XV CONVEGNO ANNUALE
DELL'ASSOCIAZIONE ITALIANA DEI PROFESSORI UNIVERSITARI
DI DIRITTO COMMERCIALE "ORIZZONTI DEL DIRITTO COMMERCIALE"

***"IMPRESA E MERCATI: NUMERI E* COMPUTER SCIENCE"**
Roma, 23-24 febbraio 2024

ANDREA CARDANI

DOTTORANDO DI RICERCA IN *BUSINESS AND LAW*, UNIVERSITÀ DEGLI STUDI DI BERGAMO

ISACCO GIRARDI

DOTTORANDO DI RICERCA IN IMPRESA, LAVORO, ISTITUZIONI E GIUSTIZIA PENALE - *CURRICULUM* DI DIRITTO COMMERCIALE, UNIVERSITÀ CATTOLICA DEL SACRO CUORE DI MILANO

Impresa bancaria ed esternalizzazione di servizi tecnologici

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 *player* 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 *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].

---

[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*, (2022), in *www.cipa.it*, 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, MCCAUL, *Supervising the future of banking: navigating the digital transformation*, (2023), in *www.bankingsupervision.europa.eu*.

[2] Le operazioni di fusione e acquisizione di società *FinTech* sembrano essere in costante aumento: CAMERA DEI DEPUTATI - SERVIZIO STUDI, *Fintech*, (2022), in *www.temi.camera.it*, 2. Sul punto, v. anche LINCIANO ET AL., *L'intelligenza artificiale nell'*asset *e nel* wealth management, (2020), in *www.consob.it*, 68.

[3] Nella letteratura economica, in relazione all'ambito tecnologico, DIBBERN - HIRSCHHEIM, *Introduction: Riding the Waves of Outsourcing Change in the Era of Digital Transformation*, in HIRSCHHEIM - HEINZL - DIBBERN (*edited by*), *Information Systems Outsourcing*, 2020, 2 e, in generale, MCCAHERY - DE ROODE, *Governance of Financial Services Outsourcing: Managing Misconduct and Third-Party Risks*, (2018), in *www.ecgi.global*, 2, nonché CAROLI - VALENTINO, *La strategia di* outsourcing, in *AGE*, 2011, 266 ss. Nella letteratura giuridica, tra i molti, MAUGERI, *Esternalizzazione di funzioni aziendali e "integrità" organizzativa nelle imprese di investimento*, in *Banca borsa tit. cred.*, 2010, I, 439, SACCO GINEVRI, *Esternalizzazione (*outsourcing*)*, in *Fintech: diritti, concorrenza, regole* (diretto da Finocchiaro - Falce), Bologna, 2019, 205, LEMMA - THORPE, *Sharing Corporate Governance: the Role of Outsourcing Contracts in Banking*, (2014), in *www.ssrn.com*, 378 e, con specifico riferimento alla riduzione dei costi, SCIARRONE ALIBRANDI, *Introduzione*, in CASAMASSIMA - NICOTRA (a cura di), *L'Outsourcing nei servizi bancari e finanziari*, Padova, 2021, XV, nonché CERA, *Esternalizzazioni di gestione, mandato generale e rappresentanza legale nelle società per azioni*, in *Riv. dir. priv.*, 2013, 327 s.

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 Europea ha verificato che il 48,5% delle spese sostenute dalle banche cc.dd. *significant*[6] in ambito tecnologico è da ricondurre alla pratica di affidare a terzi tali funzioni[7]. 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[8], 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*»[9]. Con particolare riferimento al *cloud computing*[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

---

Pur con un'osservazione limitata al *cloud computing*, a livello istituzionale, cfr. EUROPEAN BANKING AUTHORITY (EBA), *Report on the prudential risks and opportunities arising for institutions from fintech*, (3 luglio 2018), in *www.eba.europa.eu*, 53.

[4] In questo senso, COMMISSIONE EUROPEA, *Impact Assessment Report Accompanying the document for DORA Regulation* [SWD(2020) 198 final], (2020), in *www.eur-lex.europa.eu*, 17.

[5] EUROPEAN SUPERVISORY AUTHORITIES (ESAS), *Report on the landscape of ICT third-party providers in the EU*, (27 settembre 2023), in *www.esma.europa.eu*, 6.

[6] I parametri per qualificare una banca come *significant* sono indicati nell'art. 6, par. 4, regolamento (UE) n. 1024/2013.

[7] BANCA CENTRALE EUROPEA (BCE), *IT and cyber risk – key observations*, (15 novembre 2023), in *www.bankingsupervision.europa.eu*, 3.

[8] Il riferimento è a CIPA - ABI (nt. 1).

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

[10] Per un approfondimento sul punto, FINANCIAL STABILITY BOARD, *Third-party dependencies in cloud services. Considerations on financial stability implications*, (9 dicembre 2019), in *www.fsb.org*, 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»: ALPA, Fintech: *un laboratorio per giuristi*, in *Contratto e Impresa*, 2009, 381. Più ampiamente, il novero dei servizi tecnologici esternalizzati è enucleato da EBA (nt. 3), 12 ss.

