



UNIVERSITÀ DEGLI STUDI DI MILANO
DIPARTIMENTO DI STUDI INTERNAZIONALI
GIURIDICI E STORICO-POLITICI



LESS SIGNIFICANT BANKS (LSI) ALLA RICERCA DELLA PROPORZIONALITÀ NELLE CRISI BANCARIE

a cura di

ALLEGRA CANEPA, GIAN LUCA GRECO, UGO MINNECI



G. Giappichelli Editore

LESS SIGNIFICANT BANKS (LSI)
ALLA RICERCA DELLA PROPORZIONALITÀ
NELLE CRISI BANCARIE

a cura di

ALLEGRA CANEPA, GIAN LUCA GRECO, UGO MINNECI



G. Giappichelli Editore

© Copyright 2026 - G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111
<http://www.giappichelli.it>

ISBN/EAN 979-12-211-1979-4
ISBN/EAN 979-12-211-8483-9 (ebook - pdf)
ISBN/EAN 979-12-211-8484-6 (ebook - epub)

*La pubblicazione del volume è stata finanziata con i fondi del Progetto di ricerca “Proportionat-
ing rules on bank crisis prevention and management to the case of retail banks: an analysis on the
European and national legal framework (Pro.Re.Ba.)”, codice progetto: 2022YXTHZF_003,
CUP Master: H53D23002980006, CUP derivato: G53D23002350006, finanziato dal-
l’Unione Europea - Next Generation EU, PNRR, Missione 4, Componente 2, Investimento
1.1. - Bando PRIN 2022.*



CC BY-NC-ND
Attribuzione - Non Commerciale - Non Opere Derivate

Publicato online nel mese di maggio 2026

Indice

	<i>pag.</i>
<i>Informazioni sugli Autori</i>	XIII
<i>Introduzione</i> di Iacopo Donati e Irene Mecatti	XV

Sezione I

LESS SIGNIFICANT INSTITUTION (LSI) E CRISI TRA PROPORZIONALITÀ E RESILIENZA

LA PROPORZIONALITÀ DELL'ASSETTO ISTITUZIONALE DEL SISTEMA DAL LATO DELLE COMPETENZE RELATIVE ALLE SITUAZIONI DI CRISI, ANCHE TEMPORANEA, DELLE IMPRESE BANCARIE

Gianluca Romagnoli

1. Considerazioni introduttive	3
2. Un quadro d'insieme: le amministrazioni coinvolte nelle crisi reversibili ed irreversibili	7
3. L'utilità di una valutazione dell'assetto esistente attraverso il parametro della proporzionalità	12
4. Uno sguardo all'assetto istituzionale europeo	15
5. Uno sguardo all'assetto istituzionale domestico	19
6. Una conclusione	22

LA PROPORZIONALITÀ NELLA GESTIONE DELLE CRISI DELLE MEDIE E PICCOLE BANCHE: UN TENTATIVO DI UN APPROCCIO EMPIRICO

Gianluca Aloia

1. Premessa	25
2. Le determinanti delle crisi degli intermediari bancari e finanziari	26
3. La declinazione della proporzionalità nella concreta azione di gestione della crisi	27
4. La proporzionalità è sempre diretta?	35
5. Proporzionalità, discrezionalità e <i>level playing field</i>	37

	<i>pag.</i>
6. Proporzionalità e semplificazione	39
7. Conclusioni	41
CRITICA ALLA (S)PROPORZIONALITÀ NEGLI AIUTI DI STATO ALLE BANCHE NON SISTEMICHE	
Gian Luca Greco	
1. Cenni telegrafici di storia recente della “dottrina” degli aiuti di Stato al sistema bancario	45
2. Sullo (s)bilanciamento degli interessi nel <i>burden sharing</i> “preventivo” per le piccole banche	49
3. Aiuti di Stato, <i>burden sharing</i> “preventivo” e tutela del risparmio individuale: un bilanciamento da rivedere	52
4. Aiuti di Stato e BRRD: serve una riforma congiunta	55
EARLY INTERVENTION MEASURES AND PROPORTIONALITY	
Marco Lamandini	
1. A premise	57
2. Looking backward	58
3. Looking into the present	60
4. Looking into the future	62
CESSIONE E GESTIONE DEI CREDITI IN SOFFERENZA	
Ugo Minneci	67
LE CRISI DELLE BANCHE MEDIO-PICCOLE TRA PROCEDURE SPECIALI E DI DIRITTO COMUNE	
Marco Novara	
1. Oggetto dell’analisi e punto di osservazione	71
2. La crescente assimilazione del diritto comune della crisi alla disciplina speciale delle crisi bancarie	72
3. La FOLTF <i>assessment</i> e l’accertamento del “rischio di rischio” di dissesto	75
4. Il ruolo degli amministratori	79
5. Conclusioni	81

pag.

L'ENTE-PONTE COME STRUMENTO PER LA SOLUZIONE DELLA CRISI DI BANCHE NON SISTEMICHE: LA QUESTIONE DELLA PROPORZIONALITÀ

Michele Cossa

1. Premessa	85
2. <i>Bridge banks</i> e crisi bancarie: l'esperienza nazionale ed internazionale	87
3. Le caratteristiche e la complessità dell'istituto	91
4. Lo strumento dell'ente-ponte in un sistema a doppio binario	95
5. La <i>bridge bank</i> alla luce del giudizio di proporzionalità	96

I COMMISSARI IN TEMPORANEO AFFIANCAMENTO

Sido Bonfatti

1. La struttura della disciplina delle crisi delle banche	101
2. I presupposti generali della applicazione della disciplina delle situazioni di "crisi" delle banche e la tipologia degli interventi ipotizzabili	103
3. Gli interventi sugli organi di amministrazione e controllo della banca	103
4. <i>Segue. Removal</i> "collettivo", <i>removal</i> "individuale", "Commissari in affiancamento" e "scioglimento" degli organi	107
5. Gli interventi "provvisori" o "temporanei" sull'organo di amministrazione della banca. Le modifiche alla legge bancaria e al Testo unico bancario apportate dal recepimento della dir. 2014/59/UE	108
6. I presupposti della adottabilità della " <i>misura di intervento precoce</i> " della nomina del Commissario in temporaneo affiancamento	110
7. Il procedimento di nomina ed i poteri e funzioni dei Commissari in temporaneo affiancamento	112
8. Gli effetti dell'adozione della nomina del Commissario in temporaneo affiancamento: il rinvio alle disposizioni dell'amministrazione straordinaria	114
9. <i>Segue.</i> Gli effetti della proposizione dell'azione di responsabilità sociale nei confronti degli amministratori "affiancati" dai Commissari in temporaneo affiancamento	117
10. <i>Segue.</i> La natura giuridica dei Commissari in temporaneo affiancamento e la soggezione al Codice deontologico per i componenti degli organi nominati dalla Banca d'Italia	118
11. I Commissari in temporaneo affiancamento nei confronti della "capo-gruppo" e delle società di un gruppo bancario	118
12. I singoli casi di specie	119
13. Conclusioni	122

