Impresa bancaria ed esternalizzazione di servizi tecnologici

Banks and outsourcing of technological services

Andrea Cardani*, Isacco Girardi**

ABSTRACT:

Il presente articolo esamina il rapporto tra banche e sviluppo tecnologico dall'angolo visuale dell'esternalizzazione di servizi tecnologici. Nel contesto della sua crescente diffusione, tale pratica aziendale incrementa i rischi intrapresi dagli enti creditizi e risulta dunque determinante indagare la fase genetica e dinamica del rapporto con il fornitore. Nella prima prospettiva, l'articolo identifica i criteri che orientano la decisione degli amministratori di affidarsi a terzi nello svolgimento dell'attività di impresa nonché la selezione della controparte contrattuale. Nella seconda prospettiva, si analizza l'impatto di tali criteri sotto il profilo del monitoraggio sul fornitore e dei rimedi attivabili dalla banca in situazioni patologiche. Alla luce dell'adozione del Regolamento DORA, assume infine particolare rilievo il regime di *enforcement* pubblico come strumento per governare le asimmetrie di potere esistenti tra banche e fornitori di servizi tecnologici, senza trascurare il ruolo complementare assolto dalla responsabilità civile.

This article examines the interplay between banks and technology development from the perspective of the outsourcing of technological services. In the context of its growing spread, this business practice increases the risks undertaken by credit institutions, and therefore it is crucial to investigate the relationship with the provider. From a first standpoint, the article identifies the criteria that guide the directors' decision to outsource and the selection of the contractual counterparty. From a second standpoint, the article analyz-

* Dottorando di ricerca in *Business and Law*, Università degli Studi di Bergamo; e-mail: andrea.cardani@unibg.it.

** Dottore di ricerca in Diritto commerciale, Università Cattolica del Sacro Cuore; e-mail: isacco.girardi@unicatt.it. L'articolo è frutto di una riflessione comune e condivisa degli Autori. A fini meramente istituzionali, i paragrafi 2, 3, 4, 5, 6, 7 e 8 sono da attribuirsi ad Andrea Cardani e i paragrafi 1, 9, 10, 11 e 12 a Isacco Girardi. Il lavoro espande il *paper* presentato al XV Convegno annuale dell'Associazione Italiana dei Professori Universitari di Diritto Commerciale "Orizzonti del Diritto Commerciale", "Impresa e mercati: numeri e *computer science*". Un sentito ringraziamento va ai Professori Giovanni Meruzzi e Massimo Bianca per il proficuo confronto e al *referee* per le puntuali indicazioni. Il lavoro ha inoltre giovato dei preziosi consigli della dott.ssa Giovanna Partipilo, a cui siamo profondamente grati.

es the impact of these criteria on the monitoring activity of the supplier and the remedies potentially exercised by the bank in case of violations. Finally, in light of the DORA Regulation adoption, the public enforcement regime governing the power asymmetries between banks and technological service providers is discussed, without neglecting the complementary role played by civil liability.

SOMMARIO:

1. *L'emersione del fenomeno.*

Il ricorso a tecnologie all'avanguardia è diventato un imperativo strategico per le società bancarie. Una pluralità di fattori favorisce il percorso di trasformazione digitale: l'impatto dell'emergenza pandemica sull'operatività delle banche, la netta preferenza dei clienti per soluzioni digitali nella gestione quotidiana dei servizi bancari, la possibilità per la banca di efficientare i propri processi interni e la pressione competitiva di nuovi *players* in grado di elaborare tecniche di automazione pionieristiche in ambito finanziario [1].

Le banche possono "stare al passo" con la rivoluzione tecnologica decidendo di sviluppare internamente e autonomamente le tecnologie che le stesse considerano opportune per automatizzare la loro attività. La strategia di realizzazione *in house* impone alle società bancarie di assumere personale con un elevato *expertise* in ambito tecnologico e avviare piani di formazione delle risorse già incardinate nell'organigramma. Un'ulteriore scelta strategica che rientra nel modello in discussione è la possibilità di effettuare direttamente l'acquisizione o fondersi con

[1] Per una completa ricognizione dei *driver* relativi al percorso di trasformazione digitale delle banche italiane e l'indicazione della loro rilevanza, cfr. CIPA, ABI, *Rilevazione sull'IT nel settore bancario italiano. La trasformazione digitale della banca* (Maggio 2022), reperibile al seguente indirizzo: https://www.cipa.it/rilevazioni/tecnologiche/2021/index.html, 25. In una prospettiva europea, ritiene che i principali fattori della trasformazione digitale delle banche siano le mutate preferenze dei consumatori, l'efficienza e la pressione competitiva realizzata dai nuovi protagonisti del settore bancario, E. MCCAUL, *Supervising the future of banking: navigating the digital transformation* (March 2023), reperibile al seguente indirizzo: https://www.bankingsupervision.europa.eu/press/blog/2023/html/ssm.blog230310~d91c37f468.en.html.

start-up che abbiano realizzato tecnologie avanzate per l'erogazione di servizi bancari o lo svolgimento di funzioni interne [2].

In alternativa, al fine di intercettare i benefici derivanti dalla digitalizzazione dell'attività bancaria, la banca può affidare a terzi servizi tecnologici (d'ora in poi, "servizi IT"): come indicato dalla letteratura economica e giuridica, tale scelta comporta il duplice vantaggio di ottenere risparmi di spesa in ragione delle economie di scala del fornitore e, nel contempo, un servizio di elevata qualità per la presenza di un soggetto dotato di risorse specializzate [3].

I vantaggi derivanti dal ricorso al mercato per la prestazione di servizi IT trovano conferma nell'elevata diffusione del fenomeno [4], mostrata dai dati raccolti in ambito bancario. A livello europeo, un recente *report* realizzato dalle autorità di vigilanza europee – sulla base di un campione di quindicimila fornitori e circa milleseicento istituzioni finanziarie – mostra come più dell'80% di questi enti deleghi a terzi lo svolgimento di servizi IT a supporto di funzioni essenziali o importanti [5]. Coerentemente, l'ultima rilevazione condotta dalla Banca centrale eu-

---

[2] Le operazioni di fusione e acquisizione di società *FinTech* sembrano essere in costante aumento: CAMERA DEI DEPUTATI, *Fintech* (settembre 2022), reperibile al seguente indirizzo: https://temi.camera.it/leg18/temi/fintech.html, 2. Sul punto, v. anche N. LINCIANO ET AL., *L'intelligenza artificiale nell'*asset *e nel* wealth management (Giugno 2022), reperibile al seguente indirizzo: https://www.consob.it/web/area-pubblica/ft9, 68, spec. nt. 172.

[3] Nella letteratura economica, in relazione all'ambito tecnologico, J. DIBBERN, R. HIRSCHHEIM, *Introduction: Riding the Waves of Outsourcing Change in the Era of Digital Transformation*, in *Information Systems Outsourcing*[5], edited by R. HIRSCHHEIM, A. HEINZL, J. DIBBERN, Cham, Springer, 2020, 2 e, in generale, J.A. MCCAHERY, F.A. DE ROODE, *Governance of Financial Services Outsourcing: Managing Misconduct and Third-Party Risks* (September 2018). ECGI – *Law Working Paper* No. 417/2018, reperibile al seguente indirizzo: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3241196, 2, nonché M. CAROLI, A. VALENTINO, *La strategia di* «outsourcing», in *AGE*, 2011, 266 ss. Nella letteratura giuridica, tra i molti, M. MAUGERI, *Esternalizzazione di funzioni aziendali e "integrità" organizzativa nelle imprese di investimento*, in *Banca borsa tit. cred.*, 2010, I, 439; A. SACCO GINEVRI, *Esternalizzazione (*outsourcing*)*, in *Fintech: diritti, concorrenza, regole*, diretto da G. FINOCCHIARO, V. FALCE, Bologna, Zanichelli, 2019, 205; V. LEMMA, J.A. THORPE, *Sharing Corporate Governance: the Role of Outsourcing Contracts in Banking* (2014), reperibile al seguente indirizzo: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2576920, 378 e, con specifico riferimento alla riduzione dei costi, A. SCIARRONE ALIBRANDI, *Introduzione*, in *L'Outsourcing nei servizi bancari e finanziari*, a cura di S. CASAMASSIMA, M. NICOTRA, Padova, Cedam, 2021, XV, nonché M. CERA, *Esternalizzazioni di gestione, mandato generale e rappresentanza legale nelle società per azioni*, in *Riv. dir. priv.*, 2013, 327 s. Pur con un'osservazione limitata al *cloud computing*, a livello istituzionale, cfr. EUROPEAN BANKING AUTHORITY (d'ora in poi, "EBA"), *Report on the prudential risks and opportunities arising for institutions from fintech* (3 luglio 2018), reperibile al seguente indirizzo: https://www.eba.europa.eu/publications-and-media/press-releases/eba-assesses-risks-and-opportunities-fintech-and-its-impact, 53.

[4] In questo senso, COMMISSIONE EUROPEA, *Impact Assessment Report Accompanying the document for DORA Regulation* [SWD(2020) 198 final] (24 September 2020), reperibile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020SC0198, 17.

[5] EUROPEAN SUPERVISORY AUTHORITIES (d'ora in poi, "ESAs"), *Report on the landscape of ICT*

ropea (d'ora in poi, "BCE") ha verificato che il 48,5% delle spese sostenute dalle banche *significant* in ambito tecnologico è da ricondurre alla pratica di affidare a terzi tali funzioni [6]. Le risposte al questionario impiegato per la redazione del documento «Rilevazione sull'IT nel settore bancario italiano», promosso dalla Convenzione Interbancaria per l'Automazione e dall'Associazione Bancaria Italiana [7], mostrano come la pratica aziendale risulti essere diffusa anche tra i principali gruppi bancari attivi in Italia. Pur ritenendo molto rilevante l'impiego di «competenze interne» per lo svolgimento di iniziative tecnologiche significative, particolare importanza assume il «reperimento delle competenze» presso «società di consulenza», «*global vendor*» e «[*o*]*utsourcer*» [8]. Con particolare riferimento al *cloud computing* [9], secondo una tendenza confermata a livello europeo [10], lo studio afferma che il 58% delle banche rispondenti gode di servizi prestati da fornitori esterni e il 29% delle stesse ha iniziato un percorso di transizione tecnologica per fruire di servizi *cloud* [11]. Da una rilevazione successiva, si evince che nel 2022 la maggior parte delle banche nel campione ha fruito di servizi *cloud* o intende avviare un percorso per affidarne la realizzazione a imprese terze [12].

Pur essendo innegabili i vantaggi derivanti dal ricorso al mercato, l'affidamento a terzi di attività tecnologiche per la realizzazione di una frazione dell'impresa comporta un incremento dei rischi intrapresi dalla banca [13]. La di-

---

third-party providers in the EU (27 September 2023), reperibile al seguente indirizzo: https://www.esma.europa.eu/press-news/esma-news/esas-publish-report-landscape-ict-third-party-providers-eu, 6.

[6] BCE, *IT and cyber risk – key observations*, https://www.bankingsupervision.europa.eu/banking/srep/2023/html/ssm.srep2023_ITandcyberrisk.en.pdf, 3.

[7] Il riferimento è a CIPA, ABI, (nt. 1), 37 ss.

[8] CIPA, ABI, (nt. 1), 35 s.

[9] Per un approfondimento sul punto, FINANCIAL STABILITY BOARD, *Third-party dependencies in cloud services. Considerations on financial stability implications* (9 December 2019), reperibile al seguente indirizzo: https://www.fsb.org/2019/12/third-party-dependencies-in-cloud-services-considerations-on-financial-stability-implications/, 5 ss. Per quanto si tratti della tecnologia più esternalizzata, ulteriori servizi affidati a terzi possono riguardare la «*robo-advisory*» e l'«uso dei dati biometrici»: G. ALPA, Fintech: *un laboratorio per giuristi*, in *Contr. impr.*, 2009, 381. Più ampiamente, il novero dei servizi tecnologici esternalizzati è indicato in EBA, (nt. 3), 12 ss.

[10] BCE, *ECB Guide on outsourcing cloud services to cloud service providers*, reperibile al seguente indirizzo: https://www.bankingsupervision.europa.eu/legalframework/publiccons/pdf/ssm.pubcon240603_draftguide.en.pdf.

[11] CIPA, ABI, (nt. 1), 11.

[12] CIPA, ABI, *Rilevazione sull'IT nel settore bancario italiano. Il cloud computing e le banche* (Maggio 2023), reperibile al seguente indirizzo: https://www.cipa.it/rilevazioni/tecnologiche/2022/index.html, 29.

[13] L'ultimo *Supervisory Review and Evaluation Process* (d'ora in poi, "SREP") condotto dalla BCE ha identificato tra le maggiori vulnerabilità in ambito operativo i rischi derivanti dal-

pendenza da fornitori terzi di servizi IT costituisce una componente del rischio operativo [14], può impattare su altri rischi tradizionali (il rischio di reputazione o di *compliance*) e porre rischi nuovi, come quello di concentrazione [15]. Il rischio di concentrazione può rilevare sia in una prospettiva micro-prudenziale che macro-prudenziale [16]. Nella prima prospettiva, la stipulazione di molteplici accordi con lo stesso fornitore di servizi IT o con un fornitore non sostituibile può pregiudicare – in caso di malfunzionamento o interruzioni del servizio – l'operatività della banca e comprometterne la stabilità economica. Nella seconda prospettiva, quando il mercato dei servizi IT è concentrato nelle mani di pochi [17], i fornitori assumono

---

l'esternalizzazione di servizi tecnologici (in particolare, BCE, *Aggregated results of SREP 2023* (2023), reperibile al seguente indirizzo: https://www.bankingsupervision.europa.eu/banking/srep/2023/html/ssm.srep202312_aggregatedresults2023.en.html, par. 5.5.2). In termini generali, per l'affermazione che le "attività esternalizzate sono considerate più rischiose, siano esse conferite a soggetti all'interno del gruppo di appartenenza dell'ente creditizio oppure a fornitori terzi»: BCE, *Guida alla valutazione delle domande di autorizzazione all'esercizio dell'attività bancaria* (gennaio 2019), reperibile al seguente indirizzo: https://www.bankingsupervision.europa.eu/legalframework/supervisorypolicy/html/supervisoryguides.en.html, par. 5.2. In tema, F. URBANI, *I rapporti di terza parte nel governo delle banche: rischi, regolazione e "frammentazione" dell'assetto* (2022), reperibile al seguente indirizzo: https://www.orizzontideldirittocommerciale.it/giuscommercialisti-in-erba-18-novembre-2022/, 37. Per una generale enunciazione delle diverse categorie di rischio associate all'*outsourcing*, BASEL COMMITTEE ON BANKING SUPERVISION (d'ora in poi, "BCBS"), *Outsourcing in Financial Services* (febbraio 2005), reperibile al seguente indirizzo: https://www.bis.org/publ/joint12.htm, 11 s.

[14] L'art. 85, primo par., Direttiva 36/2013/UE (d'ora in poi, "CRD IV") ricomprende i «rischi derivanti dall'esternalizzazione» nel rischio operativo. Si fa poi espresso riferimento al c.d. rischio *outsourcing* IT, che viene definito come «[t]he risk that engaging a third party, or another Group entity (intra-group outsourcing), to provide ICT systems or related services adversely impacts the institution's performance and risk management»: EBA, *Final Report. Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process* (*SREP*) (11 May 2017), reperibile al seguente indirizzo: https://www.eba.europa.eu/publications-and-media/press-releases/eba-publishes-final-guidelines-assess-ict-risk, 11.

[15] Sulla possibilità che i rapporti di terza parte possano comportare un «aggravamento dei rischi "tipici" del settore creditizio» e possano porre rischi «di nuova formazione» (come, per esempio, quello *cyber* o di concentrazione macro-prudenziale), F. URBANI, (nt. 13), 35 ss.

[16] Sulle due prospettive del rischio di concentrazione, cfr. EBA, *Orientamenti in materia di esternalizzazione* (25 febbraio 2019), reperibile al seguente indirizzo: https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-outsourcing, par. 66, lett. a) e art. 29, primo par., Regolamento (UE) 2022/2554 (d'ora in poi, "Regolamento DORA"). Ponendo l'accento sulla natura macro-prudenziale del rischio di concentrazione, L. SPITALERI, *L'*outsourcing *nei servizi bancari e finanziari, profili di* governance *e prospettive di vigilanza*, in *Riv. trim. dir. econ.*, 2023, 136.

