il rischio muta qualificazione prima ancora che intervenga una piena sedimentazione normativa. È il passaggio in cui ciò che, fino a poco tempo prima, era percepito come questione eminentemente tecnica viene progressivamente attratto nell'area della responsabilità organizzativa e della supervisione degli organi sociali. Nel settore bancario, tale slittamento è oggi particolarmente evidente con riferimento all'impiego di sistemi di intelligenza artificiale capaci non solo di supportare l'analisi dei sistemi informativi, ma anche di accelerare l'individuazione e, in ipotesi, lo sfruttamento di vulnerabilità su scala e con velocità inedite.

È qui che si manifesta una delle trasformazioni più rilevanti del costituzionalismo economico nell'età digitale: il rischio tecnologico non resta confinato nella dimensione dell'efficienza, ma incide sulle condizioni stesse di affidabilità dell'intermediario, sulla continuità dei servizi essenziali e, in ultima analisi, sulla fiducia che sorregge il rapporto tra sistema bancario, mercato e cittadino-cliente.

La questione, pertanto, non può più essere letta soltanto in termini di efficienza operativa o di opportunità tecnologica. Essa investe il nucleo della governance del rischio, poiché l'intelligenza artificiale contribuisce a modificare il profilo di esposizione degli intermediari, la velocità di propagazione degli eventi avversi e, di conseguenza, le modalità attraverso cui deve essere esercitata la funzione di indirizzo, supervisione e controllo. Per un lettore professionale, il punto rilevante è che l'innovazione non genera semplicemente un nuovo rischio, ma altera le condizioni di esercizio di obblighi già esistenti: dalla sana e prudente gestione alla resilienza operativa digitale, fino alla documentabilità delle decisioni assunte dagli organi di vertice.

In altri termini, l'IA non chiede soltanto nuovi strumenti di compliance: costringe a rileggere categorie tradizionali — diligenza, prudenza, adeguatezza organizzativa, responsabilità degli amministratori — dentro un ambiente in cui la vulnerabilità non è più eccezione, ma condizione strutturale dell'operare digitale.

In questo scenario, il punto di equilibrio tra innovazione e controllo non si gioca più soltanto nei dipartimenti IT.

vedi l'articolo online

Si sposta anche nei lavori dei Consigli di amministrazione.

Anzi, si potrebbe dire che il consiglio di amministrazione diventa il luogo nel quale la vulnerabilità tecnologica deve essere trasformata in decisione organizzativa: non attraverso una impossibile pretesa di controllo totale, ma mediante la costruzione di procedure, competenze e responsabilità capaci di rendere governabile l'incertezza.

2. Dalla sicurezza tecnica alla governance: il ruolo centrale degli organi sociali

Le interlocuzioni sviluppatesi nel corso del 2026 tra autorità e intermediari, anche alla luce delle notizie relative a modelli di IA particolarmente efficaci nell'individuazione di vulnerabilità (si ricorda in particolare minaccia cyber di Claude Mythos, IA di Anthropic), hanno riportato al centro una questione che il quadro europeo già conteneva in nuce: la gestione del rischio ICT non è materia delegabile in via esclusiva alle strutture tecniche, ma rientra nella responsabilità ultima del vertice aziendale. In questa prospettiva, il dibattito non riguarda soltanto la pericolosità dei nuovi strumenti, bensì la capacità degli intermediari di dimostrare che il consiglio di amministrazione e gli organi con funzione di supervisione strategica comprendono il rischio, ne definiscono la tolleranza e presidiano l'adeguatezza delle risposte organizzative.

La vera questione, dunque, non è se il board debba diventare un organo tecnico. Non deve esserlo. La questione è se esso sia posto nelle condizioni di esercitare una funzione autenticamente strategica rispetto a rischi che, pur avendo origine tecnica, producono effetti giuridici, reputazionali, patrimoniali e sistemici.

Le indicazioni delle autorità europee convergono su un punto essenziale: il rischio cyber, accelerato dall'IA, impone una assunzione di responsabilità diretta da parte degli organi di vertice.