LA RESILIENZA DEL MERCATO BANCARIO ALLA PROVA
DELLA FRAMMENTAZIONE GEOECONOMICA
E DELLE VULNERABILITÀ TECNOLOGICHE

Allegra Canepa

- | | | |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 1. | Evoluzione del mercato bancario e aggiornamento delle tipologie di vulnerabilità tra tecnologia e geopolitica | 125 |
| 2. | L'impatto delle relazioni internazionali sull'entità del rischio geopolitico: il caso delle esternalizzazioni | 128 |
| 2.1. | L'esternalizzazione dei servizi cloud e la dipendenza da Paesi terzi tra revisione del Cybersecurity Act e discussione del Cloud and AI Development Act (c.d. CADA) | 131 |
| 3. | La dimensione incerta della vulnerabilità tecnologica: quando il rischio è amplificato dal modello di business e dalla comunicazione digitale | 133 |
| 4. | Qualche considerazione conclusiva | 136 |

Sezione II

VIGILANZA E RISOLUZIONE NELLE LSI E NELLE BANCHE
DI CREDITO COOPERATIVO

LE VALUTAZIONI DISCREZIONALI DEL *SINGLE RESOLUTION BOARD*
IN MATERIA DI RISOLUZIONE DELLE CRISI BANCARIE ALLA LUCE
DELL'EROSIONE SOSTANZIALE DELLA "DOTTRINA" SULLA (NON)
DELEGABILITÀ DI POTERI ALLE AGENZIE EUROPEE

Gianni Capobianco

- | | | |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 1. | Il fenomeno dell' <i>agencification</i> : il <i>Single Resolution Board</i> come agenzia europea | 141 |
| 2. | Il problema della (non) delegabilità di poteri discrezionali a soggetti estranei al circuito democratico-rappresentativo. Le condizioni fissate nel caso <i>Meroni c. Alta Autorità</i> e la successiva giurisprudenza della Corte di Giustizia | 144 |
| 3. | Le valutazioni discrezionali demandate al <i>Single Resolution Board</i> nella procedura di risoluzione delle crisi bancarie e il ruolo della Commissione europea | 146 |
| 3.1. | Il problema del mancato coinvolgimento della Commissione in caso <i>non-resolution decisions</i> del SRB | 151 |
| 4. | Riflessioni conclusive: l'incerta persistenza (e consistenza) della dottrina sulla non delegabilità di poteri discrezionali nel quadro di gestione delle crisi bancarie | 153 |

La resilienza del mercato bancario alla prova della frammentazione geoeconomica e delle vulnerabilità tecnologiche

Allegra Canepa

SOMMARIO: 1. Evoluzione del mercato bancario e aggiornamento delle tipologie di vulnerabilità tra tecnologia e geopolitica. – 2. L’impatto delle relazioni internazionali sull’entità del rischio geopolitico: il caso delle esternalizzazioni. – 2.1. L’esternalizzazione dei servizi cloud e la dipendenza da Paesi terzi tra revisione del Cybersecurity Act e discussione del Cloud and AI Development Act (c.d. CADA). – 3. La dimensione incerta della vulnerabilità tecnologica: quando il rischio è amplificato dal modello di business e dalla comunicazione digitale. – 4. Qualche considerazione conclusiva.

1. Evoluzione del mercato bancario e aggiornamento delle tipologie di vulnerabilità tra tecnologia e geopolitica

Come ricordato da K. Knot, chair del Financial Stability Board (FSB), nel suo intervento dell’aprile 2025, il monitoraggio e la sorveglianza del sistema finanziario risultano fondamentali. Tale affermazione appare ancor più centrale se si considera il possibile emergere di “nuove” vulnerabilità, quali ad esempio quelle generate dallo sviluppo tecnologico, o la rinnovata attualità di fragilità indotte dagli scenari geopolitici¹. In entrambe le situazioni, ciò che risulta di interesse sono proprio le modalità attraverso le quali queste possono presentarsi, soprattutto se prive di segnali “premonitori”, come nel caso del Covid-19, e repentine, come avvenuto nella crisi delle banche della Silicon Valley del 2023.

Proprio per questo la riflessione si concentrerà sull’attualità e la possibile coesistenza di rischi geopolitici o tecnologici capaci di produrre effetti non lineari e più o meno rilevanti. Ciò significa in primo luogo distinguere tra rischi “interni” intesi come quelli derivanti da cambiamenti avvenuti nel modello di business degli operatori finanziari, e rischi “esterni”, come quelli indotti da mutati scenari geopolitici.

¹ Si veda K. KNOT, *FSB Chair’s letter to G20 Finance Ministers and Central Bank Governors*, aprile 2025, 23 maggio 2025, <https://www.fsb.org/2025/04/fsb-chairs-letter-to-g20-finance-ministers-and-central-bank-governors-april-2025/>.

Il primo aspetto appare ben esemplificato dal caso della crisi delle banche americane della Silicon Valley, caratterizzate da un modello di business “ad alta digitalizzazione”.

Il rischio geopolitico, inteso come minaccia e/o come realizzazione di eventi avversi, compresi quelli derivanti da attacchi cyber, associati a guerre, terrorismo e tensioni tra stati ed attori politici, nonché alle vulnerabilità delle infrastrutture, capaci di influenzare il corso pacifico delle relazioni internazionali², assume rilievo proprio in quanto fattore capace di generare rischio sistemico all’interno del settore bancario europeo³.

Pur essendo molteplici le situazioni di conflitto e di mutamento degli equilibri nelle relazioni multilaterali foriere di rischi, basti pensare al conflitto nell’area mediorientale o alle tensioni tra Stati Uniti e Cina, uno degli esempi al quale fare riferimento può essere quello del conflitto tra Russia e Ucraina dove l’ambito finanziario riveste anche un ruolo attivo in quanto strumento per esercitare pressione ed imporre aggravii ai sistemi economici. Emblematica, in tal senso, appare sia l’esclusione delle banche russe dal sistema SWIFT⁴ sia, nell’ambito delle sanzioni economiche applicate dall’UE, la vicenda del sequestro degli asset.