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

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 dipendenza 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 una sostanziale rilevanza sistemica, in quanto

---

[12] CIPA - ABI, *Rilevazione sull'IT nel settore bancario italiano. Il cloud computing e le banche*, (18 luglio 2023), in *www.cipa.it*, 29.

[13] Per l'affermazione che «[l]e 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), in *www.bankingsupervision.europa.eu*, par. 5.2. In tema, v. anche la tesi di dottorato di URBANI, *I rapporti di terza parte nel governo delle banche: rischi, regolazione e "frammentazione" dell'assetto*, (2022), in *www.orizzontideldirittocommerciale.it*, 37. Per una generale enunciazione delle diverse categorie di rischio associate all'*outsourcing*: BASEL COMMITTEE ON BANKING SUPERVISION (BCBS), *Outsourcing in Financial Services*, (febbraio 2005), in *www.bis.org*, 11 s.

[14] L'art. 85, par. 1, 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, *Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process* (*SREP*), (11 settembre 2017), in *www.eba.europa.eu*, 4.

[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), URBANI (nt. 13), 35 ss.

[16] Sulle due prospettive del rischio di concentrazione, cfr. EBA, *Orientamenti*, par. 66, lett. a) e art. 29, par. 1, Regolamento DORA e par. 116, lett. e). Con riferimento all'ultimo aspetto, cfr. Considerando n. 31, Regolamento DORA. Ponendo l'accento sulla natura macro-prudenziale del rischio di concentrazione, 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*

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 normativi[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

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 (nt. 4), 18. Nella dottrina, v. SCHNEIDER, *La resilienza operativa digitale come materia di corporate governance: prime riflessioni a partire dal DORA*, in *Rivista* Corporate Governance, 2022, 556. Seppure con considerazioni prospettiche, in termini generali, v. GUACCERO, *Automazione dei processi e dei servizi, imputazione e responsabilità*, in CIAN - SANDEI (a cura di), *Diritto del Fintech*, Padova, 2020, 63, secondo cui «[l]o 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 (CEBS), *Guidelines on Outsourcing*, (14 dicembre 2006), in *www.eba.europa.eu* [per un'analisi sistematica di tale documento: LEMMA - THORPE (nt. 3), 378 ss.]; successivamente, EBA, *Raccomandazioni in materia di esternalizzazione a fornitori di servizi* cloud, (28 marzo 2018), in *www.eba.europa.eu*. Per l'affermazione che tali documenti costituiscono il fondamento degli attuali Orientamenti EBA: CAPRIGLIONE - SACCO GINEVRI, *Metamorfosi della* governance *bancaria*, Torino, 2019, 223 s.

[19] Le disposizioni di vigilanza sulle banche attribuiscono efficacia vincolante alle regole contenute negli Orientamenti EBA 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, *Orientamenti*, 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., 2 ottobre 2006, n. 21287; 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 CAVALLARO, *L'esternalizzazione della funzione di* compliance*: riparto di responsabilità tra l'intermediario e l'*outsourcer]. 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, *Orientamenti*, 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, *Orientamenti*, 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

European Banking Authority (d'ora in poi, "Orientamenti EBA"). Da ultimo, il legislatore europeo ha deciso di introdurre un quadro normativo specificamente dedicato all'affidamento di servizi IT con il Regolamento (UE) 2022/2554[20] (d'ora in poi, "Regolamento DORA").

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 i relativi atti di esecuzione, la sua entrata in vigore e l'imminente applicazione 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.

Orientamenti EBA e focalizzata sull'esternalizzazione da parte degli intermediari finanziari, MAUGERI (nt. 3), 440 ss.

[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 dagli Orientamenti EBA, 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 dagli Orientamenti EBA 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.

2.1 *La competenza*

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 285/2013 adottata da Banca d'Italia. Infatti, nell'ambito delle strategie aziendali, l'organo con funzione di supervisione strategica (= il consiglio di amministrazione nel sistema tradizionale) 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, par. 1, punto 22, Regolamento DORA). Si pensi, per esempio, a tecniche di automazione impiegate per l'esecuzione delle segnalazioni di vigilanza[22] o per la determinazione dei requisiti di capitale.

In questo quadro normativo, l'assetto di competenze viene dunque a differenziarsi a seconda della tipologia di funzione esternalizzata: (1) 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[23]; diversamente, (2)

[22] Così BANCA D'ITALIA, *Nota di chiarimenti sul sistema dei controlli interni, il sistema informativo e la continuità operativa*, (2014), in *www.bancaditalia.it*, 13, riportata anche in FALCONE, *Profili problematici dell'esternalizzazione di funzioni ed attività "tipiche" da parte degli intermediari del mercato finanziario*, in LENER - LUCHENA - ROBUSTELLA (a cura di), *Mercati regolati e nuove filiere di valore*, 2021, 285, nt. 24.

