DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

L'outsourcing nel settore finanziario

Dall'evoluzione regolamentare alle nuove frontiere della resilienza digitale

Novembre 2025

Debora Motta, Partner, Atrigna & Partners
Federico Morri, Of Counsel, Atrigna & Partners
Alberto Molle, Associate, Atrigna & Partners

Debora Motta, Partner, Atrigna & Partners

Federico Morri, Of Counsel, Atrigna & Partners

Alberto Molle, Associate, Atrigna & Partners

Debora Motta

È entrata a far parte dello Studio Atrigna & Partners dal 2016, occupandosi principalmente di questioni inerenti il diritto dei mercati finanziari, bancario e societario. Si occupa in particolare di gestione collettiva del risparmio, corporate e M&A, diritto e regolazione degli emittenti quotati. Debora Motta è iscritta all'Ordine degli Avvocati di Milano dal 2019.

1. L'evoluzione regolamentare nelle entità vigilate tra outsourcing "tradizionale" e "ICT"

In un contesto di mercato sempre più globalizzato, alla ricerca di soluzioni altamente innovative e allo stesso tempo competitive, il fenomeno dell'*outsourcing* nel settore finanziario ha visto una forte crescita, attirando su di sé una maggiore attenzione da parte delle Autorità di Vigilanza unionali e nazionali.

L'*outsourcing*, infatti, se da un lato permette alle entità finanziarie di avvalersi di competenze (anche tecnologiche) altamente qualificate e specializzate, senza l'onere di svilupparle internamente, dall'altro, presuppone una relazione tra cliente e fornitore ben strutturata e trasparente. Il rapporto tra l'impresa che esternalizza (*outsourcee*) e l'azienda alla quale è affidata l'attività (*outsourcer*), infatti, oltre a prevedere il coinvolgimento strategico del fornitore in processi aziendali più o meno importanti, può giungere nel tempo ad instaurare una dipendenza, tale da rendere particolarmente complessa per l'*outsourcee* la sostituibilità dell'*outsourcer*

Proprio in virtù di tali circostanze sono emersi i primi interrogativi sui rischi legati all'*outsourcing* e la conseguente regolamentazione che ne è scaturita, a vari livelli, per tutte le entità finanziarie[1].

Nel linguaggio regolamentare, in termini generali, con "esternalizzazione" ci si riferisce all'accordo in qualsiasi forma tra un intermediario vigilato e un fornitore di servizi, in base al quale il fornitore realizza un processo, un servizio o un'attività che sarebbe altrimenti svolto dallo stesso intermediario[2].

1 Senza pretesa di esaustività si vedano: A. Polizzi in S. Casamassima – M. Nicotra (a cura di), *L'Outsourcing nei servizi bancari e finanziari – La disciplina dell'esternalizzazione alla luce dei recenti interventi regolamentari (Linee guida EBA Febbraio 2019 ed aggiornamento Circolare 285 della Banca d'Italia)* , CEDAM, 2021; in relazione alle imprese assicurative, S. Micheli e U. Cunial, *I presidi in materia di esternalizzazione nel quadro normativo di Solvency II*, dirittobancario.it; in materia di imprese di investimento, M. Maugeri, *Esternalizzazione di funzioni aziendali e "integrità" organizzativa nelle imprese di investimento*, BBTC , fasc. 4.

2 Per la corretta definizione di "esternalizzazione" si vedano: a) per le banche e le SIM di classe 1, la Circolare 285/2015, Parte I, Titolo IV, Cap. 3, Sez. I, par. 3; b) per gli intermediari finanziari iscritti all'albo previsto dall'art. 106 TUB, la Circolare 288/2015, Titolo III, Cap. 1, Sez. I, par. 3, lett. j; c) per gli intermediari che prestano servizi e attività di investimento e di gestione collettiva del risparmio, l'articolo 2, comma 1, numero 4, del Regolamento 5 dicembre 2019; d) per le imprese assicurative, l'articolo 1, comma 1, lett. n-quinquies, del Decreto Legislativo 7 settembre 2005, n. 209. A tal riguardo, si evidenzia, in aggiunta, che la Suprema Corte ha fornito una definizione di esternalizzazione che ricomprende ogni possibile tecnica attraverso la quale un'impresa dismette la gestione diretta di alcuni segmenti dell'attività produttiva e dei servizi estranei al *core business*, cosi: Cass., 2 ottobre 2006, n. 21287.

