Dialoghi di Diritto dell'Economia

Gennaio 2025

ARTICOLI

La gestione e supervisione dei rischi ICT e di sicurezza nelle attività finanziarie esternalizzate tra DORA e CRD VI

Paola Lucantoni
Professore Ordinario di Diritto dei mercati finanziari
Università di Roma Tor Vergata

Chiara Villani
Dottoranda di Ricerca in Diritto e Tutela
Università di Roma Tor Vergata

Dialoghi di Diritto dell'Economia

Criteri di Revisione

I contributi proposti alla Rivista per la pubblicazione sono sottoposti a una previa valutazione interna da parte della Direzione o di uno dei Direttori d'Area; il quale provvede ad assegnare il contributo a un revisore esterno alla Rivista, selezionato, rationes materiae, fra professori, ricercatori o assegnisti di ricerca.

La rivista adotta il procedimento di revisione tra pari a singolo cieco (single blind peer review) per assicurarsi che il materiale inviato rimanga strettamente confidenziale durante il procedimento di revisione.

Qualora il valutatore esprima un parere favorevole alla pubblicazione subordinato all'introduzione di modifiche, aggiunte o correzioni, la Direzione si riserva di negare la pubblicazione dell'articolo. Nel caso in cui la Direzione decida per la pubblicazione, deve verificare previamente che l'Autore abbia apportato le modifiche richieste dal Revisore.

Qualora il revisore abbia espresso un giudizio negativo, il contributo può essere rifiutato oppure inviato, su parere favorevole della maggioranza dei Direttori dell'area competente rationes materiae, a un nuovo revisore esterno per un ulteriore giudizio. In caso di nuovo giudizio negativo, il contributo viene senz'altro rifiutato.

La gestione e supervisione dei rischi ICT e di sicurezza nelle attività finanziarie esternalizzate tra DORA e CRD VI

Paola Lucantoni
Professore Ordinario di Diritto dei mercati finanziari
Università di Roma Tor Vergata

Chiara Villani
Dottoranda di Ricerca in Diritto e Tutela
Università di Roma Tor Vergata

1. Globalizzazione dei mercati ed esternalizzazione delle attività d'impresa nel sistema aristotelico[01].

Il pensiero aristotelico secondo cui «il tutto è più della somma delle sue parti»[02] si presta bene a descrivere l'organizzazione dell'attività d'impresa nel contesto dei mercati globalizzati, caratterizzata da una notevole complessità e dall'interconnessione tra attività interne e attività esternalizzate, con particolare riferimento all'ambito *ICT* (*Information and Communications Technology*), che ricomprende l'insieme dei metodi e delle tecniche utilizzate nella trasmissione, ricezione ed elaborazione di dati e informazioni. L'esternalizzazione, invero, non riguarda solo una scelta tattica di delega operativa, ma

01 Anche se il lavoro è frutto di una riflessione comune, i §§ 2, 4 e 6 sono attribuiti a Paola Lucantoni, mentre i §§ 1, 3 e 5 sono attribuiti a Chiara Villani; il § 7 è attribuito a entrambe le autrici.

02 Aristotele, Metafisica, Libro VIII, 1045a

si inserisce in una rete di rapporti interdipendenti tra aziende, fornitori tecnologici e il mercato globale, in cui il valore generato dalla collaborazione supera il contributo di ogni singolo attore.

L'esternalizzazione delle attività aziendali è, infatti, un fenomeno strettamente connesso con la globalizzazione dei mercati; avendo quest'ultima comportato la competizione delle imprese su scala internazionale, e generato così nuove dinamiche di mercato ed esigenze operative, il ricorso all'esternalizzazione di attività, funzioni e processi risponde alla logica di incrementare la flessibilità operativa e ridurre i costi. L'*outsourcing*, infatti, permette alle organizzazioni di focalizzarsi sul proprio *core business* e, grazie alla collaborazione con fornitori specializzati, di accedere a competenze tecnologiche e infrastrutture avanzate senza l'onere di svilupparle internamente[03].

Questo aspetto è particolarmente rilevante nei settori ad alta intensità tecnologica, dove l'innovazione è rapida e richiede un costante aggiornamento delle competenze[04]; fra queste, rientra certamente il settore finanziario inteso in senso ampio – comprensivo dei tre mercati finanziario in senso stretto, bancario e assicurativo - da sempre

---

03 In letteratura, cfr. F. W. McFarlan - R. L. Nolan, *How to manage an IT outsourcing alliance*, in *MIT Sloan Management Review*, 36(2), 1995, 9; W. L. Currie, V. Michell, O. Abanishe, *Knowledge process outsourcing in financial services: The vendor perspective*, in *European Management Journal*, 26(2), 2008, 94; R. González, J. Gascó, J. Llopis, *Information systems outsourcing reasons and risks: review and evolution*, in *Journal of Global Information Technology Management*, 19(4), 2016, 223; M. Könning, M. Westner, S. Strahringer, *A systematic review of recent developments in IT outsourcing research*, in *Information Systems Management*, 36(1), 2019, 78.

04 Sul tema si richiama L. Murphy, *The influence of IT outsourcing on organisational success and innovation*, in *Futur Bus J* 10, 84, 2024. L'autore studia analizza il fenomeno dell'IT *outsourcing* (ITO), concentrandosi sulle implicazioni per il successo o il fallimento organizzativo e sull'impatto sull'innovazione. Il presupposto dello studio è l'individuazione di significative lacune nella letteratura, tra le quali la carenza di studi empirici sugli esiti dell'ITO per le organizzazioni, sull'influenza dell'ITO sull'innovazione e sull'effetto del settore industriale sull'esito dell'ITO. Per rispondere a queste carenze, l'Autore ha formulato tre domande di ricerca (*To what extent do organisations perceive IT outsourcing to be a success or failure? What influence does IT outsourcing have on an organisation's ability to innovate? What influence does an organisation's industry have on the perceived success or failure of IT outsourcing?*) che hanno portato allo sviluppo di un modello concettuale innovativo per valutare l'impatto dell'ITO sulle organizzazioni. I risultati evidenziano un elevato tasso di insuccesso percepito dell'ITO e dimostrano che il settore industriale di appartenenza può influenzarne l'esito. Inoltre, emerge che l'ITO ha un impatto negativo sull'innovazione organizzativa. Sulla base di queste evidenze, lo studio propone otto *best practices* per migliorare i risultati dell'ITO, tra le quali: condurre ricerche di mercato sulle competenze e sull'esperienza dei fornitori; definire contratti ben strutturati; rispettare rigorosamente gli SLA senza periodi di tolleranza; preferire progetti di breve durata; adottare strategie di *multi-sourcing*; rafforzare le competenze interne in ambito IT; promuovere la comprensione del valore dell'ITO tra i dipendenti; implementare una *governance* rigorosa. Lo studio riconosce i propri limiti, suggerendo la necessità di ulteriori ricerche con un campione più ampio e una rappresentazione settoriale più diversificata per validare ed estendere i risultati ottenuti.

incline all'evoluzione tecnologica, come l'espressione *FinTech*[05] – nota crasi tra le parole finanza e tecnologia – fa intendere[06]. Il settore bancario, ad esempio, risulta fortemente interessato dall'*outsourcing* nella gestione delle infrastrutture necessarie per i bonifici istantanei[07]; questi richiedono, infatti, la collaborazione con *provider* di servizi di pagamento o reti esterne, come *TIPS* (*Target Instant Payment Settlement*), per garantire l'accesso diretto alle infrastrutture, oltre al ricorso a soluzioni di *cloud computing*[08] per l'archiviazione e l'elaborazione dei dati in modo scalabile e in tempo reale. Rilevante è anche l'adozione di modelli *SaaS* (*Software as a Service*)[09], ovvero piattaforme esterne per l'esecuzione e il monitoraggio delle transazioni, nonché di sistemi di sicurezza *IT* avanzati per la protezione delle operazioni finanziarie.

Ne consegue che i soggetti vigilati affidano sempre più segmenti specifici della propria catena organizzativa a *start-up* tecnologiche, *BigTech* e grandi fornitori di tecnologia tramite rapporti di *outsourcing*, rappresentando questo il modo più rapido per acce-

05 Il *FinTech* è definibile, infatti, come un «ampio insieme di innovazioni – osservabili in campo finanziario in senso lato – che sono rese possibili dall'impiego delle nuove tecnologie sia nell'offerta di servizi agli utenti finali sia nei "processi produttivi" interni agli operatori finanziari nonché nel disegno di imprese-mercato (il c.d. *financial marketplace*)»; così C. Schiena, A. Tanda, C. Arlotta., G. Potenza, *Lo sviluppo del FinTech*, in *Quaderni FinTech*, CONSOB, 1/2018, VIII. Per precisione, si aggiunge che «Il Fintech è per sua natura un fenomeno in continua evoluzione, non racchiudibile in un contenitore e non definibile in modo statico» così R. Lener., *Spunti di riflessione sugli sviluppi del Fintech*, in *I diversi settori del Fintech. Problemi e prospettive*, E. Corapi – R. Lener (a cura di), Milano, 2019, 1. Sul tema anche F. Annunziata, La disciplina del mercato mobiliare, Torino, 2021, 28.