[23] Seppure in termini generali, cfr. CERA (nt. 3), 334.

nelle altre ipotesi, la scelta e la gestione relativa all'accordo di esternalizzazione deve essere rimessa agli amministratori con deleghe[24] (quando presenti[25]), coadiuvati dalle rilevanti funzioni aziendali.

2.2 *Scelta informata e valutazione del rischio*

In termini generali, il primo compito richiesto agli amministratori di banca in sede di scelta consiste nell'assunzione degli elementi su cui fondare la decisione di esternalizzare. In proposito, i membri dell'organo gestorio devono confrontarsi con un paradigma di amministratore informato ampiamente dettagliato dal Regolamento DORA e dagli Orientamenti EBA[26]. Infatti, tale quadro normativo specifica i fattori che gli amministratori devono prendere in considerazione «prima di stipulare l'accordo contrattuale»: (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

[24] La chiarezza della Circolare 285/2013 aiuta dunque a interpretare il testo ambiguo degli orientamenti EBA, ove sembrano condizionare ad eventualità il coinvolgimento del consiglio di amministrazione con riferimento alle funzioni essenziali o importanti («se del caso»: EBA, *Orientamenti*, par. 42, lett. *a*). In tema v. anche EBA, *Orientamenti*, 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, v. 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»: URBANI (nt. 13), 230.

[25] Infatti, con riferimento alle «banche di minor complessità» 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 di un servizio o una funzione: MAUGERI (nt. 3), 460.

[26] In applicazione dell'art. 28, par. 10, Regolamento DORA, le Autorità di vigilanza europee (ESAs) 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: v. JOINT COMMITTEE OF THE ESAS, *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 gennaio 2024), in *www.esmaeuropa.eu*.

fornitore; (5) l'esistenza di conflitti di interesse (art. 28, par. 4, 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 dal consiglio di amministrazione, segnando una biforcazione nel modello dell'agire informato.

Nel caso di funzione non essenziale o importante, l'amministratore 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[27] –, nonché l'eventuale affidamento infragruppo del servizio[28]. Diversamente, nel caso di funzione essenziale e importante, il consiglio di amministrazione è tenuto ad estendere il proprio patrimonio informativo all'adeguatezza della struttura organizzativa[29]; al pregio del servizio in termini tecnico-informatici[30]; alla concentrazione dei servizi IT[31]; all'eventualità di un conseguente sub-appalto[32]; alle regole applicabili al fornitore, con particolare riguardo alle disposizioni che ne governano l'eventuale crisi[33] e all'effettiva applicazione della legge in caso di paese terzo[34].

La distinzione dei fattori da prendere in considerazione risulta determinante in quanto amplia o restringe la premessa informativa sulla cui base viene impostata e orientata la successiva fase di valutazione del rischio. La discrezionalità degli amministratori 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

[27] EBA, *Orientamenti*, par. 71, lett. a).
[28] EBA, *Orientamenti*, par. 71, lett. c).
[29] EBA, *Orientamenti*, 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».
[30] 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, *Orientamenti*, par. 70.
[31] Art. 29, par. 1, co. 1 e 4, Regolamento DORA.
[32] Art. 29, par. 2, co. 1, Regolamento DORA e EBA, *Orientamenti*, par. 76 ss.
[33] Art. 29, par. 2, co. 2, Regolamento DORA.
[34] Art. 29, par. 2, co. 3, Regolamento DORA.

all'(eventuale) esternalizzazione del servizio IT[35]. 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 in proporzione alla capacità della banca di mitigare tale rischio tramite dispositivi di *governance* e diritti contrattuali. In ultima analisi, il risultato di tale valutazione determina il c.d. rischio residuo che la banca è tenuta a sopportare.

2.3 *I paradigmi della scelta*

È a questo punto che si innesta la scelta definitiva da parte degli amministratori. Tale decisione viene a confrontarsi con due rilevanti paradigmi di gestione. Nel primo, sulla base delle premesse informative e del rischio residuo 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[36]. In questo caso, tale scelta sarebbe coperta da *business judgement rule* e risulterebbe pertanto insindacabile, al di fuori delle ipotesi di scelta non informata o manifestamente irragionevole[37]. Indicazioni in questo senso si rintracciano anche nel regime giuridico in materia di *outsourcing*. In primo luogo, nella

[35] 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 valutazione quando decidono se esternalizzare la funzione a un fornitore di servizi»: EBA, *Orientamenti*, par. 64.

[36] Così 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».

