



BANCA D'ITALIA
EUROSISTEMA

Credito e innovazione: evoluzione del mercato e profili di vigilanza

Intervento di Giuseppe Siani

Capo del Dipartimento Vigilanza bancaria e finanziaria della Banca d'Italia

CETIF – Università Cattolica del Sacro Cuore

Milano, 14 ottobre 2026

1. Introduzione

Ringrazio gli organizzatori per l'invito, che mi offre l'opportunità di condividere alcune riflessioni sul rapporto tra la gestione dei processi creditizi e la crescente diffusione delle nuove tecnologie nel sistema bancario.

Viviamo in un contesto caratterizzato da shock ripetuti, elevata incertezza geopolitica, una profonda trasformazione tecnologica, rapidi cambiamenti nelle condizioni finanziarie. La capacità delle banche di affrontare queste sfide dipende non solo dalla solidità dei bilanci, ma anche dalla qualità delle strategie, degli assetti di governo e dei sistemi di controllo.

Nel mio intervento mi soffermerò dapprima sull'andamento e sulla qualità del credito. Illustrerò poi come la maggiore disponibilità di dati, l'automazione e l'intelligenza artificiale (IA) stiano modificando il processo creditizio. Affronterò quindi i rischi della crescente dipendenza dalla tecnologia per concludere con alcune considerazioni sul ruolo della regolamentazione e della supervisione.

2. L'andamento del credito e la qualità degli attivi

Dopo una lunga fase di contrazione, dalla primavera dello scorso anno il credito a famiglie e imprese è tornato a crescere, accelerando progressivamente. A luglio i prestiti al settore privato non finanziario sono aumentati del 3,3 per cento sui dodici mesi, nonostante il rialzo dei tassi di interesse.

L'accelerazione è stata trainata dai finanziamenti alle imprese più grandi, mentre dall'inizio dell'anno la dinamica dei prestiti alle famiglie è rimasta su valori sostanzialmente stabili. Il credito concesso alle piccole imprese ha continuato invece a contrarsi, ma a ritmi più contenuti rispetto al passato e solamente per quelle finanziariamente meno solide. L'espansione del credito si è concentrata nella componente a breve termine, anche a fronte di maggiori esigenze di liquidità emerse a seguito dei rincari energetici.

Dalle ultime indagini condotte presso banche e imprese, non emergono chiari segni di una restrizione dell'offerta di credito¹. Nei prossimi mesi, tuttavia, l'orientamento più restrittivo della politica monetaria e l'incertezza derivante dalle tensioni geopolitiche potrebbero indurre le banche a maggiore cautela, aumentando i tassi d'interesse e rendendo i criteri di offerta più stringenti.

La qualità del credito rimane elevata. Il rapporto tra i prestiti deteriorati e il totale dei finanziamenti è stabile su valori storicamente bassi e paragonabili a quelli medi dell'area dell'euro; anche il flusso di nuovi prestiti deteriorati si mantiene contenuto; i tassi di copertura sono elevati. Tuttavia, l'elevata incertezza legata principalmente agli sviluppi geopolitici non consente di abbassare la guardia. È necessario continuare a identificare precocemente eventuali vulnerabilità e classificare correttamente i prestiti contabilizzando le eventuali perdite anche in ottica prospettica.

L'elevata qualità del credito è il frutto di un percorso di risanamento dei bilanci bancari a cui hanno contribuito gli intermediari, la regolamentazione e l'attività di supervisione. Nell'ambito di iniziative promosse dall'SSM, stiamo ora compiendo un ulteriore passo in questa direzione con la progressiva estensione anche alle banche di minore dimensione (le *Less significant institutions*; LSI) del cosiddetto approccio di calendario di vigilanza per la copertura dei crediti deteriorati erogati prima del 2019², fino ad oggi applicato solamente alle banche di maggiore dimensione (*Significant institutions*; SI).

L'estensione avverrà comunque con gradualità e tenendo conto delle specificità dei singoli intermediari, evitandone l'applicazione ad alcune specifiche linee di attività (in particolare l'acquisizione e la gestione di crediti deteriorati e il factoring su crediti verso enti della pubblica amministrazione) per evitare effetti distorsivi. Le esenzioni saranno valutate caso per caso, anche per prevenire fenomeni di arbitraggio.