vedi l'articolo online

All'interno della nozione generale di esternalizzazione, un ruolo centrale è attribuito dal legislatore europeo e nazionale alla categoria delle funzioni essenziali o importanti (FEI)[3] o funzioni operative importanti (FOI)[4], acronimi che segnano una prima linea di demarcazione tra forme di *outsourcing* "ordinario" e situazioni che, per la loro rilevanza strategica o sistemica, richiedono presidi organizzativi, contrattuali e di controllo di natura rafforzata. Si tratta di funzioni idonee a compromettere gravemente - qualora si verificasse un'anomalia nella loro esecuzione o la stessa venisse meno - i risultati finanziari, la solidità o la continuità dell'attività dell'ente di conformarsi nel continuo alle condizioni e agli obblighi derivanti dalla sua autorizzazione o agli obblighi previsti dalla disciplina di vigilanza, o, ancora, di funzioni relative ad attività sottoposte a riserva di legge, nella misura in cui la presentazione di tali attività richieda l'autorizzazione da parte di un'Autorità di Vigilanza, ovvero riguardi compiti operativi delle funzioni aziendali di controllo[5].

La distinzione tra *outsourcing* "ordinario" e *outsourcing* di FEI/FOI, dunque, non rileva esclusivamente sul piano terminologico, bensì, incide profondamente sugli adempimenti che la normativa pone a carico degli intermediari.

Basti qui rilevare che agli stessi è richiesto: (i) per tutti gli accordi di esternalizzazione, a prescindere quindi dalla qualificazione del servizio come FEI o FOI, di formalizzare, quale contenuto *de minimis* dell'accordo, la durata, i termini di rinnovo e di preavviso, il costo, la tipologia e le caratteristiche della funzione esternalizzata; e (ii) in aggiunta, per i soli accordi di esternalizzazione di FEI o FOI, di motivare le ragioni della classificazione, svolgere una valutazione dei rischi derivanti dall'esternalizzazione, effettuare e pianificare verifiche di *audit*, valutare il livello di sostituibilità del fornitore, applicare presìdi in caso di subesternalizzazione e, infine, di individuare efficaci strategie di *exit* in grado di garantire che l'attività prosegua senza soluzioni di continuità.

Chiarito quanto sopra, uno degli aspetti preliminari e spesso problematici delle decisioni di *outsourcing* è proprio la corretta individuazione delle attività da esternalizzare e il loro corretto inquadramento quali FEI o FOI[6].

In tale contesto, le decisioni di esternalizzazione possono - in prima battuta - essere assunte attraverso l'analisi di quattro dimensioni strategiche:

- criticità strategica delle attività;
- esposizione al rischio;
- rilevanza sul processo di creazione del valore;
- impiego di risorse e competenze.

Solo a seguito di tale analisi preliminare potrà, poi, procedersi alla valutazione di tutti gli altri fattori (inclusa la selezione dell'*outsourcer* più adatto), garantendo un corretto presidio del rischio di affidare a soggetti terzi l'espletamento di attività la cui interruzione danneggerebbe in misura rilevante l'intermediario, le sue attività e/o i suoi clienti.

L'*outsourcing* per le entità finanziarie, pertanto, non è e non può essere ridotto ad un mero e sempli-

3 Così definita: a) per le banche e le SIM di classe 1, dalle disposizioni della Circolare 285/2015, Parte I, Titolo IV, Cap. 3, Sez. I, par. 3; b) per gli intermediari che prestano servizi e attività di investimento, dall'articolo 4, comma 1, del Regolamento 5 dicembre 2019; c) per gli intermediari che prestano servizi di gestione collettiva del risparmio, dall'articolo 31, comma 1, del Regolamento 5 dicembre 2019; d) per le imprese assicurative, dall'articolo 2, comma 1, lett. c, del Regolamento IVASS n. 38 del 3 luglio 2018.