[37] In ambito bancario, cfr., avuto riguardo all'irragionevolezza della scelta gestoria, 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, MONTALENTI, *Assetti organizzativi e organizzazione dell'impresa tra principi di corretta amministrazione e* business judgement rule: *una questione di sistema*, in *Il nuovo diritto delle società*, 2021, 20 e, nell'ambito della disciplina con parti correlate, ID., *Impresa, società di capitali, mercati finanziari*, Torino, 2017, 247. Per ulteriori riferimenti dottrinali e giurisprudenziali, RIGANTI, *La Responsabilità degli amministratori. Rassegna di giurisprudenza*, in *Giur. comm.*, 2023, II, 181 ss. e MONTALENTI - RIGANTI, *La responsabilità degli amministratori di società per azioni. Rassegna di giurisprudenza*, in *Giur. comm.*, 2017, II, 780.

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. 1, punto 22, Regolamento DORA; Orientamenti EBA, par. 29, lett. *a*, punto *ii*).

Nel secondo, una volta stabilito il livello di rischio residuo, gli amministratori 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 residuo 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.

2.4 *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[38]. 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[39].

[38] Cfr. EBA, *Orientamenti,* 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, par. 4, Regolamento DORA; EBA, *Orientamenti*, par. 61).

[39] 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 da

Nella sintomatica definizione fornita dal legislatore europeo, la «resilienza 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, par. 8, co. 1, 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, par. 8, co. 2, 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, così integrando in tale ambito il canone della sana e prudente gestione della banca[40].

BCBS, *Principles for Operational Resilience*, (marzo 2021), in *www.bis.org*, 1, ove 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 (IOSCO), *Principles on Outsourcing. Final Report*, (ottobre 2021), in *www.iosco.org*, 13.

[40] Sulla generale rilevanza del principio per l'azione gestoria degli amministratori di banche, v., per tutti, NIGRO, *Il nuovo ordinamento bancario e finanziario europeo: aspetti generali*, in *Giur. comm.*, 2018, I, 186 s., GUIZZI, *Appunti in tema di interesse sociale e* governance *nelle società bancarie*, in *Riv. dir. comm.*, 2017, 248 ss., MIRONE, *Regole di governo societario e assetti statutari delle banche tra diritto speciale e diritto generale*, in *Banca impr. soc.*, 2017, 44 ss. e ANGELICI, *Introduzione (intervento al convegno "Società bancarie e società di diritto comune. Elasticità e permeabilità dei modelli")*, in *Dir. banca e mercato finanz.*, 2016, 761 ss.

2.5 *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 comprende 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 gli aspetti della prestazione del servizio, offre la propria collaborazione ad un prezzo significativamente inferiore rispetto ai *competitor* 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 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 sull'operatività del fornitore. Come infatti viene sancito dal legislatore europeo, in caso di rischio di concentrazione, la banca deve vagliare «i benefici e i costi di soluzioni alternative, quali il ricorso a diversi fornitori terzi di servizi TIC» (art. 29, par. 1, co. 2, Regolamento DORA).

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[41]. È soltanto in assenza di quest'ultima opzione strategica che la banca sarà tenuta a realizzare il servizio *in house*.

[41] 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, *Orientamenti*, par. 68, lett. *f*).

In questa prospettiva, gli amministratori sono tenuti a dare conto delle ragioni per cui la selezione del fornitore non presenti un rischio residuo tale da compromettere gli interessi protetti dal legislatore e, nel contempo, non dimentica esigenze di efficienza. Né pare possibile giustificare scelte non equilibrate, ricorrendo ad un innalzamento della dotazione patrimoniale dell'ente per assorbire le perdite derivanti dagli eventuali pregiudizi causati dal fornitore. La strategia normativa diretta a imporre ulteriori requisiti di capitale (in luogo di presidi *ex ante*) è stata vagliata[42] e 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[43]. Inoltre, quand'anche le banche accettassero di rispettare un'aggiuntiva riserva di capitale, la Commissione sostiene che non verrebbero comunque implementate le misure organizzative che sono concretamente idonee a garantire la riduzione del rischio operativo[44]. Il legislatore europeo sconfessa dunque l'assunzione di rischio tramite "garanzia patrimoniale", imponendo scelte e misure che possano direttamente assicurare il rispetto della continuità e della qualità operativa[45].

È possibile in conclusione tracciare – pur con un certo grado di sintesi – il quadro della responsabilità per gli amministratori della banca con riferimento alla scelta di esternalizzare servizi IT. Gli amministratori saranno chiamati a rispondere di tale decisione ogni volta che non danno conto delle informazioni a supporto della decisione (= non assumono una decisione informata) oppure, sulla base delle informazioni raccolte e del rischio misurato, non motivano le ragioni per cui la scelta del fornitore è in grado di soddisfare gli interessi protetti dal legislatore. In queste due

---

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

[43] 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*».

[44] 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)*».

[45] 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).

ipotesi, se si condividono i rilievi per cui l'amministratore si confronta con un paradigma di gestore specificamente informato[46] e la scelta è positivamente orientata dai predetti criteri conformativi, si potranno agevolmente comprendere gli argomenti per cui la regola di insindacabilità delle scelte gestorie subisce un restringimento entro tale contesto normativo.