L’European Banking Authority (EBA), nei suoi Risk Assessment Reports (RAR) di giugno e dicembre 2025⁵, aveva già evidenziato un incremento delle criticità derivanti proprio dagli scenari geopolitici e da possibili interruzioni degli scambi commerciali, dovute anche all’introduzione di dazi, con conseguente produzione di incertezza per consumatori e imprese e di effetti sui mercati finanziari⁶. Del resto, nell’aprile 2025, il solo annuncio dell’introduzione di ulteriori

² Su questa definizione di rischio geopolitico correlato al mercato bancario si veda in particolare D. CALDARA, M. IACOVIELLO, *Measuring geopolitical risk*, in *American Economic Review*, 112(4), p. 1194 ss. e M. BEHN, J.H. LANG, A. REGHEZZA, *120 years of insight: Geopolitical risk and bank solvency*, in *Economics Letters*, 2025, p. 112 ss.

³ Un recente report della BCE individua 5 categorie di rischio geopolitico capaci di influire sulla stabilità finanziaria e nello specifico: 1) conflitti militari e guerre 2) vulnerabilità delle infrastrutture comprese quelle energetiche e digitali 3) turbamenti del commercio e sanzioni 4) rischi finanziari 5) fattori politici o sociali. Si veda ECB, ESRB, *Financial stability risks from geoeconomic fragmentation*, gennaio 2026, https://www.ecb.europa.eu/pub/pdf/other/ecb.report202601_financialstability-risks.en.pdf.

Sul punto si veda anche M. ALBORI, *Politics will tear us apart, again. Geopolitical risk, fragmentation, and capital flows*, Occasional Papers di Banca d’Italia, n. 974, ottobre 2025.

⁴ Sul punto si vedano in particolare A. LUPOI, B. PEZZULLI, *Deterrenza e fuoco amico. Gli effetti delle sanzioni internazionali sul debito estero della Federazione Russa e sull’ordine finanziario globale*, in *Dialoghi dir. econ.*, 2022, p. 1 ss. e M. MAGGIOLINO, *La globalizzazione finanziaria in crisi: tra neutralità economica e valori occidentali*, in *Riv. trim. dir. econ.*, 2024, 3, p. 111 ss.

⁵ Si veda EBA, *Risk Assessment Report*, giugno 2025, <https://www.eba.europa.eu/publications-and-media/publications/risk-assessment-report-june-2025> e dicembre 2025, <https://www.eba.europa.eu/sites/default/files/2025-12/8acb45c4-912b-4f0f-b887-37b8fc058779/Risk%20Assessment%20Report%20Autumn%202025.pdf>.

⁶ Sul tema si veda in particolare P. AVRIL, P. BOCHMANN, S. FAHR, A. HORAN, C. PANCARO., R.

dazi da parte degli Stati Uniti aveva incrementato notevolmente la volatilità dei prezzi azionari, anche nel segmento bancario, fino a raggiungere i livelli precedenti alla fase pandemica. Del resto, quello dei mercati finanziari è uno dei canali di trasmissione attraverso i quali gli shock possono compromettere la stabilità finanziaria e tradursi in perdite per le banche sui portafogli titoli dovute a riduzioni di liquidità e deflussi di risorse. Ad esso si aggiunge quello dell'economia reale, visto che l'aumento dei costi dovuto alle interruzioni delle catene del valore determina aumenti dei costi e maggiore difficoltà nel rimborso dei crediti, con tutto ciò che ne consegue per le banche. Infine, è utile ricordare anche il canale associato agli attacchi informatici in grado di compromettere l'infrastruttura finanziaria.

La Banca centrale europea (BCE), visto l'aumento crescente del rischio geopolitico, non solo ha deciso di mantenerlo tra le priorità di supervisione per il periodo 2026-2028, ma ha anche stabilito di condurre uno stress test inverso tematico, cioè incentrato sul rischio geopolitico, per valutare l'impatto dei cambiamenti negli assetti commerciali e sulla redditività e solvibilità⁷.

Questa tipologia di vulnerabilità non è una novità, ma ha assunto una rilevanza crescente nel quadro attuale, vista la possibilità di produrre effetti non solo sulle grandi banche con filiali estere e attività nei Paesi terzi, ma anche sulle altre, tenuto conto della struttura proprietaria e dell'elevato livello di esternalizzazione di funzioni critiche⁸.

Peraltro, l'ultimo rapporto dell'International Monetary Fund (IMF) sulla stabilità finanziaria globale⁹, evidenzia come la valutazione sugli effetti in questo caso non possa essere effettuata solo tenendo conto degli effetti immediati, ma debba considerare anche quelli di lungo periodo derivanti da un clima di minore certezza capace di produrre ripercussioni su investimenti e crescita economica.

Da quanto richiamato, deriva la necessità per le banche di disporre di modelli di business solidi rispetto a tali rischi, tenuto conto anche delle implicazioni sul credito e sul debito sovrano.

Infatti, le tensioni tra gli Stati e le relative conseguenze sulle relazioni commerciali possono richiedere un rafforzamento degli investimenti, in particolare in

PIZZEGHELLO, *Risks to euro area financial stability from trade tensions*, in European Central Bank, *Financial Stability Review*, maggio 2025; https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202505_02~4603d3e42a.en.html.

⁷ Lo stress test interesserà 110 banche sottoposte a vigilanza diretta. Si veda il comunicato stampa della BCE del 12 dicembre 2025, *ECB to assess banks' stress testing capabilities to capture geopolitical risk*, <https://www.dirittobancario.it/wp-content/uploads/2025/12/Comunicato-stampa-BCE-12-dicembre-2025.pdf>. I risultati di questo stress test saranno resi noti nell'estate del 2026.

⁸ Questa situazione, ad esempio, caratterizza la maggior parte delle 113 banche supervisionate dalla BCE. Proprio su questi aspetti si veda T. BECK, B. BRUNO, E. CARLETTI, *The impact of geopolitical shocks on banks' financial soundness in the Banking Union*, European Parliament, Economic Governance Support Unit, PE 773.718, novembre 2025.

⁹ IMF, *Global Financial Stability report, Shifting Ground beneath the Calm*, 2025, p. 47 ss., <https://www.imf.org/-/media/files/publications/gfsr/2025/october/english/text.pdf>.

ambito tecnologico e di sicurezza, con tutto ciò che ne consegue, anche dal punto di vista dell'impiego delle risorse pubbliche e delle differenti disponibilità tra gli Stati membri, alla luce delle singole situazioni di indebitamento.