4 Così definita: a) per gli istituti di pagamento e gli istituti di moneta elettronica, dalle disposizioni di vigilanza per IP e IMEL, Capitolo 6, Allegato B; b) per gli intermediari finanziari iscritti all'albo previsto dall'art. 106 TUB, dalle disposizioni della Circolare 288/2015, Titolo III, Cap. 1, Sez. I, par. 3, lett. h.

5 Per la definizione di "funzioni aziendali di controllo" si vedano: a) per le banche e le SIM di classe 1, la Circolare 285/2015, Parte I, Titolo IV, Cap. 3, Sez. I, par. 3; b) per gli intermediari finanziari iscritti all'albo previsto dall'art. 106 TUB, la Circolare 288/2015, Titolo III, Cap. 1, Sez. I, par. 3, lett. f; c) per gli intermediari che prestano servizi e attività di investimento e di gestione collettiva del risparmio, l'articolo 2, comma 1, numero 5, del Regolamento 5 dicembre 2019. Per quanto di interesse in questo contesto, una definizione simile in ambito assicurativo, si può trarre dall'articolo 30, comma 2, lett. e, del Decreto Legislativo 7 settembre 2005, n. 209.

6 Basti qui rilevare che gli "Orientamenti in materia di esternalizzazione" dell'European Banking Authority del 25 febbraio 2019 specificano che non devono essere considerate esternalizzazione: (i) una funzione che a norma di legge deve essere svolta da un fornitore di servizi; (ii) i servizi di informazione sui mercati; (iii) le infrastrutture di rete globali; (iv) gli accordi ci compensazione e regolamento tra organismi di compensazione, controparti centrali e istituti di regolamento e loro membri; (v) le infrastrutture globali di messaggistica finanziaria soggette alla vigilanza delle pertinenti Autorità; (vi) i servizi bancari di corrispondenza, e (vii) l'acquisizione di servizi che altrimenti non sarebbero intrapresi dall'ente o dall'istituto di pagamento.

ce accordo contrattuale, caratterizzandosi, invece, come un processo articolato in varie fasi, le quali hanno certamente il loro punto di partenza nell'analisi strategica dell'attività/processo/funzione che si intende esternalizzare, ma non si esauriscono poi nella sottoscrizione dell'accordo. Non può, infatti, essere trascurata la fase istruttoria (*due diligence*), atta a raccogliere tutta la documentazione necessaria ad avviare la successiva fase valutativa, per poi proseguire alla fase esecutiva, la quale, in ogni caso, non termina il processo, che prosegue con il monitoraggio continuo dell'efficienza ed efficacia delle attività prestate dall'*outsourcer*.[7]

È proprio grazie al corretto espletamento di tutte le fasi di tale processo che l'intermediario può gestire i rischi sottostanti all'esternalizzazione, individuando anche presidi (flussi informativi, KPI, SLA, clausole di risoluzione e recesso, penali) idonei a tutelarlo dalle responsabilità che, anche in caso di esternalizzazione, continuano a gravare sullo stesso. L'intermediario, infatti, pur trasferendo all'esterno l'esecuzione di determinate attività, non trasferisce la responsabilità della loro corretta esecuzione, né della conformità complessiva alle disposizioni di legge e regolamentari. Invero, la responsabilità ultima rimane in capo all'intermediario che sarà chiamato a giustificare le proprie scelte in materia di esternalizzazione e il complessivo assetto dei controlli interni adottato.

In tale prospettiva, è sull'organo di supervisione strategica che grava - in prima battuta - l'onere di definire una politica aziendale in materia di esternalizzazione che individui con chiarezza le responsabilità interne connesse alle fasi del processo di esternalizzazione, per poi verificarne la corretta attuazione.

1.1 *L'esternalizzazione ICT*

In tempi più recenti, accanto a un quadro normativo già da tempo volto a presidiare i rischi connessi alle esternalizzazioni "tradizionali", si è progressivamente affermata un'attenzione crescente verso una delle aree più sensibili che gli intermediari tendono ad affidare a soggetti esterni: i servizi informatici e digitali. Tale ambito rappresenta oggi uno dei principali snodi dell'evoluzione organizzativa e tecnologica del settore. In particolare, l'utilizzo di infrastrutture e servizi "*cloud*" ha profondamente modificato il modo in cui le entità finanziarie gestiscono le proprie attività operative e i propri dati.