Questa evoluzione è perfettamente coerente con:

- il Regolamento DORA (Digital Operational Resilience Act), che attribuisce al management body la responsabilità ultima della gestione del rischio ICT;
- la Direttiva NIS2, che rafforza il ruolo degli organi di amministrazione nella supervisione delle misure di cybersicurezza, prevedendo anche forme di responsabilità in caso di inadempimento.

La convergenza tra le principali fonti europee è, sotto questo profilo, particolarmente significativa. Il Regolamento DORA attribuisce espressamente al management body la responsabilità ultima della gestione del rischio ICT e gli impone di definire, approvare, sorvegliare e riesaminare l'intero assetto di resilienza digitale, inclusi strategia, continuità operativa, risposta agli incidenti e governo delle terze parti ICT. In termini applicativi, ciò significa, ad esempio, che un consiglio di amministrazione non può limitarsi a ricevere report periodici sulla sicurezza, ma deve essere posto in condizione di deliberare sulla tolleranza al rischio ICT, sull'allocazione di budget adeguati, sulle priorità di remediation e sui criteri di classificazione delle funzioni critiche o importanti. Parallelamente, la Direttiva NIS2 rafforza il ruolo degli organi di amministrazione prevedendo che essi approvino le misure di gestione del rischio cyber, ne sorveglino l'attuazione e possano essere chiamati a rispondere delle violazioni imputabili all'ente. Il dato più innovativo, in chiave giuridica, è che la cybersicurezza cessa definitivamente di essere una materia meramente tecnica per diventare oggetto di una responsabilità di governance formalizzata e verificabile.

Questa formalizzazione non è un dettaglio procedurale. È il punto in cui il diritto europeo mostra la propria cifra più caratteristica: non vietare l'innovazione, ma costituzionalizzarne le condizioni organizzative di sostenibilità. La resilienza digitale non è soltanto una misura difensiva; diventa una qualità istituzionale dell'intermediario.

Alla luce delle nuove capacità dell'intelligenza artificiale, questa impostazione acquista una profondità ulteriore. Non si tratta più solo di vigilare sull'adeguatezza dei controlli, ma di comprendere come il rischio stesso evolva e si trasformi.

Il board, in questa prospettiva, non è chiamato a certificare ex post l'esistenza di presidi, ma a orientare ex ante la capacità dell'organizzazione di apprendere, reagire e correggersi. È qui che la governance diventa non solo controllo del rischio, ma architettura della responsabilità.

vedi l'articolo online

3. La crisi del tempo: quando il diritto incontra la velocità della tecnologia

Uno dei profili più delicati emersi nel confronto regolamentare recente concerne la compressione del tempo che intercorre tra scoperta della vulnerabilità, rilascio della correzione e possibile sfruttamento. È un punto solo apparentemente tecnico. In realtà, esso investe direttamente il diritto dell'organizzazione bancaria, poiché mette in discussione l'adeguatezza dei processi decisionali, dei flussi informativi e delle deleghe interne. Se, infatti, modelli di IA sempre più sofisticati sono in grado di ridurre drasticamente la finestra temporale utile per la remediation, allora anche la nozione di adeguatezza dei presidi deve essere riletta alla luce di un requisito implicito di tempestività. Un esempio concreto può chiarire il punto: una banca che mantenga cicli di patching mensili per sistemi che supportano funzioni critiche potrebbe trovarsi formalmente dotata di policy coerenti, ma sostanzialmente esposta a un rischio non più compatibile con il nuovo contesto tecnologico. In tale scenario, la criticità non risiede soltanto nel difetto tecnico, bensì nell'eventuale scollamento tra rischio effettivo, tempi di escalation e capacità del vertice di pretendere azioni correttive coerenti con l'urgenza del caso.

Il tempo diventa così una categoria giuridica. Non nel senso astratto della decorrenza di un termine, ma nel senso sostanziale della capacità dell'organizzazione di decidere prima che il rischio si trasformi in danno. La tempestività non è più soltanto efficienza operativa: è parte della diligenza richiesta agli organi sociali.

Questo fenomeno mette sotto pressione non solo i sistemi tecnologici, ma anche i modelli decisionali su cui si fonda la governance.