[17] Specie nell'ambito dei servizi *cloud*, la concentrazione dei fornitori è un dato ormai ampiamente riconosciuto: «the widespread use of a limited number of closely connected ICT TPPs by a large number of financial institutions can lead to macro-prudential risks, such as concentration and systemic risks. This can adversely impact financial stability in the event that one or more of the critical providers experience a major disruption in providing their services»: COMMISSIONE EUROPEA,

una sostanziale rilevanza sistemica, in quanto il "fallimento" di uno si espande ad una pluralità di enti vigilati, finendo per mettere in pericolo la stabilità dell'intero sistema finanziario. È in questa prospettiva che matura l'esigenza di non rimettere la disciplina della materia ai soli meccanismi di mercato. Tale preoccupazione ha trovato condivisione nei primi interventi in materia [18] e, successivamente, ha posto le basi per una regolamentazione organica in ambito bancario delle pratiche di esternalizzazione di funzioni [19] con gli Orientamenti adottati dalla *European ban-*

(nt. 4), 18; ma v. anche BCE, (nt. 10), 1. In dottrina, G. SCHNEIDER, *La resilienza operativa digitale come materia di* corporate governance*: prime riflessioni a partire dal DORA*, in *Riv. cor. gov.*, 2022, 556. Seppure con considerazioni prospettiche, in termini generali, A. GUACCERO, *Automazione dei processi e dei servizi, imputazione e responsabilità*, in *Diritto del Fintech*[1], a cura di M. CIAN, C. SANDEI, Padova, Cedam, 2020, 63, secondo cui lo «sviluppo di un mercato di sistemi evoluti porterà tipicamente, tenuto conto degli importanti investimenti tecnologici richiesti, alla concentrazione dell'offerta, con l'effetto di produrre una potenziale duplice restrizione competitiva. Alla concentrazione di un numero di fornitori di sistemi di elaborazione fondati sull'intelligenza artificiale corrisponderà infatti la diffusione più ampia di un numero limitato di sistemi».

[18] Cfr. COMMITTEE OF EUROPEAN BANKING SUPERVISORS, *Guidelines on Outsourcing* (14 December 2006), reperibile al seguente indirizzo: https://www.eba.europa.eu/guidelines-2006 [per un'analisi sistematica di tale documento, V. LEMMA, J.A. THORPE, (nt. 3), 378 ss.]; successivamente, EBA, *Raccomandazioni in materia di esternalizzazione a fornitori di servizi* cloud, reperibile al seguente indirizzo: https://www.eba.europa.eu/documents/10180/2170125/ca84f597-f930-4918-8ae8-a4c2bd441e8d/Recommendations%20on%20Cloud%20Outsourcing%20(EBA-Rec-2017-03)_IT.pdf. Per l'affermazione che tali documenti costituiscono il fondamento degli attuali Orientamenti EBA, F. CAPRIGLIONE, A. SACCO GINEVRI, *Metamorfosi della* governance *bancaria*, Torino, Utet Giuridica, 2019, 223 s.

[19] Le disposizioni di vigilanza sulle banche attribuiscono efficacia vincolante alle regole contenute in EBA, (nt. 16) e, dunque, si deve guardare a tale fonte per comprendere quando la prestazione di servizi tecnologici rientri nella nozione normativa di esternalizzazione di funzioni (Circolare 285/2013, Parte I, Titolo IV, Cap. 3, Sez. IV, par. 1). Per prima cosa, la nozione di «funzione» è particolarmente ampia e ricomprende l'attribuzione a terzi dello svolgimento di un servizio o una sua parte [EBA, (nt. 16), par. 2; nella giurisprudenza italiana, si afferma che il fenomeno dell'*outsourcing* «comprende tutte le possibili tecniche mediante le quali un'impresa dismette la gestione diretta di alcuni segmenti dell'attività produttiva e dei servizi estranei alle competenze di base (c.d. *core business*)»: Cass. civ., sez. IV, 2 ottobre 2006, n. 21287, in *Foro it.*, 2007, 114; esclude, nondimeno, che una «delimitata attività di supporto consultivo e assistenziale» alla funzione di *compliance* possa qualificarsi come «esternalizzazione»: App. Catania, 22 gennaio 2019, n. 133, in *Riv. trim. dir. econ.*, 2020, II, 7, con nota di G. CAVALLARO]. Gli altri due elementi per qualificare un accordo come esternalizzazione di funzioni sono la ricorrenza del servizio prestato dal fornitore e l'astratta capacità della banca di svolgere da sé la funzione, anche se questa non è mai stata sviluppata *in house* [EBA, (nt. 16), par. 26]. Proprio in ragione di tale ultima caratteristica, gli Orientamenti EBA forniscono un elenco di attività che non possono essere qualificate come esternalizzazione di funzioni poiché sono necessariamente svolte da soggetti diversi dalla banca [per un'elencazione dei diversi servizi, EBA, (nt. 16), par. 28]. Si pensi, per esempio, alla revisione legale dei conti: tale servizio deve essere svolto da un soggetto terzo a norma di legge e, per conseguenza, non può mai essere realizzato da funzioni interne alla banca. Per un'ampia trattazione sul punto, pur precedente agli Orientamenti EBA e focalizzata sull'esternalizzazione da parte degli intermediari finanziari, M. MAUGERI, (nt. 3), 440 ss.

king authority (d'ora in poi, nel testo, "Orientamenti EBA") il 25 febbraio 2019. Da ultimo, il legislatore europeo ha deciso di introdurre un quadro normativo specificamente dedicato all'affidamento di servizi IT con il Regolamento DORA [20].

In tale contesto economico e normativo polarizzato tra istanze di efficienza e riduzione del rischio, l'articolo intende individuare i criteri che orientano le società bancarie nella selezione del fornitore e nella gestione del relativo rapporto contrattuale, nonché, di riflesso, il ruolo delle autorità di vigilanza nell'assicurare la protezione degli interessi pubblici coinvolti. Prima di avviare l'indagine, è necessario fare solo una notazione metodologica: nell'affrontare la domanda di ricerca, si farà riferimento alle regole contenute negli Orientamenti EBA e alle disposizioni introdotte nell'ordinamento europeo dal Regolamento DORA. Benché il Regolamento si applicherà a partire dal 17 gennaio 2025 [21] e dovranno essere emanati diversi atti di esecuzione [22], la sua entrata in vigore e l'imminente appli-

[20] Il Regolamento DORA ha introdotto l'ampia nozione di servizi relativi alle tecnologie dell'informazione e della comunicazione, che sono definiti come i «servizi digitali e di dati forniti attraverso sistemi di TIC a uno o più utenti interni o esterni su base continuativa» (art. 3, n. 21, Regolamento DORA). Confrontando tale nozione normativa con quella di esternalizzazione di funzioni delineata da EBA, (nt. 16), par. 26 si può notare come il legislatore europeo abbia inteso estendere il novero dei rapporti contrattuali di terza parte soggetti a regolamentazione. Per l'applicazione delle disposizioni contenute nel Regolamento DORA è infatti sufficiente la fornitura di un servizio tecnologico in via ricorrente, rimanendo esclusa qualsiasi valutazione relativa alla capacità della banca di realizzare *in house* l'attività. Atteso che il Regolamento DORA ha superato la fattispecie normativa dell'«esternalizzazione» di funzioni prevista da EBA, (nt. 16), par. 26 tramite il concetto di fornitura di servizi IT, qualsiasi riferimento nel testo all'esternalizzazione assume significato equivalente alla più recente nozione dettata dal legislatore europeo.

[21] Art. 64 Regolamento DORA.

[22] Dopo l'adozione del Regolamento DORA è stata avviata una intensa attività di produzione regolamentare di dettaglio con riferimento al tema oggetto di ricerca; tra gli interventi più rilevanti e recenti si devono menzionare: (1) JOINT COMMITTEE OF THE ESAS, *Final report on Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554* (26 July 2024), reperibile al seguente indirizzo: https://www.dirittobancario.it/art/dora-le-rts-esas-sul-subappalto-dei-servizi-ict/; (2) JOINT COMMITTEE OF THE ESAS, *Final Report on Joint Guidelines on the oversight cooperation and information exchange between the ESAs and the competent authorities under Regulation (EU) 2022/2554* (26 July 2024), reperibile al seguente indirizzo: https://www.dirittobancario.it/art/dora-standard-tecnici-esas-su-segnalazione-di-incidenti-informatici-e-sorveglianza/; (3) JOINT COMMITTEE OF THE ESAS, *Final Report Draft Regulatory Technical Standards on harmonisation of conditions enabling the conduct of the oversight activities* (17 July 2024), reperibile al seguente indirizzo: https://www.dirittobancario.it/art/dora-standard-tecnici-esas-su-segnalazione-di-incidenti-informatici-e-sorveglianza/; (4) Regolamento Delegato (UE) 2024/1773, che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che precisano il contenuto dettagliato della politica relativa agli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC; (5) Regolamento Delegato (UE) 2024/1502, che integra il regolamento (UE)

cazione hanno suggerito di considerare la novella europea alla stregua del diritto attualmente vivente.

2. *La decisione di esternalizzare servizi tecnologici.*

La banca dispone di diverse modalità per integrare servizi IT nella propria attività, che spaziano dalla realizzazione *in house* a pratiche di esternalizzazione. La conformazione tecnologica delle attività e dei processi bancari transita da questa importante decisione strategica, della quale diviene indispensabile – in punto di poteri e responsabilità – stabilire i criteri che ne guidano l'assunzione.

3. *La competenza dell'organo amministrativo.*

Risulta in primo luogo necessario stabilire quale organo sociale sia deputato ad assumere la scelta di esternalizzare un servizio IT. Al riguardo, significative indicazioni sono fornite dalla Circolare n. 285/2013 adottata da Banca d'Italia. Infatti, nell'ambito delle strategie aziendali, l'organo con funzione di supervisione strategica è incaricato di definire l'«eventuale adozione di modelli imprenditoriali, applicazioni, processi o prodotti nuovi, anche con modalità di *partnership* o esternalizzazione, connessi all'offerta di servizi finanziari ad alta intensità tecnologica (*Fintech*)» (Parte Prima, Titolo IV, Cap. 1, Sez. III, par. 2.2, lett. *f*, punto ii). Nella medesima prospettiva, l'organo con funzione di supervisione strategica «definisce e approva la strategia ICT», che a sua volta comprende le «dipendenze chiave da soggetti terzi» (Parte Prima, Titolo IV, Cap. 4, Sez. II, par. 2.1, lett. *a*). La Circolare 285/2013 aggiunge inoltre che l'organo con funzione di supervisione strategica non dovrebbe essere «investito di questioni che – *per il loro contenuto o rilevanza non strategica* – possono più efficacemente essere affrontate dall'organo con funzione di gestione o dalle strutture aziendali» (Parte Prima, Titolo IV, Cap. 1, Sez. III, par. 2.2, lett. *e*).

A ben vedere, la medesima distinzione per impatto strategico si riscontra anche nell'ambito dell'esternalizzazione di servizi IT. Infatti, la legge riconosce l'essenzialità o l'importanza della funzione quando è destinata ad incidere sui «risultati finanziari» della banca, sulla «solidità o continuità» dei servizi finanziari e sul «costante adempimento» degli «obblighi previsti dalla normativa applicabile in materia di servizi finanziari» (art. 3, punto 22, Regolamento DORA). Si pensi, per esempio, a tecniche di automazione impiegate per l'esecuzione delle segnalazioni di vigilanza [23] o per la determinazione dei requisiti di capitale.

2022/2554 del Parlamento europeo e del Consiglio specificando i criteri per la designazione dei fornitori terzi di servizi TIC come critici per le entità finanziarie.

[23] Così BANCA D'ITALIA, *Nota di chiarimenti sul sistema dei controlli interni, il sistema informa-*

In questo quadro normativo, l'assetto di competenze viene dunque a differenziarsi a seconda della tipologia di funzione esternalizzata e risente del sistema di amministrazione e controllo adottato dalla società bancaria.

Nel sistema tradizionale e monistico, quando l'*outsourcing* riguarda una funzione essenziale o importante, gli indici normativi sono sufficientemente univoci nell'indicare il consiglio di amministrazione quale soggetto titolare della scelta [24]; diversamente, nelle altre ipotesi, la scelta e la gestione relativa all'accordo di esternalizzazione deve essere rimessa agli amministratori con deleghe [25] (quando presenti [26]).

Nel sistema dualistico [27], il consiglio di sorveglianza concorre con il consiglio di gestione alla supervisione strategica dell'ente quando lo statuto gli attribuisca il compito di deliberare «in ordine alle operazioni strategiche e ai piani, industriali e finanziari della società» (art. 2409-*terdecies*, primo comma, lett. *f-bis*, c.c.). Nei termini propri della regolamentazione bancaria, la «funzione di supervisione stra-

---

tivo e la continuità operativa, reperibile al seguente indirizzo: https://www.bancaditalia.it/compiti/vigilanza/normativa/archivionorme/circolari/c285/Circ-285-nota-chiarimenti-controlli-interni.pdf, 13, riportata anche in G. FALCONE, *Profili problematici dell'esternalizzazione di funzioni ed attività "tipiche" da parte degli intermediari del mercato finanziario*, in *Mercati regolati e nuove filiere di valore*, a cura di R. LENER, G. LUCHENA, C. ROBUSTELLA, Torino, Giappichelli, 2021, 285, nt. 24.

[24] Seppure in termini generali, M. CERA, (nt. 3), 334.

[25] La chiarezza della Circolare n. 285/2013 aiuta dunque a interpretare il testo ambiguo degli orientamenti EBA e della fonte secondaria del Regolamento DORA, che sembra condizionare ad eventualità il coinvolgimento del consiglio di amministrazione con riferimento alle funzioni essenziali o importanti [«se del caso»: EBA, (nt. 16), par. 42, lett. *a*); art. 4, lett. *a*), Regolamento Delegato (UE) 2024/1773]. In tema v. anche EBA, (nt. 16), par. 55, lett. *d*), là dove si richiede che il registro delle informazioni relative agli accordi aventi per oggetto l'esternalizzazione di funzioni essenziali o importanti devono contenere l'indicazione dell'«individuo o l'organo decisionale (ad esempio, l'organo di amministrazione) dell'ente o dell'istituto di pagamento che ha approvato l'accordo di esternalizzazione». In dottrina, M. MAUGERI, (nt. 3), 459 s., secondo cui ove la delega di funzioni è generale, la competenza a esternalizzare spetta all'organo delegato, mentre ove la delega di funzioni è parziale, la decisione di esternalizzare funzioni essenziali o importanti è da imputare al consiglio di amministrazione. Nonostante tali aspetti, conclude per la «permanenza di tutti i poteri decisori in capo all'organo gestorio nella sua interezza, alla luce di un difficile (se non impossibile) scissione fra componente gestoria (in senso stretto) e organizzativa del rapporto di esternalizzazione, potendosi al più attribuire agli organi delegati (o all'alta dirigenza dell'ente) funzioni esecutive e attuative nell'ambito dello stesso»: F. URBANI, (nt. 13), 230.

[26] Con riferimento alle «banche di minor complessità», per esempio, andrebbe evitata la nomina di un amministratore delegato e di un direttore generale: Circolare 285/2013, Parte Prima, Titolo IV, Cap. 1, Sez. III, par. 2.2, lett. *i*). Nel caso di assenza di delega, conclude per la competenza del consiglio di amministrazione a deliberare la scelta di esternalizzare un servizio o una funzione, M. MAUGERI, (nt. 3), 460.

[27] Per una generale disamina delle regole speciali in materia bancaria, V. CARIELLO, *Il sistema dualistico*, Torino, Giappichelli, 2012, 63 ss. e per alcune questioni problematiche, G.B. PORTALE, *La* corporate governance *delle società bancarie*, in *Riv. soc.*, 2016, 56 s., nonché ID., *Amministrazione e controllo nel sistema dualistico delle società bancarie*, in *Riv. dir. civ.*, 2013, I, 32 ss.

tegica (…) viene (…) incentrata sul consiglio di sorveglianza» (Circolare 285/2013, Parte Prima, Titolo IV, Capitolo 1, Sezione I, par. 1). Considerato che la decisione di esternalizzare funzioni essenziali o importanti può essere qualificata anche direttamente dallo statuto come operazione strategica per il suo potenziale e non trascurabile impatto sui risultati della banca [28], la relativa competenza spetta al consiglio di gestione e al consiglio di sorveglianza secondo la seguente distribuzione di compiti: il primo organo deve proporre [29] ed eseguire l'operazione [30], ferma la responsabilità per gli «atti compiuti» in relazione alle «operazioni strategiche e ai piani industriali e finanziari della società» (art. 2409-*terdecies*, primo comma, lett. *f-bis*, c.c.); il secondo deve autorizzare, approvare l'operazione o scegliere tra le diverse opzioni proposte [31]. Al fine di indirizzare il consiglio di gestione nella predisposizione della proposta, il consiglio di sorveglianza può formulare proprie posizioni e, *a fortiori*, proporre eventuali modifiche a quelle già configurate, soltanto nel caso di esternalizzazioni qualificate come «operazioni strategiche fondamentali» (Circolare 285/2013, Parte Prima, Titolo IV, Capitolo 1, Sezione III, par. 2.2., lett. *j*) [32]. Nelle ipotesi diverse dall'*out-*

---

[28] Sul punto, F. BORDIGA, *La funzione del consiglio di sorveglianza. Tra controllo e indirizzo dell'impresa*, Milano, Giuffrè, 2016, 202, secondo cui il coinvolgimento "strategico" deve avvenire per decisioni che «incidano significativamente sulle prospettive reddituali, finanziarie e patrimoniali della società».

[29] Lo statuto della banca, infatti, deve «qualificare natura e contenuti del potere decisionale riconosciuto al consiglio medesimo rispetto alle competenze del consiglio di gestione, fermo restando il potere di proposta di quest'ultimo» (Circolare 285/2013, Parte Prima, Titolo IV, Capitolo 1, Sezione III, par. 2.2., lett. *j*).