06 Sui tre settori del mercato finanziario in senso ampio – mercato finanziario in senso stretto, mercato bancario e mercato assicurativo - cfr., per tutti, P. Corrias e R. Lener (a cura di), *Manuale di diritto dell'economia. I mercati finanziari e dell'energia,* di Torino, 2024, *passim*. Sul tema v. altresì CIPA – ABI, *Rilevazione sull'IT nel settore bancario italiano, Profili economici e organizzativi, Esercizio 2023*, in *www.cipa.it*, ottobre 2024, 5 rileva che il modello prevalente per il *sourcing* dell'IT con riferimento all'operatività bancaria è l'*outsourcing*, affidando il 63% delle banche la gestione del Data centre e delle Applicazioni a uno o più fornitori.

07 Sulle novità in tema di bonifici istantanei si veda C. Villani, *Instant Payments Regulation: la svolta per i pagamenti elettronici in euro?*, in *FCHub.it*, 31 maggio 2024.

08 In tema di *cloud computing*, alla luce delle particolari problematicità connesse al servizio, dovute principalmente al fatto che vengono esternalizzati dati appartenenti all'impresa esternalizzante, il Garante della Protezione dei dati ha pubblicato una scheda di documentazione nella quale viene enfatizzata la necessità di una stringente *due diligence* rispetto all'ente al quale vengono esternalizzate attività e funzioni. Il riferimento è a Garante della Protezione dei dati, *Cloud computing: indicazioni per l'utilizzo consapevole dei servizi*, scheda di documentazione, 23.06.2011. Anche l'ESMA si è espressa in materia: ESMA, *Orientamenti in materia di esternalizzazione a fornitori di servizi cloud*, 10.05.2021, ESMA50-164-4285. Si veda anche U. Piattelli, *La regolamentazione del Fintech, Dai nuovi sistemi di pagamento all'intelligenza artificiale*, Torino, 2023, §3.8.

09 CIPA – ABI, *Rilevazione sull'IT nel settore bancario italiano, Profili economici e organizzativi, Esercizio 2023*, in *www.cipa.it*, ottobre 2024, 2 rileva che ben 21 gruppi bancari su 22 adottano modelli *SaaS*.

dere alle competenze e alle infrastrutture pertinenti[10]. Nella prospettiva sistematica aristotelica, l'*outsourcing* nel *FinTech* prova come la sinergie tra soggetti vigilati e *provider* tecnologici vada ben oltre la mera somma delle risorse coinvolte: l'interazione tra conoscenze specializzate, infrastrutture tecnologiche e accesso ai mercati globali crea nuove opportunità operative e innovative che una singola entità, operando isolatamente, non potrebbe raggiungere.

2. La gestione dei rischi della esternalizzazione dei servizi *ICT* nella prospettiva regolatoria

L'esternalizzazione di attività comporta, tuttavia, rischi significativi, particolarmente enfatizzati nel mondo finanziario, tra i quali (i) vulnerabilità informatiche, (ii) minacce alla *privacy* e (iii) possibili impatti sistemici.

In merito alla (i) vulnerabilità informatica, un'indagine del 2020 ha rilevato come il 20% del totale degli attacchi *cyber* riguardi proprio il settore finanziario[11]. Di particolare importanza è altresì il tema in tema delle (ii) minacce alla *privacy*, posto che il mercato finanziario «si alimenta di informazioni»[12], che riguardano non solo dati aziendali relativi alle attività delle imprese, ma anche dati sensibili riferiti a singoli individui. Rispetto ai (iii) possibili impatti sistemici, i moderni mercati finanziari sono strettamente interconnessi e interdipendenti, e quindi l'innesco di un meccanismo non può essere limitato al mercato specifico in cui si verifica ma ha un effetto esplosivo anche sugli altri, il c.d. effetto cascata: determinati fornitori, locati in nodi critici della rete, potrebbero infatti diventare *single points of failure* cui potrebbero conseguire effetti di *spill-over* nell'intero sistema finanziario[13].

Un *vulnus* ad uno di questi profili, talvolta interrelati e complementari tra loro, lede la fiducia degli investitori, disincentivandone gli investimenti, e mina di conseguenza l'in-

10 Sui criteri che orientano alla decisione di affidarsi a terzi nello svolgimento dell'attività di impresa bancaria e su quelli seguiti nella selezione della controparte contrattuale si veda A. Cardani, I. Girardi, *Impresa bancaria ed esternalizzazione di servizi tecnologici,* in *Orizzonti del Diritto Commerciale*, 2/2024, 594. Sull'attività assicurativa, si veda invece il *report* di Carlino, Costanzo & Associati, *La Rivoluzione Digitale nel settore assicurativo. Big Tech, Big Data e Intelligenza Artificiale: facciamo chiarezza*, Milano, 12 gennaio 2024.

11 GCSEC - Global Cyber Security Center, *L'impatto del cyber risk sul mercato finanziario*, *Case Studies*, marzo 2020.

12 Così S. Seminara, *Disclose or abstain? La nozione di informazione privilegiata tra obblighi di comunicazione al pubblico e divieti di insider trading: riflessioni sulla determinatezza delle fattispecie sanzionatorie*, in *Banca borsa e titoli di credito*, 3/2008, 331.

13 E. Cerrato, E. Detto, D. Natalizi, F. Semorile, F. Zuffranieri, *I fornitori di tecnologia nel sistema dei pagamenti: evoluzione di mercato e quadro normativo, in Mercati, infrastrutture, sistemi di pagamento (Markets, Infrastructures, Payment Systems)*, Banca d'Italia, n. 47, marzo 2024, 11.

tegrità del mercato finanziario stesso[14]. In chiave aristotelica, l'effetto cascata in caso di crisi sistemiche è provocato proprio dalla natura del "tutto" che trascende la somma delle singole parti.

La coscienza di queste vulnerabilità ha mosso i Ministri delle Finanze e i Governatori delle banche centrali del G7 a focalizzare l'attenzione sui pericoli associati all'uso di servizi offerti da terze parti; il riferimento è al documento "*The G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector*", aggiornato nell'ottobre 2022, che evolve i principi originariamente introdotti nel 2016. Il documento offre una serie di linee guida di carattere generale fondamentali per gestire i rischi informatici derivanti dall'esternalizzazione dei servizi *ICT* e dalle nuove minacce nella catena finanziaria. Le aree chiave trattate includono: *governance*; gestione del rischio; risposta agli incidenti; piani di emergenza e strategie di uscita; monitoraggio del rischio sistemico; coordinamento intersettoriale; specificità delle terze parti nel settore finanziario[15]. Più recentemente, il G7 sulla cybersicurezza, riunitosi il 3 dicembre 2024 presso la sede romana dell'ACN, ha dato seguito al mandato ricevuto dai *leader* del G7 durante il vertice di giugno 2024 in Puglia il cui documento finale, al paragrafo dedicato alla sicurezza informatica, esplicitava l'impegno comune ad adottare misure concrete per rafforzare la resilienza collettiva attraverso il neoistituito G7 *Cybersecurity Working Group*. Tra i temi tecnici discussi nei vari tavoli tematici del G7 Cybersecurity, è emersa in particolare l'attenzione alla protezione degli ecosistemi digitali, con un *focus* sulla *supply chain* di beni e servizi *ICT*.

Mette conto segnalare un attacco *cyber* del febbraio 2024, noto alle cronache come "truffa dell'anno"[16], in cui è stato creato un clone *deepfake* di un dirigente in posizione apicale che, durante una videoconferenza, ha imposto ad un impiegato a versare 25 milioni di dollari su cinque conti correnti. Fidandosi dell'autenticità della conferenza, l'impiegato effettua l'operazione, cadendo pienamente nel sofisticato inganno: la videochiamata era stata creata con l'intelligenza artificiale e i personaggi che interagivano

14 L'interrelazione tra condotte abusive, ivi intese in senso lato, e la fiducia degli investitori, è ben espressa nella disciplina specifica degli abusi di mercato. In tal senso, il Considerando n. 2 della Direttiva 2003/6/CE afferma: «Un mercato finanziario integrato ed efficiente non può esistere senza che se ne tuteli l'integrità. Il regolare funzionamento dei mercati mobiliari e la fiducia nel pubblico dei mercati costituiscono fattori essenziali di crescita e di benessere economico. Gli abusi di mercato ledono l'integrità dei mercati finanziari e compromettono la fiducia del pubblico nei valori mobiliari e negli strumenti derivati».

15 E. Cerrato, E. Detto, D. Natalizi, F. Semorile, F. Zuffranieri, *I fornitori di tecnologia nel sistema dei pagamenti: evoluzione di mercato e quadro normativo,* cit., 14.