3. *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 da parte della banca. Lo svolgimento di un'adeguata attività di controllo è assicurato tramite due principali strategie normative: la conformazione degli assetti organizzativi della banca[47] 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[48]. Come chiaramente indicato dagli Orientamenti EBA, tale attività di controllo è ultimamente funzionale ad aggiornare regolarmente la valutazione di rischio compiuta in sede di scelta[49] e verificare la *compliance* dell'attività del fornitore con gli obblighi normativi e contrattuali[50].

---

[46] V. *supra* par. 2.2.

[47] Gli Orientamenti EBA prevedono che l'esternalizzazione di un servizio non dovrebbe consentire una riduzione dei requisiti di idoneità degli amministratori e dei soggetti apicali (par. 37). Inoltre, la banca è tenuta a 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 (par. 38, lett. *c*).

[48] 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, par. 75, lett. *h* e *p*; analogamente, art. 30, par. 3, lett. *e*, Regolamento DORA). Con riferimento all'esternalizzazione di funzioni non essenziali o importanti i contratti devono esclusivamente prevedere che la funzione di *internal audit* debba esaminare il servizio affidato al fornitore (par. 85). In dottrina, sottolinea la conformazione della struttura di *governance* e del sistema dei controlli interni, nonché del contratto, FALCONE (nt. 22), 276. In questo senso, l'esternalizzazione presenta valenza organizzativa e contrattuale: URBANI (nt. 13), 197 ss.

[49] EBA, *Orientamenti*, par. 102. Cfr., inoltre, art. 28, par. 2, 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».

[50] Tale aspetto è desumibile da EBA, *Orientamenti*, 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

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[51]. Il *framework* normativo europeo afferma espressamente che l'attività di controllo del servizio esternalizzato deve essere diretta a verificare la *performance* del fornitore[52]. 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[53]. 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). Come osservato prima, tali criteri 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[54]. La nozione di «*performance*» deve pertanto interpretarsi in maniera ampia di modo da ricomprendere i predetti elementi, idonei a incidere sul tasso qualitativo del servizio e sulla sua continua disponibilità. 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

esternalizzata in modo efficace o *in conformità delle leggi applicabili e degli obblighi normativi* [enfasi aggiunta]».

[51] Cfr. EBA, *Orientamenti*, 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».

[52] Sul punto, v. EBA, *Orientamenti*, par. 100: «[g]li enti e gli istituti di pagamento dovrebbero monitorare … la *performance* dei fornitori». Cfr., inoltre, art. 30, par. 3, Regolamento DORA, lett. e), 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».

[53] I livelli di servizio concordati devono essere previsti all'interno del contratto di esternalizzazione avente per oggetto funzioni essenziali o importanti: EBA, *Orientamenti*, par. 75, lett. i). Analogamente, v. anche art. 30, par. 3, lett. a), Regolamento DORA. Per una disamina degli indicatori di *performance* in tali contratti, v. IZZO, *Il contratto di* outsourcing, in CASAMASSIMA - NICOTRA (a cura di), *L'Outsourcing nei servizi bancari e finanziari*, Padova, 2021, 69 ss.

[54] *Supra* par. 2.2.

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*»[55]. 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[56]. In questi termini, la banca non potrà limitarsi a compiere indagini periodiche sul fornitore né attivarsi alla sola presenza di segnali d'allarme[57]. 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*[58] – di vicende

[55] La citazione nel testo è tratta dal documento FINANCIAL STABILITY BOARD, *Enhancing Third-Party Risk Management and Oversight*, (4 dicembre 2023), in *www.fsb.org*, 15.

[56] Così EBA, *Orientamenti*, par. 100.

[57] 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*, (ottobre 2022), in *www.ecb.europa.eu*, 3.

[58] 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 subesternalizzazione) (EBA, *Orientamenti*, 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, *Orientamenti*, par. 75, lett. *j*). Tale ultima previsione è presente anche nel Regolamento DORA: art. 30, par. 3, lett. b). Con riferimento all'obbligo di comunicare lo spostamento del luogo in cui è realizzata la funzione in *outsourcing*, v. EBA, *Orientamenti*, par. 75, lett. f).

idonee ad alterare o modificare la valutazione dei rischi svolta in sede di selezione del fornitore[59].

Nei casi in cui si determina un incremento significativo del rischio o l'attività del fornitore non risulti conforme con gli obblighi normativi e contrattuali, la banca potrebbe esercitare diversi strumenti di reazione aventi come esito la cessazione del contratto oppure la messa a punto del servizio o della struttura organizzativa del fornitore. Come osservato in precedenza (*supra* par. 2.4), 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[60] come *extrema ratio* rispetto a quelli che consentono la conservazione del rapporto contrattuale con il fornitore di servizi IT[61]. Tale esito ermeneutico è confermato dalla previsione per cui l'autorità di vigilanza competente può 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).