2. L'impatto delle relazioni internazionali sull'entità del rischio geopolitico: il caso delle esternalizzazioni

La crescente frammentazione finanziaria, accompagnata da processi di riallocazione delle risorse lungo direttrici anche di sintonia economica e politica, apre nuove riflessioni e rende di grande attualità la valutazione del rischio geopolitico, anche per le implicazioni su altre tipologie di rischio esistenti, come quelle di credito, di mercato, di liquidità e operativo, che lo rendono una categoria sempre più "iperconnessa" e capace di influenzare le altre. Del resto, se ad esempio si considera il credito, il mutato scenario, rende necessario includere una "visione a catena" dei prestiti e dei clienti che tenga conto dell'articolazione delle catene del valore dalla fornitura alla distribuzione e può indurre l'adozione anche di strategie di riduzione del rischio quali il congelamento di nuove linee di credito¹⁰.

Tra gli aspetti che potrebbero essere presi in esame ve n'è però uno di particolare interesse che è quello del legame tra variazioni negli equilibri delle relazioni internazionali ed esternalizzazione di funzioni ad operatori terzi, specialmente di ambito tecnologico, perlopiù extra-europei.

Questo aspetto assume rilievo non solo sul piano dei rischi operativi, sui quali, come sarà descritto, l'Europa è intervenuta con il regolamento c.d. DORA, ma anche sui rapporti contrattuali, sulle implicazioni economiche e sulla necessità di incremento "dell'autosufficienza" tecnologica.

Negli ultimi anni si è registrato un crescente ricorso a fornitori esterni per disporre di competenze specialistiche, ridurre i costi e offrire servizi concorrenziali sul mercato, ad esempio nell'ambito dei bonifici istantanei. Questo ha dato luogo ad una molteplicità di accordi rispetto ai quali sono sorte implicazioni di supervisione legate sia ad aspetti di sicurezza, specialmente per quanto concerne l'ambito ICT, sia alla normativa applicabile, tenuto conto che spesso solo una delle parti ha natura finanziaria ed è perciò sottoposta alla conseguente normativa. Del resto, la BCE aveva sottolineato come la spesa per esternalizzazioni risultasse in

¹⁰ Si rilevano anche differenze nella categorizzazione del rischio paese perché, proprio alla luce del conflitto tra Russia e Ucraina, sono stati inclusi anche la mobilità degli asset e le implicazioni su di essi derivanti dall'applicazione di sanzioni. Sulle tipologie di minacce che possono dare luogo all'applicazione di sanzioni e sulle misure adottate nei confronti della Russia si veda in particolare *Quaderni dell'antiriciclaggio, Rassegna normativa*, Banca d'Italia, II-2024, p. 10 ss. Da ultimo con il reg. 2025/2600 del 12 dicembre 2025 è stato vietato qualsiasi trasferimento diretto o indiretto di attività o riserve della Banca centrale di Russia (art. 2).

costante crescita, specialmente per i servizi cloud necessari per l'archiviazione ed elaborazione dei dati¹¹, senza che vi fosse una contestuale garanzia sulla qualità dell'offerta, anche per le attività critiche¹² e con possibili rischi di vulnerabilità operative e di sicurezza dei dati,

Se guardiamo specificamente al segmento finanziario su questi aspetti il reg. 2022/2554, Digital Operational Resilience Act, c.d. DORA, ha previsto la necessità, per le entità finanziarie, di attuare un quadro per la gestione ed il controllo interno derivanti dalle tecnologie dell'informazione e della comunicazione, applicabile a tutti i fornitori terzi di servizi di Tecnologie dell'Informazione e della Comunicazione (TIC)¹³. Nello specifico, è stato introdotto un test di resilienza operativa, i cui esiti costituiscono parte dei processi di supervisione, nonché di monitoraggio e classificazione degli incidenti ITC e delle minacce informatiche¹⁴.

¹¹ È utile ricordare come al cloud possibili rischi possano derivare anche da hardware e dai Large Language Model (LLM) che possono avere costi molto elevati. Sul punto si veda in particolare FSB, *The Financial stability implications of Artificial Intelligence*, 14 novembre 2024, p. 6, <https://www.fsb.org/2024/11/the-financial-stability-implications-of-artificial-intelligence/#:~:text=14%20November%202024%20FSB%20assesses,and%20regulatory%20frameworks%20and%20capabilities.>

Sulla frammentazione della catena valore e l'outsourcing la Bank of England ha pubblicato un documento specifico nel febbraio 2023, *Outsourcing and Third Party Risk Management Supervisory Statement: recognised payment system operators and specified service providers*, 8 febbraio 2023, <https://www.bankofengland.co.uk/paper/2023/ss/outsourcing-third-party-risk-management-ss-recognised-payment-system-operators.>

Sul tema in dottrina si vedano tra gli altri A. SACCO GINEVRI, *Esternalizzazione (outsourcing)*, in *Fintech: diritti, concorrenza, regole*, diretto da G. Finocchiaro, V. Falce, Bologna, 2019, p. 205 A. SCIARRONE ALIBRANDI, *Innovazione tecnologica, regolazione e supervisione dei mercati*, e M. SEPE, *Prestazione frazionata e regole di rapporto tra imprese*, entrambi in R. LENER, G. LUCHENA, C. ROBUSTELLA (a cura di), *Mercati regolati e nuove filiere del valore*, Torino, 2021, rispettivamente p. 5 e p. 233 ss.; A. CANEPA, *Big Tech e mercati finanziari: "sbarco pacifico" o "invasione"? Analisi di un "approdo" con offerta "à la carte"*, in *Riv. trim. dir. econ.*, 2021, 3, p. 465 ss.; V. TROIANO, *Soggettività finanziaria e forme di aggregazione*, *ivi*, 2022, 1, p. 92 ss.; F. CIRAOLO, *L'ecosistema digitale e l'evoluzione dei mercati*, *ivi*, 2022, 4, p. 342 ss.; L. SPITALERI, *L'outsourcing nei servizi bancari e finanziari, profili di governance e prospettive di vigilanza*, *ivi*, 2023, p. 136 ss. e L. AMMANNATI, *I nuovi paradigmi dell'impresa bancaria in epoca di transizione*, in *Quaderno di ricerca giuridica*, Banca d'Italia, n. 99, 2024.

¹² Si veda BCE, *Supervisory Review and Evaluation Process (SREP) Aggregated results of SREP 2023*, par. 5.5.2. Operational risk.