Il mercato secondario dei prestiti deteriorati ha contribuito al risanamento dei bilanci e rimane una componente importante per la stabilità del sistema. Il monitoraggio svolto regolarmente dalla Banca d'Italia indica che, a copertura di operazioni di cartolarizzazione di crediti deteriorati, fino alla fine dello scorso anno erano stati emessi titoli per un valore nominale di circa 80 miliardi di euro. Di questi, circa 22 rappresentavano tranche *senior* con garanzia pubblica emessa nell'ambito del programma Gacs (garanzia sulla cartolarizzazione delle sofferenze)³. I rimborsi sinora effettuati su queste ultime hanno ridotto l'esposizione dello Stato a 6,3 miliardi.

¹ Cfr. [Bollettino economico n. 3 – 2026](#) e [Indagine sul credito bancario nell'area dell'euro](#), entrambi riferiti al secondo trimestre del 2026.

² Nell'aprile del 2019 il legislatore europeo ha inserito all'interno del Regolamento sui requisiti prudenziali delle banche e delle imprese di investimento (CRR) una norma, nota come backstop prudenziale, che richiede alle banche di adottare l'approccio di calendario per tutti i finanziamenti erogati successivamente a quella data. Questa norma è vincolante e si applica a tutte le banche dell'Unione europea (incluse quindi le banche meno significative).

³ I restanti 58 miliardi sono composti da titoli derivanti da operazioni non facenti parte del programma Gacs o da titoli *junior* e *mezzanine* di operazioni Gacs.

Le proiezioni degli incassi attesi dai *servicer* riguardo alle cartolarizzazioni assistite da Gacs mostrano un rallentamento nell'attività di recupero, in particolare per le operazioni realizzate prima del 2019 (e quindi prive dei correttivi successivamente apportati per renderle più robuste)⁴. Tra le cause più ricorrenti dei minori recuperi figurano la durata e la complessità delle procedure concorsuali e il decremento del valore commerciale degli attivi a garanzia. Per le operazioni prive di garanzia pubblica non si registrano peggioramenti nell'attività di recupero. Tuttavia, circa un quinto del valore nominale dei crediti cartolarizzati presenta ritardi nei pagamenti rispetto a quanto preventivato dai *servicer*.

3. La trasformazione tecnologica del processo del credito

In questo contesto si inserisce una trasformazione strutturale del processo del credito, determinata dalla crescente disponibilità di dati e dal rapido sviluppo delle nuove tecnologie. Su questa trasformazione la Banca d'Italia dispone di un osservatorio privilegiato, grazie al dialogo con gli intermediari, alle analisi dedicate alla digitalizzazione del settore finanziario e all'attività di vigilanza.

Le nostre indagini⁵ indicano che negli ultimi anni gli investimenti in tecnologie digitali delle entità vigilate hanno registrato una significativa accelerazione, sebbene con notevoli differenze tra intermediari. Come è normale attendersi, gli investimenti più rilevanti si riscontrano presso gli istituti di maggiore dimensione, ma non mancano intermediari più piccoli all'avanguardia. Le soluzioni adottate non sono inoltre omogenee per livello di sofisticazione, ambito di applicazione e integrazione nei processi aziendali.

La quasi totalità delle LSI che hanno partecipato a una specifica raccolta di dati nel 2026⁶ ha dichiarato di disporre di una strategia digitale⁷ e, nei casi più virtuosi, di aver attuato il continuo monitoraggio dell'avanzamento dei progetti, dei relativi progressi e dei connessi benefici. Inoltre, solo circa un terzo delle banche ha dichiarato di avere già in uso sistemi di IA o di avere in programma un loro sviluppo. Nel complesso, strategie, competenze e capacità di controllo risultano piuttosto eterogenee e devono essere valutate in funzione della dimensione e della complessità delle banche.