16 Corriere, *La truffa dell'anno: creano un clone deepfake del suo capo e lo convincono a versare 25 milioni di dollari*, 7 febbraio 2024, al link: https://www.corriere.it/tecnologia/24_febbraio_07/la-truffa-dell-anno-creano-un-clone-deepfake-del-suo-capo-e-lo-convincono-a-versare-25-milioni-di-dollari-fcb62466-31eb-421a-93be-79b935d2dxlk.shtml?refresh_ce_____(ultima consultazione 24.10.2024)

con l'impiegato erano solo dei *deep fakes*[17]. Nuovamente soccorre la logica aristotelica espressa nella *Poetica* secondo cui la mimesi, come la rappresentazione della realtà, non sia necessariamente una copia fedele, ma piuttosto qualcosa che appare credibile e coerente, capace di ingannare o persuadere lo spettatore grazie alla sua somiglianza con il reale. Nel caso dell'attacco *deepfake*, l'inganno si fonda sulla capacità dell'intelligenza artificiale di creare una rappresentazione estremamente verosimile delle persone coinvolte, capace di evocare un'immagine talmente plausibile da superare il filtro critico della vittima. Se, come ci ricorda proprio Aristotele, l'uomo è un animale sociale la cui capacità di giudizio è fortemente influenzata dalle relazioni e dal contesto, la truffa sfrutta proprio questa dinamica; l'impiegato, immerso in un ambiente apparentemente familiare e strutturato secondo le regole sociali e aziendali, sospende il proprio spirito critico perché ciò che vede e sente corrisponde alle sue aspettative relazionali. Questa riflessione filosofica mette in luce l'urgenza di una nuova prospettiva di *governance* interna e di vigilanza esterna che consenta di discernere tra reale e simulato in un'epoca di rappresentazioni sempre più sofisticate.

L'area del *FinTech* è così stata sottoposta a un'intensa regolamentazione[18] che cerca di bilanciare innovazione e sicurezza ma che si scontra con il problema della rapidità evolutiva della tecnologia[19]. Vi è stato anche un tentativo, infruttuoso, da parte della

17 Sono ormai lontani i tempi dei primi *deep fakes* che si limitavano a rallentare e distorcere video preesistenti: si ricorda il caso Nancy Pelosi, la *speaker* democratica della Camera Usa, prima vittima di *deep fakes* che in un video manipolato del maggio 2019 appare come se stesse parlando a un convegno completamente ubriaca. Un caso che già allora aveva sollevato questioni, anche giuridiche, circa le conseguenze sia rispetto alla creazione e diffusione di tale video nonché sul suo mantenimento sulle diverse piattaforme *social*: YouTube, facente capo a Google, aveva deciso di rimuovere il contenuto perché violativo degli *standard* di correttezza; Facebook, invece, aveva lasciato le immagini sulla piattaforma, limitandone tuttavia la condivisione, nella convinzione che la notizia non fosse più la presunta ubriachezza della *speaker*, bensì che un video fosse stato manipolato. Per maggiori informazioni e per visionare il video si consulti The New York Times, *Distorted Videos of Nancy Pelosi Spread on Facebook and Twitter, Helped by Trump*, May 24, 2019 al link: https://www.nytimes.com/2019/05/24/us/politics/pelosi-doctored-video.html (ultima consultazione 24.10.2024)

18 Nel diritto internazionale, infatti, la c.d. guerra cibernetica non è regolata né da norme di *jus cogens* né da trattati vincolanti (*hard law*). L'unico riferimento è il "Manuale di Tallin", un atto di *soft law* elaborato dal Centro NATO per la cyberdifesa, che aggiorna il diritto bellico rispetto alle nuove tecnologie. L'ultima edizione, del 2017, mira a razionalizzare le prassi adottate da alcuni Stati membri della NATO. Tuttavia, la cibersicurezza pone sfide rilevanti per il diritto internazionale, in particolare per attribuire responsabilità statale agli atti ostili cibernetici (come hackeraggi o interruzioni di servizi). Queste difficoltà pratiche ostacolano lo sviluppo di norme pattizie o consuetudinarie universali. Sul tema A. Lauro, *Vulnerabilità e tutela dei diritti fondamentali alla prova della guerra cibernetica*, in *DPCE Online*, 61/2024, 485, §2. L'Autore si sofferma in particolare sul rischio che lo spazio cibernetico si trasformi in uno spazio di arbitrio rendendo vulnerabili i diritti fondamentali.

19 Sul tema della disciplina europea del FinTech si richiama C. Sandei, *FinTech, quo vadis? Un'introduzione allo studio del diritto europeo del FinTech*, in *Diritto del FinTech*, M. Cian, C. Sandei (a cura di), Milano, 2024, XXIX. In particolare, eloquente è il titolo del §2 "*Il diritto del fintech: un puzzle in continuo movimento*".

Commissione Europea, con il *Fintech Action Plan del 2018*[20], di introdurre strumenti regolatori *soft* per promuovere un'innovazione responsabile ed evitare una regolamentazione eccessivamente «prescrittiva e precipitosa. I recenti interventi normativi europei di *hard law*, come il Regolamento *DORA* (di cui *infra*)[21], dimostrano come la sicurezza informatica non sia più un tema esclusivamente tecnico, ma un aspetto strategico che riguarda la stabilità economica e i diritti fondamentali degli individui[22]. I soggetti vigilati devono quindi rafforzare la propria resilienza operativa e adottare *standard* di sicurezza adeguati, mantenendo alta l'attenzione verso le vulnerabilità introdotte dall'esternalizzazione digitale[23]; catene di fornitura in continua espansione e complessità, accompagnate da un aumento e una diversificazione degli operatori coinvolti aumentano infatti sensibilmente l'area esposta ad attacchi *cyber*[24].

In particolare, la diffusione dell'*outsourcing* nei settori regolamentati porta in primo

20 Commissione Europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, alla Banca Centrale Europea, al Comitato economico e sociale europeo e al Comitato delle regioni, Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo*, Bruxelles, 8.3.2018, COM(2018) 109 final.

21 Oltre al *DORA*, con particolare riferimento al tema dell'*outsourcing* tecnologico si ricordano anche la Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 (c.d. Direttiva NIS) recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, attuata nell'ordinamento italiano con il Decreto Legislativo 18 maggio 2018 n. 65; il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (c.d. GDPR), il quale definisce la posizione e le responsabilità dell'esternalizzante e dell'esternalizzato; il Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

22 La sicurezza e la resilienza cibernetica sono oggetto di attenzione anche nell'ordinamento nazionale e costituiscono una delle priorità del Piano Nazionale di Ripresa e Resilienza (PNRR), sviluppato nell'ambito dell'iniziativa europea *Next Generation EU* (NGEU). Per realizzare gli obiettivi previsti dal PNRR, il governo Draghi ha approvato il Decreto-Legge n. 82 del 14 giugno 2021, successivamente convertito nella Legge n. 109 del 4 agosto 2021, intitolata "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale". Con questa legge, è stata ridefinita l'architettura nazionale cibernetica ed è stata istituita l'Agenzia per la Cybersicurezza Nazionale (ACN), ente di diritto pubblico incaricata di rafforzare l'autonomia strategica nazionale ed europea nel settore digitale, operando in sinergia con il sistema produttivo nazionale e coinvolgendo il mondo dell'università e della ricerca. Inoltre, il legislatore nazionale, con la Legge di Bilancio 2023, ha previsto l'istituzione di un "Fondo per l'attuazione della Strategia Nazionale di Cybersicurezza" e di un "Fondo per la gestione dei progetti di cybersecurity". Infine, il 19 gennaio 2023, è entrata in vigore la Determina del 3 gennaio 2023 dell'ACN, che rappresenta l'ultimo elemento normativo volto a regolamentare i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica. Per un approfondimento sulla cospicua normativa volta a disciplinare il settore della cybersicurezza nell'ordinamento interno alla luce della normativa europea si richiama F. Camisa, A. Simoncini, *Il fattore umano e la regolazione della cybersecurity*, in *Mondo Digitale*, marzo 2024.

23 Sul tema si veda N. Michieli, *Cybersecurity e gestione del rischio ICT: l'impatto sulla corporate governance*, in *Banca, Impresa, Società*, 2/2024, 243.

24 Per un'analisi dei dati sul tema si consulti European Union Agency for Cybersecurity (ENISA), *Enisa threat landscape 2024, July 2023 to June 2024*, September 2024.

piano le problematiche di *governance* associate a questo fenomeno, mettendo in discussione la struttura stessa del modello di *business* tradizionale dei soggetti vigilati; l'organizzazione produttiva tende così a frammentarsi in più segmenti affidati a diversi soggetti, sia vigilati che non vigilati, coinvolgendo anche operatori "alternativi" a quelli specializzati del sistema.

Ne consegue che nei settori regolamentati l'emersione del fenomeno delle esternalizzazioni ha fin da subito catturato l'attenzione delle autorità di vigilanza; a livello europeo, il primo intervento organizzativo è riconducibile alle *Guidelines on Outsourcing* del *CEBS* (*Committee of European Banking Supervisors*), emanate nel 14 dicembre 2006[25] in ambito bancario. Queste linee guida erano strettamente legate alle pratiche allora in uso e agli orientamenti europei del *Joint Forum*, ed avevano lo scopo di armonizzare i diversi mercati bancari e promuovere un approccio uniforme, alla luce delle differenti risposte delle autorità di vigilanza nazionali. Le *Guidelines* miravano inoltre a garantire coerenza con le normative del settore finanziario ossia, all'epoca, la Direttiva MiFID I. La *Guideline* 1, alla lett. a), forniva una prima definizione di *outsourcing*[26] nei termini di «utilizzo da parte di un'entità autorizzata di una terza parte (il "fornitore di servizi in *outsourcing*") per svolgere attività che normalmente sarebbero svolte dall'entità autorizzata, ora o in futuro. Il fornitore può essere esso stesso un'entità autorizzata o non autorizzata»[27].