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, «facilitare il trasferimento della funzione esternalizzata a un altro fornitore», reintegrare la funzione all'interno dell'ente[62], nonché imporre l'adozione di strategie di uscita idonee ad

---

[59] Cfr. EBA, *Orientamenti*, 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».

[60] Tali rimedi devono essere contemplati dal contratto anche per alcune ipotesi espressamente indicate dalla normativa: EBA, *Orientamenti*, par. 98 e art. 28, par. 7, Regolamento DORA.

[61] 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*»: ENRIQUES - RINGE, *Bank-Fintech Partnerships, Outsourcing Arrangements and the Case for a Mentorship Regime*, (2020), in *www.ecgi.global*, 12.

[62] Così, EBA, *Orientamenti*, par. 99 e art. 28, par. 8, 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

evitare qualsiasi interruzione dell'attività di impresa[63] sono strumenti che possono comunque risultare problematici per la banca e avere impatti sulla continuità del servizio. 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 domanda formulata dalla banca e perdita dei benefici derivanti dal coordinamento con la struttura aziendale della stessa. Oppure, al termine del periodo di transizione, la banca potrebbe non aver ancora individuato un nuovo fornitore di servizi IT che rispetta gli *standard* normativi.

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 raccomandazioni nei confronti del fornitore. L'ammissibilità di questo rimedio trova, del resto, giustificazione nell'ampiezza delle «misure correttive» consentite dal legislatore quando vengano individuate «carenze» nella prestazione del servizio (Orientamenti EBA, par. 105). 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 degli Orientamenti EBA, 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[64], quanto possono riguardare anche gli assetti di

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*).

[63] In tema, v. EBA, *Orientamenti*, parr. 106 ss. e art. 28, par. 8, Regolamento DORA.

[64] Gli ambiti rilevanti sono contenuti nell'art. 33, par. 3, Regolamento DORA. L'art. 35, par. 1, 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*).

governance e organizzativi del fornitore di servizi[65]. Prendere a modello quanto previsto dal Regolamento DORA per ricostruire il confine del potere di formulare raccomandazioni organizzative ha il sicuro pregio di consentire 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[66].

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)[67]; interessi non riscontrabili in una dimensione più propriamente contrattuale. Se si condivide tale perplessità, si muove verso una prospettiva *de jure condendo*: sarebbe, pertanto, opportuno che il legislatore prevedesse espressamente il potere per la banca di fornire raccomandazioni nei confronti dei soggetti che prestano servizi digitali a supporto di funzioni essenziali o importanti.

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

Le considerazioni svolte sinora presuppongono un monitoraggio "perfetto" da parte della banca in grado di rilevare nel continuo le criticità della fornitura di servizi IT e approntare tempestivamente i rimedi

---

[65] In questa seconda categoria, possono ricomprendersi le raccomandazioni riguardanti: (1) i «processi di gestione del rischio (art. 33, par. 3, 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, par. 3, lett. *d*).

[66] 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*.

[67] Sul punto, v. il 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».

opportuni. Tuttavia, è sufficiente immaginare la difficoltà per un ente creditizio di contestare l'imperfetto funzionamento del *software* di gestione del portafoglio fornito da un soggetto come *Black Rock*[68]. Tale esempio mostra come il monitoraggio della banca si confronti con il problema dell'asimmetria di potere di cui può godere il fornitore[69], specialmente all'interno di un mercato di servizi IT particolarmente concentrato. Tale asimmetria può essere ricondotta almeno ad una triplice forma: (1) un *outsourcer* troppo influente per dimensioni e reputazione perché la banca possa incidere sulla sua operatività; (2) un *outsourcer* troppo "unico" nel proprio ruolo perché la banca possa sostituirlo facilmente; (3) un *outsourcer* troppo integrato nei sistemi operativi perché la banca possa supplire a tale fornitura. In questi casi, la banca potrebbe attuare un monitoraggio adeguato senza avere la forza di "farsi rispettare" e assicurare la continuità e la qualità del servizio. In altri termini, la condotta della banca si configura come attiva e diligente, ma si inserisce un fattore esterno (= il potere negoziale dell'*outsourcer*) che impedisce di dare seguito alle risultanze del monitoraggio.

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*, 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 che usufruiscono del (difettoso) servizio IT offerto dal fornitore. In questo modo, la stabilità del sistema finanziario e la fiducia dei depositanti potrebbero essere compromessi o quantomeno inficiati.

5. *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

---

[68] I *software* di gestione del portafoglio creati da *Black Rock* sono esternalizzati con grande frequenza, v. BUCKLEY ET AL, *The Dark Side of Digital Financial Transformation: The New Risks of Fintech and the Rise of TechRisk*, (2019), in *www.ssrn.com*, 30 s.