Nella prima fase della rivoluzione informatica, i servizi oggetto di fornitura riguardavano tipicamente l'esercizio di applicazioni informatiche basilari e standardizzate, che trovavano la loro ragion d'essere nella necessità, specie per le imprese di dimensioni più ridotte, di esternalizzare competenze tecniche non sempre disponibili internamente, così da assicurare uno svolgimento efficace ed efficiente di tali attività.

Nel contesto finanziario contemporaneo, tuttavia, la pervasività e diffusione dei servizi informatici ha portato a un radicale cambio di prospettiva: la sicurezza informatica ha assunto una rilevanza sistemica. Non si tratta più di un mero presidio di tutela dei sistemi informatici e dei dati, ma di un elemento costitutivo della stabilità economica e della fiducia nei mercati. La *resilienza* operativa digitale rappresenta dunque un presupposto imprescindibile di affidabilità dell'intermediario e di tutela dei diritti degli utenti[8].

In tale prospettiva, l'esternalizzazione di attività/servizi/processi ICT ("*Information and Communication Technology*") ha progressivamente attirato l'attenzione delle Autorità di Vigilanza europee, che sono intervenute con l'emanazione di specifiche linee guida volte a disciplinare i profili di rischio e di *governance*. Invero, dapprima l'EBA con gli Orientamenti sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione e di sicurezza (di seguito, anche gli "Orientamenti EBA ICT")[9] e successivamente, nello stesso solco, l'ESMA con gli Orientamenti in materia di esternalizzazione a fornitori di servizi *cloud* (di seguito, anche gli "Orientamenti ESMA ICT")[10], hanno definito un quadro di principi e *best practices* per assicurare che l'esternalizzazione di attività ICT avvenga nel rispetto di adeguati presidi di controllo, sicurezza e continuità operativa.

7 Senza pretesa di esaustività si veda: F. Bertola, F. Bonardi, *L'esternalizzazione nel regime EBA: profili organizzativi e di responsabilità*, dirittobancario.it, dicembre 2021.

8 In tal senso, si veda: *Banca d'Italia, Cybersecurity for financial stability*, bancaditalia.it; Sull'aumento dell'esposizione ai rischi, si veda: *Sadibaquarantotto*, Intervento di Giuseppe Siani, Capo del Dipartimento Vigilanza Bancaria e Finanziaria Banca d'Italia, 28 marzo 2025.

9 EBA/GL/2019/04, 28 novembre 2019, *Orientamenti dell'EBA sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) e di sicurezza*.

10 ESMA65-294529287-4737, 30 settembre 2025, *Orientamenti dell'ESMA in materia di esternalizzazione a fornitori di servizi cloud*.

vedi l'articolo online

Questo percorso regolatorio, articolato in interventi di *soft law*, ha progressivamente costruito una cornice di principi comuni, ma ha anche mostrato i limiti di una disciplina frammentata, incapace di rispondere in modo unitario alla complessità del rischio digitale.

Il recente intervento normativo europeo di *hard law*, attraverso il Regolamento (UE) 2022/2554 – *Digital Operational Resilience Act* (di seguito, anche "DORA")[11], rappresenta la risposta organica dell'Unione europea a tali criticità, istituendo un quadro comune di regolamentazione in materia di ICT, volto a superare la parzialità degli approcci precedenti e armonizzando le normative nazionali[12].

Nella prospettiva armonizzatrice dell'intervento regolamentare che ha introdotto il DORA si colloca la Comunicazione della Banca d'Italia del 30 dicembre 2024[13], con la quale l'Autorità ha richiamato l'attenzione degli intermediari sull'applicazione del DORA, definendo tale regolamento come un *framework* armonizzato in materia di *governance* del rischio ICT, in continuità con gli Orientamenti EBA ICT.

Il processo di aggiornamento del quadro normativo si è ulteriormente consolidato con un recente intervento dell'EBA[14], volto a modificare gli Orientamenti EBA ICT, nei quali l'Autorità ha riconosciuto la prevalenza del DORA e ha conseguentemente limitato il loro ambito applicativo. Le sezioni relative alle definizioni, ai destinatari e ai requisiti contrattuali sono state in larga parte abrogate o sostituite, mantenendo in vigore soltanto le disposizioni riferite a soggetti non inclusi nel perimetro del DORA. Tale modifica segna il definitivo superamento del modello di *soft law* e il consolidamento del DORA come fonte primaria e autonoma per la disciplina della *resilienza* digitale nel settore finanziario.