Le indicazione del *CEBS* trovavano applicazione solo con riferimento alle *material activities* esternalizzate dagli istituti bancari, ossia a: (i) attività di importanza tale che qualsiasi insufficienza o mancanza nella fornitura di tali attività potrebbe avere un effetto significativo sulla capacità dell'ente autorizzato di adempiere alle proprie responsabilità regolamentari e/o di continuare a operare; (ii) qualsiasi altra attività che richieda un'autorizzazione da parte dell'autorità di vigilanza; (iii) qualsiasi attività che abbia un impatto significativo sulla gestione del rischio; e (iv) la gestione dei rischi connessi a tali attività[28]. Veniva invece fatto espresso divieto, tutt'ora vigente nei diversi mercati regolamentati del credito, della finanza e delle assicurazioni, all'esternalizzazione di

25 Committee of European Banking Supervisors (CEBS), *Guidelines on Outsourcing*, 14 dicembre 2006.

26 Definizione che non è valsa a superare la confusione tra il concetto di "*outsourcing*" e quello di "acquisti". Il problema è stato ovviato dalla ISO 9001:2015 che supera la distinzione tra acquisti e *outsourcing* della precedente norma ISO 9001:2008 (rispettivamente al par. 7.4 e al par. 4.1) con un più generico concetto di «*external provision of good and services*», ossia di fornitura esterna di beni e servizi. In tal modo, si sono superate le difficoltà riscontrate dalle organizzazioni nel dover individuare quale fosse la disciplina applicabile al negozio concreto da esse poste in essere, essendo ora rilevante solamente la considerazione circa i rischi associati al singolo fornitore, prodotto, servizio o processo esterno per definire controlli adeguati.

27 Traduzione delle autrici. Di seguito il testo originale: «*outsourcing: an authorised entity's use of a third party (the "outsourcing service provider") to perform activities that would normally be undertaken by the authorised entity, now or in the future. The supplier may itself be an authorised or unauthorised entity*».

28 *Guideline* 1, lett. f), CEBS *Guidelines on Outsourcing*.

funzioni di gestione "*core*"[29] poiché in contrasto con l'obbligo imposto ai vertici aziendali e del personale *risk taker* di gestire l'impresa sotto la propria responsabilità: infatti, tra le varie disposizioni[30], il CEBS poneva anche il principio cardine in base al quale, in caso di *outsourcing*, la responsabilità ricadeva sull'ente esternalizzante, attribuendola in ogni caso al «*senior management*», i.e. a coloro che gestiscono concretamente le attività dell'ente creditizio[31].

Questo principio è stato ulteriormente rafforzato dall'EBA (*European Banking Authority*), che il 25 febbraio 2019 ha pubblicato la versione definitiva delle *Guidelines on Outsourcing arrangements*[32] relative all'esternalizzazione di funzioni operative essenziali o importanti[33]. Queste *Guidelines* hanno l'obiettivo di promuovere una maggiore armonizzazione degli accordi di *outsourcing* stipulati da tutti gli intermediari bancari e finanziari, grazie al vasto insieme di soggetti inclusi nel campo d'azione dell'EBA[34]. Il documento, di natura ampia e basato su principi, dedica alla disciplina della *governance* il titolo III, suddiviso in sette sezioni (dalla 5 alla 11). Tra le altre, si ricorda in particolare la Sezione 6, al cui par. 35 si ribadisce che «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»; in definitiva, si conferma l'impostazione della responsabilità dell'organo gestorio[35], attraverso un principio di *governance* dei controlli interni centrato sull'autoregolamen-

29 *Guideline* 3, par. 1, CEBS *Guidelines on Outsourcing*, il quale annovera, tra le funzioni di gestione *core*, la definizione della strategia di rischio, della politica di rischio e, di conseguenza, della capacità di rischio dell'istituto.

30 Per un approfondimento sulle CEBS *Guidelines on Outsourcing* cfr. A. Polizzi, *La regolamentazione sull'outsourcing negli intermediari bancari e finanziari*, in *L'outsourcing nei servizi bancari e finanziari*, S. Casamassima, M. Nicotra (a cura di), Milano, 2021, 1.

31 *Guideline* 1, lett. g), CEBS *Guidelines on Outsourcing*.

32 European Banking Authority (EBA), *Guidelines on Outsourcing arrangements*, 25.02.2019, EBA/GL/2019/02.

33 Le previsioni delle *Guidelines* EBA sono state interamente recepite a livello nazionale con l'Aggiornamento n. 34 del 23 settembre 2020 alla Circolare 285 del 17 dicembre 2013 di Banca d'Italia, recante le "Disposizioni di vigilanza per le banche"; in particolare, si veda la Circolare 285, Parte I, Titolo IV, Capitolo 3, Sezione IV, paragrafo I: «Le banche che ricorrono all'esternalizzazione di funzioni aziendali all'interno o all'esterno del gruppo applicano i Titoli I, II, III e IV degli Orientamenti in materia di *outsourcing* dell'EBA».

34 Ossia gli enti creditizi e le imprese di investimento di cui all'art. 4, par. 1 del Regolamento (UE) 575/2013, gli istituti di pagamento di cui all'art. 4, par. 4 della Direttiva 2015/2366/UE e agli istituti di moneta elettronica di cui all'art. 2, par. 1 della Direttiva 2009/110/CE.

35 Si ricorda anche che, in continuità con le regolamentazioni più recenti, in base al par. 37 delle EBA *Guidelines on Outsourcing arrangements* del 2019 «(l)'esternalizzazione non dovrebbe abbassare i requisiti di idoneità applicati ai membri dell'organo di amministrazione di un ente, ai direttori e alle persone responsabili della gestione dell'istituto di pagamento e il personale che riveste ruoli chiave. Gli enti e gli istituti di pagamento dovrebbero avere competenze adeguate e risorse sufficienti e debitamente qualificate per assicurare un'adeguata gestione e supervisione degli accordi di esternalizzazione».

tazione degli istituti finanziari, i quali devono implementare normative interne per una corretta gestione delle esternalizzazioni e un sistema solido di monitoraggio[36].

Nella medesima prospettiva mette conto segnale le *Guidelines On certain aspects of the MiFID II compliance function requirements,* emanate nel 2021 dall'ESMA, al fine di chiarire i requisiti di MiFID II[37] relativi all'esternalizzazione, basati su obblighi organizzativi posti in capo all'ente esternalizzante, al fine di assicurare «alle autorità di vigilanza di controllare che le imprese di investimento adempiano a tutti i loro obblighi»[38]. Le *Guidelines* ESMA, al par. 77, esplicitamente confermano che «(l)e imprese possono esternalizzare soltanto i compiti, non le responsabilità; pertanto, le imprese che intendono ricorrere all'esternalizzazione restano pienamente responsabili dei compiti esternalizzati».

Con la *DORA*, come si vedrà nel paragrafo successivo, sembra entrare in crisi il principio della imputazione della responsabilità in capo al soggetto vigilato per le attività esternalizzate.

3. La resilienza operativa digitale nel regolamento *DORA*

L' accelerazione dell'esternalizzazione determinata dalle esigenze del *Fintech*, ha portato alla *Digital Finance Strategy*[39] del 2020, con la previsione nel *FinTech Action Plan* del 2018, del Regolamento (UE) 2022/2554, (*Digital Operational Resilience Act*, meglio noto come *DORA*)[40], che mira a proteggere il settore finanziario dai rischi legati alle tecnologie dell'informazione e della comunicazione, le c.d. *ICT*[41].

---

36 Per un approfondimento sulle EBA *Guidelines on Outsourcing arrangements* del 2019 cfr. S. Casamassima, *Le regole di governance in tema di esternalizzazione delle funzioni*, in *L'outsourcing nei servizi bancari e finanziari*, S. Casamassima, M. Nicotra (a cura di), Milano, 2021, 31.

37 Direttiva 2014/65/UE del Parlamento europeo e del Consiglio del 15 maggio 2014 relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE.

38 Art. 16, par. 5 MiFID II.

39 Commissione Europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni relativa a una Strategia in materia di finanza digitale per l'UE*, Bruxelles, 24.9.2020, COM(2020) 591 final. Sul tema P. Ciocca, *Pacchetto Finanza Digitale - Audizione della CONSOB presso la VI Commissione permanente (Finanze) della Camera dei deputati*, www.consob.it, 2021.

Sul tema si veda D.A. Zetzsche, F. Annunziata, D.W. Arner, R.P. Buckley, *The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy*, in *Capital Markets Law Journal*, 2021, 203-206.

40 Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011.