Al momento per molti intermediari le strategie digitali non comportano una modifica dei processi, ma tendono ad automatizzare quelli esistenti. Le strategie si concentrano infatti sulle fasi di accesso ai servizi e di acquisizione delle informazioni: identificazione a distanza, firma elettronica, raccolta e classificazione automatica dei documenti, precompilazione

⁴ La Gacs è stata attiva dal 2017 al 2019 e successivamente prorogata, con modifiche, fino al 2022. I requisiti per l'ammissione alla Gacs sono stati resi più stringenti per le operazioni di cartolarizzazione condotte dopo il 6 marzo del 2019, per le quali è stato introdotto un sistema di monitoraggio molto accurato. In particolare, i pagamenti dovuti al *servicer* sono in tutto o in parte condizionati a obiettivi di risultato (recupero/incasso); in caso di mancato rispetto, sono previste penalità come il differimento dei compensi o la sostituzione del *servicer*.

⁵ Ad esempio, si veda ["Indagine Fintech sugli intermediari bancari e finanziari – 2025"](#).

⁶ La rilevazione ha coinvolto la quasi totalità delle LSI, ad eccezione delle Raiffeisen.

⁷ Con "strategia digitale" si intende l'insieme delle azioni intraprese dagli intermediari per adottare soluzioni tecnologiche finalizzate a offrire prodotti e servizi finanziari digitali alla clientela, innovare i processi operativi, fornire supporto alla conduzione delle attività aziendali.

delle informazioni e interazione digitale con il cliente. Circa un quinto dei nuovi clienti sono stati acquisiti mediante procedure interamente *online*.

Variano, inoltre, le modalità con cui gli intermediari adottano queste nuove tecnologie in funzione delle dimensioni e dell'ambito di applicazione. Ad esempio, gli intermediari di maggiore dimensione si affidano spesso a soluzioni sviluppate internamente, anche se spesso ospitate in *cloud* di terze parti, mentre le banche più piccole e gli altri intermediari ricorrono più frequentemente a fornitori specializzati. Entrambi gli approcci contribuiscono alla scomposizione e frammentazione della catena del valore nella produzione e fornitura dei servizi bancari e finanziari. Tale fenomeno consente di aumentare l'efficienza, ma genera interdipendenze su cui tornerò più avanti.

La diversità degli approcci e la gradualità con cui gli intermediari adottano le nuove tecnologie riflettono la necessità di integrare con prudenza le nuove soluzioni in architetture informatiche spesso complesse, di assicurare la qualità e la disponibilità dei dati e di adeguare processi, anche quelli creditizi, competenze e controlli.

4. Intelligenza artificiale e decisioni creditizie

Questa maggiore cautela non sta però impedendo una graduale diffusione di applicazioni di IA nel processo creditizio. Pur nella diversità degli approcci, è possibile identificare alcuni tratti comuni.

Già da tempo gli intermediari utilizzano sistemi di IA predittivi, o di *machine learning*, che permettono di individuare relazioni tra variabili difficili da cogliere attraverso i tradizionali approcci statistici. Questi sistemi sono poi spesso affiancati da forme di IA che organizzano le informazioni presenti in grandi basi dati spesso destrutturate, migliorando la precisione e la tempestività delle valutazioni. Nel perseguire un adeguato bilanciamento tra capacità predittiva, affidabilità e complessità delle tecniche utilizzate, rimane molto spesso rilevante anche il ruolo di modelli statistici tradizionali.

La diffusione e le modalità di impiego dell'IA dipendono dalle caratteristiche della clientela e dei prodotti. Nel credito alle persone fisiche, la maggiore standardizzazione e la disponibilità di informazioni strutturate provenienti da diverse fonti consentono un livello più elevato di automazione, soprattutto nella fase di erogazione del credito.

Nel finanziamento alle imprese, specie per le PMI, la situazione è diversa. La varietà dei modelli operativi, la minore standardizzazione dei prodotti e la rilevanza delle informazioni qualitative rendono ancora importanti la conoscenza diretta delle imprese e del territorio. L'IA viene quindi utilizzata maggiormente nella fase di monitoraggio, perché consente una lettura integrata di tutti gli indicatori disponibili, rendendo più efficienti le attività di classificazione, revisione e controllo delle posizioni creditizie, e permette di identificare tempestivamente i casi da sottoporre a una valutazione esperta.