¹³ Il regolamento è stato poi seguito da due regolamenti delegati, pubblicati in GU UE del 25 giugno 2024, rispettivamente n. 1772/2024 sui criteri per la classificazione degli incidenti connessi alle Tecnologie dell'IC e n. 2024/1774 sulla gestione dei rischi informatici. Sul regolamento ed i rischi operativi si vedano in particolare i contributi di R. LENER, *Regolazione fintech e Testo unico bancario* e F. ANNUNZIATA, *Fintech e infrastrutture tecnologiche e intelligenza artificiale*, entrambi in *Quaderni di ricerca giuridica della consulenza legale*, Banca d'Italia, n. 100, 2024 e P. LUCANTONI, C. CACCIAVILLANI, *La gestione e supervisione dei rischi ITC e di sicurezza nelle attività finanziarie esternalizzate tra DORA e CRD VI*, in *Dialoghi dir. econ.*, 2025, p. 1 ss.

¹⁴ È utile ricordare che il reg. 2025/302, con riferimento ai sistemi di AI fornisce agli enti finanziari modelli standardizzati per la segnalazione di incidenti rilevanti relativi alle ICT e la notifica di minacce informatiche significative.

L'obiettivo, ai sensi dell'art. 6 del regolamento, è quello di disporre di un quadro per la gestione dei rischi efficace sia sulla prevenzione che su un'efficace gestione anche attraverso adeguate competenze degli organi di governance.

Proprio per questo le entità finanziarie devono tenere conto, alla luce delle esternalizzazioni effettuate, anche della natura e dell'importanza della dipendenza dai fornitori TIC, e alla loro attività si affianca quella delle autorità di vigilanza¹⁵, visto il rilievo per la stabilità finanziaria nell'individuazione dei fornitori critici e nel controllo del rischio di concentrazione, che in questa fase può essere accentuato anche da quello correlato all'andamento delle relazioni con i Paesi sede delle imprese interessate. In particolare, a livello italiano, è necessario che gli intermediari informino tempestivamente la Banca d'Italia prima di concludere accordi contrattuali per l'utilizzo di servizi ITC.

Inoltre, ai sensi dell'art. 33 del DORA vi è la possibilità di imporre misure nei confronti di quei fornitori critici che non dimostrino di aver posto in essere tutto ciò che era necessario per la gestione dei rischi informatici.

Proprio nel novembre scorso le ESAs hanno pubblicato la lista di quegli operatori critici ai sensi di DORA, capaci, in caso di malfunzionamento, di generare conseguenze rilevanti di sistema, e tra di essi figurano anche Amazon web services e Google cloud¹⁶. Proprio in riferimento a questi ultimi, assumono particolare rilievo anche altre possibili questioni, non strettamente connesse alle misure di prevenzione e gestione del rischio, bensì alla difficoltà di scegliere tra gli operatori, vista la differente rilevanza sul mercato, e di contrattare termini e condizioni quando sussiste un forte squilibrio tra le parti. In tali situazioni, più volte osservate quando la controparte è una Big Tech, la conclusione del contratto o la sua rinegoziazione possono essere caratterizzate da una non piena negoziabilità delle condizioni a causa di quella che può essere identificata come una dipendenza economica¹⁷.

Emblematico in tal senso appare il caso di Amazon, non solo con riferimento agli accordi con i venditori interessati a far parte del suo marketplace¹⁸ ma anche

¹⁵ Si veda l'ultima consultazione EBA, *Draft consultation paper on the guidelines on sound management of third-party risk*, EBA/CP/2025/12, 8 luglio 2025.

¹⁶ La lista contiene, ai sensi dell'art. 31, comma 9, un elenco di 19 fornitori critici. Si veda https://www.esma.europa.eu/sites/default/files/2025-11/List_of_designated_CTPPs.pdf.

¹⁷ Sul tema esiste un'ampia letteratura tra gli altri si vedano R. NATOLI, *L'abuso di dipendenza economica: il contratto ed il mercato*, Napoli, 2004; A. BARBA, *Studi sull'abuso di dipendenza economica*, Padova, 2018; M. MAUGERI, *Subfornitura e abuso di dipendenza economica: fra diritto civile e della concorrenza*, Torino, 2022; M. LIBERTINI, *La prima decisione sui provvedimenti dell'Agcm contro gli abusi di dipendenza economica rilevanti per la concorrenza ed il mercato*, in *Giorn. dir. amm.*, 2023, p. 669 ss.; G. COLANGELO, V. MINERVINI (a cura di), *La nuova stagione dell'abuso di dipendenza economica*, Bologna, 2023; A.M. GAMBINO, *Abuso tecnologico di dipendenza economica*, in *Nuovo dir. civ.*, 2025, p.181; M. MAUGERI, *Piattaforme e abuso di dipendenza economica*, in *An. giur. econ.*, 2025, p. 67 ss.

¹⁸ Basti pensare, ad esempio, come il contratto di Business Solution del servizio "vendere su Amazon" avesse tra le altre una previsione di necessaria parità di condizioni che il venditore doveva

con gli operatori di pagamento che offrono il servizio ai suoi utenti. A tal proposito è utile ricordare, pur non potendolo approfondire in questa sede, che, la tipologia di accordo tra l'operatore di pagamento e la Big tech, presenta caratteristiche particolari in quanto l'operatore finanziario fornisce un servizio distribuito agli utenti sotto il "marchio" della piattaforma ed è stato pertanto definito *white labelling*¹⁹.

Proprio nell'ambito di uno di questi accordi tra Amazon e Visa, qualche anno fa, in sede di revisione, Amazon aveva ritenuto le commissioni interbancarie applicate in alcuni Paesi troppo elevate e capaci di generare insoddisfazione tra gli utenti. Pertanto, vista l'iniziale indisponibilità di Visa a trattare su questo aspetto, aveva reso nota al pubblico la decisione di procedere ad una sospensione della possibilità di utilizzare Visa per gli acquisti su Amazon a partire dal Regno Unito, dove la questione si era posta²⁰. A fronte di un simile rischio di esclusione da un marketplace come Amazon, con un numero di utenti fidelizzati molto elevato, e vista la presenza nello stesso marketplace di accordi con altri concorrenti, come MasterCard, Visa aveva rivisto la sua posizione, accogliendo quanto richiesto da Amazon ed annunciando il raggiungimento di un accordo nel febbraio 2022²¹.

2.1. L'esternalizzazione dei servizi cloud e la dipendenza da Paesi terzi tra revisione del Cybersecurity Act e discussione del Cloud and AI Development Act (c.d. CADA)

Come anticipato, la BCE già nel 2023 aveva segnalato un trend di crescita delle esternalizzazioni nei servizi cloud evidenziandone la potenziale criticità.

mantenere tra i prodotti proposti sul marketplace e quelli su altri canali di vendita in modo che questi secondi non potessero risultare maggiormente concorrenziali. In sostanza il venditore era libero di determinare quali prodotti offrire sul marketplace di Amazon ma era obbligato a mantenere le medesime condizioni, compresi i servizi di assistenza, tra i prodotti offerti tramite gli altri canali di vendita.