41 *ICT*, acronimo che ha iniziato dai primi anni 2000, sta per *Information and Communications Technology*, risultante dall'unione di IT (*Information Technology*) e CT (*Communication Technology*). L'*ICT* comprende l'insieme di metodi e tecniche utilizzate per trasmettere, ricevere ed elaborare dati e informazioni, incluse le tecnologie digitali, e coinvolge tutti i settori professionali dedicati alla progettazione e allo sviluppo tecnico della comunicazione digitale.

Approvato nel 2022 e con implementazione obbligatoria a partire dal 17 gennaio 2025, il *DORA* introduce nuove disposizioni per i *test* digitali, la condivisione delle informazioni e la gestione dei rischi legati ai fornitori terzi, istituendo inoltre un sistema di sorveglianza per monitorare i rischi digitali dei fornitori di servizi *ICT* critici[42].

L'obiettivo del regolamento *DORA* è la "resilienza operativa digitale", un concetto che merita attenzione per la scelta di termini specifici come "resilienza", "operativa", e "digitale". Rispetto al termine più tradizionale di "sicurezza", la resilienza abbraccia un significato più ampio. Se la sicurezza si concentra principalmente sulla protezione dai rischi, la resilienza comprende anche la capacità di identificare, prevenire, gestire, rispondere e ripristinare le attività operative dopo un evento avverso. Questa sfumatura di significato è particolarmente rilevante nel contesto del rischio cibernetico. La resilienza è definita "operativa" perché mira a garantire il funzionamento regolare e ininterrotto delle organizzazioni e del settore finanziario, e "digitale" per riflettere l'uso diffuso di tecnologie e risorse informatiche[43]. *DORA*, quindi, adotta un approccio integrato e moderno, che va oltre la semplice sicurezza per garantire una capacità di adattamento e ripresa efficace in un ecosistema digitale complesso e interconnesso, potenziando la capacità del sistema a resistere ai «rischi informatici», definiti dalla stessa *DORA* (art. 3, co. 1, n. 5) come «qualunque circostanza ragionevolmente identificabile in relazione all'uso dei sistemi informatici e di rete che, qualora si concretizzi, può compromettere la sicurezza dei sistemi informatici e di rete, di eventuali strumenti o processi dipendenti dalle tecnologie, di operazioni e processi, oppure della fornitura dei servizi causando effetti avversi nell'ambiente digitale[44] o fisico».

Il Regolamento è destinato a ben venti soggetti regolamentati nell'Unione Europea, confluenti nell'ampia definizione di «entità finanziaria»[45] fornita dal regolamento stesso all'art. 2, co. 1, con il fine di garantire un'applicazione dello stesso uniforme e coerente, tutelando la concorrenza tra operatori finanziari e tenendo conto delle differenze di dimensioni, caratteristiche aziendali ed esposizione al rischio digitale.

---

42 In tal senso, il Considerando n. 62 *DORA* afferma che: «per un solido monitoraggio dei rischi informatici derivanti da terzi nel settore finanziario, è necessario stabilire una serie di norme basate su principi che guidino le entità finanziarie nel monitoraggio dei rischi che si presentano nel contesto di funzioni esternalizzate a fornitori terzi di servizi *ICT*, in particolare per i servizi *ICT* a supporto di funzioni essenziali o importanti, nonché più in generale nel contesto di tutte le dipendenze da terzi nel settore delle *ICT*».

43 E. Cerrato, E. Detto, D. Natalizi, F. Semorile, F. Zuffranieri, *I fornitori di tecnologia nel sistema dei pagamenti: evoluzione di mercato e quadro normativo*, cit., 19.

44 In A. Perazzali, *Cyber sicurezza: Una continua sfida per l'economia e per la società*, in *www.bancaditalia.it*, 10 febbraio 2023, si osserva efficacemente che «(i)l *cyber*-spazio è la quinta dimensione della conflittualità – dopo terra, mare, aria e spazio extra-atmosferico – e costituisce uno degli elementi dello scenario in cui si innesta la politica internazionale».

45 Sul *DORA* con specifico riferimento al settore bancario si veda A. Cardinali, *Il processo di digitalizzazione in Europa e il ruolo del sistema bancario*, in *Studi e ricerche del Dipartimento di Economia Aziendale*, A. Pezzi (a cura di), 223, §4.

DORA conferma esplicitamente l'approccio *cross*-settoriale, orientato al rischio e fondato su pochi principi generali da declinare in modo più specifico in base alle peculiarità di determinati ambiti, adottato dalla *Digital Finance Strategy*[46], che richiama il principio di proporzionalità adottato nel *report* finale del dicembre 2019 del ROFIEG (*Expert Group on Regulatory Obstacles to Financial Innovation*)[47]. Difatti, nell'apertura del *DORA*, è presente un articolo dedicato proprio al "principio di proporzionalità", il quale chiarisce che non esistono misure *standard* universali per proteggere le organizzazioni da rischi e responsabilità; piuttosto, la conformità agli obblighi legali deve essere valutata caso per caso, in base alla specifica entità finanziaria, «tenendo conto delle loro dimensioni, del loro profilo di rischio complessivo, nonché della natura, della portata e della complessità dei loro servizi, delle loro attività e della loro operatività» (art. 4 *DORA*). In conformità a questo principio generale, viene introdotto un sistema di tutele e obblighi variabili, prevedendo, ad esempio, un quadro semplificato per le piccole entità finanziarie (art. 16 *DORA*) e più intenso per i sistemi di pagamento (art. 23 *DORA*)[48].

4. I *critical third party providers* (CTPP) e la supervisione da parte del *lead overseer*

Nel quadro normativo contenuto nel *DORA*, vi sono disposizioni specifiche relative all'esternalizzazione.

Tra gli elementi di continuità con il passato, vi è il requisito per gli organi di vertice di possedere conoscenze e competenze in materia di *outsourcing* e di gestione dei relativi rischi - in questo caso, *ratione materiae*, in ambito *ICT*. In particolare, l'art. 5, par. 4, *DORA* stabilisce che i membri del Consiglio di amministrazione debbano «mantenere attivamente aggiornate le conoscenze e le competenze necessarie per comprendere e valutare i rischi *ICT* e il loro impatto sulle operazioni dell'entità finanziaria».

D'altra parte, da un punto di vista quantitativo, vi è un notevole rafforzamento degli obblighi legali, ma sempre legati a una serie di doveri relativi alla pianificazione, selezione, verifica, monitoraggio e documentazione degli accordi di esternalizzazione, ora

46 Sull'approccio trasversale della *Digital Finance Strategy* cfr. A. Sciarrone Alibrandi, *Introduzione*, in *L'outsourcing nei servizi bancari e finanziari*, S. Casamassima, M. Nicotra (a cura di), Milano, 2021, XV.

47 Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG), *Thirty Recommendations on Regulation, Innovation and Finance*, *Final Report to the European Commission*, 13 *December* 2019. Queste raccomandazioni propongono un cambio di approccio normativo nell'ambito dell'innovazione finanziaria, evidenziando la necessità di una regolazione comune a livello europeo per il *FinTech* in quanto l'attuale frammentazione normativa tra Stati membri ostacola sia la creazione di un mercato unico nonché la competitività rispetto agli operatori americani e asiatici. Le proposte, in un'ottica applicativa trasversale, suggeriscono di affrontare i nuovi rischi tecnologici, in particolare quelli legati all'*AI*, ed alla *blockchain*, di bilanciare la protezione dei dati e il *data sharing*, e di valutare l'impatto del *FinTech* sui consumatori. Del *report*, si ricorda in particolare, *rationae materiae*, la *Recommendation 5 – Outsourcing guidelines and certification/licensing*.

48 Sul tema *Digital Operational Resilience Act* cfr. C. Sandei, *FinTech e gestione del rischio informatico*, in *Diritto del FinTech*, M. Cian, C. Sandei (a cura di), Milano, 2024, 19.

descritti in modo più preciso e specifico, in quanto riguardanti esclusivamente i rischi di *cybersecurity*. Ad esempio, mentre le *Guidelines* dell'EBA si limitavano ad affermare succintamente, al paragrafo 82, che «gli istituti di pagamento dovrebbero definire i requisiti di sicurezza dei dati e dei sistemi nell'accordo di esternalizzazione e monitorarne costantemente il rispetto», l'art. 30, par. 2, *DORA* affronta la questione in modo molto più dettagliato: infatti, è previsto l'obbligo di specificare contrattualmente il comportamento del fornitore di servizi *ICT* in caso di situazioni critiche durante il rapporto, come l'insolvenza, la cessazione delle operazioni, la risoluzione degli accordi o un incidente *ICT* legato al servizio fornito; il fine è quello di fornire all'entità finanziaria adeguate garanzie di accesso, recupero e restituzione dei dati, personali e non, in un formato facilmente accessibile.

La proposta più innovativa all'interno del *DORA* riguarda i fornitori terzi di servizi *ICT* considerati «critici» (i c.d. «*critical third party providers*» – CTPP), i quali saranno soggetti alla supervisione di un «*lead overseer*», ossia di un'autorità di vigilanza capofila[49].