Vi sono evidenze a sostegno della tesi che l'utilizzo dell'IA possa ampliare l'accesso al credito per i debitori marginali. Se da un lato ciò ha conseguenze positive, sia per la clientela sia per gli intermediari, dall'altro è necessario essere ben consapevoli dei rischi

per entrambi. Un accesso al credito troppo ampio per la clientela marginale può portare a fenomeni di sovraindebitamento e a un deterioramento della qualità degli attivi.

Un ambito distinto è infine quello dei modelli regolamentari per il calcolo dei requisiti patrimoniali, dove la diffusione dell'IA procede più lentamente. Al momento queste applicazioni vengono utilizzate prevalentemente per specifiche finalità (stima delle probabilità di default), ma sempre all'interno di modelli che continuano a fondarsi su metodologie statistiche tradizionali.

Anche in questo caso, le ragioni della gradualità sono comprensibili e dipendono in larga misura dall'incertezza circa la possibilità di soddisfare i requisiti normativi e le aspettative delle autorità di vigilanza in sede di autorizzazione e di supervisione. Per ridurre questa incertezza, negli anni recenti l'Autorità Bancaria Europea (ABE) e il Meccanismo di Vigilanza Unico (MVU) hanno chiarito come i principi generali previsti dalla regolamentazione debbano essere applicati anche ai modelli basati sull'IA⁸. Hanno inoltre confermato che tutte le funzioni coinvolte nel ciclo di vita del modello, comprese le funzioni di controllo e gli organi aziendali, dispongano di adeguate competenze.

5. Regolamentazione, rischi e azione di Vigilanza

A prescindere dei casi d'uso, siano essi legati ai processi creditizi o meno, le opportunità offerte dalla tecnologia si accompagnano a rischi che devono essere identificati e governati anche alla luce della loro valenza sempre più strategica. Alcuni sono propri dell'intelligenza artificiale, altri appartengono al più ampio novero del rischio informatico.

Per governarli l'Unione europea ha introdotto un robusto quadro regolamentare basato sul Regolamento DORA e sull'AI Act. Il primo mira a rafforzare la resilienza operativa digitale, indicando quali assetti organizzativi, controlli e capacità di risposta debbano essere adottati dagli intermediari per preservare la continuità delle funzioni essenziali. Il secondo classifica i sistemi di IA sulla base del rischio di violare i diritti fondamentali degli individui e introduce requisiti differenziati in funzione delle caratteristiche e delle finalità dei casi d'uso.

I due Regolamenti presentano tra loro alcuni punti di contatto e interagiscono in misura più o meno diretta con altre norme⁹ (*in primis* quelle prudenziali), costituendo un quadro regolamentare complesso che solleva sfide applicative sia per gli intermediari sia per i supervisori.

La Vigilanza ha adottato un approccio pragmatico, equo e basato sul rischio. Pragmatico, perché l'attenzione si concentra sull'effettiva capacità dei presidi organizzativi di ridurre i rischi; equo, perché trattiamo in modo uniforme situazioni caratterizzate da rischi comparabili; basato sul rischio, perché intensità e profondità dell'azione di vigilanza

⁸ Cfr. le raccomandazioni dell'ABE contenute nel [Follow-up Report on the use of machine learning for internal ratings-based models](#) pubblicato nel 2023 e la [Guida della BCE ai modelli interni](#) del 2025.

⁹ L'ABE ha condotto lo scorso anno una mappatura delle varie normative applicabile e ha concluso che le norme esistenti sono complementari e non presentano contraddizioni.

riflettono la rilevanza delle attività, la complessità delle tecnologie utilizzate e le possibili conseguenze per gli intermediari, la clientela e il sistema.

Le attività svolte in vista dell'entrata in vigore del DORA costituiscono un esempio di questo approccio. Dalla fine del 2024 abbiamo avviato un programma organico sviluppato lungo tre direttrici complementari: le analisi e gli esercizi di monitoraggio a livello di sistema (attività orizzontali), gli interventi sui singoli intermediari (attività verticali), e la sorveglianza diretta sui fornitori terzi.