[30] Sul punto, P. MONTALENTI, *Il sistema dualistico: il consiglio di sorveglianza tra funzioni di controllo e funzioni di alta amministrazione*, in *AGE*, 2007, 276, là ove afferma che il «consiglio di gestione è pur sempre giudice sulla scelta finale dell'attuazione o non della decisione»; in senso analogo, V. CARIELLO, (nt. 27), 101. In effetti, per le disposizioni di vigilanza, l'«attribuzione di compiti di supervisione strategica al consiglio di sorveglianza non deve condurre a ingerenze di quest'ultimo nella gestione» (Circolare 285/2013, Parte Prima, Titolo IV, Capitolo 1, Sezione III, par. 2.2., lett. *j*).

[31] Benché con riferimento alle disposizioni di vigilanza, ma con argomentazioni valide anche per l'ordinamento vigente, G. A. RESCIO, *L'adeguamento degli statuti delle banche alle disposizioni di vigilanza 4 marzo 2008 in materia di organizzazione e governo societario (con particolare riferimento alle banche a sistema dualistico)*, in *Banca borsa tit. cred.*, 2008, I, 739 ss. Secondo l'A. il consiglio di sorveglianza può esercitare il potere di proposta solo quando «quest'ultimo non venisse esercitato per motivazioni diverse dal dissenso interorganico sulla opportunità e/o sulle modalità dell'operazione e vi fosse assoluta urgenza di procedere» (spec. 741). Sulla differenza tra potere di autorizzazione, approvazione e decisione, P. MONTALENTI, (nt. 30), 275 ss. e F. BORDIGA, (nt. 28), 204 s., che, nondimeno, esclude – in conformità alla dottrina prevalente – la possibilità di coinvolgere il consiglio di sorveglianza secondo le ultime due modalità sopra indicate. *Contra*, seppure in senso dubitativo e solo con riferimento al potere decisorio, P. ABBADESSA, *Il sistema dualistico in Italia: l'evoluzione del modello*, in *Sistema dualistico e* governance *bancaria*, a cura di P. ABBADESSA, F. CESARINI, Torino, Giappichelli, 2009, 11 s.

[32] Le esemplificazioni compiute dalle disposizioni di vigilanza (= «fusioni» e «acquisizioni di

sourcing di servizi essenziali o importanti, invece, la competenza relativa alla decisione di esternalizzare deve ritenersi rimessa ai soggetti delegati dal consiglio di gestione ai sensi dell'art. 2409-*novies*, primo comma, c.c., quando presenti.

Nei casi in cui il consiglio di sorveglianza non abbia funzione di supervisione strategica, la competenza sull'esternalizzazione di funzioni essenziali o importanti spetta al consiglio di gestione, mentre, per gli altri accordi, la competenza ricade – se presenti – sui consiglieri delegati. Il consiglio di sorveglianza potrebbe, in ogni caso, rivolgere atti di indirizzo "debole" e non vincolanti nei confronti del consiglio di gestione, a fronte della sua originaria impronta gestoria [33].

4. *Il ruolo delle funzioni aziendali.*

Nell'esercizio della loro competenza decisionale, l'organo di supervisione strategica e quello di gestione sono coadiuvati dalle funzioni aziendali interne. La politica di esternalizzazione deve, infatti, prevedere il «coinvolgimento delle funzioni di controllo interno e di altri soggetti con riferimento agli accordi di esternalizzazione» (Orientamenti EBA, par. 42, lett. *b*). La normativa non precisa, tuttavia, il momento dal quale l'attivazione delle funzioni aziendali interne costituisce un atto dovuto. Diversi argomenti depongono nel senso che tale compartecipazione è richiesta sin dalla fase di selezione del fornitore.

Dal punto di vista letterale, occorre soffermarsi sul significato da attribuire al termine «coinvolgimento». Quando tale vocabolo è utilizzato nei confronti dell'attività in capo all'organo di amministrazione, la disciplina chiarisce espressamente che, tra gli ambiti nel quale deve esplicarsi il contributo gestorio, è ri-

---

particolare rilievo») mostrano che le «operazioni strategiche fondamentali» consistono in atti potenzialmente idonei ad alterare in maniera significativa le condizioni di rischio dell'attività bancaria [sulla scarsa comprensibilità della fattispecie e sul fatto che il consiglio di sorveglianza può incidere sulla proposta formulata dal consiglio di gestione solo in tale ipotesi, G.A. RESCIO, (nt. 31), 741]. Si può ritenere che l'esternalizzazione ricada nella fattispecie in esame quando abbia ad oggetto servizi la cui scarsa qualità o incostanza può impedire lo svolgimento o pregiudicare significativamente il *core business* della banca (ciò accadrà, per esempio, nelle ipotesi di malfunzionamenti in caso di *full outsourcing*: sulla fattispecie, Circolare 285/2013, Parte Prima, Titolo IV, Capitolo 4, Sezione VI, par. 1).

[33] Anche in assenza di una specifica previsione statutaria *ex* art. 2409-*terdecies*, primo comma, lett. *f-bis*) ritengono che il consiglio di sorveglianza possa comunque svolgere attività di indirizzo programmatico e di orientamento della gestione, A. MIRONE, *Regole di governo societario e assetti statutari delle banche tra diritto speciale e generale*, in *Banca impr. soc.*, 2017, I, 77; M. LIBERTINI, *La funzione di controllo nell'organizzazione della società per azioni, con particolare riguardo ai c.d. sistemi alternativi*, in *Società, banche e crisi d'impresa.* Liber amicorum *Pietro Abbadessa*, diretto da M. CAMPOBASSO ET AL., Torino, Utet Giuridica, 2014, 1088 s., che distingue tra «"potere di indirizzo debole"» e «potere di "direttiva"); P. FERRO-LUZZI, *L'esercizio di impresa tra amministrazione e controllo*, in *AGE*, 2007, 249.

compreso il «processo decisionale» (Orientamenti EBA, par. 42, lett. *a*). Pertanto, al termine «coinvolgimento» dovrebbe essere attribuito il medesimo significato quando ricorre nei confronti delle funzioni aziendali: la partecipazione delle funzioni interne è, dunque, richiesta sin dalla fase decisionale. Tale osservazione trova conferma nel fatto che la funzione di *risk management* deve fornire supporto alle decisioni che implicano l'assunzione di rischi [34] e l'affidamento a terzi di attività tecnologiche rientra in tale categoria, incrementando i rischi (in particolare, quello operativo) intrapresi dall'ente (*supra*, n. 1). L'ordinamento italiano, infine, prevede una forma di coinvolgimento *ex ante* della funzione di *compliance* nei «progetti innovativi (…) che la banca intenda» avviare (Circolare n. 285/2013, Parte I, Titolo IV, Capitolo 3, Sezione III, par. 3.2), tra i quali potrebbe rientrare l'attribuzione di servizi tecnologici a soggetti altamente specializzati.

Occorre ora identificare le forme in cui si deve concretizzare il coinvolgimento delle funzioni aziendali nella scelta di esternalizzare servizi tecnologici. In primo luogo, i responsabili del *risk management* e della *compliance* sono tenuti ad attivare flussi informativi verso l'organo di gestione [35]. In qualità di interlocutori privilegiati dei componenti dell'organo di amministrazione [36], nelle materie di loro competenza, i capi delle funzioni di controllo interessate dovranno fornire ad essi tutti i dati necessari per comprendere i rischi associati all'esternalizzazione e ponderare al meglio la decisione di esternalizzazione. Sempre i soggetti al vertice di tali funzioni potranno confrontarsi direttamente con l'organo amministrativo o gli organi delegati, formulando suggerimenti [37] o mettendo in discussione la decisio-

---

[34] In tema, EBA, *Orientamenti sulla* governance *interna* (2 luglio 2021), reperibile al seguente indirizzo: https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-internal-governance, parr. 152, 187, 188 e 195.

[35] Sui flussi informativi tra le funzioni di controllo interno, i loro responsabili e gli amministratori rilevano una pluralità di disposizioni regolamentari: EBA, (nt. 34), parr. 173, 200, secondo cui il «responsabile della funzione di gestione dei rischi dovrebbe avere il compito di fornire informazioni esaurienti e comprensibili sui rischi» e 210, là dove prevede che la «funzione di conformità dovrebbe informare l'organo di gestione e comunicare, eventualmente, con la funzione di gestione dei rischi, in merito al rischio di conformità dell'ente e alla sua gestione».

[36] Cfr. EBA, (nt. 34), parr. 172 e 173. Nell'ordinamento italiano, Circolare n. 285/2013, Parte I, Titolo IV, Capitolo 3, Sezione III, par. 1, lett. *c*), secondo cui i responsabili delle funzioni aziendali di controllo comunicano con l'organo amministrativo «senza restrizioni o intermediazioni».

[37] In tema, EBA, (nt. 34), parr. 195 e 200, là ove prevede che il «responsabile della funzione di gestione dei rischi dovrebbe avere il compito di (…) consigliare l'organo di gestione»; avuto riguardo alla funzione di *compliance*, par. 209, secondo cui la «funzione di conformità dovrebbe consigliare l'organo di gestione in merito alle misure da adottare per garantire la conformità a leggi, norme, regolamenti e *standard* applicabili e dovrebbe valutare il possibile impatto di eventuali modifiche del contesto giuridico o normativo sulle attività e sul quadro di conformità dell'ente». In riferimento alla funzione di *compliance*, nell'ordinamento italiano, Circolare n. 285/2013, Parte I, Titolo IV, Capitolo 3, Sezione III, par. 3.2, che contempla tra i compiti di tale componente dei controlli interni la proposta di «modifiche organizzative e procedurali finalizzate ad assicurare un adeguato

ne che gli stessi intendono adottare [38]. Tale prerogativa non può, però, spingersi fino a bloccare la decisione di esternalizzare i servizi tecnologici: la competenza e la responsabilità ultima di tale atto rimane in capo ai componenti dell'organo amministrativo [39].

Il ruolo dei vertici delle funzioni interne di controllo risulta, tuttavia, più circoscritto quando la banca nomina un soggetto responsabile per la gestione e il monitoraggio del rischio di esternalizzazione. In tale ipotesi, considerata la diretta responsabilità verso l'organo di gestione per il governo dei rischi di *outsourcing* [40], è possibile ritenere che tale figura costituisca l'interlocutore principale dei componenti dell'organo amministrativo. Il soggetto responsabile per l'*outsourcing* sarà, dunque, deputato a rappresentare i dati necessari all'organo di gestione e a partecipare alla decisione di esternalizzazione, fermo restando in ogni caso il previo confronto con i responsabili delle altre funzioni di controllo interno.

Da ultimo, l'attività dei responsabili del *risk management*, della *compliance*, della eventuale funzione di controllo dei rischi ICT e della funzione di esternalizzazione beneficia degli esiti dell'attività istruttoria svolta dalle funzioni di appartenenza nelle rispettive aree di competenza [= rispettivamente, (1) l'identificazione dei rischi associati all'esternalizzazione [41] e la valutazione dell'impatto della scelta sul profilo di rischio dell'ente [42]; (2) la gestione del rischio di non conformità riferito alla disciplina applicabile ai rapporti di terza parte [43]; (3) il puntuale trattamento dei rischi ICT e sicurezza [44]]. Qualora la banca abbia deciso di de-

presidio dei rischi di non conformità identificati» e la prestazione di consulenze e «assistenza nei confronti degli organi aziendali della banca in tutte le materie in cui assume rilievo il rischio di non conformità».

[38] Sul punto, EBA, (nt. 34), par. 173, secondo cui, in termini generali, i «responsabili delle funzioni di controllo interno dovrebbero poter accedere e riferire direttamente all'organo di gestione nella sua funzione di supervisione strategica, al fine di sollevare dubbi e avvisare la funzione di supervisione strategica». Con specifico riferimento all'ambito del *risk management*, par. 202, che assegna al titolare di tale funzione il potere di «mettere in discussione le decisioni prese dalla dirigenza dell'ente e dal relativo organo di gestione».

[39] Con particolare riferimento alla funzione di gestione dei rischi, il punto è affermato espressamente in EBA, (nt. 34), par. 188, dove viene previsto che la «responsabilità delle decisioni adottate dovrebbe restare in capo alle unità operative e interne e, in ultima analisi, all'organo di gestione».

[40] Come stabilito in EBA, (nt. 16), par. 38, lett. *c*), la banca dovrebbe istituire una apposita funzione o designare un soggetto apicale dell'organizzazione che risponda direttamente al consiglio di amministrazione e abbia a livello interno la responsabilità di gestire i rischi connessi ai contratti di esternalizzazione.

[41] Cfr. EBA, (nt. 34), par. 191.

[42] Sul punto, EBA, (nt. 34), par. 195.

[43] In tema, EBA, (nt. 34), par. 204 e, nell'ordinamento italiano, Circolare n. 285/2013, Parte I, Titolo IV, Capitolo 3, Sezione III, par. 3.2.

[44] La funzione trova puntuale disciplina nell'ordinamento italiano e, in particolare, v. Circolare 285/2013, Parte Prima, Titolo IV, Capitolo 4, Sezione II, par. 4. L'istituzione di una funzione di

dicare all'esternalizzazione un'apposita struttura aziendale, si deve ritenere che l'attività istruttoria dovrà essere svolta da quest'ultima, con l'ausilio delle altre funzioni.

Alcune precisazioni alle considerazioni svolte si rendono necessarie con riferimento ai sistemi alternativi di amministrazione e controllo. Nell'ambito del sistema dualistico, il consiglio di sorveglianza può beneficiare di un canale informativo diretto con la struttura aziendale e attivare un contatto diretto con l'autorità di vigilanza, anche sulla base degli elementi informativi emersi nell'esercizio delle proprie prerogative. In qualità di titolare della funzione di controllo, il consiglio di sorveglianza può infatti ricevere direttamente dalle funzioni aziendali interne «adeguati flussi informativi periodici o relativi a specifiche situazioni o andamenti aziendali» (Circolare n. 285/2013, Parte Prima, Titolo IV, Capitolo 1, Sezione III) e informare «senza indugio la Banca d'Italia di tutti gli atti o i fatti (…) che possano costituire una irregolarità nella gestione delle banche o una violazione delle norme disciplinanti l'attività bancaria» (art. 52, primo comma, t.u.b.). Nel sistema monistico, considerazioni analoghe valgono con riferimento al comitato per il controllo sulla gestione, che potrà, dunque, godere di un canale informativo diretto e privilegiato rispetto agli altri amministratori e giocare un ruolo proattivo verso l'autorità di vigilanza.

5. *Scelta informata e valutazione del rischio.*

Il primo compito richiesto ai componenti dell'organo amministrativo di una banca in sede di scelta consiste nella valutazione degli elementi su cui fondare la decisione di esternalizzare. In proposito, i componenti devono confrontarsi con un paradigma di gestore informato ampiamente dettagliato dal Regolamento DORA e dagli Orientamenti EBA [45]. Infatti, tale quadro normativo specifica i fattori che gli organi competenti devono prendere in considerazione «prima di stipulare l'accordo contrattuale»: (1) l'essenzialità o l'importanza della funzione a supporto

controllo responsabile della gestione e sorveglianza dei rischi informatici è ora prevista imperativamente dall'art. 6, quarto par., Regolamento DORA per gli enti finanziari diversi dalle microimprese.

[45] In applicazione dell'art. 28, decimo par., primo e secondo comma, Regolamento DORA, le Autorità di vigilanza europee hanno inviato alla Commissione europea una bozza di *Regulatory Technical Standard*, destinati a specificare con maggior grado di dettaglio i fattori che la banca dovrà considerare al fine di concludere un accordo di esternalizzazione di funzioni essenziali o importanti: Joint Committee of the ESAs, *Final Report on Draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554* (17 January 2024), reperibile al seguente indirizzo: https://service.betterregulation.com/document/702869; il lavoro delle ESAs è ora confluito nell'adozione del Regolamento Delegato (UE) 2024/1773.

della quale è impiegato il servizio IT; (2) il rispetto delle condizioni di vigilanza; (3) i rischi rilevanti; (4) l'idoneità del potenziale fornitore; (5) l'esistenza di conflitti di interesse (art. 28, quarto par., Regolamento DORA). Seppure tali elementi risultino collocati sullo stesso piano, la valutazione del servizio come essenziale o importante assume un ruolo preliminare: se svolta positivamente, comporta un arricchimento dei fattori che devono essere considerati dall'organo di amministrazione, segnando una biforcazione nel modello dell'agire informato.

Nel caso di funzione non essenziale o importante, l'organo delegato deve valutare, accanto al rispetto delle condizioni di vigilanza e all'esistenza di conflitti di interesse, la sostenibilità economica e finanziaria dell'*outsourcer* – avendo particolare riguardo al *business model* e alla struttura proprietaria [46] –, nonché l'eventuale affidamento infragruppo del servizio [47]. Diversamente, nel caso di funzione essenziale e importante, l'organo amministrativo è tenuto ad estendere il proprio patrimonio informativo all'adeguatezza della struttura organizzativa [48]; al pregio del servizio in termini tecnico-informatici [49]; alla concentrazione dei servizi IT [50]; all'eventualità di un conseguente sub-appalto [51]; alle regole applicabili al fornitore, con particolare riguardo alle disposizioni che ne governano l'eventuale crisi [52] e all'effettiva applicazione della legge in caso di paese terzo [53].