I criteri per valutare i fornitori terzi «critici» di servizi *ICT*, ossia quei fornitori il cui malfunzionamento potrebbe avere un impatto rilevante sul sistema finanziario, sono definiti all'art. 31, paragrafo 2, *DORA*. Questi criteri considerano vari fattori, quali: (i) la gravità di un' interruzione operativa del fornitore e l'influenza sulla stabilità, continuità e qualità dei servizi finanziari, incluso il numero di entità finanziarie che dipendono da quel fornitore e il valore complessivo delle loro attività; (ii) il ruolo sistematico delle entità finanziarie che si affidano al fornitore e, in particolare, quanti enti finanziari rilevanti a livello globale o a livello nazionale dipendono da quel fornitore nonché le interconnessioni tra questi enti sistemici e altre entità finanziarie, soprattutto quando forniscono servizi finanziari essenziali ad altri; (iii) la dipendenza delle entità finanziarie sui servizi del fornitore per funzioni critiche o importanti, sia direttamente, sia indirettamente tramite subappalti; (iv) la complessità della eventuale sostituzione del fornitore, correlata alla disponibilità di alternative sul mercato, quota di mercato del fornitore, complessità tecnica dei servizi offerti e uso di tecnologie proprietarie, nonché difficoltà legate alla migrazione verso un altro fornitore, come costi, tempi e rischi informatici o operativi associati a tale processo.

L'autorità di vigilanza capofila per ciascun fornitore terzo critico viene designata, ai sensi dell'art. 31 par. 1 del *DORA*, dalle Autorità Europee di Vigilanza (AEV); la scelta ricade sulla AEV responsabile delle entità finanziarie che, nel complesso, detengono la quota più alta delle attività totali, calcolata sommando i bilanci delle entità finanziarie che utilizzano i servizi di quel fornitore critico di servizi *ICT*.

Le modalità di supervisione seguite dall'autorità di vigilanza capofila sono descritte nel

49 Sul tema della convergenza, cooperazione, coordinamento e frammentazione della vigilanza in cui si inserisce *DORA* si veda C.P. Buttigieg, B. Brunelli Zimmermann, *The Digital Operational Resilience Act: Challenges and Some Reflections on the Adequacy of Europe's Architecture for Financial Supervision*, in *https://papers.ssrn.com/*, Jun 2024.

capitolo 5, sezione 2, *DORA*. Pertanto, oltre all'ordinario potere di condurre ispezioni, indagini e *audit*, l'art. 33, par. 2, *DORA* conferisce alle autorità di vigilanza capofila il diritto di imporre misure specifiche direttamente ai fornitori critici, laddove questi non dimostrino di aver «predisposto norme, procedure, meccanismi e accordi esaustivi, solidi ed efficaci per gestire i rischi informatici cui esso può esporre le entità finanziarie». I fornitori critici possono, quindi, essere a tutti gli effetti considerati enti sottoposti a vigilanza.

Viene dunque superato il principio del mantenimento della responsabilità solo a carico dell'intermediario per funzioni, attività o processi esternalizzati, introducendo un regime di vigilanza sul fornitore per una protezione più rigorosa contro rischi specifici. In questo modo, coerentemente con il principio di proporzionalità cui dichiara di conformarsi, il *DORA, in tema di governance* dell'esternalizzazione, sembra introdurre un'eccezione al principio della responsabilità e vigilanza esclusiva del soggetto vigilato esternalizzante il cui impatto sistematico è rilevante[50]. Da un lato, infatti, le previsioni *DORA* di una vigilanza diretta sui fornitori critici non comportano un indebolimento degli oneri gravanti sulle entità finanziarie e sui loro dirigenti nella gestione dei rischi e nel rispetto delle normative[51], i quali restano comunque responsabili quando le funzioni

50 Sul tema si veda ancora A. Cardani, I. Girardi, *Impresa bancaria ed esternalizzazione di servizi tecnologici*, cit., §12.

51 L'importanza del Consiglio di amministrazione nella gestione del rischio *ICT*, sancita dal *DORA*, si riflette in obblighi simili presenti in diverse giurisdizioni a livello globale. Sul tema si veda R. Ni Thuama – S.S. Costigan, *DORA - Understanding the New Regulatory Framework on Digital Operational Resilience*, in *SSRN*, August 23, 2023. Gli autori riconoscono che la responsabilità del Consiglio di amministrazione è riconosciuta sia nei sistemi di *common law* che in quelli di *civil law*, detenendo, questo organo, l'autorità decisionale ultima. Ad esempio, nel contesto del diritto inglese e gallese, il *Companies Act 2006* (sezione 174) stabilisce che i direttori devono esercitare ragionevole cura, competenza e diligenza, senza escludere i rischi legati alla sicurezza informatica. In Canada, la sezione 122 del *Canadian Business Corporations Act* impone obblighi simili, mentre in Australia la sezione 180 del *Corporations Act* richiede che i dirigenti agiscano con attenzione e diligenza nell'esercizio delle loro funzioni. Anche in Irlanda, il *Companies Act 2014* (articolo 228) prevede *standard* comparabili. Negli Stati Uniti, la responsabilità dei direttori è stata chiarita attraverso diverse decisioni giudiziarie, rientrando nel dovere fiduciario che impone loro di monitorare e supervisionare adeguatamente l'attività aziendale.

critiche e importanti sono affidate a fornitori di servizi *ICT* terzi[52]. Dall'altro lato, invece, l'estensione della supervisione ai soggetti cui l'attività è esternalizzata di fatto ampia il perimetro delle attività soggette a vigilanza prudenziale oltre i settori soggetti a riserva di attività[53].

Nella prospettiva empirica mette conto segnalare uno studio del 2022 condotto attraverso interviste con *manager* di alto livello nel campo della sicurezza presso organizzazioni di servizi finanziari (FSO) nei Paesi Bassi[54] da cui è emerso come la gestione del rischio delle terze parti *ICT* sia considerata uno dei principali benefici del *DORA*, considerando vuoi la visione completa e integrata dei rischi *ICT*, sia interni che esterni, che offre; vuoi l'introduzione di un comitato di supervisione diretta per i principali fornitori *ICT*, ritenuto dagli intervistati particolarmente significativo per i principali operatori del mercato *cloud*, come Microsoft Azure, AWS e Google, contribuendo a migliorare la resilienza della catena di fornitura e idoneo a distinguere i fornitori di qualità da quelli meno affidabili, rafforzando la fiducia nel sistema.

Allo contempo, tuttavia, nello stesso campo del *cloud computing*, si è osservato che i

52 In questo senso il *Consultation Paper 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*, pubblicato il 19 giugno 2023 congiuntamente da parte delle *ESA's*. In particolare, il par. 3, punto 7 afferma che: «*The use of ICT service providers cannot reduce the responsibility for the financial entities and their management bodies to manage their risks and to comply with legislative requirements, especially when critical and important functions are supported by ICT third party service providers. The draft RTS includes provisions that ensure that financial entities clearly assign the internal responsibilities for the approval, management, control, and documentation of contractual arrangements on the use of ICT services provided by ICT third-party service providers to support their critical or important functions. Such provisions strengthen the accountability within the involved business areas within financial institutions*». Nello stesso senso, il par. 4, punto 7: «*The ultimate responsibility of the management body in managing a financial entity's ICT risk is an overarching principle which is also applicable regarding the use of ICT third-party service providers. This responsibility should be further translated into the continuous engagement of the management body in the control and monitoring of ICT risk management, including in the adoption and review, at least once per year, of the policy on the use of ICT services supporting critical or important functions by ICT third-party service providers*». Nel senso di estendere la supervisione anche ai *provider* terzi, l'art. 3 par. 7 prevede che: «*The policy referred to in paragraph 1 shall ensure that the relevant contractual arrangements are consistent with the financial entity's ICT risk management framework referred to in Article 6(1), the information security policy under Article 9(4), the business continuity policy under Article 11 and the requirements on incident reporting under Article 19 of Regulation (EU) 2022/2554*».

53 Inoltre, in J. Woxholth – D.A. Zetzsche, *DORA on DEFI*, in *https://papers.ssrn.com/*, Jun 2024, si osserva che l'approccio gerarchico del *DORA* è in contrasto con l'approccio orizzontale della finanza decentralizzata (DeFi) e che le sue regole sui servizi ICT di terzi possono mettere sotto pressione i modelli commerciali della DeFi. Pertanto, gli autori sostengono la necessità di norme di attuazione della *DORA* su misura per la DeFi,

54 J.B. ter Haar, *DORA: Friend or Foe? A Qualitative Study into the Perceptions of the Financial Sector in the EU on the Expectation of the Digital Operational Resilience Act*, Amsterdam, November 2022.

cloud service providers "critici" (CCSPs) sono soggetti a più regimi normativi, incluso il GDPR per la protezione dei dati personali, la direttiva NIS 2 per la sicurezza informatica e il *DORA* per la resilienza operativa digitale, portando alla sovrapposizione di regimi di sorveglianza diversi; una situazione, questa, che potrebbe portare alla violazione del principio del *ne bis in idem*, sancito dall'Articolo 50 della Carta dei diritti fondamentali dell'UE[55].

Si segnalano, infine, fra gli ultimi *standard* tecnici pubblicati sotto il *DORA* in tema di esternalizzazioni, gli RTS su *outsourcing* e subappalto di servizi *ICT*[56] e gli ITS per il registro degli *outsourcing ICT*[57].