Le analisi orizzontali indicano che nel periodo 2023-25 il totale degli incidenti informatici che hanno coinvolto intermediari italiani sono aumentati dell'80 per cento rispetto al triennio precedente. Nel 2025 quelli di natura cibernetica costituivano circa un quarto del totale. Le difese dagli attacchi esterni sono dunque importanti, ma il presidio dei processi interni rimane fondamentale. Oltre i due terzi degli incidenti hanno comportato una interruzione dei servizi, la cui durata media è aumentata negli ultimi anni. In pochi casi l'interruzione si è protratta per oltre 24 ore, indicando la necessità di migliorare le capacità di risposta. Infine, la metà delle segnalazioni coinvolge direttamente o indirettamente un fornitore o subfornitore di servizi, confermando il ruolo centrale delle terze parti nella gestione del rischio ICT.

Le analisi dei registri delle informazioni¹⁰ consentono di quantificare la dimensione della dipendenza tecnologica delle entità finanziarie direttamente vigilate dalla Banca d'Italia: lo scorso anno abbiamo censito oltre 3.700 fornitori e subfornitori ICT e circa 10.000 contratti, per una spesa annua di 2,4 miliardi di euro. Le evidenze mostrano una forte dipendenza da fornitori extra-gruppo, presso i quali si concentra la quasi totalità delle controparti, dei contratti e della spesa. Le catene di fornitura sono complesse e possono arrivare a comprendere fino a cinque livelli. Circa la metà dei fornitori che supportano funzioni critiche è considerata non sostituibile o difficilmente sostituibile.

Le nostre rilevazioni sull'applicazione del Regolamento DORA da parte degli intermediari di competenza della Banca d'Italia evidenziano che il percorso di adeguamento dei presidi alla nuova normativa è avviato, ma resta la necessità di migliorare alcuni profili. Mi riferisco in particolare all'esigenza di continuare a rafforzare i sistemi di controllo e monitoraggio della sicurezza delle infrastrutture, i processi interni di analisi del rischio IT, i meccanismi per contenere la propagazione degli attacchi, la capacità di utilizzare l'esito degli incidenti e dei test interni per rafforzare i presidi, l'adeguamento dei contratti con i fornitori.

Le informazioni raccolte hanno contribuito al processo di revisione e valutazione prudenziale e ci permettono di accompagnare gli intermediari nel percorso di implementazione del DORA, con particolare attenzione a quelli di minori dimensioni.

Il rischio ICT assume una rilevanza ancora maggiore con l'aumento dell'utilizzo dell'IA in funzione della maggiore rilevanza della *governance* dei dati e della complessità dei modelli.

¹⁰ Si tratta di una segnalazione introdotta dal DORA per consentire alle autorità di vigilanza di disporre di una mappatura degli accordi relativi ai servizi ICT.

Dati “contaminati” da eventuali attacchi o da processi interni inadeguati possono portare a risultati formalmente convincenti ma sostanzialmente inattendibili, influenzando interi processi e, dunque, le decisioni finali. Da qui l’importanza di applicare correttamente i principi stabiliti a livello internazionale riguardo alla tracciabilità dei dati, sui quali è stata intensificata l’attività della Vigilanza europea e nazionale negli ultimi anni. La maggiore complessità dei modelli rende più difficile valutarne criticamente i risultati, anche quando la presenza umana nei processi è formalmente assicurata. Il principio dello ‘human in the loop’ va applicato in termini sostanziali: la supervisione umana non è sufficiente se non si dispone delle informazioni, delle competenze e del tempo necessari.

L’impiego di dati non sufficientemente rappresentativi, o comunque contenenti discriminazioni pregresse che vengono replicate o amplificate dal modello, oppure scelte non adeguate nella progettazione e nello sviluppo degli algoritmi possono inoltre generare discriminazioni ingiustificate nell’accesso al credito, col rischio di compromettere il rispetto dei diritti fondamentali delle persone.