Le norme – DORA in primis – richiedono:

- capacità di identificazione tempestiva dei rischi
- gestione strutturata degli incidenti
- continuità operativa anche in scenari estremi

Anche il recente posticipo di alcuni obblighi previsti dall'AI Act sottolinea la velocità di evoluzione della tecnologia, che mette alla prova i tempi del diritto.

La distanza tra il tempo della regolazione e il tempo della tecnologia non può essere colmata soltanto con nuove norme. Deve essere colmata attraverso organizzazioni capaci di incorporare l'anticipazione come metodo: risk assessment dinamici, escalation rapide, simulazioni di crisi, flussi informativi comprensibili al board e una cultura interna nella quale la segnalazione della vulnerabilità non sia vissuta come fallimento, ma come condizione ordinaria della resilienza.

Tuttavia, il presupposto implicito è che esista un tempo sufficiente per agire.

Quando questo tempo si riduce drasticamente, la vera questione diventa:

gli organi di governance sono in grado di assumere decisioni efficaci in tempi compatibili con il rischio?

Il problema non è quindi solo di compliance, ma di capacità decisionale.

Ed è precisamente su questo terreno che la responsabilità degli organi sociali assume una dimensione nuova: non soltanto avere approvato policy corrette, ma avere costruito un assetto decisionale capace di funzionare quando la normalità viene meno.

4. Il paradigma regolamentare: continuità delle norme, discontinuità nell'applicazione

Un aspetto particolarmente interessante, anche per la dottrina, è che le autorità non sembrano orientate a costruire un nuovo sottosistema normativo dedicato all'IA offensiva o al cyber risk aumentato dall'automazione. Al contrario, il messaggio che emerge è di continuità dell'impianto regolamentare e di discontinuità sul piano dell'interpretazione applicativa. In altri termini, DORA, NIS2 e gli orientamenti di vigilanza già offrono un perimetro sufficiente; ciò che cambia è l'intensità con cui tali obblighi devono essere letti, attuati e dimostrati. Per gli intermediari, questo produce una conseguenza rilevante: il baricentro della compliance si sposta dall'adozione formale di presidi alla capacità di provare che quei presidi sono effettivamente calibrati su uno scenario in rapida evoluzione. Si pensi, ad esempio, alla gestione dei fornitori ICT critici: non è più sufficiente che il contratto contenga clausole corrette in astratto; occorre che l'intermediario sia in grado di valutare la dipendenza operativa, presidiare il rischio di concentrazione e integrare il monitoraggio del fornitore nei flussi informativi destinati al board.

Questa è una delle cifre più significative della stagione regolatoria europea: il diritto non rincorre ogni

vedi l'articolo online

singola tecnologia con una norma speciale, ma innalza il livello di responsabilità organizzativa richiesto a chi utilizza quella tecnologia. La discontinuità non sta necessariamente nel testo della regola, ma nel modo in cui la regola deve essere resa viva dentro l'impresa.

Al contrario, viene ribadita la piena attualità dei framework esistenti:

- DORA per la resilienza digitale
- NIS2 per la sicurezza delle reti e dei sistemi
- le linee guida EBA sul rischio ICT e di sicurezza

Il messaggio è chiaro:
non è il quadro normativo a essere insufficiente, ma è la sua attuazione a dover evolvere.

Questo comporta un cambiamento fondamentale per gli intermediari finanziari. La compliance non può più essere interpretata come adempimento formale. Deve diventare:

- capacità di anticipare i rischi
- rapidità di esecuzione
- integrazione tra controllo e innovazione

Qui si coglie il passaggio dalla compliance come "prova documentale" alla compliance come "capacità istituzionale". Non basta poter mostrare una procedura; occorre poter dimostrare che quella procedura è stata capita, aggiornata, stressata, utilizzata e, se necessario, superata da una decisione responsabile.

5. IA e cyber risk: amplificazione delle vulnerabilità esistenti

L'interazione tra intelligenza artificiale e rischio cyber introduce una caratteristica nuova: la capacità di amplificare vulnerabilità esistenti.