La distinzione dei fattori da prendere in considerazione risulta determinante in quanto delimita il perimetro dell'attività istruttoria e informativa assolta dalle funzioni interne di controllo, sulla cui base l'organo di gestione orienta la propria valutazione del rischio e la decisione finale. La discrezionalità degli amministratori o dei consiglieri entra in gioco, infatti, nella determinazione del livello di rischio associato all'assetto che verrebbe a configurarsi. Come esemplificato dal quadro normativo, l'analisi dei diversi fattori indicati risulta funzionale alla valutazione del rischio associato all'(eventuale) esternalizzazione del servizio IT [54].

---

[46] EBA, (nt. 16), par. 71, lett. *a*).

[47] EBA, (nt. 16), par. 71, lett. *c*).

[48] EBA, (nt. 16), par. 70. Tale disposizione dovrebbe essere interpretata nel senso di una verifica dell'idoneità quali-quantitativa degli assetti societari e aziendali. In questa direzione propende il riferimento letterale alla «reputazione commerciale», alle «abilità adeguate e sufficienti», alla «competenza», alla «capacità» e alle «risorse».

[49] Un elemento letterale per questa prospettiva si rintraccia nel dovere della banca di valutare che le «risorse informatiche» del fornitore siano tali da svolgere la funzione «in modo affidabile e professionale»: EBA, (nt. 16), par. 70.

[50] Art. 29, primo par., primo e quarto comma, Regolamento DORA.

[51] Art. 29, secondo par., primo comma, Regolamento DORA e EBA, (nt. 16), par. 76 ss.

[52] Art. 29, secondo par., secondo comma, Regolamento DORA.

[53] Art. 29, secondo par., terzo comma, Regolamento DORA.

[54] Così, ad esempio, l'indicazione per cui la banca dovrebbe «valutare l'impatto potenziale degli accordi di esternalizzazione in termini di rischio operativo» e «tenere conto dei risultati di tale valu-

Sembra possibile affermare che tale valutazione del rischio contempla, con un certo grado di approssimazione, due passaggi principali. Inizialmente, viene stabilito un primo livello di rischio connesso al potenziale *outsourcer* individuato, tanto in termini di affidabilità operativa quanto in termini di solidità organizzativa e sostenibilità economico-finanziaria. In un secondo momento, tale livello viene ridotto sulla base di un giudizio prognostico circa la capacità della banca di mitigare tale rischio tramite i dispositivi di *governance* e i diritti contrattuali [55]. Il risultato di tale valutazione sarà, in ultima istanza, il parametro di riferimento per la banca nella scelta di esternalizzare i servizi IT.

6. *I paradigmi della scelta.*

È a questo punto che si innesta la scelta definitiva da parte degli amministratori o dei consiglieri. Tale decisione viene a confrontarsi con due rilevanti paradigmi di gestione.

Nel primo, sulla base delle premesse informative e del rischio misurato, gli amministratori della banca compiono la scelta di esternalizzare il servizio, dopo aver svolto una analisi dei costi e dei benefici derivanti dal ricorso alla pratica aziendale [56]. In questo caso, tale scelta sarebbe coperta dalla *business judgement rule* e risulterebbe pertanto insindacabile, al di fuori delle ipotesi di scelta non informata o manifestamente irragionevole [57]. Indicazioni in questo senso si rintrac-

---

tazione quando decidono se esternalizzare la funzione a un fornitore di servizi»: EBA, (nt. 16), par. 64. Per l'indicazione puntuale dei rischi considerati dalla relativa valutazione, art. 5, secondo par., Regolamento Delegato (UE) 2024/1773.

[55] Per il rilievo generale che «[s]ulla base delle valutazioni dei rischi, gli istituti finanziari dovrebbero determinare quali sono le misure essenziali per ridurre a livelli accettabili i rischi ICT e di sicurezza individuati», EBA, *Orientamenti sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione e di sicurezza* (28 novembre 2019), reperibile al seguente indirizzo: https://www.eba.europa.eu/guidelines-ict-and-security-risk-management, par. 22. Nella medesima prospettiva, EBA, (nt. 34), par. 153, per cui la politica di gestione dei rischi di una banca dovrebbe contenere misure volte a ridurre i rischi individuati.

[56] Così F. URBANI, (nt. 13), 208, secondo cui l'«esternalizzazione, in questa prospettiva, è frutto della discrezionalità e della diligenza gestoria degli amministratori, chiamati a valutare se – ed eventualmente come – una simile formula operativa possa essere utile ai fini del migliore svolgimento dell'attività d'impresa, dovendosi valutare la convenienza sia di una simile soluzione di per sé considerata, sia delle specifiche modalità con cui essa si ipotizza potrà essere effettivamente strutturata».

[57] In ambito bancario, avuto riguardo all'irragionevolezza della scelta gestoria, V. CALANDRA BUONAURA, *L'impatto della regolamentazione sulla governance bancaria*, in *Banca impr. soc.*, 2019, 33. Si veda, inoltre, con specifico riferimento all'irrazionalità della scelta, P. MONTALENTI, *Assetti organizzativi e organizzazione dell'impresa tra principi di corretta amministrazione e* business judgement rule: *una questione di sistema*, in *NDS*, 2021, 20 e, nell'ambito della disciplina con parti correlate, ID., *Impresa, società di capitali, mercati finanziari*, Torino, Giappichelli, 2017, 247. Per ulteriori riferimenti dottrinali e giurisprudenziali, F. RIGANTI, *La Responsabilità degli ammini-*

ciano anche nel regime giuridico in materia di *outsourcing*. In primo luogo, nella valutazione del rischio propedeutica alla decisione, l'autorità di vigilanza competente richiede alla banca di «considerare i benefici e i costi attesi dell'accordo di esternalizzazione proposto» (Orientamenti EBA, par. 66). Sulla stessa linea, le funzioni aziendali sono ritenute essenziali o importanti anche quando la loro interruzione «comprometterebbe sostanzialmente i risultati finanziari» della banca (art. 3, punto 22, Regolamento DORA; Orientamenti EBA, par. 29, lett. *a*, punto *ii*).

Nel secondo paradigma di gestione, una volta stabilito il livello di rischio residuo, gli amministratori e i consiglieri non beneficiano di una piena libertà decisionale, ma sono tenuti a contemplare all'interno della loro scelta alcuni interessi che la legge intende proteggere. La scelta di esternalizzare sarebbe consentita soltanto nel caso in cui – alla luce del rischio misurato (o misurabile) – tali interessi non siano pregiudicati. In questo caso, la *business judgement rule* subirebbe un parziale restringimento, in quanto la discrezionalità degli amministratori sarebbe conformata da criteri normativi. La scelta del modello cui adeguare l'azione gestoria dipende necessariamente dal quadro normativo dettato dal legislatore.

7. *Continuità e qualità del servizio come criteri conformativi della scelta.*

Occorre ora stabilire se il legislatore abbia individuato con un sufficiente grado di chiarezza alcuni criteri in grado di conformare la scelta gestoria. In proposito, le regole che espressamente governano l'«analisi preventiva» dell'esternalizzazione si limitano a indicare dal punto di vista metodologico i fattori da considerare, senza nulla dire intorno all'obiettivo cui tale valutazione risulta servente [58]. La ricerca di eventuali criteri normativamente rilevanti deve pertanto essere allargata ad un esame sistematico delle disposizioni in materia di *outsourcing*. Al riguardo, sembra necessario muovere dalla finalità di resilienza operativa digitale che, come noto, informa l'intera strategia normativa sottesa al Regolamento DORA [59]. Nella sintomatica definizione fornita dal legislatore europeo, la «resilienza

stratori. Rassegna di giurisprudenza, in *Giur. comm.*, 2023, II, 181 ss. e P. MONTALENTI, F. RIGANTI, *La responsabilità degli amministratori di società per azioni. Rassegna di giurisprudenza*, in *Giur. comm*., 2017, II, 780.

[58] Cfr. EBA, (nt. 16), sezione 12, ove peraltro l'utilizzo dell'espressione citata. I fattori sono: (1) l'essenzialità o l'importanza della funzione a supporto della quale è impiegato il servizio IT; (2) il rispetto delle condizioni di vigilanza; (3) i rischi rilevanti; (4) l'idoneità del potenziale fornitore; (5) l'esistenza di conflitti di interesse [art. 28, quarto par., Regolamento DORA; EBA, (nt. 16), par. 61].

[59] Sul punto, v. il Considerando n. 1 Regolamento DORA, per cui l'«uso onnipresente dei sistemi di TIC e l'elevata digitalizzazione e connettività sono oggi caratteristiche fondamentali delle attività delle entità finanziarie dell'Unione, ma la loro resilienza digitale deve ancora essere affrontata e integrata in maniera più efficace nei loro quadri operativi di portata più ampia». La rilevanza della resilienza operativa era già stata segnalata dal BCBS, *Principles for Operational Resilience* (31

operativa digitale» della banca che presta attività «direttamente o indirettamente tramite il ricorso ai servizi offerti dai fornitori terzi» si identifica in due caratteristiche fondamentali: la «costante offerta dei servizi e la loro qualità» (art. 3, punto 1, Regolamento DORA). In tale contesto normativo, assume dunque primaria importanza la necessità di garantire la continuità e la qualità del servizio. Ulteriori indici normativi in questa direzione si rinvengono nelle disposizioni relative al monitoraggio e alla cessazione dell'accordo di esternalizzazione, confermando come tali criteri informino l'intera durata del rapporto di fornitura di servizi IT. In primo luogo, con grande enfasi, il legislatore europeo ha dichiarato che il «monitoraggio dei rischi» associati al fornitore di servizi IT deve essere svolto «in ultima analisi sulla base di un'attenta valutazione di eventuali impatti sulla continuità e la qualità dei servizi finanziari» (Considerando n. 64 Regolamento DORA). Echeggiando tale rilievo, il legislatore europeo ha inoltre richiesto alle banche di avviare strategie di uscita nell'ipotesi del «deterioramento della qualità dei servizi TIC forniti», nonché nel caso di «gravi rischi connessi all'adeguatezza e alla continuità dell'esercizio del rispettivo servizio TIC» (art. 28, ottavo par., primo comma, Regolamento DORA). Infine, in caso di cessazione dell'accordo contrattuale, le banche devono garantire di non «pregiudicare la continuità e la qualità dei servizi forniti ai clienti» (art. 28, ottavo par., secondo comma, Regolamento DORA; Orientamenti EBA, par. 107). In questi termini, quando viene in rilievo la prestazione di servizi IT, il legislatore sembra identificare nella continuità e nella qualità del servizio i criteri conformativi della discrezionalità degli amministratori.

Per la verità, sarebbe possibile pervenire a una conclusione analoga applicando in tale sede il canone della sana e prudente gestione di un ente creditizio. Per quanto tale criterio sia pensato come obiettivo di vigilanza di Banca d'Italia, BCE ed EBA [60], è ormai diffusa la convinzione che tale clausola generale sia in grado di orientare anche l'azione degli amministratori di banca [61]. Del resto, tale canone

March 2021), reperibile al seguente indirizzo: https://www.bis.org/bcbs/publ/d516.htm, 1, dove l'affermazione che: «in light of the critical role that banks play in the operation of the global financial infrastructure, increasing their resilience would provide additional safeguards to the financial system». Similmente, INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS, *Principles on Outsourcing. Final Report* (October 2021), reperibile al seguente indirizzo: https://www.iosco.org/search/, 13.

[60] Cfr., rispettivamente, art. 5, primo comma, d.lgs. 1° settembre 1993, n. 385 – Testo unico delle leggi in materia bancaria e creditizia (d'ora in poi, "t.u.b.") e art. 1, primo comma, Regolamento (UE) n. 1024/2013, per cui l'Autorità ha il compito istituzionale di «contribuire alla sicurezza e alla solidità degli enti creditizi»; con riferimento all'EBA, manca una espressa indicazione che ricomprenda la sana e prudente gestione nelle sue finalità istituzionali. Tuttavia, se si conviene che la stabilità macro-prudenziale dipende da una gestione sana e prudente delle banche a livello micro-prudenziale, è possibile ritenere che tale secondo obiettivo costituisca il presupposto del primo e debba ispirare, seppure indirettamente, l'attività dell'EBA.

[61] La dottrina maggioritaria ritiene che gli enti vigilati sono destinatari del precetto: così G. LEMME, *Amministrazione e controllo nella società bancaria*, Milano, Giuffrè, 2007, 48, che parla di duplicità di destinatari della normazione secondaria emanata da Banca d'Italia. Dà per implicito

ispira l'intera disciplina regolamentare in misura tale che l'adesione alle prescrizioni in essa contenute equivale a orientare l'attività amministrativa al perseguimento della sana e prudente gestione. Tale principio può essere generalmente declinato nella finalità di assicurare la tenuta patrimoniale e finanziaria degli enti creditizi [62]; nello specifico ambito dell'esternalizzazione di servizi IT, l'esigenza di garantire una gestione in linea con le finalità della regolamentazione bancaria si tradurrebbe nell'adozione di una condotta prudente nella decisione di esternalizzazione e nella selezione del fornitore. Non si ignora, tuttavia, l'ampio spazio di discrezionalità concesso dalla clausola generale della sana e prudente gestione, in quanto tale suscettibile di diverse declinazioni a livello applicativo. È per tale ragione che l'identificazione dei canoni di continuità e qualità del servizio contribuisce a tradurre in modo più pregnante il paradigma della sana e prudente gestione nell'ambito della conformazione tecnologica dell'attività bancaria.

8. *La composizione dei criteri e la responsabilità degli amministratori.*

Alla luce di tali considerazioni, la scelta di esternalizzare servizi IT deve essere subordinata al perseguimento dell'efficienza e al contemporaneo soddisfacimento degli *standard* di continuità e qualità del servizio. Due esempi aiutano a comprendere la portata applicativa del risultato raggiunto. In un primo scenario, la scelta della banca potrebbe ricadere in favore di un fornitore che, pur presentandosi critico sotto l'aspetto della prestazione del servizio, offre la propria collaborazione ad un prezzo significativamente inferiore rispetto ai *competitors* sul mercato. In questo caso, la necessità di rispettare entrambi i criteri impedisce alla banca di stipulare l'accordo di esternalizzazione IT con quel fornitore. In un secondo scenario, la banca potrebbe avvalersi di un fornitore che, pur offrendo un

---

l'assunto, qualificando la clausola generale come «regola di comportamento» per gli enti, C. LAMANDA, *Le finalità della vigilanza*, in *La nuova legge bancaria. Il t.u. delle leggi sull'intermediazione bancaria e creditizia e le disposizioni di attuazione*, a cura di P. FERRO-LUZZI, G. CASTALDI, 1, Milano, Giuffrè, 1996, 171. Più di recente, A. NIGRO, *Il nuovo ordinamento bancario e finanziario europeo: aspetti generali*, in *Giur. comm.*, 2018, I, 186 s.; G. GUIZZI, *Appunti in tema di interesse sociale e* governance *nelle società bancarie*, in *Riv. dir. comm.*, 2017, I, 248 ss., A. MIRONE (nt. 33), 44 ss. e C. ANGELICI, *Introduzione (intervento al convegno "Società bancarie e società di diritto comune. Elasticità e permeabilità dei modelli")*, in *Dir. banc. merc. fin.*, 2016, 761 ss. Con particolare riferimento all'ordinamento europeo, confermano tale assunto K. LIEVERSE, C. BULTEN, *Corporate Law versus Financial Regulatory Rules. The Impact on Managing Directors and Shareholders of Banks*, in *Governance of Financial Institutions*, edited by D. BUSCH, G. FERRARINI, G. VAN SOLINGE, Oxford, Oxford University Press, 2019, 95, sottolineando come «a bank not only has to comply with company law, but also with the rules on corporate governance arising from the financial regulatory rules».

[62] Sembra essere questo il senso del Considerando n. 34 CRD IV, là dove stabilisce espressamente che gli interventi europei nel diritto bancario «sono volti ad assicurare la solvibilità degli enti».

significativo vantaggio in termini di competitività, beneficia di un potere negoziale difficilmente governabile. In un contesto di mercato che continua ad essere caratterizzato da un forte grado di concentrazione, la banca dovrà privilegiare i soggetti che – a parità di asimmetria di potere – offrono i migliori *standard* qualitativi e i più ampi poteri di controllo sulla loro operatività.

Nell'impossibilità di individuare fornitori adeguati, la banca non è tuttavia immediatamente costretta a internalizzare l'esecuzione del servizio IT. L'opzione intermedia è costituita dalla fornitura infragruppo: da un lato, l'istanza di efficienza è garantita dal maggior grado di specializzazione che consegue alla segmentazione dell'impresa; per altro verso, il rischio di pregiudizi all'operatività è significativamente mitigato per il fatto che la banca è in grado di esercitare un più elevato controllo sull'operatività della società controllata [63]. È soltanto in assenza di quest'ultima opzione strategica che la banca sarà tenuta a realizzare il servizio *in house* [64].

In questa prospettiva, gli amministratori sono tenuti a dare conto delle ragioni per cui la selezione del fornitore non presenta un rischio residuo tale da compromettere gli interessi protetti dal legislatore e, nel contempo, non dimentica esigenze di efficienza. La qualità e la continuità del servizio IT, ricavabili dagli indici normativi indicati e dal principio di sana e prudente gestione dell'ente (*supra*, n. 7), conformano in maniera imperativa la scelta di esternalizzare servizi, senza soffrire di alcuna eccezione.