I primi stabiliscono i requisiti per la gestione e il controllo dei fornitori di servizi *ICT* di terze parti, con particolare attenzione a quelli che supportano funzioni critiche o importanti[58]. Fra le previsioni di maggior rilievo si ricordano: l'art. 1, il quale richiede alle entità finanziarie di considerare vari fattori per valutare i contratti con fornitori di servizi *ICT*, tra i quali la tipologia di servizi *ICT* critici o importanti, la localizzazione dei fornitori e dei subappaltatori e la lunghezza della catena di subappaltatori e concentrazione dei rischi; l'art. 3, il quale prevede a carico delle entità finanziarie l'esecuzione di un'attenta *due diligence* prima di stipulare contratti di *outsourcing* o subappalto che valuti l'affidabilità dei fornitori e dei subappaltatori, inclusa la loro capacità operativa e

55 Così E. Kun, *Challenges in regulating cloud service providers in EU financial regulation: From operational to systemic risks, and examining challenges of the new oversight regime for critical cloud service providers under the Digital Operational Resilience Act*, in *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 52, 2024. In particolare, il *DORA* riconosce la correlazione tra la sua esistenza e la Direttiva NIS 2 al Considerando 20 e all'art. 32 par. 4 lett. e). Per quanto riguarda la sovrapposizione della sorveglianza nel GDPR e nel *DORA*, invece, l'A. afferma la mancanza di un quadro di coordinamento che attenui efficacemente le misure di applicazione ridondanti; ciò suscita preoccupazioni in merito alla possibilità di sanzioni duplicate, che possono potenzialmente minare il principio del *ne bis in idem*. L'A. ritiene, dunque, che sarebbe più vantaggioso migliorare la collaborazione e la cooperazione tra le attuali autorità di vigilanza, o, in alternativa, che l'UE istituisca un'autorità competente a livello europeo per affrontare i problemi di sicurezza informatica, in particolare alla luce della natura transnazionale dei CCSP. L'istituzione di un tale organismo di supervisione potrebbe offrire una strategia completa per la supervisione e l'attuazione, garantendo così un maggior grado di uniformità ed efficacia nella gestione e mitigazione dei rischi sistemici.

56 EBA, EIOPA and ESMA, *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*, JC 2024 53, 26 July 2024.

57 EBA, EIOPA and ESMA, *Final Report on 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*, JC 2023 85, 10 January 2024.

58 Si ricorda che l'art. 30 par. 5 *DORA* prevede che «Le AEV, tramite il comitato congiunto, elaborano progetti di norme tecniche di regolamentazione per specificare ulteriormente gli elementi di cui al paragrafo 2, lettera a), che l'entità finanziaria deve determinare e valutare quando subappalta servizi TIC a supporto di funzioni essenziali o importanti.»

finanziaria, e la garanzia che i contratti includano diritti di accesso e *audit* lungo tutta la catena di subappalto; l'art. 4 che delinea una gestione contrattuale precisa, dovendo i contratti devono specificare chiaramente responsabilità dei fornitori, quali servizi possono essere subappaltati e a quali condizioni, obblighi di monitoraggio per i fornitori terzi rispetto ai subappaltatori, requisiti di sicurezza *ICT* e piani di continuità operativa; infine, l'art. 7 in base al quale l'entità finanziaria ha il diritto di terminare il contratto con un fornitore *ICT* terzo in caso di modifiche non approvate agli accordi di subappalto o di subappalto non consentito o violazione dei termini contrattuali. Gli RTS sono ancora soggetti a revisione da parte della Commissione Europea per l'adozione finale.

Gli *ITS* per il registro degli *outsourcing ICT* forniscono, invece, un modello *standard* per mantenere un registro centralizzato e aggiornato di tutte le relazioni contrattuali con fornitori *ICT* terzi. Si ricorda, infatti, che l'art. 28 par. 3 *DORA* prevede che nella gestione dei rischi informatici, le entità finanziarie debbano tenere «un registro di informazioni su tutti gli accordi contrattuali per l'utilizzo di servizi TIC prestati da fornitori terzi»; l'art. 28, par. 9 *DORA* incarica le AEV di elaborare una bozza di *Implementing Technical Standards* per stabilire i modelli *standard* di tale registro. In adempimento di tale incarico, le AEV hanno pubblicato la bozza di ITS la quale prevede che il registro deve rispettare requisiti formali e includere informazioni chiave, fra le quali dati dettagliati su tutti i servizi *ICT* forniti dai fornitori terzi diretti nonché su tutti i subappaltatori che supportano funzioni critiche o importanti. Questo registro standardizzato permette alle autorità competenti di valutare rapidamente i rischi associati ai fornitori terzi e garantire che le entità rispettino i requisiti di *DORA*. Inoltre, l'uso di un modello comune per i registri facilita la trasparenza tra le entità finanziarie e i regolatori, migliorando la gestione delle relazioni con terze parti e la preparazione alle ispezioni regolamentari. Tuttavia, il 3 settembre 2024, la Commissione UE ha comunicato alle autorità di vigilanza il suo rifiuto rispetto alla bozza, ritenendo inopportuno obbligare le entità finanziarie ad utilizzare il LEI (identificatore di entità giuridica) per identificare i fornitori terzi di servizi *ICT* registrati nell'UE, preferendo invece far scegliere tra il LEI o l'EUID (identificatore unico europeo). Le AEV hanno presentato un parere su tale bocciatura, esprimendo preoccupazioni sull'introduzione dell'EUID, ritenendolo complesso, impattante negativamente sulla gestione delle informazioni con conseguente aggravio dell'onere di segnalazione per le entità finanziarie nel contesto del *DORA* e rallentante l'identificazione dei fornitori critici. Le AEV sollecitano una rapida decisione sull'uso degli identificatori e invitano gli enti finanziari a prepararsi per l'implementazione entro il 2025.

Da ultimo, il 4 dicembre 2024 le AEV hanno pubblicato un documento[59] con il quale rammentano alle entità finanziarie e ai fornitori di terze parti l'importanza di prepararsi adeguatamente all'entrata in vigore del *DORA*, non prevedendo un periodo transitorio. In particolare, le AEV ricordano che, entro i primi mesi del 2025, le entità finanziarie devono avere pronti i registri aggiornati sugli accordi contrattuali con i fornitori *ICT*, i quali

59 EBA, EIOPA and ESMA, *DORA application*, JC 2024 99, 4 December 2024.

verranno trasmessi dalle autorità competenti alle AEV entro il 30 aprile 2025; queste devono anche essere preparate a classificare e segnalare gli incidenti *ICT* significativi fin dalla data di applicazione; invece, i fornitori *ICT* critici devono valutare la propria operatività rispetto ai requisiti del *DORA* e la prima designazione dei CTPPs è prevista nella seconda metà del 2025.

5. La vigilanza sui soggetti terzi fornitori di attività *ICT* esternalizzate nella *CRD* VI

In tema di supervisione delle attività esternalizzate, sulla stessa linea tracciata dal *DORA* si colloca la Direttiva (UE) 2024/1619 (*Capital Requirements Directive VI - "CRD VI"*)[60], entrata in vigore il 9 luglio 2024, che rivede le norme bancarie dell'UE con l'obiettivo di garantire la stabilità del sistema finanziario e la resilienza delle istituzioni finanziarie nell'Unione.

Ad esempio, l'art. 65, par. 4, lett. a, punto vi, della *CRD VI* prevede che le autorità competenti dispongano di tutti i poteri necessari per raccogliere informazioni e condurre indagini utili per l'esercizio delle loro funzioni. Questi poteri includono la facoltà di richiedere a persone fisiche o giuridiche di fornire informazioni necessarie, comprese quelle da presentare periodicamente e in formati specifici per scopi di vigilanza e statistici. Tali richieste possono essere estese anche a terzi ai quali sono state esternalizzate funzioni o attività, compresi i fornitori di servizi *ICT* "critici" come definiti dal *DORA*.

In questo senso, anche l'art. 100, par. 3, della CRD VI, stabilisce obblighi e restrizioni per le entità e i consulenti terzi che le assistono nei *test* di stress, esercizi volti a valutare la resilienza delle entità a *shock* economici o finanziari. L'obiettivo di questa norma è garantire l'integrità di tali *test*, prevenendo comportamenti opportunistici o collusivi che potrebbero distorcerne i risultati. In particolare, le entità e i consulenti devono astenersi dallo svolgere attività che potrebbero compromettere la validità o l'affidabilità dei *test*. Le autorità competenti sono investite del potere di raccogliere informazioni e condurre indagini per identificare potenziali violazioni, incluso l'accesso ai dati e alle informazioni necessari. La disposizione richiama inoltre altre normative pertinenti, così che le autorità competenti non solo debbano vigilare sull'integrità dei *test* di *stress*, ma anche garantire la conformità a tutte le altre normative collegate.