Per valutare come tali rischi si manifestino concretamente, la Banca d’Italia sta conducendo una campagna conoscitiva sui sistemi di IA impiegati nella valutazione del merito creditizio, esaminandone il governo, la strategia, le metodologie, i sistemi informativi e i controlli interni. Alcune evidenze preliminari puntano all’importanza del ruolo del Consiglio di Amministrazione in fase di indirizzo e supervisione; all’esigenza di integrare il sistema di gestione e valutazione dei rischi con indicatori specifici per quelli connessi con l’IA e di definire un quadro organico di regole per lo sviluppo, la validazione, l’utilizzo e il monitoraggio dei modelli. Le prime evidenze confermano inoltre la necessità di rafforzare l’adeguatezza della *governance* dei dati e dei sistemi informativi, anche prevedendo percorsi formativi coerenti con le responsabilità attribuite al personale.

Queste attività sono anche propedeutiche allo svolgimento dei nuovi compiti assegnati alla Banca d’Italia a seguito dell’attuazione nazionale dell’AI Act. Il nostro Istituto è stato infatti designato, insieme a IVASS e Consob, quale autorità responsabile della sorveglianza (*Market Surveillance Authority*) per i sistemi IA ad alto rischio utilizzati dagli intermediari e direttamente connessi con la prestazione di servizi finanziari. Le finalità e i poteri previsti dal Regolamento si pongono in larga misura in continuità con le attività già svolte dalla Banca nell’ambito della vigilanza prudenziale e di tutela, consentendo di valorizzare competenze e processi già esistenti.

Così come è stato fatto per DORA, anche per l’applicazione dell’AI Act il continuo dialogo con l’industria ci permetterà di guidare gli intermediari e di meglio comprendere le difficoltà che incontreranno nell’attuare le misure richieste dalla normativa.

6. L’IA agantica

Negli ultimi mesi grande attenzione è stata posta alle conseguenze della diffusione dell’IA agantica, ovvero di sistemi che prevedono l’utilizzo di agenti software dotati di autonomia nell’accedere a dati e sistemi per eseguire una serie di attività prima affidate persone.

Questi sistemi possono osservare i dati, formulare piani, attivare flussi di lavoro e adattare le proprie azioni con un intervento umano limitato. La potenzialità di generare benefici significativi è evidente, ma autonomia, velocità, scalabilità possono amplificare i rischi. Ancora una volta, il punto è come implementare questi sistemi in modo responsabile, senza indebolire la *governance*, la responsabilità decisionale e la fiducia.

Il quadro normativo composto da DORA, AI Act, disciplina sulla protezione dei dati personali e regolamentazione finanziaria offre un punto di partenza importante, ma non elimina le criticità poste dall'IA agentica. L'aumento dell'autonomia dei sistemi rischia infatti di mettere sotto pressione categorie giuridiche e presidi di controllo sviluppati per modelli decisionali tradizionali. Per evitare che emergano zone d'ombra sotto il profilo della responsabilità e della supervisione, è necessario declinare e, ove opportuno, rafforzare alcuni principi fondamentali: la tracciabilità, la chiara delimitazione del livello di delega e un'applicazione rigorosa del principio di proporzionalità basata sui rischi.

Indipendentemente dalla tecnologia adottata, gli intermediari devono mantenere una netta attribuzione delle responsabilità e la capacità di ricostruire il processo attraverso cui decisioni e azioni sono state generate. È necessaria una chiara definizione delle azioni che possono essere delegate, a quali condizioni e con quali forme di supervisione umana. Gli assetti di governance, i meccanismi di supervisione umana, le attività di test e i sistemi di monitoraggio dovrebbero essere proporzionati alla rilevanza del caso d'uso, al grado di autonomia, all'ampiezza del perimetro operativo e al potenziale impatto su clienti, imprese e stabilità finanziaria. Dovranno essere valutate anche eventuali estensioni al perimetro delle funzioni di controllo; ad esempio, se i controlli di linea dovranno comprendere anche le attività di *human oversight*, quelle di secondo livello potrebbero considerare non solo la coerenza tra le decisioni adottate e la propensione al rischio (*risk appetite*) definito dall'Organo amministrativo, ma anche 'come' le decisioni vengono sostenute mediante l'utilizzo dell'IA. Le stesse funzioni di controllo potrebbero a loro volta avvalersi dell'IA agentica come supporto per le proprie attività.