Ciò comporta che non è possibile giustificare scelte non equilibrate ricorrendo ad un innalzamento della dotazione patrimoniale dell'ente al fine di assorbire le perdite derivanti dagli eventuali pregiudizi causati dal fornitore. I requisiti di capitale per il rischio di esternalizzazione rientrano tra i fondi propri che la banca deve detenere a copertura del rischio operativo ai sensi del Regolamento (UE) n. 575/2013 (d'ora in poi, "CRR") [65]. La strategia diretta a imporre ulteriori requisiti

---

[63] Se è vero che la fornitura infragruppo di servizi TIC «non dovrebbe essere automaticamente considerata meno rischiosa della fornitura di servizi TIC da parte di fornitori al di fuori di un gruppo finanziario e dovrebbe pertanto essere soggetta allo stesso quadro normativo», è altrettanto vero che «quando i servizi TIC sono forniti dall'interno dello stesso gruppo finanziario, le entità finanziarie potrebbero esercitare un livello di controllo più elevato sui fornitori infragruppo, il che dovrebbe essere preso in considerazione nella valutazione complessiva del rischio» [Considerando n. 31 Regolamento DORA; similmente EBA, (nt. 16), par. 68, lett. *f*]. Sul punto, v. anche il Considerando n. 5 Regolamento Delegato (UE) 2024/1773, secondo cui i «rischi posti dai fornitori intragruppo di servizi TIC possono essere diversi».

[64] I costi per realizzare in proprio un servizio tecnologico potrebbero essere particolarmente elevati in caso di banche di piccole-medie dimensioni. In tal caso, spese elevate da una parte e rischi significativi di *outsourcing* dall'altra potrebbero condurre alla situazione paradossale in cui la banca è impossibilitata a implementare nella propria impresa servizi tecnologici. Al fine di evitare tale risultato, gli enti saranno tenuti a comparare i costi del servizio rispetto alle potenziali perdite derivanti dai rischi di esternalizzazione e assumere la relativa decisione, che dovrebbe essere sufficientemente motivata in tal senso.

[65] Più nello specifico, il regime normativo ora vigente prevede che le banche possano calcolare

di capitale rispetto a quelli imposti dal CRR per mitigare gli effetti negativi del rischio di esternalizzazione (in luogo di presidi *ex ante*) è stata vagliata [66] ed espressamente accantonata dalla Commissione europea in sede di adozione del Regolamento DORA. Con significative argomentazioni, la Commissione ha infatti affermato che l'aumento dei requisiti patrimoniali non costituisce una misura sufficiente, in quanto accresce la solidità finanziaria della banca senza "intercettare" l'istanza principale: la resilienza operativa [67]. Inoltre, quand'anche le banche accettassero di rispettare un'aggiuntiva riserva di capitale, la Commissione sostiene che non sarebbero comunque implementate le misure organizzative che risultano concretamente idonee a garantire la riduzione del rischio operativo [68]. Il legislatore europeo, nelle proprie intenzioni e nella strategia normativa selezionata, ha dunque sconfessato l'assunzione di rischio tramite "garanzia patrimoniale", imponendo scelte e misure in grado di assicurare direttamente il rispetto della continuità e della qualità operativa [69].

È possibile in conclusione tracciare – pur con un certo grado di sintesi – il quadro della responsabilità degli amministratori e dei consiglieri della banca. Il mancato rispetto dei criteri conformativi della scelta di esternalizzare può qualifi-

---

tale requisito di capitale secondo molteplici modalità, che si fondano su due metodi di determinazione del fabbisogno patrimoniale di natura opposta (artt. 315-322 CRR). Ad un estremo, vi sono il metodo di base e il metodo standardizzato, che calcolano la quota di patrimonio richiesta al fine di mitigare gli impatti delle perdite "operative" attraverso il prodotto tra un indicatore rilevante espressivo dei ricavi generati dall'ente e fattori fissati in via imperativa dal legislatore europeo. All'altro estremo, vi è il metodo avanzato di misurazione grazie al quale la banca può calcolare i fondi propri necessari attraverso una stima delle perdite attese e inattese, effettuata con l'ausilio dei propri modelli interni. Il quadro attualmente vigente è destinato a mutare con il recepimento nell'ordinamento europeo delle recenti novità internazionali nel quadro di Basilea III. La riforma – tra i vari punti toccati – modificherà la disciplina prudenziale del rischio operativo contenuta nel CRR, introducendo un unico metodo di calcolo *standard* basato su fattori predeterminati e sulla dimensione del *business* (il c.d. indicatore di attività), nella prospettiva di consentire una misurazione più precisa dell'esposizione della banca alla tipologia di rischio considerata e ridurre la variabilità di stime effettuate secondo modelli interni [artt. 312, 313, 314 e 315, Regolamento (UE) 2024/1623].

[66] Vedi COMMISSIONE EUROPEA, (nt. 4), 27 ss.

[67] COMMISSIONE EUROPEA, (nt. 4) 37: «[this policy option] will have only limited effects on increasing the operational, as opposed to financial, resilience of the EU financial sector, as provisioning more capital to cater for losses stemming from ICT-related incidents would be an insufficient measure».

[68] COMMISSIONE EUROPEA, (nt. 4), 37: «while firms may be incentivised to take measures to improve their resilience in order to reduce their capital requirements, there is no clarity on the nature of these measures or the degree to which firms will actually strive to adopt such measures (or just accept the capital charge)».

[69] In quest'ultima prospettiva si comprende la «necessità di assicurare un livello di investimenti connessi alle TIC e un bilancio complessivo dell'entità finanziaria che consentirebbero all'entità finanziaria di conseguire un elevato livello di resilienza operativa digitale» (Considerando n. 46 Regolamento DORA).

carsi come inadempimento di un dovere imposto dalla legge e, per conseguenza, comporta – al ricorrere degli altri presupposti – la responsabilità verso la società degli amministratori e dei consiglieri (di gestione o sorveglianza [70]) ai sensi dell'art. 2392 c.c. [71].

Gli amministratori e i consiglieri della banca saranno dunque chiamati a rispondere ogni volta che la scelta del fornitore (1) non consegue a una decisione informata e assunta secondo il corretto *iter* procedurale oppure (2) non è in grado di soddisfare gli interessi protetti dal legislatore. In queste due ipotesi, se si condividono i rilievi per cui gli amministratori e i consiglieri si confrontano con un paradigma di gestore specificamente informato (*supra*, n. 5) e la scelta è positivamente orientata dai predetti criteri conformativi, si potrà agevolmente comprendere come la regola di insindacabilità delle scelte gestorie subisca un restringimento entro tale contesto normativo e non potrà essere invocata dalle parti o impiegata dal giudice per escludere la responsabilità [72].

Infine, le condotte in grado di integrare la responsabilità degli amministratori e dei consiglieri dovrebbero consentire ai soci di revocare il loro incarico per giusta

---

[70] Nelle ipotesi in cui la decisione di esternalizzare funzioni essenziali o importanti spetti a entrambi gli organi sarà configurabile una responsabilità concorrente degli stessi. Nella fattispecie prevista dall'art. 2409-*terdecies*, primo comma, lett. *f-bis*) parte della dottrina, infatti, argomenta in favore di una responsabilità "aggiuntiva" del consiglio di sorveglianza: F. BORDIGA, *sub* art. 2409-terdecies, in *Le società per azioni. Codice civile e norme complementari*, diretto da P. ABBADESSA, G.B. PORTALE e a cura di M. CAMPOBASSO, V. CARRIELLO, U. TOMBARI, 1, Milano, Giuffrè, 2016, 1949; V. CARIELLO, *Sulla responsabilità del consiglio di sorveglianza*, in *RDS*, 2011, I, 70 ss.; P. MONTALENTI, (nt. 30), 275 e F. MASSA FELSANI, *"Interferenze" del consiglio di sorveglianza nella gestione dell'impresa: appunti dalla disciplina del governo delle banche*, in *Riv. dir. comm.*, 2008, I, 898 s., pur sollevando dubbi per il fatto che l'art. 2409-*terdecies*, primo comma, lett. *f-bis*) mantiene ferma la responsabilità del consiglio di gestione.

[71] Il dovere di selezionare fornitori capaci di prestare con costanza servizi di qualità può considerarsi di natura determinata, anche alla luce dei fattori considerati dalle fonti normative in materia di *outsourcing*. Pacifica è la responsabilità degli amministratori per violazione di doveri specifici: *ex multis*, F. BONELLI, *Responsabilità degli amministratori di s.p.a.*, in *Giur. comm.*, 2004, I, 623 ss., nonché V. DI CATALDO, *Problemi nuovi in tema di responsabilità di amministratori di società per azioni: dal possibile affievolimento della solidarietà all'incerto destino dell'azione della minoranza*, in *Giur. comm.*, 2004, I, 646 s.; da ultimo, S. AMBROSINI, *La responsabilità degli amministratori*, in *Trattato delle società*, diretto da V. DONATIVI, 2, Torino, Utet Giuridica, 2022, 2014 ss. e ID., *La responsabilità degli amministratori*, in *Trattato di diritto commerciale*, diretto da G. COTTINO, 4*, Padova, Cedam, 2010, 664 ss.

[72] Esclude l'applicabilità della *business judgement rule* alle violazioni di regole dirette a disciplinare l'attività sociale, C. ANGELICI, *La società per azioni. Principi e problemi*, in *Trattato di diritto civile e commerciale*, già diretto da A. CICU, F. MESSINEO, L. MENGONI e continuato da P. SCHLESINGER, Milano, Giuffrè, 2012, 403 ss. e ID. *Interesse sociale e* business judgement rule, in *Riv. dir. comm.*, 2012, I, 582 s., nonché, in precedenza, ID., Diligentia quam in suis *e* business judgement rule, in *Riv. dir. comm.*, 2006, I, 688. In giurisprudenza, da ultimo, esclude la rilevanza della *business judgement rule* in presenza di «inequivoche violazioni di legge», Cass. civ., sez. I, 25 marzo 2024, n. 8069, in *Foro it.*, 2024, 1502.

causa, nei casi di particolare gravità (si consideri, per esempio, l'esternalizzazione di un *full outsourcing* a un fornitore del tutto inaffidabile) [73].

9. *Monitoraggio e rimedi verso il fornitore di servizi tecnologici.*

La rilevanza normativa dell'accordo tra banca e fornitore di servizi IT non si esaurisce al termine della scelta; a tale fase, segue la cruciale attività di monitoraggio sulla controparte contrattuale svolta dalla banca e, in particolare, dai soggetti responsabili del monitoraggio [74], nonché dalle funzioni di controllo interne [75]. Lo svolgimento di un'adeguata attività di controllo è assicurato tramite due principali strategie normative: la conformazione degli assetti organizzativi della banca e la eterodeterminazione da parte del legislatore europeo di alcune clausole del contratto concluso con il fornitore di servizi IT a supporto di funzioni essenziali o importanti [76]. La politica di esternalizzazione deve poi prevedere i diversi metodi attraverso cui la banca deve condurre la propria attività di monitoraggio [77]. Tale attività è ultimamente funzionale ad aggiornare regolarmente la valutazione di ri-

[73] Per l'affermazione che la nozione di giusta causa comprende la grave violazione di obblighi di natura gestoria, V. DI CATALDO, S. ROSSI, *Osservazioni in tema di revoca per giusta causa degli amministratori di società di capitali*, in *Giur. comm.*, 2022, I, 540; P. M. SANFILIPPO, D. ARCIDIACONO, *Il rapporto di amministrazione: costituzione e cause di cessazione,* in *Trattato delle società*, diretto da V. DONATIVI, 2, Torino, Utet Giuridica, 2022, 1809; ID., *sub* art. 2387, *Le società per azioni. Codice civile e norme complementari*, diretto da P. ABBADESSA, G.B. PORTALE e a cura di M. CAMPOBASSO, V. CARRIELLO, U. TOMBARI, 1, Milano, Giuffrè, 2016, 1223. Nella manualistica, in senso analogo, P.M. SANFILIPPO, *Gli amministratori*, in *Diritto commerciale*, a cura di M. CIAN, 3, Torino, Giappichelli, 2024, 500 dove alcune pronunce giurisprudenziali rilevanti.

[74] Art. 3, quinto par., Regolamento Delegato (UE) 2024/1773, secondo cui la politica di esternalizzazione deve individuare «chiaramente il ruolo o il dirigente di rango elevato responsabile del monitoraggio degli accordi contrattuali pertinenti. La politica specifica le modalità di collaborazione tra il ruolo o il dirigente di rango elevato e le funzioni di controllo, salvo nel caso in cui ne faccia parte, e definisce le linee gerarchiche di comunicazione all'organo di gestione».

[75] La fonte secondaria europea sembrerebbe attribuire tale compito alla funzione di *internal audit* [sul punto, EBA, (nt. 16), par. 85], mentre l'art. 6, quarto par., Regolamento DORA, pur non riferendosi al fenomeno dell'esternalizzazione, sembrerebbe attribuire l'incombenza ad una apposita funzione di gestione dei rischi IT. Nondimeno, considerati i diversi rischi sollevati dalla pratica aziendale, si deve ritenere che il monitoraggio dovrà essere condiviso con le altre funzioni di controllo interne.

[76] Il contratto di esternalizzazione avente per oggetto funzioni essenziali o importanti deve contenere imperativamente il diritto della banca a monitorare costantemente la *performance* del fornitore, nonché a ispezionarlo e sottoporlo a verifiche di *audit* [rispettivamente, EBA, (nt. 16), par. 75, lett. *h*) e *p*); analogamente, art. 30, terzo par., lett. *e*), Regolamento DORA]. In dottrina, sottolinea la conformazione della struttura di *governance*, del sistema dei controlli interni e del contratto, G. FALCONE, (nt. 23), 276.

[77] Nel dettaglio, art. 8, secondo e terzo par., Regolamento Delegato (UE) 2024/1773.

schio compiuta in sede di scelta [78] e verificare la *compliance* dell'attività del fornitore con gli obblighi normativi e contrattuali [79].

A questo scopo, diviene cruciale definire il perimetro sul quale deve ricadere l'attività di monitoraggio nel rispetto del dovere di diligenza richiesto alle banche [80]. Il *framework* normativo europeo afferma espressamente che l'attività di controllo del servizio esternalizzato deve essere diretta a verificare la *performance* del fornitore [81]. I numerosi riferimenti da parte del legislatore alla «*performance*» del servizio potrebbero essere intesi come rivolti all'esclusivo rispetto dei livelli di servizio prescritti a livello contrattuale [82]. Se così fosse, verrebbe segnalata una restrizione del perimetro del monitoraggio in confronto al novero di fattori esaminato in sede di scelta.

Tale interpretazione restrittiva è tuttavia superata dalla forza espressiva della previsione per cui il monitoraggio è ultimamente governato dalla «valutazione di eventuali impatti sulla continuità e la qualità dei servizi finanziari» (Considerando n. 64 Regolamento DORA); in conformità a tale approccio, il diritto europeo prevede che la banca «è tenuta a valutare se i fornitori (…) soddisfano *standard* (…) di qualità adeguati» [art. 9, secondo par., Regolamento Delegato (UE) 2024/1773]. Come osservato prima, i criteri indicati richiedono un'indagine di tutti i fattori individuati dal legislatore in sede di analisi preventiva ed esaminati dalla banca prima di concludere l'accordo con il fornitore (*supra*, n. 5). La nozione di «*performance*» deve pertanto interpretarsi in maniera ampia e deve leggersi in relazione alla verifica sulla qualità, sicché il monitoraggio deve ricomprendere i predetti

---

[78] EBA, (nt. 16), par. 102 e art. 28, secondo par., Regolamento DORA, secondo cui l'«organo di gestione riesamina periodicamente i rischi individuati in relazione agli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti»; esplicitamente, art. 9, terzo par., Regolamento Delegato (UE) 2024/1773.

[79] Tale aspetto è desumibile da EBA, (nt. 16), par. 105, là dove si afferma che gli «enti e gli istituti di pagamento dovrebbero svolgere verifiche ogni volta che vi siano segnali che i fornitori di servizi potrebbero non eseguire la funzione essenziale o importante esternalizzata in modo efficace o in conformità delle leggi applicabili e degli obblighi normativi».

[80] Cfr. EBA, (nt. 16), par. 101: «[n]el monitorare e gestire gli accordi di esternalizzazione, gli enti e gli istituti di pagamento dovrebbero applicare la debita competenza, cura e diligenza».

[81] Sul punto, EBA, (nt. 16), par. 100: «[g]li enti e gli istituti di pagamento dovrebbero monitorare (…) la *performance* dei fornitori». Cfr., inoltre, art. 30, terzo par., primo comma, lett. *e*), Regolamento DORA, secondo cui il contratto che affidi a terzi lo svolgimento di servizi IT deve necessariamente prevedere in capo alla banca il «diritto di monitorare costantemente le prestazioni del fornitore terzo di servizi TIC»; in senso analogo, art. 9, primo par., Regolamento Delegato (UE) 2024/1773.