Dal punto di vista normativo, la *CRD* VI dovrà essere recepita da parte degli Stati membri nel diritto nazionale entro il 10 gennaio 2026. In quanto direttiva, agli Stati membri è lasciato un certo margine di discrezionalità nel modo in cui adattare le sue disposizioni alla propria legislazione nazionale; tuttavia, eventuali modifiche dovranno comunque garantire il raggiungimento degli obiettivi fissati dalla normativa europea ed essere compatibili con i principi fondamentali del diritto dell'UE. Dunque, nel recepirla, gli ordinamenti nazionali presumibilmente non si discosteranno molto da questo approccio.

60 Direttiva (UE) 2024/1619 del Parlamento europeo e del Consiglio del 31 maggio 2024 che modifica la Direttiva 2013/36/UE per quanto riguarda i poteri di vigilanza, le sanzioni, le succursali di paesi terzi e i rischi ambientali, sociali e di *governance*.

6. Una sintetica analisi comparativa delle politiche di esternalizzazione negli USA e nel Regno Unito

Negli Stati Uniti, l'uso di fornitori terzi per i servizi e prodotti finanziari è regolato da tempo, con un programma inter-agenziale per la supervisione tecnologica in atto da diversi anni. Il *Bank Service Company Act* (BSCA) affida alla *Federal Reserve*, alla *Federal Deposit Insurance Corporation* (FDIC) e all'*Office of the Comptroller of the Currency* (OCC) la regolamentazione di servizi eseguiti da terzi. Quando un servizio è coperto dal BSCA, le agenzie possono regolamentare ed esaminare l'attività con la stessa invasività utilizzabile nei riguardi dell'istituto finanziario. Le agenzie conducono esami sui fornitori di servizi tecnologici che rappresentano un rischio significativo per le istituzioni finanziarie clienti e per il settore finanziario, concentrandosi sulla gestione della tecnologia, sull'integrità dei dati, sulla riservatezza delle informazioni, sulla disponibilità dei servizi e sulla conformità. I risultati degli esami vengono messi a disposizione del fornitore di servizi e delle istituzioni finanziarie esternalizzanti, potendo i risultati contribuire a un monitoraggio costante[61].

Nel dicembre 2013, la *Federal Reserve* ha emanato una *Guidance on Managing Outsourcing Risk*[62], che include raccomandazioni per la selezione e la supervisione dei fornitori, il monitoraggio del rischio e la protezione dei dati. Questo documento, esteso a tutte le banche vigilate dalla FED, promuove il controllo sui fornitori terzi, la continuità aziendale e l'adeguata valutazione dei rischi ed integra l'*Outsourcing Technology Services Booklet* del *Federal Financial Institutions Examination Council* (FFIEC), del giugno 2004[63]. La *Guidance* identifica diverse categorie di rischio (conformità, concentrazione, reputazionale, legale, operativo e di Paese) che le istituzioni finanziarie devono valutare prima e durante l'*outsourcing*[64]. In questo contesto, è fondamentale effettuare una valutazione preliminare dei rischi legati all'attività da esternalizzare[65]. Inoltre, il programma di gestione dei rischi associati all'attività del fornitore di servizi esternalizzati dovrebbe prevedere un livello di sorveglianza e controllo adeguato al grado di rischio e in linea con gli accordi di esternalizzazione[66]. Dell'attuazione di queste politiche è responsabile il *top management*[67].

61 Board of Governors of the Federal Reserve System, *Supervision and Regulation Report*, May 2022, box 3, 17.

62 Board of Governors of the Federal Reserve System, *Guidance on Managing Outsourcing Risk*, December 5, 2013.

63 Federal Financial Institutions Examination Council (FFIEC), *Outsourcing Technology Services Booklet*, IT Examination Handbook, June 2004.

64 Par. II - Risks from the Use of Service Providers, *Guidance on Managing Outsourcing Risk*.

65 Par. IV - Service Provider Risk Management Programs, Sez. IV.A - Risk Assessments, *Guidance on Managing Outsourcing Risk*.

66 Par. IV - Service Provider Risk Management Programs, *Guidance on Managing Outsourcing Risk*.

67 Par. III - Board of Directors and Senior Management Responsibilities, *Guidance on Managing Outsourcing Risk*.

Parimenti, nel Regno Unito, il *discussion paper DP3/22 – Operational resilience: Critical third parties to the UK financial sector* del 2022[68], nel riconoscere la dipendenza del settore finanziario del Paese dai servizi tecnologici di terze parti, ha sollecitato pareri su misure di regolamentazione per mitigare i rischi derivanti da alcune terze parti critiche (CTP) e rendere i servizi da esse forniti più resilienti. Questo documento richiama anche il precedente *Bank of England policy on Operational Resilience of FMIs*[69] del 2021 con il quale le autorità di vigilanza hanno introdotto regole per rafforzare la resilienza operativa delle aziende e delle FMI, ritenendo le aziende responsabili della gestione dei rischi operativi anche quando fanno uso di terze parti.

Nel 2023 è stato così pubblicato il *consultation paper CP26/23 - Operational resilience: Critical third parties to the UK financial sector*[70] proponendo requisiti per gestire i rischi per la stabilità e la fiducia finanziaria derivanti da possibili guasti o interruzioni dei servizi dei CTP: con questo documento, le autorità di vigilanza ritengono opportuno un intervento normativo che introduca un regime di sorveglianza per i CTP, progettato per integrarsi al meglio con i regimi analoghi, attuali e futuri, in particolare con il Regolamento *DORA* e il BSCA[71] menzionati precedentemente[72].

7. Riflessioni finali: un nuovo perimetro di vigilanza oltre le attività riservate

La previsione normativa della vigilanza sui soggetti che prestano le attività esternalizzate ai soggetti finanziari regolati pone un interrogativo in merito al perimetro della vigilanza che sembra andare oltre quello della riserva di attività. In altre parole, come noto, la riserva di attività tradizionalmente persegue la finalità di porre una disciplina a carattere soggettivo, regolando l'attività delle entità che accedono a tale attività riservata, anche attraverso regole di comportamento e di stabilità a carico degli operatori

68 Prudential Regulation Authority, Financial Conduct Authority and Bank of England, *DP3/22 – Operational resilience: Critical third parties to the UK financial sector*, Discussion Paper, 21 July 2022.

69 Prudential Regulation Authority, Financial Conduct Authority and Bank of England, *Bank of England policy on Operational Resilience of FMIs*, 29 March 2021.

70 Prudential Regulation Authority, Financial Conduct Authority and Bank of England, *Consultation paper CP26/23 - Operational resilience: Critical third parties to the UK financial sector*, 7 December 2023.

71 Cfr. par. 11.31 *Consultation paper CP26/23 - Operational resilience: Critical third parties to the UK financial sector*: «*The Bank considers that the proposed CTP regime supports its financial stability objective by increasing the operational resilience of designated CTPs that offer services to firms or FMIs operating in another country, which can be argued as contributing positively to financial stability in that country. The regulators also note that the proposals allow for overseas entities to be designated as CTPs, and it can be argued that oversight of a designated CTP also enhances financial stability in other countries or territories which that CTP provides services to. Furthermore, the proposed oversight regime for CTPs has been designed to be as interoperable as reasonably practicable with similar regimes, such as the EU's DORA and the US's BSCA*».

72 Sulla comparazione USA, UE, UK in materia di utilizzo di fornitori terzi si veda D. Roselli, *Outsourcing: Terze Parti fornitrici e governo del rischio*, in www.dirittobancario.it, 21 marzo 2024.

del settore per servire al meglio l'interesse dei clienti e per l'integrità dei mercati[73]. Se, così, parte delle attività sono esternalizzate e sui soggetti che erogano dette attività esternalizzate si estendono i poteri di vigilanza delle autorità di settore, ci si potrebbe chiedere se dette attività esternalizzate debbano essere altresì sottoposte a riserva di attività.

Uno spunto in tal senso sembra cogliersi, sebbene su un piano non pienamente coincidente, nel ROFIEG (*Expert Group on Regulatory Obstacles to Financial Innovation*), in particolare nella *Recommendation 5 – Outsourcing guidelines and certification/licensing* del già citato *report Thirty Recommendations on Regulation, Innovation and Finance*, ove è disposto che dispone che «la Commissione, in collaborazione con le AEV, dovrebbe valutare la necessità di introdurre un regime di certificazione o di licenza per i terzi che forniscono servizi tecnologici ai soggetti regolamentati»[74].

73 Sul tema cfr. R. Lener – P. Lucantoni, *Il Mercato Finanziario*, in P. Corrias - R. Lener, *op. cit.*, p. 459.

74 Traduzione delle autrici. Di seguito, per ragioni di completezza, il testo integrale della *Recommendation 5* in lingua originale: «*The Commission, in cooperation with the ESAs and the ESCB, international standardsetting bodies and other relevant authorities, should regularly monitor the extent and structure of outsourcing of critical services by financial institutions, and assess the appropriateness of tools in place to mitigate concentration risks, operational risks and systemic risk, taking account of the potential impact on innovation and competition. On this basis: - the ESAs should regularly review the outsourcing guidelines with a view to maintaining their proportionality in light of technological developments, new risks and new market conditions; - the Commission, in cooperation with the ESAs, should consider the need to introduce a certification or licensing regime for third parties providing technology services to regulated entities*».