L'IA agentica può anche essere utilizzata per identificare con estrema precisione e rapidità vulnerabilità informatiche in precedenza sconosciute, soprattutto se combinata con l'utilizzo di modelli particolarmente avanzati (cd. Modelli IA di frontiera). Se da un lato questi modelli possono consentire agli intermediari di rafforzare le proprie difese, dall'altro costituiscono uno strumento che accresce le capacità dei criminali informatici di condurre attacchi potenzialmente molto dannosi.

Il tema ha raggiunto velocemente una dimensione globale. In poco più di un trimestre, almeno quindici autorità e organismi internazionali, tra cui autorità di vigilanza e di regolamentazione, banche centrali, autorità macroprudenziali, agenzie di cybersicurezza, hanno pubblicato comunicazioni, documenti di analisi o richiami al mercato dedicati a questi sviluppi.

Anche in risposta a una raccomandazione del Consiglio Europeo per il Rischio Sistemico (CERS) e in analogia a quanto fatto dalla Banca Centrale Europea (BCE), la Banca d'Italia ha richiamato gli intermediari vigilati direttamente a valutare tempestivamente il livello di esposizione ai rischi derivanti dai modelli IA di frontiera. In coerenza con i requisiti

di DORA e con le evidenze delle analisi sopra menzionate, la Vigilanza ha chiesto di verificare l'adeguatezza dei presidi relativi alla *governance*, all'igiene informatica¹¹, alla gestione delle risorse ICT e delle vulnerabilità, al monitoraggio e alle capacità di difesa, alle prove di resilienza. La valutazione deve tradursi nell'identificazione di responsabilità, in adeguati investimenti e in verifiche sull'avanzamento delle iniziative di rimedio. I relativi piani dovranno essere inviati ai supervisori entro la fine del 2026.

7. Conclusioni

La regolamentazione e la vigilanza non intendono frenare la trasformazione tecnologica, né indicare una soluzione o un modello operativo preferibile. Oggi disponiamo di un quadro di regole e di principi che, seppur sviluppato in un contesto diverso e in continua evoluzione, consente di individuare alcune direttrici per innovare, preservando la solidità degli intermediari e la tutela della clientela.

Il nostro approccio prevede un ciclo integrato: le evidenze raccolte attraverso le analisi orizzontali orientano l'azione di vigilanza sui singoli soggetti, le risultanze delle attività verticali contribuiscono a loro volta a rafforzare la comprensione delle vulnerabilità sistemiche e dei rischi emergenti. Il dialogo attivo con l'industria consente di condividere le aspettative di vigilanza e, al tempo stesso, di comprendere le soluzioni adottate e i principali ostacoli incontrati dagli intermediari. Tutte queste attività contribuiscono ad informare il lavoro di policy e la regolamentazione. Lo scopo è creare le condizioni affinché l'innovazione possa svilupparsi in modo sicuro, responsabile e sostenibile.

Gli intermediari devono quindi continuare a sperimentare e trasformare i propri processi. Ma per innovare occorrono strategie chiare, investimenti adeguati, dati affidabili, competenze diffuse e responsabilità ben definite. L'innovazione può certamente migliorare anche la gestione del credito in tutte le sue fasi, ma solamente se inserita all'interno di una strategia complessiva che ne assicuri un governo robusto.

La resilienza raggiunta dal sistema bancario è il presupposto per affrontare le trasformazioni in corso. Le risorse disponibili vanno utilizzate anche per continuare a investire in innovazione e sicurezza dei sistemi informatici. Solo in tal modo sarà possibile migliorare la qualità dei servizi, gestire i rischi delle nuove tecnologie e preservare la sostenibilità del modello di attività nel lungo periodo. In un mercato in rapida evoluzione rinviare le scelte può rappresentare un rischio non meno rilevante di quello derivante da scelte non adeguatamente governate.

¹¹ L'igiene informatica è l'insieme delle pratiche organizzative, procedurali e tecniche di base finalizzate a mantenere un adeguato livello di sicurezza dei sistemi informativi come, ad esempio, la tenuta di registri completi e aggiornati degli asset informatici, la gestione granulare delle abilitazioni, con particolare attenzione a quelle dotate di elevati privilegi, l'utilizzo di sistemi di autenticazione forte basati su più fattori.