¹⁹ Secondo il Report dell'EBA *On white labelling*, EBA/REP/2025/30 del 30 ottobre 2025, il modello è piuttosto diffuso essendo utilizzato dal 35% delle banche che hanno partecipato all'indagine effettuata nella primavera del 2025 e varia sulla base di 7 elementi chiave individuati nello status normativo del fornitore e del partner, nella ripartizione dei compiti, la natura del modello di business di *white labelling* per il fornitore ed il partner, i prodotti ed i servizi distribuiti, i clienti target, la distribuzione geografica ed il modello tariffario.

²⁰ Era stato indicato anche un termine a decorrere dal quale la decisione sarebbe divenuta operativa nel 19 gennaio 2022, a seguire vi sarebbe stata l'applicazione di un sovrapprezzo pari allo 0,5% per gli acquisti conclusi da utenti in Australia e Singapore se effettuati con Visa.

²¹ In questo caso, come ricordato anche dalla Financial Conduct Authority (FCA), Amazon ha esercitato il proprio potere contrattuale nei confronti di Visa, facendo leva sul suo elevato numero di utenti, ai quali avrebbe potuto impedire di utilizzare Visa per effettuare pagamenti sul marketplace. Sulla questione si veda in particolare FCA, *The potential competition impacts of Big Tech entry and expansion in retail financial services*, Discussion Paper DP22/5, ottobre 2022, p. 23 ss.

Quest'ultima può risultare ulteriormente incrementata alla luce dell'evoluzione degli scenari geopolitici e delle dipendenze, nelle catene di approvvigionamento, da fornitori terzi di infrastrutture e servizi. In esse possono essere coinvolti Paesi terzi di appartenenza delle imprese, non sempre capaci di garantire un livello di affidabilità in termini di sicurezza informatica, e, inoltre, l'eccessiva concentrazione su alcuni grandi operatori di mercato, come quelli statunitensi, ha ripercussioni sulla competitività e sulla capacità di negoziazione delle condizioni contrattuali.

Tutti questi aspetti venivano evidenziati anche nel rapporto Draghi *The future of European Competitiveness* presentato nel 2024, dove si ricordava come il più grande operatore europeo rappresentasse solo il 2% del mercato europeo e come a fronte di una diminuzione della stabilità politica, le dipendenze europee si fossero rivelate vulnerabilità²². Del resto, il Comitato europeo per il rischio sistemico ha identificato in questo assetto una potenziale vulnerabilità sistemica, poiché anche incidenti informatici localizzati potrebbero avere ripercussioni immediate sull'intero sistema.

Proprio per far fronte a tali rischi, a livello europeo, è in discussione un pacchetto di riforme volto ad una revisione del reg. 2019/881 (c.d. Cybersecurity Act) e alla modifica di alcuni aspetti della dir. 2022/2555 (c.d. Network and Information Society – NIS 2) sulla resilienza operativa digitale per il settore finanziario, al fine di ridurre la frammentazione. A tali interventi se ne aggiunge uno specifico, il Cloud and AI Development ACT (c.d. CADA)²³, diretto a superare le frammentazioni nazionali, anche in termini di incremento della capacità cloud, e ad integrare il Data Act, favorendo il processo di switching tra operatori. Quest'ultimo aspetto appare di interesse per il segmento finanziario, perché contribuisce a quanto stabilito dal regolamento DORA in materia di diversificazione dei provider, al fine di ridurre i rischi di concentrazione, dai quali possono derivare rischi sistemici.

Tra gli obiettivi perseguiti, ve n'è anche uno diretto a rafforzare la sovranità europea, perché, in alcuni casi qualificati come critici, si prevede il ricorso esclusivamente a capacità cloud altamente sicure ed europee. Ciò dovrebbe essere reso possibile grazie all'ulteriore obiettivo di triplicare l'attuale capacità entro 5-7 anni. In particolare, dal punto di vista della sicurezza, una relazione della commissione per l'industria, la ricerca e l'energia (ITRE) del Parlamento europeo evidenzia come si sia cercato anche di avviare un sistema di certificazione della sicurezza informatica, finalizzato all'identificazione dei servizi cloud europei

²² Si veda p. 5 ss. Il rapporto è su https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.

²³ Su quest'iniziativa si veda in particolare il documento di briefing [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/779251/EPRS_BRI\(2025\)779251_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/779251/EPRS_BRI(2025)779251_EN.pdf) nonché la *Call for evidence for an impact assessment*, Ares(2025)2878100 – 9 aprile 2025, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14628-AI-Continent-new-cloud-and-AI-development-act_en.

che garantivano determinati standard di sicurezza, ma sul punto non è stato raggiunto un accordo.

3. La dimensione incerta della vulnerabilità tecnologica: quando il rischio è amplificato dal modello di business e dalla comunicazione digitale

Il perimetro dei fattori di vulnerabilità, come evidenziato, include anche quello tecnologico, inteso non solo come inserimento di soggetti non finanziari nella catena del valore, ma anche come progressivo ampliamento della quota di istituzioni non bancarie (c.d. NBFi) caratterizzate da modelli di business ad “alta digitalizzazione” che erogano servizi, come ad esempio quello creditizio, e contribuiscono ad uno spostamento di queste attività verso aree di regolazione meno stringenti. Un esempio in tal senso è rappresentato nel credito al consumo dalle piattaforme di Buy Now Pay Later (BNPL) che, hanno beneficiato per un certo periodo di tempo dell’incertezza sulla natura del nuovo servizio offerto, caratterizzato, in certi casi, anche da un’erogazione di credito per somme molto esigue²⁴, rispettando la sola normativa sui pagamenti. Sul punto, l’European Banking Authority (EBA) e Banca d’Italia sono intervenute, evidenziando la natura creditizia del servizio²⁵ e la nuova direttiva sul credito al consumo, n. 2023/2225, lo ha esplicitamente incluso nell’accesso al credito, assoggettandolo alle relative previsioni di valutazione del merito creditizio ed includendo anche i crediti esigui. Ciò significa, in primo luogo, un’attenta e approfondita valutazione del merito creditizio, nonché l’applicazione di adeguate misure di trasparenza, e, infine, se vi è ricorso al credit scoring, il rispetto delle misure previste dal regolamento europeo in materia di intelligenza artificiale, 1689/2024, per i sistemi ad alto rischio, fra i quali il BNPL è incluso. Su quest’ultimo punto è utile evidenziare come le misure per i sistemi così qualificati entrino in vigore nell’agosto del 2026, ma vi sia una proposta di regolamento, COM(2025) 836, c.d. Digital Omnibus, volta ad introdurre uno slittamento dell’entrata in vigore al momento in cui saranno disponibili gli standard armonizzati o linee guida sulla sicurezza. Non è però ancora chiaro se tale proposta potrà essere approvata in tempo utile rispetto alla scadenza già prevista.