[82] I livelli di servizio concordati devono essere previsti all'interno del contratto di esternalizzazione avente per oggetto funzioni essenziali o importanti: EBA, (nt. 16), par. 75, lett. i). Analogamente, art. 30, terzo par., primo comma, lett. *a*), Regolamento DORA. Per una disamina degli indicatori di *performance* in tali contratti, v. R. IZZO, *Il contratto di* outsourcing, in *L'Outsourcing nei servizi bancari e finanziari*, a cura di S. CASAMASSIMA, M. NICOTRA, Padova, Cedam, 2021, 69 ss.

elementi, idonei a incidere sulla continua disponibilità del servizio e sul suo tasso qualitativo [83]. Così, la banca dovrà monitorare la struttura organizzativa del fornitore, in quanto l'uscita dall'organigramma dei soggetti preposti allo sviluppo della tecnologia fornita potrebbe, per esempio, incidere in via prospettica sull'affidabilità del *software* fornito. Oppure, potendo compromettere la corretta operatività del servizio, lo spostamento della sede del fornitore in un paese che non garantisce un'adeguata protezione dei dati dovrà essere attentamente controllato dalla banca.

Né tale conclusione trova obiezione nel fatto che in questo modo le banche dovrebbero sopportare costi di monitoraggio tali da ridurre i benefici dell'esternalizzazione. Come segnalato da un documento del *Financial stability board*, infatti, «[a]lthough due diligence is linked to pre-contractual activities, financial institutions usually update their due diligence (…) as part of their ongoing monitoring of the service provider or within an appropriate period after the commencement of the service» [84]. Al fine di non sottovalutare i rischi associati alle pratiche di esternalizzazione, la prassi di mercato testimonia la disponibilità delle banche a intraprendere un'attività di controllo ad ampio spettro.

Rimane da definire la modalità di esercizio di tale monitoraggio. Gli Orientamenti EBA sono univoci nel prevedere che tale attività di controllo debba avvenire su base continuativa e, cioè, lungo tutta la pendenza del rapporto con il fornitore di servizi IT [85]. In questi termini, la banca non potrà limitarsi a compiere indagini periodiche sul fornitore né attivarsi alla sola presenza di segnali d'allarme [86]. Questi ultimi incidono soltanto sul grado di intensità del controllo dovuto. Infatti, la banca sarà tenuta a un supplemento di diligenza e dovrà verificare direttamente l'attendibilità delle informazioni attinenti al fornitore quando venga a conoscenza – tramite propria indagine o notifica da parte dell'*outsourcer* [87] – di vicende ido-

[83] Per una simile soluzione, seppur riferita solamente alla «quality of the provider's management», BCE, (nt. 10), 15.

[84] La citazione nel testo è tratta dal documento FINANCIAL STABILITY BOARD, *Enhancing Third-Party Risk Management and Oversight* (4 December 2023), reperibile al seguente indirizzo: https://www.fsb.org/2023/12/final-report-on-enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities/, 15.

[85] Così EBA, (nt. 16), par. 100.

[86] Per la verità, un allentamento della diligenza richiesta in sede di monitoraggio è possibile con riferimento a funzioni non essenziali o importanti. Infatti, «[m]onitoring should be proportionate to the materiality of the risk»: G7, *Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector* (October 2022), reperibile al seguente indirizzo: https://www.gov.uk/government/publications/g7-fundamental-elements-for-third-party-cyber-risk-management-in-the-financial-sector, 3.

[87] Al fine del corretto svolgimento di tale attività, la politica di esternalizzazione deve prevedere «procedure di notifica … riguardanti un accordo di esternalizzazione o un fornitore di servizi (ad esempio, la sua posizione finanziaria, la sua struttura organizzativa o proprietaria, la subesternaliz-

nee ad alterare o modificare la valutazione dei rischi svolta in sede di selezione del fornitore [88].

Nei casi in cui si accerti un'anomalia nell'esecuzione del contratto o nell'operatività del fornitore, la banca potrebbe esercitare strumenti di reazione aventi come esito la cessazione del contratto oppure la messa a punto del servizio o della struttura organizzativa del fornitore. Al riguardo, il contratto di esternalizzazione deve stabilire in via imperativa le fattispecie [89] al ricorrere delle quali la banca può risolvere [90] il rapporto contrattuale con il fornitore di servizi tecnologici. Come

---

zazione)» [EBA, (nt. 16), par. 42, lett. *d*), n. ii]. Sempre nella medesima prospettiva il contratto avente per oggetto l'esternalizzazione di funzioni essenziali o importanti deve prevedere in capo al fornitore obblighi di *reporting* su «qualsiasi sviluppo che possa avere un impatto rilevante» sulla capacità del fornitore di «svolgere efficacemente la funzione essenziale o importante» [EBA, (nt. 16), par. 75, lett. *j*]. Tale ultima previsione è presente anche nel Regolamento DORA (art. 30, terzo par., primo comma, lett. *b*). Con riferimento all'obbligo di comunicare lo spostamento del luogo in cui è realizzata la funzione in *outsourcing*, EBA, (nt. 16), par. 75, lett. *f*).

[88] Cfr. EBA, (nt. 16), par. 105: gli «enti e gli istituti di pagamento dovrebbero svolgere verifiche ogni volta che vi siano segnali che i fornitori di servizi potrebbero non eseguire la funzione essenziale o importante esternalizzata in modo efficace o in conformità delle leggi applicabili e degli obblighi normativi».

[89] Sul punto, v. le ipotesi previste dall'art. 28, settimo par., Regolamento DORA e da EBA, (nt. 16), par. 98. Per ipotesi specifiche con riferimento all'esternalizzazione dei servizi *cloud*, BCE, (nt. 10), 12.

[90] Benché le fattispecie contenute nella previsione indicata nella nota precedente facciano riferimento a casi di inadempimento contrattuale e, come tali, idonei ad essere ricompresi in una clausola risolutiva espressa [in questo senso, art. 28, settimo par., Regolamento DORA e art. 10 Regolamento Delegato (UE) 2024/1773, che utilizzano l'espressione «risoluzione degli accordi contrattuali», nonché la precedente versione delle disposizioni di vigilanza (in dottrina, sul punto, F. IELPO, *L'*outsourcing *ai fornitori di servizi* cloud, in *L'Outsourcing nei servizi bancari e finanziari*, a cura di S. CASAMASSIMA, M. NICOTRA, Padova, Cedam, 2021, 239 s.)], pure il diritto di recesso può essere configurato in via negoziale come strumento di autotutela di una parte contrattuale [M. FRANZONI, *Degli effetti del contratto*[2], in *Il Codice civile. Commentario*, fondato da P. SCHLESINGER e diretto da F.D. BUSNELLI, 1, Milano, Giuffrè, 2013, 378; C.M. BIANCA, *Diritto civile. Il contratto*[3], 3, Milano, Giuffrè, 2019, 697 s. e, per una disamina di alcune ipotesi legali di tale tipologia di recesso, V. ROPPO, *Il contratto*[2], in *Trattato di diritto privato*, a cura di G. IUDICA, P. ZATTI, Milano, Giuffrè, 2011, 519 ss.; nelle disposizioni di vigilanza, si fa espresso riferimento al diritto di recesso nel caso di esternalizzazione del trattamento del contante (Circolare n. 285/2013, Parte I, Titolo IV, Capitolo 3, Sezione IV, par. 3)]. Entrambi i rimedi sono, dunque, strumenti di reazione a possibili inadempimenti contrattuali del fornitore di servizi tecnologici. La scelta del rimedio, peraltro, non pare comportare rilevanti ricadute applicative: salvo diversa pattuizione delle parti, nei contratti a esecuzione continuata e periodica è fatto salvo l'effetto delle prestazioni già eseguite ai sensi degli artt. 1373, secondo comma, c.c. e 1458, primo comma, c.c. (in dottrina, inoltre, si ritiene applicabile direttamente l'art. 1458, primo comma, c.c. anche all'ipotesi di recesso previsto per inadempimento lieve: M. FRANZONI, *cit.*, 379). In tema, v. G. SICCHIERO, *La risoluzione per inadempimento*, in *Il Codice civile. Commentario*, fondato da P. SCHLESINGER e diretto da F.D. BUSNELLI, Milano, Giuffrè, 2007, 379, là dove sostiene che – salvo nel caso di contratti plurilaterali – la differenza tra recesso per ipotesi predeterminate di inadempimento e clausola risolutiva espressa è solamente formale.

osservato in precedenza (*supra*, n. 7), anche la fase rimediale risulta governata dai canoni di continuità e qualità del servizio, orientando l'appropriata selezione delle misure correttive. Il dovere per la banca di assicurare la continuità del servizio suggerisce di considerare l'esercizio di rimedi demolitori come *extrema ratio* rispetto a quelli che consentono la conservazione del rapporto contrattuale con il fornitore di servizi IT [91].

Tale esito ermeneutico è confermato da alcuni indici normativi. Anzitutto, si prevede che l'autorità di vigilanza competente possa richiedere alla banca di cessare l'accordo solo dopo aver considerato l'esigenza dell'ente di «operare su base continuativa» e aver valutato l'inefficacia di altri mezzi per la risoluzione delle carenze o delle violazioni identificate (Orientamenti EBA, par. 118). In maniera coerente, il Regolamento DORA consente alle autorità competenti di richiedere alle banche di sospendere o cessare la fornitura di servizi tecnologici solo «come misura di ultima istanza» (art. 42, sesto par., Regolamento DORA). Una qualche gradazione tra gli strumenti di reazione esercitabili dalla banca è poi segnalata dal fatto che il Regolamento DORA – innovando il quadro normativo precedente – impone ai contratti di *outsourcing* di prevedere la possibilità per la banca di risolvere il contratto solo in casi gravi, ovvero quando vi siano una «rilevante violazione» della disciplina (normativa o contrattuale) applicabile o «modifiche di rilievo che incidano sull'accordo o sulla situazione» del fornitore di servizi tecnologici (art. 28, settimo par., Regolamento DORA). Nel regime normativo sulla sub-esternalizzazione di funzioni, analogamente, gli Orientamenti EBA impongono alle banche di risolvere il contratto quando la pratica adottata dal fornitore di servizi possa comportare «effetti negativi rilevanti sull'accordo di esternalizzazione di una funzione essenziale o importante o (…) un aumento sostanziale del rischio» (Orientamenti EBA, par. 80). La soluzione ricostruita, peraltro, pare seguire la medesima logica della lettura che, nell'ordinamento civilistico, consente di sindacare l'esercizio di una clausola risolutiva espressa quando l'inadempimento dell'altra parte non raggiunga la soglia dell'effettività alla luce dell'obbligo di eseguire il contratto secondo buona fede [92].

---

[91] Seppure nell'articolazione di un caso esemplificativo, sostengono che «[o]f course, it [the supervisor] may ban the outsourcing bank from retaining its relationship with a delinquent outsourcee, but that may be too drastic or too untimely a solution compared to a scenario in which the outsourcee is fully within the regulatory perimeter»: L. ENRIQUES, W.-G. RINGE, *Bank-Fintech Partnerships, Outsourcing Arrangements and the Case for a Mentorship Regime* (August 2020). ECGI – *Law Working Paper* N° 572/2020, reperibile al seguente indirizzo: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3625578#, 12.

[92] Nella giurisprudenza di legittimità, si è affermato che la buona fede può assurgere a «criterio di valutazione (…) del conseguente legittimo esercizio del potere unilaterale» e che l'«inadempimento all'obbligazione, contrattualmente previsto come integrativo del potere di provocare in via potestativa la risoluzione del contratto, deve essere (…) effettivo»: così Cass. civ., 23 novembre 2015, n. 23868, in *Contr.*, 661, con nota di F. PIRAINO. In termini analoghi, di recente, v.

Né la conclusione dovrebbe mutare per la presenza di mezzi astrattamente capaci di assicurare la continuità del servizio anche in caso di cessazione. Ad esempio, gli strumenti contenuti nei piani di continuità operativa [93] [= «facilitare il trasferimento della funzione esternalizzata a un altro fornitore», reintegrare la funzione all'interno dell'ente [94], nonché imporre l'adozione di strategie di uscita idonee ad evitare qualsiasi interruzione dell'attività di impresa [95]] possono comunque risultare problematici per la banca e avere impatti sulla continuità del servizio [96]. Quando l'attività del fornitore è perfettamente integrata nella realtà aziendale, la scelta di un *outsourcer* diverso potrebbe risultare molto costosa in termini di puntuale comprensione della tecnologia fornita [97] e perdita dei benefici derivanti dal

Cass. civ., 23 marzo 2023, n. 8282, in *Dejure*, che, riprendendo il precedente citato, sostiene che «qualora il comportamento del debitore, pur integrando il fatto contemplato dalla suddetta clausola, appaia comunque conforme al criterio della buona fede, non sussiste l'inadempimento, né i presupposti per invocare la risoluzione, dovendosi ricondurre tale verifica non [al] requisito soggettivo della colpa, ma quello, oggettivo, della condotta inadempiente». In dottrina, V. ROPPO, (nt. 90), 905, secondo cui qualora le parti prevedano una clausola risolutiva espressa è «escluso il sindacato giudiziale sull'importanza che l'obbligazione inadempiuta ha nell'economia del contratto; ma *non anche quello sull'entità della lesione che l'obbligazione abbia ricevuto*» e M.G. CUBEDDU, *L'importanza dell'inadempimento*, Torino, Giappichelli, 1995, 168 ss., che – ritenendo applicabile il principio ricavabile dall'art. 1455 c.c. anche alla clausola risolutiva espressa – osserva come l'autonomia delle parti non si possa «estendere fino ad affermare che qualsiasi violazione dell'obbligo preso in considerazione dalle parti, o qualsiasi scarto tra il risultato dovuto e quello realizzato legittimi la pretesa di avvalersi della clausola». Per una posizione analoga, ma meno netta e argomentata in relazione al principio di buona fede, C.M. BIANCA, *Diritto civile. La responsabilità*[2], 5, Milano, Giuffrè, 2012, 344 e, in precedenza, L. MOSCO, *La risoluzione del contratto per inadempimento*, Napoli, Jovene, 1950, 204 s., che esclude l'esistenza in capo alle parti del potere di prevedere clausole attivabili per una «inadempienza lievissima e trascurabile». Contrario a tale orientamento per il fatto che un simile modo di ragionare re-introdurrebbe la «verifica giudiziale che proprio la clausola intende evitare anche nel concreto», G. SICCHIERO, (nt. 90), 596.

[93] Così R. IZZO, (nt. 82), 95. In ambito istituzionale, sui piani di continuità operativa, cfr. EBA, (nt. 16), parr. 48 e 49 e, in generale, EBA, (nt. 34), par. 225 ss., spec. par. 227, dove si afferma che lo scopo di tale strumento è «quello di ridurre le ricadute operative, finanziarie, giuridiche, reputazionali e altre ripercussioni sostanziali derivanti da incidenti o catastrofi o da blocchi prolungati che colpiscono tali risorse, e dalla conseguente interruzione delle procedure operative ordinarie dell'ente».

[94] Così, EBA, (nt. 16), par. 99 e art. 28, ottavo par., quarto comma, Regolamento DORA. Gli orientamenti EBA, nello specifico, impongono alle parti di inserire nel contratto di esternalizzazione: (1) gli «obblighi in capo all'attuale fornitore di servizi» (lett. *a*); (2) un periodo di transizione «durante il quale il fornitore di servizi, dopo la risoluzione dell'accordo di esternalizzazione, continuerebbe a eseguire la funzione esternalizzata per ridurre il rischio di interruzioni» (lett. *b*); (3) l'«obbligo del fornitore di servizi di sostenere l'ente o l'istituto di pagamento nel trasferimento ordinato della funzione» (lett. *c*).

[95] In tema, EBA, (nt. 16), parr. 106 ss. e art. 28, ottavo par., primo comma, Regolamento DORA. Con riferimento ad alcune cautele che le banche devono adottare quando esternalizzano servizi *cloud*, BCE, (nt. 10), 13 s.

[96] Ed infatti, si fa riferimento all'esistenza del c.d. «lock-in risk», BCE, (nt. 10), 8.

[97] Sul punto, BCE, (nt. 10), 8, secondo cui «[c]oncentration risks are generally exacerbated by a

coordinamento della stessa con la struttura aziendale. Oppure, al termine del periodo di transizione, la banca potrebbe non aver ancora individuato un nuovo fornitore di servizi IT che rispetti gli *standard* normativi. Possono infine ricorrere ipotesi in cui l'*outsourcer* – grazie al proprio potere contrattuale – si opponga all'introduzione nel contratto di esternalizzazione di specifiche clausole volte a consentire alla banca un'ordinata transizione verso una diversa organizzazione del servizio interessato.