Dal punto di vista giuridico, ciò implica che:

- il perimetro del rischio ICT si espande
- aumentano le interdipendenze (supply chain, open source, terze parti)
- si rafforza la necessità di un approccio "end-to-end" alla sicurezza

In termini normativi, questo si traduce in:

- maggiore rilevanza degli obblighi di gestione del rischio di terza parte ICT (DORA)
- rafforzamento delle responsabilità in materia di cyber hygiene e prevenzione (NIS2)
- centralità dei processi di incident reporting e gestione delle crisi

Sotto questo profilo, l'interazione tra IA e cyber risk non crea soltanto nuove minacce, ma amplifica vulnerabilità organizzative già note: dipendenze da librerie open source, concentrazione presso pochi fornitori cloud, catene di subfornitura poco trasparenti, frammentazione delle responsabilità interne. È qui che il diritto bancario incontra la concretezza dei modelli operativi. Si immagini il caso di un intermediario che utilizzi un servizio SaaS per una funzione rilevante, integrato con componenti di terze parti e modelli generativi per attività di assistenza o analisi: un incidente originato presso il fornitore non resta confinato alla sfera tecnica, ma può tradursi in interruzione del servizio, obblighi di segnalazione, attivazione dei piani di continuità e scrutinio della vigilanza sulla qualità della supervisione esercitata dagli organi aziendali. In questa prospettiva, il rischio di terza parte, l'incident reporting e la crisis governance cessano di essere ambiti separati e diventano espressione di un medesimo dovere di governo integrato del rischio.

La vulnerabilità, dunque, non è soltanto nel codice. È nella catena di dipendenze, nella qualità dei dati, nella governance dei modelli, nella capacità contrattuale di pretendere informazioni dai fornitori, nella leggibilità dei report destinati agli organi sociali. È una vulnerabilità tecnica, ma anche organizzativa, informativa e giuridica.

vedi l'articolo online

- comprendere i nuovi rischi (non solo tecnici ma sistemici)
- definire priorità coerenti con il profilo di rischio
- allocare risorse in modo tempestivo

In questa prospettiva, la banca non può più limitarsi a chiedersi se un sistema sia sicuro in sé. Deve chiedersi se l'intero ecosistema nel quale quel sistema opera sia governabile, documentabile e reversibile. La reversibilità — cioè la possibilità di contenere, isolare, sospendere o sostituire componenti critiche — diventa una dimensione essenziale della resilienza.

6. Verso una governance adattiva: il nuovo standard implicito

La trasformazione in atto suggerisce che il vero standard richiesto agli intermediari non è più solo quello della conformità, ma quello della capacità di adattamento e di trasformazione.

Le indicazioni operative che emergono – accelerazione del patch management, rafforzamento delle capacità di detection, integrazione dell'IA nelle difese – non sono semplici best practice. Rappresentano: nuovi standard impliciti di diligenza organizzativa e di gestione del rischio ICT.

È qui che il concetto di governance adattiva assume un significato preciso: non una governance elastica nel senso debole del termine, ma una governance capace di aggiornare continuamente la propria percezione del rischio, di apprendere dagli incidenti, di rivedere le soglie di tolleranza e di trasformare l'esperienza operativa in decisione strategica.

In questo contesto, la responsabilità degli organi sociali assume una dimensione più ampia:

- non solo garantire l'adeguatezza dei presidi
- ma assicurare la capacità dell'organizzazione di evolvere nel tempo

È una responsabilità che richiama, in chiave moderna, i principi tradizionali di diligenza e prudenza, ma li declina in un contesto di complessità tecnologica crescente.

Diligenza e prudenza, nell'età dell'intelligenza artificiale, non significano immobilismo. Significano capacità di innovare senza perdere il controllo dell'innovazione. Significano introdurre tecnologie difensive, ma anche governarne i limiti, i bias, le dipendenze e i rischi di opacità. Significano, soprattutto, non confondere l'automazione del presidio con la delega della responsabilità.