Quello dei rischi generati dalle interconnessioni tra banche ed istituzioni non

²⁴ Secondo il Rapporto CRiF 2023, il ticket medio del BNPL era molto inferiore rispetto a quello del credito tradizionale ed il 50% delle richieste è inferiore ai 500 euro. Si veda il Rapporto CRIF dedicato al BNPL del settembre 2023.

²⁵ Nello specifico, nella sua Opinion sul BNPL l’EBA ha evidenziato come «the core service provided is of a lending nature and should be consider as granting credit» Si veda l’*Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366, on payment services in the internal market (PSD2)*, EBA/Op/2022/06 e la comunicazione della Banca d’Italia del 28 ottobre 2022, www.bancaditalia.it/compiti/tutelaeducazione/avvisi-comunicazioni/2022.10.28/index.html.

bancarie²⁶ è un tema molto ampio, non trattabile in questa sede, ma, se lo consideriamo dal punto di vista delle loro risorse, perlopiù costituite da depositi non assicurati e come tali soggetti ad alta volatilità, ci consente di soffermarci su come proprio la velocità di movimentazione dei depositi non assicurati, indotta dalla digitalizzazione, possa rappresentare una nuova modalità di manifestazione di rischio.

Per comprendere quest'aspetto, può essere utile prendere in esame le banche digitali per approfondire se il ricorso alla tecnologia abbia influenza solo sulla fisionomia dei servizi, resi accessibili 24 ore su 24, nonché più veloci e personalizzati.

In realtà, già l'esame dei servizi mostra anche una specializzazione nell'offerta, caratterizzata da una selezione dei servizi erogabili incentrata su quelli potenzialmente più redditizi come i sistemi di pagamento, la gestione patrimoniale e il trading.

Ciò che, però, può assumere più rilievo sotto il profilo del rischio è la possibile combinazione di un livello elevato di depositi non assicurati, altamente sensibili alle variazioni dei tassi d'interesse ed alle notizie di andamento di mercato, e la possibilità di divulgazione di tali informazioni attraverso strumenti di comunicazione che garantiscono ampia diffusione e istantaneità nel raggiungimento dei possibili interessati.

Quello appena descritto è proprio ciò di cui si è avuto un esempio nella crisi delle banche della Silicon Valley del 2023.

Nel caso di specie, le banche interessate erano caratterizzate da una concentrazione di depositi sia per tipo di cliente sia per settore, poiché si trattava prevalentemente di società orientate al settore tecnologico²⁷. Molti di essi non erano assicurati e proprio per questo, già prima della dichiarazione di insolvenza della Federal Deposit Insurance Corporation avvenuta il 10 marzo 2023, vi era stato uno spostamento notevole dei depositi verso "sedi" più redditizie²⁸, a seguito dell'aumento dei tassi deciso dalla Fed.

Un simile deflusso di risorse aveva comportato un intervento diretto a limitare il perdurare di simili movimenti, che aveva generato una crescita degli interessi passivi da 0,1 a 1,2 miliardi di dollari in un anno. A rendere il quadro più complesso si era aggiunta la perdita derivante dai titoli a lunga scadenza venduti anticipatamente per coprire i prelievi sui depositi²⁹.

²⁶ Per approfondire lo stato di avanzamento di queste interconnessioni, si veda in particolare ESRB, *EU Non-bank Financial Intermediation Risk Monitor*, n. 10, settembre 2025.

²⁷ Una riflessione sul ruolo dei depositi non assicurati nel caso SVB è presente nel documento della Federal Deposit Insurance Corporation (FDIC), *Options for Deposit Insurance Reform*, 1 maggio 2023.

²⁸ Come ricorda anche l'Evaluation Report del Board of Governors of the Federal Reserve System, la struttura di finanziamento risultava concentrata in società di private equity e venture capital e proprio per questo più soggetta a potenziale volatilità senza preavviso. Si veda il documento 2023 SR B 013, 25 settembre 2023, <https://oig.federalreserve.gov/reports/board-material-loss-review-silicon-valley-bank-sep2023.pdf>, p. 11.

²⁹ La banca aveva grandi esposizioni su portafogli a lunga scadenza. Sul punto si vedano i

In questo scenario, i social media attraverso la diffusione di un tweet immediatamente comprensibile in community di diretti interessati, sulla situazione delle banche in questione³⁰ aveva prodotto immediati effetti di ritiro amplificati dall'alto numero di individui coinvolti anche grazie a *retweet*³¹.

In un solo giorno, il 9 marzo 2023, era stata registrata una movimentazione addirittura di 42 bilioni di dollari, con un deflusso pari al 24%, ed un record negativo rispetto alle precedenti corse agli sportelli, come quella della Northern Rock durante la crisi finanziaria del 2007-2008³², favorito anche dal fatto che la maggior parte dei depositanti era di grandi dimensioni³³.

Un caso come quello appena descritto, oltre ad evidenziare nuove forme di manifestazione ed amplificazione del rischio indotte dallo sviluppo tecnologico, apre una riflessione sull'importanza della percentuale dei depositi non assicurati, particolarmente elevata nelle banche coinvolte³⁴ e la loro capacità di generare

documenti United States Senate Committee on Banking, Housing, and Urban Affairs, *Recent Bank Failures and the Federal Regulatory Response*, 28 marzo 2023 e United States, House of Representatives Financial Services Committee, *The Federal Regulators' Response to Recent Bank Failures*, 29 marzo 2023.

³⁰ Per avere un'idea dell'intensità è utile ricordare come su Twitter, in un lasso temporale ristretto, il numero dei tweet con la parola "run" abbinata a SVB sia stato di 6.528 e quello sul contagio SVB di 9.662. Ancor più significativo è l'inizio della "conversazione" sullo stato di difficoltà della banca con il ticker sulla SVB e i tweet di invito al ritiro. Per un'analisi dei dati sui tweet nel caso SVB si veda in particolare J.A. COOKSON, C. FOX, J. GIL-BAZO, J.F. IMBET, C. SCHILLER, *Social media as a Bank Run Catalyst*, Université Paris-Dauphine Research Paper, n. 4422754, 2023, www.wifpr.wharton.upenn.edu/wp-content/uploads/2023/09/Cookson-Fox-Gil-Bazo-Imbet-and-Schiller.pdf.