[69] Cfr. per tutti EXPERT GROUP ON REGULATORY OBSTACLES TO FINANCIAL INNOVATION (ROFIEG), *30 Recommendations on Regulation, Innovation and Finance*, (2019), in *www.europa.eu*, 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)*».

condotta del fornitore. Tuttavia, gli Orientamenti EBA configurano 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[70] e ispettivi[71] verso l'*outsourcer* consentono all'autorità di acquisire una maggior cognizione di causa del rapporto di esternalizzazione, in modo da indicare alla banca misure correttive sulla propria struttura organizzativa e patrimoniale[72] oppure richiedere

[70] Art. 65, par. 3, lett. a), CRD IV.

[71] Art. 65, par. 3, lett. b) e c), CRD IV. In chiave ispettiva, l'accordo di esternalizzazione deve prevedere il diritto di ispezione e *audit* in capo all'autorità di vigilanza verso il fornitore: EBA, *Orientamenti*, par. 75, lett. p).

[72] L'autorità di vigilanza competente può imporre all'ente vigilato l'adozione di interventi correttivi nell'ambito del processo di revisione e valutazione prudenziale ("SREP": art. 97 CRD IV; per una sintesi del processo, v. MEISSNER, *The Supervisory Review and Evaluation Process (SREP): Ultimate Test for the Banking Union?*, in *Journal of International Banking Law and Regulation*, 2016, 332 ss., ARRIGONI, *Informazioni privilegiate e funzionamento dei mercarti finanziari*, Milano, 2022, 167 s. e, con particolare riferimento agli ambiti oggetto di verifica da parte dell'autorità di vigilanza e al possibile contenuto della c.d. *SREP decision*, 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), in *www.eba.europa.eu*, 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, *Orientamenti sulle procedure*, cit., par. 553, lett. *c*). Infine, una misura specifica dell'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, *Orientamenti*, 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, *Orientamenti*, 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, *Orientamenti*, par. 56. Sulla scorta di tale prerogativa, la Banca d'Italia ha di recente emanato delle *Istruzioni per la segnalazione in materia di esternalizzazione di funzioni aziendali per gli intermediari vigilati*. La tenuta del registro da parte delle banche è prevista anche dall'art. 28, par. 3, Regolamento DORA: in materia, 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 gennaio 2024), in *www.eba.europa.eu*

l'esercizio di rimedi nei confronti del fornitore di servizi IT[73].

Lo stesso vale – nel quadro normativo italiano – con riferimento alla potestà in capo all'autorità competente di irrogare una sanzione amministrativa *ex* art. 144, co. 1, d.lgs. 1° settembre 1993, n. 385 - Testo unico delle leggi in materia bancaria e creditizia (d'ora in poi, "TUB")[74] a coloro ai «quali sono state esternalizzate funzioni aziendali» o «funzioni aziendali essenziali o importanti» per la violazione delle disposizioni da esso indicate[75]. 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 IT per la prestazione dei propri servizi. 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 nei casi di violazioni afferenti all'ipotesi dell'ostacolo alla vigilanza, riconducibile al dovere del fornitore di servizi IT di collaborare quando l'autorità di vigilanza eserciti nei suoi confronti i poteri informativi[76], ispettivi[77] e di intervento[78] a sua disposizione.

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

---

[73] 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, *Orientamenti*, par. 118). Come già visto per gli esiti dell'attività di monitoraggio condotta dalla banca, anche nei confronti dell'autorità di vigilanza i rimedi che comportano la cessazione del contratto sono da considerare residuali e il potere di richiedere alla banca di formulare raccomandazioni mirate (riconducibile alle generiche «misure appropriate») verso i fornitori di servizi IT è da preferire.

[74] Per una generale panoramica dell'impianto sanzionatorio nell'ambito dell'esternalizzazione di funzioni, cfr. VARANI, *La gestione dei rapporti con le autorità di vigilanza*, in CASAMASSIMA - NICOTRA (a cura di), *L'Outsourcing nei servizi bancari e finanziari*, Padova, 2021, 202 ss.

[75] 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, co. 1, TUB).

[76] Art. 51-*quinquies*, co. 1, TUB.

[77] Art. 54, co. 1, TUB

[78] Art. 53-*bis*, co. 1, lett. a) e co. 2, TUB.