Da questo punto di vista, l'IA difensiva può rappresentare una risorsa decisiva: sistemi di anomaly detection, strumenti di threat intelligence, modelli predittivi per l'individuazione di vulnerabilità e meccanismi di risposta assistita possono rafforzare la resilienza dell'intermediario. Ma proprio perché l'IA entra nei presidi di sicurezza, essa deve essere a sua volta oggetto di governance: validazione, auditabilità, controllo umano, tracciabilità delle decisioni e chiara definizione delle responsabilità in caso di errore o mancata attivazione.

7. Conclusioni: la governance come leva di resilienza sistemica

Se si considera il quadro nel suo insieme, emerge una linea interpretativa di particolare interesse per il diritto bancario contemporaneo. L'intelligenza artificiale non impone necessariamente una rifondazione delle categorie giuridiche esistenti; impone, però, una loro rilettura sostanziale. La resilienza operativa, la sana e prudente gestione, la responsabilità degli organi sociali e la tracciabilità delle decisioni non sono concetti nuovi. Nuova è, piuttosto, la densità tecnologica del contesto in cui essi devono operare.

Il diritto bancario, in questa fase, è chiamato a misurarsi con una forma nuova di materialità: non più soltanto quella dei capitali, degli attivi, della liquidità, ma quella delle infrastrutture digitali, dei dati, dei modelli, delle dipendenze tecnologiche. È una materialità meno visibile, ma non meno decisiva per la stabilità dell'intermediario.

L'intelligenza artificiale non introduce semplicemente nuovi rischi. Rende più evidente la natura dinamica del rischio stesso. E, nel farlo, costringe il diritto bancario a confrontarsi con una realtà in cui:

- la stabilità dipende dalla capacità di adattarsi rapidamente
- la conformità dipende dalla qualità delle decisioni

vedi l'articolo online

- la governance diventa il punto di sintesi tra tecnologia e regolamentazione

In questa luce, la sfida per il settore bancario non consiste soltanto nel rafforzare i controlli o nell'adottare nuove tecnologie difensive. Consiste, più radicalmente, nel costruire una governance capace di decidere in condizioni di incertezza accelerata, di documentare le proprie scelte e di integrare competenze tecnologiche, organizzative e giuridiche all'interno di un medesimo disegno di responsabilità. Per questo, il presidio del rischio cyber e il governo dell'IA non appaiono come due dossier distinti, ma come due manifestazioni convergenti della medesima esigenza: garantire che l'innovazione resti compatibile con la continuità dei servizi, la tutela dei clienti e la stabilità dell'intermediario.

È questa, in fondo, la vera posta in gioco: non scegliere tra innovazione e sicurezza, ma costruire un modello di governo nel quale l'innovazione sia possibile proprio perché è resa responsabile, verificabile e compatibile con la fiducia che il settore bancario deve presidiare.

Anche il prof. Leonardo Caporarello nel suo testo l'incertezza necessaria richiama queste considerazioni per stimolare l'esigenza di definire modelli organizzativi e di governance capaci di adattarsi ad un contesto incerto.

Il riferimento all'incertezza è particolarmente utile perché consente di evitare una lettura difensiva o meramente emergenziale del problema. L'incertezza non è solo un elemento da ridurre; è una condizione da organizzare. La buona governance, in questa prospettiva, non elimina l'incertezza, ma costruisce le condizioni perché l'organizzazione possa decidere responsabilmente dentro l'incertezza.

Il punto, in definitiva, è che il rischio tecnologico non può più essere trattato come una variabile accessoria, da confinare nei presidi specialistici. Esso si colloca ormai al centro della funzione di governo dell'impresa bancaria e misura, in modo sempre più visibile, la qualità della sua architettura decisionale. È in questo passaggio che si coglie il mutamento più profondo: il rischio tecnologico non è più soltanto un fenomeno da gestire, ma una dimensione da governare strategicamente, nel cuore stesso delle responsabilità degli organi sociali.

È qui che l'IA, da fattore di accelerazione del rischio, può diventare anche banco di prova della maturità istituzionale degli intermediari: non perché renda il rischio totalmente prevedibile, ma perché obbliga l'organizzazione a mostrare se possiede una governance realmente capace di apprendere, decidere e rispondere. In questa capacità di trasformare vulnerabilità in responsabilità si gioca una parte essenziale della resilienza bancaria nell'età dell'intelligenza artificiale.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it