³¹ Sul ruolo dei social media sui depositi retail si veda in particolare M. ACCORNERO, M. MOSCATELLI, *Listening to the buzz: social media sentiment and retail depositors' trust*, Working paper n. 1165, febbraio 2018, Banca d'Italia, A. CANEPA, *L'efficacia della disciplina delle crisi bancarie e le proposte di riforma tra ripartizione di competenze, banche digitali e rischi di "fuga istantanea" dei depositi*, in *Quaderni di ricerca giuridica*, Banca d'Italia, n. 99, febbraio 2023, p. 349 ss.

³² Proprio in riferimento al caso della corsa agli sportelli della Northern Rock avvenuta nel 2009, B. Bortolotti e H.S. Shin ricordavano come "Anche se i depositi possono essere prelevati su richiesta, fra i banchieri si sente spesso dire che è più facile divorziare che cambiare banca". Si veda IID., *Da Mary Poppins a Northern Rock. Spunti sulle corse agli sportelli moderne*, in *Merc. conc. reg.*, 2009, p. 81. Per una comparazione sulle corse agli sportelli verificatesi in passato si veda in particolare J. ROSE, *Understanding the speed and size of bank runs in historical comparison*, 26 maggio 2023, Federal Reserve Bank of St. Louis, <https://www.stlouisfed.org/on-the-economy/2023/may/understanding-the-speed-and-size-of-bank-runs-in-historical-comparison>.

³³ Per un approfondimento sul punto si veda in particolare M. CIPRIANI, T.M. EISENBACH, A. KOVNER, *Tracing bank run in real time*, Federal Reserve Bank of New York, paper n. 1104, maggio 2024, rivisto nel dicembre 2024, https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr1104.pdf?sc_lang=en.

³⁴ Pari al 94% dei depositi nel 2022, come si evince dall'*Evaluation Report* del Board of Governors of the Federal Reserve System, che evidenziava anche come la struttura di finanziamento risultasse concentrata in società di private equity e venture capital e, proprio per questo, più soggetta a potenziale volatilità senza preavviso. Si veda il documento 2023 SR B 013, 25 settembre 2023, <https://oig.federalreserve.gov/reports/board-material-loss-review-silicon-valley-bank-sep2023.pdf>, p. 11.

crisi di solvibilità pressoché immediate e molto difficili da gestire in quanto favorite ed amplificate dalla comunicazione digitale.

Sulla questione dell'assicurazione dei depositi è utile ricordare come, nel giugno 2025, la proposta europea per la gestione delle crisi bancarie e l'assicurazione dei depositi (CMDI)³⁵ ha visto il raggiungimento di un accordo tra Parlamento e Consiglio, diretto a consentire il ricorso al sistema di garanzia dei depositi o ai fondi di risoluzione per finanziare la risoluzione, senza l'applicazione del bail-in ai depositanti.

4. Qualche considerazione conclusiva

Il quadro attuale mostra una crescente rilevanza del rischio geopolitico, segnalata anche dalla BCE e dal Comitato per il rischio sistemico, con il quale può intrecciarsi anche quello derivante da modelli di business ad alta intensità tecnologica. La necessità di attenzione su questi aspetti deriva dal fatto che, presi singolarmente, generano implicazioni sistemiche meno frequenti, ma possono essere un potente acceleratore in presenza di criticità già esistenti. Emblematico in tal senso appare il caso della Silicon Valley, dove la diffusione così rapida di informazioni via social ha dato luogo ad una corsa digitale agli sportelli così rapida da risultare molto complessa da gestire, ma nel quale le banche interessate avevano già mostrato problemi di liquidità.

L'importanza di una previsione di questi rischi, anche grazie ad analisi di scenari e reverse stress test, utili ad anticipare, mitigare e assorbire gli shock, appare fondamentale non solo per le implicazioni negative sull'intero sistema, ma anche perché possono diventare una condizione strutturale. Ciò richiede una maggiore vigilanza sulle banche in relazione agli assetti di governance, alla valutazione dell'adeguatezza patrimoniale e della liquidità, comprensiva di un'attenta valutazione delle esposizioni verso controparti coinvolte nel rischio geopolitico, e dell'opportunità di revisione delle strategie creditizie.

Questi aspetti, però, necessitano di essere affiancati da un elevato livello di resilienza operativa e di cybersecurity, che tenga conto non solo della definizione dei livelli di sicurezza, ma anche di un attento esame dei soggetti coinvolti nelle catene del valore. Da ciò deriva una riflessione più ampia sulle dipendenze da fornitori di Paesi terzi, sulla loro identificazione e sulle possibilità di scelta esistenti nonché sui livelli di sicurezza garantiti. Su questi aspetti, l'UE ha avviato una riflessione volta a rafforzare la propria sovranità digitale, al fine di consentire una diversificazione più rapida dei fornitori, come previsto dal regolamento DORA.

In un quadro di rafforzamento della sicurezza si inserisce però anche una rinnovata necessità per le banche e le autorità di vigilanza di effettuare valutazioni

³⁵ Si tratta della proposta COM/2023/228 di modifica della dir. 2014/49/UE sui sistemi di garanzia dei depositi.

sempre più complesse, rispetto alle quali anche la tecnologia stessa può offrire un supporto attraverso l'identificazione di scenari capaci di favorire una definizione anticipata delle possibili strategie per mitigarne gli effetti.

Un simile approccio appare rilevante anche in relazione agli effetti di accelerazione generati dalle nuove vulnerabilità informative, quali, ad esempio, quelle derivanti dai social media. Infatti, gli algoritmi possono svolgere una funzione di allerta precoce attraverso l'analisi dei post e dei messaggi pubblicati sui social per comprendere se vi siano segnali di difficoltà di una banca, ai quali potrebbe seguire una rapida movimentazione dei depositi. Peraltro, una simile analisi applicata alle dichiarazioni di leader di governo e di politici può risultare utile anche per anticipare possibili cambiamenti nelle relazioni multilaterali o segnali di un possibile avvio, nel breve periodo, di un conflitto, consentendo una migliore valutazione delle conseguenze e delle contromisure adottabili. Se, ad esempio, consideriamo la necessità di salvaguardare i flussi di commercializzazione e di acquisizione di materie prime, la capacità di individuare rapidamente nuovi canali o l'opportunità di adottare misure di supporto necessarie per alcuni settori dell'economia possono generare implicazioni positive anche per il sistema bancario.

Simili considerazioni sui vantaggi non possono però non essere accompagnate anche da un'adeguata segnalazione dei rischi connessi, in termini di possibili bias e di affidabilità e/o di correttezza delle analisi e delle previsioni effettuate.