Se dunque occorre scongiurare l'esercizio di rimedi drastici che comportano la cessazione dell'accordo di esternalizzazione, è altrettanto vero che il diritto di *exit* potrebbe essere paventato dalla banca come "minaccia" in grado di accrescere la propria capacità di influenzare l'*outsourcer* e reagire con strumenti differenti. In questa prospettiva, sarebbe rafforzata l'efficacia del potere in capo all'ente vigilato di formulare indicazioni operative nei confronti del fornitore. L'ammissibilità di questo rimedio trova giustificazione nell'ampiezza delle «misure correttive» consentite dall'ordinamento europeo quando vengano individuate «carenze» nella prestazione del servizio [Orientamenti EBA, par. 105; analogamente, art. 9, quarto par., Regolamento Delegato (UE) 2024/1773]. Lo snodo particolarmente problematico riguarda gli ambiti sui quali la banca può richiedere al fornitore di attivarsi per porre rimedio alle criticità riscontrate durante il monitoraggio. Nel silenzio del diritto europeo, l'unico possibile indice normativo per risolvere la lacuna è rappresentato dai diversi ambiti sul quale possono ricadere le raccomandazioni che l'autorità di sorveglianza capofila può adottare nei confronti di fornitori di servizi IT assoggettati al regime previsto dal Regolamento DORA. A ben vedere, le indicazioni da parte dell'autorità di vigilanza europea competente ricadono tanto su elementi idonei a impattare la qualità della tecnologia fornita [98], quanto possono riguardare anche gli assetti di *governance* e organizzativi del fornitore di servizi [99]. Prendere a modello quanto previsto dal Regolamento DORA per ricostruire il confine del potere di formulare indicazioni ha il sicuro pregio di consen-

lack of knowledge about other CSPs' proprietary technology, which creates difficulties and increases the cost of switching or exiting contracts ("lock-in risk")».

[98] Gli ambiti rilevanti sono contenuti nell'art. 33, terzo par., Regolamento DORA. L'art. 35, primo par., primo comma, lett. d), infatti, rinvia a tale articolo per individuare i «settori» in relazione al quale l'autorità di sorveglianza capofila può formulare raccomandazioni al fornitore di servizi IT critici. In tale categoria, possono ricomprendersi le raccomandazioni riguardanti: (1) i requisiti «in materia di TIC» e la «capacità di mantenere *standard* … costantemente elevati» in materia di dati (lett. *a*); (2) la «sicurezza fisica» (lett. *b*); (3) i «meccanismi» di portabilità (lett. *f*); (4) l'esercizio di *test* (lett. *g*); (5) gli «*audit* in materia di TIC» (lett. *h*); (6) l'utilizzo di «pertinenti *standard* nazionali e internazionali» (lett. *i*).

[99] In questa seconda categoria, possono ricomprendersi le raccomandazioni riguardanti: (1) i «processi di gestione del rischio» (art. 33, terzo par., lett. *c*); (2) i «meccanismi di *governance*, compresa una struttura organizzativa dotata di linee e norme in materia di responsabilità chiare, trasparenti e coerenti che consentano un'efficace gestione dei rischi informatici» (art. 33, terzo par., lett. *d*).

tire alla banca il presidio di tutti i fattori che possono impattare più da vicino e con maggiore frequenza la qualità e la continuità del servizio, senza che vi siano indebite interferenze nell'autonomia privata del fornitore di servizi IT [100].

L'esito interpretativo a cui conduce l'argomentazione non va però esente da criticità. Non pare del tutto sicuro che dal punto di vista interpretativo sia consentito estendere all'intero novero dei rapporti di terza parte un frammento di disciplina rivolto alle autorità di vigilanza e orientato in ultima analisi alla protezione di interessi pubblici macro-prudenziali (la stabilità del sistema finanziario e l'integrità del mercato interno) [101]; interessi, questi, che potrebbero non riscontrarsi in una dimensione più propriamente contrattuale. La possibile obiezione, nondimeno, può perdere parte della propria forza argomentativa se si considera che le due grandezze non sono tra loro incompatibili: la soggezione degli enti vigilati al principio di sana e prudente gestione è funzionale, seppure in via indiretta, a proteggere la stabilità del sistema finanziario [102]. Ad ogni modo, muovendo verso una prospettiva *de jure condendo*, sarebbe opportuno che il legislatore disciplinasse espressamente il potere della banca di fornire indicazioni operative nei confronti dei soggetti che prestano servizi digitali a supporto di funzioni essenziali o importanti.

Dal punto di vista societario, la competenza e la responsabilità relative all'esercizio di tali rimedi correttivi seguono quanto già argomentato con riguardo alla fase di scelta (*supra*, nn. 3 e 8). Come la decisione di esternalizzare servizi IT si appunta agli amministratori o ai consiglieri della banca, anche l'esercizio di poteri che possono incidere in maniera significativa sulla scelta di affidare il servizio a una terza parte deve considerarsi rimesso a loro. Il mancato o inadeguato esercizio degli strumenti di reazione nella prospettiva dei criteri conformativi potrebbe, inoltre, fondare la responsabilità gestoria verso la società. L'inadeguato esercizio di tali poteri può rilevare almeno in una duplice ipotesi: quando non viene rispettata la "gerarchia" tra strumenti di reazione e quando le indicazioni operative ri-

[100] Tale affermazione vale in particolare nelle aree di più immediata espressione del principio di libera iniziativa economica. Sarà esclusa, per esempio, la possibilità di fornire raccomandazioni al fornitore con riferimento, per esempio, ai piani strategici o al modello di *business*.

[101] Sul punto, Considerando n. 76 Regolamento DORA: «[p]er promuovere la convergenza e l'efficienza negli approcci di vigilanza quando si affrontano rischi relativi alle TIC derivanti da terzi nel settore finanziario, nonché per rafforzare la resilienza operativa digitale delle entità finanziarie che dipendono da fornitori terzi critici di servizi TIC per la fornitura di servizi TIC che sostengono la fornitura dei servizi finanziari e contribuire così a preservare la stabilità del sistema finanziario dell'Unione e l'integrità del mercato interno per i servizi finanziari, è opportuno assoggettare i fornitori terzi critici di servizi TIC a un quadro di sorveglianza dell'Unione».

[102] Sul punto, Considerando n. 53 CRD IV, secondo cui l'assunzione di rischi eccessiva può condurre al «fallimento di singoli enti e a problemi sistemici negli Stati membri e a livello mondiale»; in dottrina, C. FRIGENI, *Le s.p.a. bancarie dopo Basilea III. Struttura patrimoniale e finanziaria*, Milano, EDUCatt, 2013, 164.

volte al fornitore trascurano ambiti particolarmente rilevanti o non contengono misure correttive idonee a ripristinare la qualità e continuità del servizio. Tali considerazioni trovano un'espressa conferma normativa nel fatto che l'organo amministrativo rimane pienamente responsabile del compito «di vigilare sulla gestione quotidiana dell'ente o dell'istituto di pagamento, compresa la gestione di tutti i rischi associati all'esternalizzazione» (Orientamenti EBA, par. 36, lett. *e*, nonché, in senso analogo, art. 5, secondo par., lett. *a*, Regolamento DORA [103]).

10. *Asimmetria di potere nell'esternalizzazione di servizi tecnologici.*

Le considerazioni svolte sinora presuppongono la possibilità di monitorare perfettamente il fornitore, potendo la banca rilevare nel continuo le criticità della fornitura di servizi IT e approntare tempestivamente i rimedi opportuni. Tuttavia, è sufficiente immaginare la difficoltà per un ente creditizio di monitorare e, successivamente, contestare il funzionamento del *software* di gestione del portafoglio fornito da un soggetto come *BlackRock* [104]. Tale esemplificazione mostra come il monitoraggio della banca si confronti con il problema dell'asimmetria di potere di cui può godere il fornitore [105], specialmente all'interno di un mercato di servizi IT particolarmente concentrato. Tale asimmetria può essere ricondotta almeno ad una triplice forma: (1) un *outsourcer* tanto influente per dimensioni e reputazione al punto di pregiudicare la capacità della banca di incidere sulla sua operatività; (2) un *outsourcer* tanto specializzato da impedire alla banca una sostituzione agevole; (3) un *outsourcer* tanto integrato nei sistemi operativi perché la banca possa supplire a tale fornitura. In questi casi, la banca potrebbe trovare difficoltà ad effettuare in maniera adeguata il monitoraggio [106] oppure a "farsi rispettare" e assicura-

[103] Nelle fonti secondarie, analogamente, Considerando n. 6 Regolamento Delegato (UE) 2024/1773.

[104] I *software* di gestione del portafoglio creati da *Black Rock* sono esternalizzati con grande frequenza. In tema, R.P. BUCKLEY ET AL., *The Dark Side of Digital Financial Transformation: The New Risks of Fintech and the Rise of TechRisk* (5 November 2019). *EBI Working Paper Series* no. 54, reperibile al seguente indirizzo: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3478640, 30 s.

[105] Cfr., per tutti, EXPERT GROUP ON REGULATORY OBSTACLES TO FINANCIAL INNOVATION (ROFIEG), *30 Recommendations on Regulation, Innovation and Finance* (13 December 2019), reperibile al seguente indirizzo: https://finance.ec.europa.eu/publications/final-report-expert-group-regulatory-obstacles-financial-innovation-30-recommendations-regulation_en, 46, secondo cui «the oligopolistic structure of the market combined with the technological dependency of regulated financial institutions on their service providers … may reverse the traditional power relationship between principal (the outsourcing financial institution) and agent (the service provider)».

[106] In particolare, secondo BCE, (nt. 10), 14, «[i]n many cases, CSPs do not provide sufficient detail about their infrastructure processes and their internal control systems, with the result that institutions often lack detailed first-hand knowledge of the CSP's premises, information systems, pro-

re la continuità e la qualità del servizio. In altri termini, la banca si attiva per adempiere ai propri obblighi, ma si inserisce un fattore esterno (= il potere negoziale dell'*outsourcer*) che, da un lato, impedisce di monitorare il fornitore o dare seguito alle risultanze del controllo e, per altro verso, conduce ad approdi incerti in tema di responsabilità degli amministratori e consiglieri della banca per l'inefficacia dell'attività di controllo svolta [107].

Tali osservazioni aiutano a comprendere le ragioni per cui la mitigazione dei rischi associati all'esternalizzazione di servizi IT non possa prescindere da un efficace regime di *enforcement* pubblico, tanto nella sua accezione di potere di vigilanza, quanto nella forma di apparato sanzionatorio. Il danno causato dall'inefficace condotta della banca sarebbe infatti destinato a impattare sulla tenuta dell'ente vigilato e a trasmettersi ai clienti. In questo modo, la stabilità del sistema finanziario e, in particolare, la fiducia dei depositanti potrebbero essere compromessi o quantomeno inficiati.

11. *L'*enforcement *di natura pubblica.*

A fronte dell'esigenza di contrastare la predetta asimmetria di potere, l'inferiorità contrattuale della banca attribuisce importanza alla previsione di poteri di vigilanza, capaci di incidere effettivamente sulla condotta del fornitore. Tuttavia, l'attuale ordinamento configura un modello di vigilanza c.d. indiretto, poiché i poteri assegnati all'autorità competente possono essere esercitati esclusivamente nei confronti della banca e, per il tramite di essa, riflettersi sulla condotta del fornitore.

Infatti, l'esercizio dei poteri informativi [108] e ispettivi [109] verso l'*outsourcer*

---

prietary technology, sub-providers and contingency plans, as the majority of entities rely solely on the CSP's statements and third-party certifications».

[107] In questo caso, per comprendere quando il fatto è imputabile è necessario fare una distinzione. Se nel mercato – al momento della scelta – erano presenti fornitori in grado di prestare un servizio IT con adeguato livello di qualità e continuità, ma con potere economico inferiore rispetto al fornitore prescelto, l'inefficacia del monitoraggio può essere imputata alla banca poiché frutto di una valutazione in spregio ai criteri conformativi della disciplina in materia di esternalizzazione. In caso di mercato altamente concentrato e con fornitori molto influenti, la soluzione al quesito potrebbe dipendere dalla teoria seguita riguardo all'imputabilità dell'impossibilità di adempiere *ex* art. 1218 c.c. al debitore. In tale fattispecie, la banca potrebbe andare esente da responsabilità solo se si aderisse alle tesi soggettivistiche o, comunque, dirette, secondo varie modalità, ad attenuare gli esiti delle teorie oggettive pure o fondate sul rischio di impresa. Per una puntuale illustrazione delle varie posizioni e gli opportuni riferimenti dottrinali, A. NICOLUSSI, *Le obbligazioni*, Padova, Cedam, 2022, 132 ss.; G. VISINTINI, *Inadempimento e mora del debitore*[2], in *Il Codice civile. Commentario*, fondato da P. SCHLESINGER e diretto da F.D. BUSNELLI, Milano, Giuffrè, 2006, 94 ss.

[108] Art. 65, terzo par., lett. *a*), CRD IV e, nell'ordinamento italiano, artt. 51, primo comma-*quinquies*, t.u.b. e 53-*bis*, secondo comma, t.u.b.

[109] Art. 65, terzo par., lett. *b*) e *c*), CR IV e, nell'ordinamento italiano, art. 54, primo comma,

consente all'autorità di acquisire una maggior cognizione di causa del rapporto di esternalizzazione, in modo da indicare alla banca le misure correttive da apportare sulla propria struttura organizzativa e patrimoniale [110] oppure richiedere l'esercizio di rimedi nei confronti del fornitore di servizi IT [111]. Nel caso di inadempi-

t.u.b. L'accordo di esternalizzazione deve fornire all'autorità di vigilanza il diritto di ispezione e *audit* verso il fornitore [EBA, (nt. 16), par. 75, lett. *p*].

[110] L'autorità di vigilanza competente può imporre all'ente vigilato l'adozione di interventi correttivi nell'ambito dello SREP (art. 97 ss. CRD IV; per una completa disamina del processo, M. Lamandini, R. D'Ambrosio, D. Ramos Muñoz, *Supervisory Review and Evaluation Process (SREP) in the Context of the Exercise of Supervisory Powers and Extraordinary Measures*, reperibile al seguente indirizzo: https://www.lamandini.org/images/pdf/articles/2021-2025/174_Srep.pdf, 6 ss.; con particolare riferimento agli ambiti oggetto di verifica da parte dell'autorità di vigilanza e al possibile contenuto della c.d. *SREP decision*, P. Lucantoni, SREP decision *e (in)dipendenza nella* governance *bancaria*, in *AGE*, 2022, 543 ss.). Il perimetro di intervento della vigilanza nell'ambito dello SREP è molto ampio e spazia dalla richiesta di incrementare il capitale [EBA, *Orientamenti sulle procedure e sulle metodologie comuni per il processo di revisione e valutazione prudenziale (SREP) e sulle prove di stress di vigilanza* (18 marzo 2022), reperibile al seguente indirizzo: https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/supervisory-review-and-evaluation-process-srep-4, parr. 366 ss. e 423 ss. e Circolare 285/2013, Parte Prima, Titolo III, Cap. 1, Sez. V, par. 5] all'indicazione di ridurre il rischio di terza parte attraverso il miglioramento dei «meccanismi di *governance* e controllo», nonché della «supervisione di attività esternalizzate» (EBA, *cit.*, par. 553, lett. *c*). Infine, una misura specifica relativa all'argomento oggetto di indagine e particolarmente rilevante per il suo impatto in termini di presidi organizzativi da adottare è il potere di richiedere alla banca di classificare una funzione esternalizzata quale essenziale o importante, con la conseguente applicazione del regime normativo più severo previsto dalla regolamentazione europea [v. come fonte l'obbligo dell'*audit* di verificare la correttezza della valutazione di essenzialità e importanza: EBA, (nt. 16), par. 51, lett. *b*]. A questo scopo, un'importante base informativa per l'autorità di vigilanza competente è rappresentata dal registro ove le banche devono detenere tutte le informazioni sugli accordi di esternalizzazione in essere [EBA, (nt. 16), par. 52 ss. e, in particolare, par. 54, lett. *b*], che impone di indicare per qualsiasi rapporto contrattuale una «breve descrizione della funzione esternalizzata». La normativa europea prevede poi che gli «enti e gli istituti di pagamento dovrebbero, su richiesta, mettere a disposizione dell'autorità competente il registro completo di tutti gli accordi di esternalizzazione in corso o sezioni specificate di esso» [EBA, (nt. 16), par. 56]. Sulla scorta di tale prerogativa, la Banca d'Italia ha emanato le "*Istruzioni per la segnalazione in materia di esternalizzazione di funzioni aziendali per gli intermediari vigilati*" il 31 maggio 2023 e le relative note di chiarimenti il 18 aprile 2024. La tenuta del registro da parte delle banche è prevista anche dall'art. 28, terzo par., Regolamento DORA e, tra le fonti secondarie, v. Joint Committee of the ESAs, *Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554* (10 January 2024), reperibile al seguente indirizzo: https://service.betterregulation.com/document/702885.

[111] L'autorità di vigilanza competente può «adottare misure appropriate», tra cui imporre alla banca di «limitare» il ricorso all'esternalizzazione di funzioni, «restringere» la platea delle attività affidate a un fornitore o, addirittura, «porre a termine» uno o più contratti di esternalizzazione [EBA, (nt. 16), par. 118]. Come già visto per gli esiti dell'attività di monitoraggio condotta dalla banca, anche con riguardo alla vigilanza i rimedi che comportano la cessazione del contratto sono da considerare residuali e l'esercizio del potere di richiedere alla banca di formulare indicazioni mirate (riconducibile alle generiche «misure appropriate») verso i fornitori di servizi IT è da considerare prioritaria.

mento delle indicazioni pubbliche senza adeguata motivazione nella prospettiva dei criteri conformativi in materia di *outsourcing*, l'autorità di vigilanza competente potrà impiegare i propri strumenti di reazione verso gli amministratori e i consiglieri della banca quali, ad esempio, i poteri di intervento previsti dall'art. 53-*bis*, primo comma, t.u.b.