(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 al fornitore il cui potere negoziale e la rilevanza sistemica finirebbero per precludere l'efficacia del tradizionale assetto di supervisione (c.d. «fornitore terzo *critico*» di servizi IT[79]). 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, parr. 1, 2, 3, Regolamento DORA). A questo scopo, l'Autorità viene investita di un ampio potere di «formulare raccomandazioni» direttamente al fornitore contenenti la condotta pretesa (art. 35, par. 1, lett. *c* e *d*, Regolamento DORA) e il fornitore di servizi IT ha il dovere di cooperare in buona fede con la stessa[80]. Per assicurare inoltre l'effettività di tale prerogativa, il legislatore europeo ha introdotto una penalità di mora, in caso di «inosservanza totale e parziale delle misure» richieste nell'arco di trenta giorni dalla loro notifica; in questo caso, l'ammontare della penalità[81] 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

[79] Cfr. art. 3, punto 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, *Orientamenti*, parr. 29, 30, 31), il fornitore è designato come critico sulla base di soglie quantitative e indicatori di natura qualitativa [per una prima indicazione: 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 settembre 2023), in *www.esmaeuropa.eu*]. All'esito di tale valutazione, l'Autorità redige una lista provvisoria degli *outsourcer* IT critici al *forum* di sorveglianza (art. 32, par. 4, DORA), che, a sua volta, deve effettuare una raccomandazione al comitato congiunto delle ESAs a cui spetta la decisione finale (art. 31, par. 1, DORA). In dottrina, v. SPITALERI (nt. 16), 139.

[80] Cfr. art. 35, par. 5, 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».

[81] 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, par. 8, 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: KOURMPETIS, *Management of ICT Third Party Risk Under the Digital Operational Resilience Act*, in BÖFFEL - SCHÜRGER (edited by), *Digitalisation, Sustainability, and the Banking and Capital Markets Union*, Berlino, 2023, 22 e SCOTT, *The E.U.'s Digital Operational Resilience Act: Cloud Services & Financial Companies*, (2021), in *www.ssrn.com*, 22.

mondiale» dal fornitore critico nel precedente esercizio (art. 35, parr. 6, 7, 8, Regolamento DORA)[82].

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[83]. Il perseguimento di tale finalità, tuttavia, non può eccedere nella misura, arrivando sino a conformare le caratteristiche del fornitore alla stregua di una società bancaria. 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 banche[84].

6. *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[85]. In questi termini, tale meccanismo di

---

[82] 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, par. 10, Regolamento DORA.

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

[84] 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, *Guidelines on internal governance*, (2 luglio 2021), in *www.eba.europa.eu*, par. 202] non dovrebbe considerarsi quale criticità e la sua risoluzione non può essere oggetto di raccomandazione.

[85] Il fornitore di servizi è il c.d. *cheapest cost avoider*: pare innegabile che l'ammontare delle risorse necessarie per risolvere, per esempio, un difetto di programmazione sia di gran lunga inferiore alle perdite subite dai clienti delle banche coinvolte dallo scandente funzionamento o interruzione del servizio. Per 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*»: WAGNER, *Robot Liability*, (2018), in *www.ssrn.com*, 10. Sulla nozione di «*cheapest cost avoider*», CALABRESI, *The Costs of Accident: a Legal and Economic Analysis*, *New Haven*, 1970, trad. it, *Costo degli incidenti*

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 applicabile, a prescindere dalle tecniche con il quale viene articolato il proprio processo produttivo. Tale aspetto, già presente negli Orientamenti EBA[86] 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, par. 1, lett. *a*, Regolamento DORA)[87]. 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[88]. 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.[89], secondo cui «il debitore che nell'adempimento

e responsabilità civile, (a cura di DE VITA - VARANO - VIGORITI), Milano, 1975, 183 ss. Per una disamina della teoria di Calabresi, CASTRONOVO, *Responsabilità civile*, 2018, Milano, 492 ss.

[86] Sul punto, v. EBA, *Orientamenti*, par. 35, che recita: «[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».

[87] Per l'applicazione di tale principio nella giurisprudenza dell'Arbitro Bancario Finanziario: cfr. Collegio di Napoli, 18 maggio 2011, decisione n. 1044, 4.

[88] Sul punto, v. GUACCERO (nt. 17), 61. In senso analogo, SPITALERI (nt. 16), 138.

[89] Così MAUGERI (nt. 3), 455 s., poiché 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, v. LINCIANO ET AL. (nt. 2), 68 e, con riferimento alla consulenza digitalizzata, CONSOB, *La digitalizzazione della consulenza in materia di investimenti finanziari*, (2019), in *www.consob.it*, in 90.

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[90]. In tale caso, la banca sarà abilitata a recuperare nei confronti del fornitore le somme versate ai clienti a titolo di risarcimento del danno o all'autorità di vigilanza quando l'inesatta o interrotta esecuzione del servizio abbiano 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[91]. 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[92] (art. 92, par. 1, 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[93]. 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.

---

[90] Seppure in termini dubitativi e con riferimento ad un'ipotetica azione di regresso della banca verso il fornitore, *contra* 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 *Contratto e impresa*, 2019, 1073.

[91] Nella dottrina civilistica, v. D'ADDA, *Ausiliari, responsabilità solidale e "rivalse"*, in *Riv. dir. civ.*, 2018, 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, 348.

[92] In Italia, la disposizione di recepimento dell'art. 92, par. 1, PSD 2 è l'art. 27 d.lgs. 27 gennaio 2010, n. 11.

[93] Sul punto, v. IZZO (nt. 53), 72.