Anche la potestà sanzionatoria vede come destinatari principali la banca e, in determinati casi, gli esponenti e il personale. Nel quadro normativo italiano, tale considerazione vale nonostante il potere in capo all'autorità competente di irrogare una sanzione amministrativa *ex* art. 144, primo comma, t.u.b. [112] a coloro ai «quali sono state esternalizzate funzioni aziendali» o «funzioni aziendali essenziali o importanti» per la violazione delle disposizioni da esso indicate [113]. Benché preveda un perimetro particolarmente ampio, infatti, tale previsione non deve essere interpretata nel senso che la potestà sanzionatoria sia diretta a punire la condotta del fornitore per la prestazione dei propri servizi IT. Appare inevitabile affermare che quest'ultimo non è un soggetto sottoposto a vigilanza pubblica e, per conseguenza, non può essere destinatario di alcun obbligo che legittimi la sanzione comminata. In questi termini, la sanzione può essere irrogata soltanto per ipotesi di ostacolo alla vigilanza, dove si materializza una violazione del dovere del fornitore di servizi IT di collaborare quando l'autorità di vigilanza eserciti nei suoi confronti poteri informativi [114], ispettivi [115] e di intervento [116].

In un tale contesto in cui l'asimmetria di potere è destinata a permanere, la preoccupazione che l'assenza di un regime sanzionatorio diretto nei confronti del fornitore di servizi IT possa pregiudicare la stabilità della banca e del sistema finanziario non è rimasta sconosciuta al legislatore europeo. Infatti, quest'ultimo ha deciso di articolare il sistema di vigilanza secondo un trattamento differenziato: in un'ottica micro-prudenziale (disciplinata dagli Orientamenti EBA), continua a valere il modello di vigilanza indiretta; in chiave macro-prudenziale, il Regolamento DORA prevede un inasprimento del regime di *enforcement* con riguardo ai fornitori il cui potere negoziale e la rilevanza sistemica finirebbero per precludere l'efficacia del tradizionale assetto di supervisione (c.d. «fornitore terzo *critico*» di

[112] Per una generale disamina dell'impianto sanzionatorio nell'ambito dell'esternalizzazione di funzioni, D. VARANI, *La gestione dei rapporti con le autorità di vigilanza*, in *L'Outsourcing nei servizi bancari e finanziari*, a cura di S. CASAMASSIMA, M. NICOTRA, Padova, Cedam, 2021, 202 ss.

[113] Il *quantum* della sanzione varia a seconda della qualifica del fornitore: nel caso di funzioni essenziali o importanti, la sanzione pecuniaria si applica «fino al massimale di euro 5 milioni ovvero fino al 10 per cento del fatturato»; negli altri casi, la sanzione pecuniaria è inferiore e si applica «da euro 30.000 fino al 10 per cento del fatturato» (art. 144, primo comma, t.u.b.).

[114] Art. 51-*quinquies*, primo comma, t.u.b.

[115] Art. 54, primo comma, t.u.b.

[116] Art. 53-*bis*, primo comma, lett. *a*) e secondo comma, t.u.b.

servizi IT [117]). Anzitutto, l'autorità di vigilanza capofila viene incaricata di sorvegliare ciascun fornitore critico di servizi IT e valutare se «abbia predisposto norme, procedure, meccanismi e accordi esaustivi, solidi ed efficaci per gestire i rischi informatici cui esso può esporre le entità finanziarie» (art. 33, secondo par., primo comma, Regolamento DORA). A questo scopo, l'autorità viene investita di un ampio potere di «formulare raccomandazioni» contenenti la condotta pretesa direttamente al fornitore (art. 35, primo par., lett. *c* e *d*, Regolamento DORA) e quest'ultimo ha il dovere di cooperare in buona fede [118]. Per assicurare l'effettività di tale prerogativa, il legislatore europeo ha introdotto una penalità di mora in caso di mancata comunicazione delle relazioni «in cui si [specificano] le azioni adottate o i rimedi applicati» (art. 35, primo par., lett. *c*, Regolamento DORA) nell'arco di trenta giorni dalla loro notifica; in questo caso, l'ammontare della penalità [119] è «imposta su base giornaliera» fino al ripristino della conformità, per un periodo non superiore a sei mesi e per un importo «fino all'1% del fatturato medio quotidiano realizzato a livello mondiale» dal fornitore critico nel precedente esercizio (art. 35, sesto, settimo e ottavo paragrafo, Regolamento DORA) [120]. La

[117] Cfr. art. 3, punti 23 e 31, Regolamento DORA. A differenza del fornitore di funzioni essenziali e importanti, che è ritenuto tale secondo una valutazione compiuta dalla banca [EBA, (nt. 16), parr. 29, 30 e 31], il fornitore è designato come critico sulla base di soglie quantitative e indicatori di natura qualitativa [sul punto, JOINT EUROPEAN SUPERVISORY AUTHORITIES, *Technical Advice to the European Commission's December 2022. Call for Advice on two delegated acts specifying further criteria for critical ICT third-party service providers (CTPPs) and determining oversight fees levied on such providers* (29 September 2023), reperibile al seguente indirizzo: https://www.esma.europa.eu/document/joint-esas-technical-advice-two-ec-delegated-acts-under-digital-operational-resilience-act; Regolamento Delegato (UE) 2024/1502]. All'esito di tale valutazione, l'Autorità redige per il *forum* di sorveglianza una lista provvisoria degli *outsourcer* IT critici (art. 32, quarto par., Regolamento DORA). Il *forum* di sorveglianza, a sua volta, deve effettuare una raccomandazione al comitato congiunto delle ESAs a cui spetta la decisione finale (art. 31, primo par., Regolamento DORA).

[118] Cfr. art. 35, quinto par., Regolamento DORA, secondo cui i «fornitori terzi critici di servizi TIC cooperano in buona fede con l'autorità di sorveglianza capofila e la coadiuvano nell'adempimento dei suoi compiti».

[119] I criteri in forza del quale l'autorità di sorveglianza capofila determina il *quantum* della penalità di mora giornaliera sono: «a) la gravità e la durata dell'inosservanza; b) se l'inosservanza sia stata commessa intenzionalmente o per negligenza; c) il livello di cooperazione del fornitore terzo di servizi TIC con l'autorità di sorveglianza capofila» (art. 35, ottavo par., primo comma, Regolamento DORA). L'assenza di un meccanismo di parametrazione della sanzione al fatto del fornitore di Servizi IT critico aveva sollevato notazioni critiche da parte della dottrina: così S. KOURMPETIS, *Management of ICT Third Party Risk Under the Digital Operational Resilience Act*, in *Digitalisation, Sustainability, and the Banking and Capital Markets Union*, edited by L. BÖFFEL, J. SCHÜRGER, Cham, Palgrave Macmillan, 2023, 22; H.S. SCOTT, *The E.U.'s Digital Operational Resilience Act: Cloud Services & Financial Companies* (August 2021), reperibile al seguente indirizzo: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3904113, 22.

[120] Inoltre, ad eccezione dell'ipotesi in cui ciò possa «mettere a rischio i mercati finanziari o possa arrecare un danno sproporzionato», l'autorità di vigilanza europea competente è tenuta a comunicare al pubblico tutte le penalità di mora inflitte: art. 35, decimo par., Regolamento DORA.

sanzione alla mancata dichiarazione dell'«intenzione di attenersi alle raccomandazioni» o all'insufficiente motivazione del discostamento dalle indicazioni fornite è di natura reputazionale: l'autorità di sorveglianza capofila è infatti tenuta a rendere pubblici tali casi, rivelando l'«identità del fornitore … nonché [le] informazioni sul tipo e la natura dell'osservanza» (art. 42, secondo par., primo comma, Regolamento DORA).

Il regime di *enforcement* costruito dal legislatore europeo è frutto di una opzione politica significativa, poiché allarga i confini della vigilanza a soggetti che tradizionalmente non sono sottoposti a sorveglianza pubblica. Il tentativo di superare il problema posto dall'asimmetria di potere nell'ambito del mercato dei servizi IT è condivisibile [121], con un solo *caveat*: la sanzione reputazionale non pare sufficiente a "vestire" le raccomandazioni di un elevato effetto deterrente; in una prospettiva *de jure condendo*, il legislatore europeo potrebbe prevedere espressamente l'imposizione della penalità di mora anche per il mancato rispetto delle indicazioni formulate dall'autorità di sorveglianza capofila. L'attività di vigilanza, infine, non può eccedere nella misura, arrivando sino a conformare le caratteristiche del fornitore alla stregua dei soggetti tradizionalmente vigilati. Per questa ragione, nello svolgere il monitoraggio sull'*outsourcer* e nel formulare le raccomandazioni, l'autorità di vigilanza competente è soggetta a un limite: dovrà considerare le caratteristiche del fornitore e proporre soluzioni che considerino le specificità del *business* e della struttura organizzativa di tali imprese, senza prendere a modello l'organizzazione aziendale e societaria delle imprese di natura finanziaria [122].

12. *L'*enforcement *di natura privata.*

La responsabilità civile del fornitore di servizi IT potrebbe giocare un ruolo significativo per il perseguimento delle finalità di tutela del Regolamento DORA, poiché potrebbe incentivarlo ad adottare le cautele necessarie affinché venga evitata ad un costo ridotto la realizzazione di danni particolarmente rilevanti [123]. In

[121] Pur con tono dubitativo, M. RABITTI, Credit scoring *via* machine learning *e prestito responsabile*, in *Riv. dir. banc.*, 2023, I, 186.

[122] Il fatto che le politiche di gestione dei rischi del fornitore, per esempio, non prevedano la possibilità per il soggetto responsabile del *risk management* di mettere in discussione le decisioni degli amministratori [EBA, (nt. 34), par. 202] non dovrebbe considerarsi quale criticità e la sua risoluzione non può essere oggetto di raccomandazione.

[123] Il fornitore di servizi è il c.d. *cheapest cost avoider* (sul quale, è d'obbligo il riferimento a G. CALABRESI, *The Costs of Accident: a Legal and Economic Analysis*, New Haven-London, Yale University Press, 1970, 135 ss.): pare innegabile che l'ammontare delle risorse necessarie per risolvere, ad esempio, un difetto di programmazione sia di gran lunga inferiore alle perdite subite dai clienti delle banche coinvolte dallo scandente funzionamento o dall'interruzione del servizio. Per

questi termini, tale meccanismo di *enforcement* pare idoneo a svolgere una funzione complementare rispetto al regime di vigilanza diretto introdotto dall'intervento normativo europeo.

Il *framework* europeo, per la verità, ruota attorno al principio cardine della responsabilità della banca per il rispetto di tutte le regole ad essa applicabili, a prescindere dalle tecniche con il quale viene articolato il proprio processo produttivo. Tale aspetto, già presente negli Orientamenti EBA [124] ha ricevuto palese conferma in ambito tecnologico nel Regolamento DORA: le «entità finanziarie … rimangono sempre pienamente responsabili del rispetto e dell'adempimento di tutti gli obblighi previsti dal presente regolamento e dalla normativa applicabile in materia di servizi finanziari» (art. 28, primo par., lett. *a*, Regolamento DORA) [125]. Il corollario di tale principio è che l'affidamento di servizi IT al di fuori dell'organizzazione aziendale non può in alcun modo rappresentare un mezzo attraverso il quale la banca trasferisce in capo al fornitore la formale imputazione delle regole imposte dal diritto bancario e dal diritto del mercato dei capitali [126]. Tale esito, del resto, non è per nulla sorprendente poiché discenderebbe anche dall'applicazione delle regole previste nel codice civile. Come sostenuto in dottrina, l'affidamento a terzi di una fase dell'impresa per l'adempimento delle obbligazioni assunte verso i clienti è riconducibile alla previsione dell'art. 1228 c.c. [127], secondo cui il «debi-

---

l'affermazione che «[i]n the case of a machine or device that comes as an integrated and closed system of hard- and software, the manufacturer is not only the cheapest cost avoider but the only party in a position to take precautions at all. This suggests that the focus of the liability system must be on the manufacturer»: G. WAGNER, *Robot Liability* (2018), reperibile al seguente indirizzo: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3198764, 10.

[124] Sul punto, v. EBA, (nt. 16), par. 35, secondo cui l'«esternalizzazione di funzioni non può comportare la delega delle responsabilità dell'organo di amministrazione. Gli enti e gli istituti di pagamento restano pienamente responsabili del rispetto di tutti i loro obblighi normativi, compresa la capacità di vigilare sull'esternalizzazione di funzioni essenziali o importanti».

[125] Per l'applicazione di tale principio nella giurisprudenza dell'ABF, Collegio di Napoli, 18 maggio 2011, decisione n. 1044, 4.

[126] Sul punto, A. GUACCERO, (nt. 17), 61 e, in senso analogo, L. SPITALERI, (nt. 16), 138.

[127] Così M. MAUGERI, (nt. 3), 455 s., secondo cui la ricorrenza della fattispecie prevista dall'art. 1228 c.c. prescinde dalla «natura del rapporto giuridico intercorrente tra debitore e ausiliario, può investire fasi o momenti meramente preparatori o preliminari della prestazione principale e, soprattutto, presuppone l'*estraneità* dell'ausiliario al vincolo obbligatorio per il cui adempimento ed esecuzione è richiesta la sua collaborazione». Tali elementi e l'esclusione da parte del legislatore di qualsiasi eccezione al principio di responsabilità della banca per il corretto svolgimento delle attività affidate al terzo conducono all'impossibilità di ricondurre la fattispecie in esame all'ipotesi contemplata dall'art. 1717 c.c., che, invece, prevede la responsabilità del mandatario solo in caso di colpa nella scelta del proprio sostituto. Per un'analoga qualificazione della fattispecie, seppure nell'ambito della gestione automatizzata del portafoglio, LINCIANO ET AL., (nt. 2), 68 e, con riferimento alla consulenza digitalizzata, CONSOB, *La digitalizzazione della consulenza in materia di investimenti finanziari* (gennaio 2019), reperibile al seguente indirizzo: https://www.consob.it/web/area-pubblica/ft3, 90.

tore che nell'adempimento dell'obbligazione si vale dell'opera di terzi, risponde anche dei fatti dolosi o colposi di costoro».

Nel silenzio della normativa, il principio di responsabilità non esclude che quando il fatto è imputabile – in tutto o in parte – all'*outsourcer* possa insorgere un inadempimento del contratto stipulato con la banca [128]. In tale caso, quest'ultima sarà abilitata a recuperare nei confronti del fornitore i danni subiti e le somme versate ai clienti a titolo di risarcimento del danno o all'autorità di vigilanza quando l'inesatta o interrotta esecuzione del servizio abbia comportato una violazione rilevante per il diritto pubblico.

Tale conclusione trova una duplice conferma. In letteratura, la dottrina civilistica contempla la possibilità per il debitore di agire nei confronti dell'ausiliario per l'inadempimento dell'eventuale contratto dagli stessi stipulato [129]. Nell'ordinamento finanziario europeo, viene in rilievo la scelta compiuta dal legislatore con la Direttiva (UE) 2015/2366 sui servizi di pagamento (d'ora in poi, "PSD2"). All'interno dell'articolato regime di responsabilità del prestatore dei servizi di pagamento, si attribuisce espressamente in favore di quest'ultimo una pretesa risarcitoria verso un diverso prestatore di servizi di pagamento o intermediario a cui sia imputabile l'inadempimento relativo all'operazione di pagamento disposta dal cliente [130] (art. 92, primo par., PSD2).

Quale nota conclusiva, non si può che mostrare il nesso tra questo regime e una pratica negoziale ampiamente diffusa nella prassi. I contratti tra banca e terza parte possono prevedere che – in caso di violazione grave o reiterata del livello di servizio concordato – il fornitore sia tenuto a pagare in favore della controparte una penale in forma di deduzione dal corrispettivo pattuito per la fornitura del servizio [131]. Il *quantum* dell'eventuale azione risarcitoria della banca dovrà, dunque, essere dedotto dell'importo di eventuali somme già corrisposte dal fornitore per il mancato rispetto dei vincoli contrattuali.

---

[128] Seppure in termini dubitativi e con riferimento ad un'ipotetica azione di regresso della banca verso il fornitore, *contra*, P. De Gioia Carabellese, *I contratti di esternalizzazione dei soggetti vigilati: normativa; potere sanzionatorio delle autorità. Il provvedimento EBA in tema di* outsourcing *bancario nella filosofia del* Single Supervisory Mechanism, in *Contr. impr.*, 2019, 1073.

[129] Nella dottrina civilistica, A. D'Adda, *Ausiliari, responsabilità solidale e "rivalse"*, in *Riv. dir. civ.*, 2018, I, 373 e Id., *I rapporti interni tra debitore ed ausiliario ex art. 1228: una opportuna messa a punto (con molte luci e qualche ombra)*, in *Nuova giur. civ. comm.*, 2020, I, 348.

[130] In Italia, la disposizione di recepimento dell'art. 92, primo par., PSD 2 è l'art. 27 del d.lgs. 27 gennaio 2010, n. 11.

[131] Sul punto, R. Izzo, (nt. 82), 72.