A tali interventi volti a riconoscere ed integrare le disposizioni normative previste dal DORA nei relativi ambiti di disciplina, si unisce la recente pubblicazione della guida BCE sull'esternalizzazione di servizi *cloud* a fornitori terzi di servizi *cloud*[15], che chiarisce le aspettative della BCE nei confronti delle banche soggette alla vigilanza della stessa in merito al rispetto dei requisiti del nuovo quadro normativo unionale.

Il DORA sposta l'attenzione dalla semplice gestione del rischio informatico al concetto di *resilienza* operativa digitale, imponendo alle entità finanziarie obblighi preventivi di protezione, monitoraggio e risposta. Inoltre, rispetto agli Orientamenti EBA ICT, il DORA amplia sensibilmente il perimetro regolamentare, passando a disciplinare in modo sistematico l'intera catena di fornitura ICT.

Tra le novità di maggior rilievo in relazione alla *governance* degli intermediari introdotte dal nuovo quadro normativo, si evidenzia l'attribuzione della responsabilità della gestione dei rischi informatici a una funzione di controllo (di seguito anche "*ICT Risk Manager*"), precisando che la stessa deve soddisfare un livello appropriato di indipendenza. Nell'analisi dei principali adempimenti introdotti dal DORA, Banca d'Italia[16] ha in tal senso rilevato – in virtù dell'assenza di disposizioni di dettaglio in ambito sovranazionale – che, nel rispetto dei principi di proporzionalità e di neutralità organizzativa, gli intermediari possano valutare se istituire o confermare un'autonoma funzione di controllo ICT, oppure attribuire i compiti di controllo ICT alla funzione di *risk management* e/o a quella di *compliance* (ove le funzioni siano affidate ad un'unica struttura, Banca d'Italia ritiene che anche la funzione di controllo ICT possa essere affidata a quest'ultima).

11 Il riferimento al DORA deve considerarsi inclusivo della normativa di secondo livello, ossia: Regolamento Delegato (UE) 2024/1772 - RTS che detta i criteri per la classificazione degli incidenti legati alle ICT; Regolamento Delegato (UE) 2024/1773 - RTS che specifica la politica sui servizi ICT forniti da fornitori terzi di ICT; Regolamento Delegato (UE) 2024/1774 - RTS che specifica gli strumenti, i processi e le politiche per la gestione dei rischi ICT; Regolamento di esecuzione (UE) 2024/2956 - ITS per stabilire i modelli per il registro delle informazioni; Regolamento Delegato (UE) 2025/301 - RTS sui contenuti, tempistiche e modalità di notifica di incidenti ICT significativi; Regolamento di esecuzione (UE) 2025/302 - ITS con i modelli standard da utilizzare per tali notifiche di incidenti ICT significativi; Regolamento Delegato (UE) 2025/1190 - RTS sui test di penetrazione guidati dalle minacce (TLPT); Regolamento Delegato (UE) 2025/532 - RTS sugli accordi di subfornitura di servizi ICT che supportano funzioni critiche o importanti.

12 Senza pretesa di esaustività si veda: A. Del Ninno, *DORA: gli adempimenti organizzativi, gestionali e documentali*, dirittobancario.it, settembre 2024; E. Fabbiani, A. Carnaccini, F. Bernardi, C. Piscopo, *Esternalizzazioni ICT: tra Regolamento DORA e Orientamenti EBA*, dirittobancario.it, marzo 2025.

13 Comunicazione della Banca d'Italia del 30 dicembre 2024 sul Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla *resilienza* operativa digitale per il settore finanziario (Regolamento DORA).

14 EBA/GL/2025/02, 11 febbraio 2025, *EBA Guidelines amending Guidelines EBA/GL/2019/04 on ICT and security risk management*.

15 BCE, 16 luglio 2025, *ECB Guide on outsourcing cloud services to cloud service providers*.

16 Si fa riferimento alla sopracitata Comunicazione della Banca d'Italia del 30 dicembre 2024 sul Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla *resilienza* operativa digitale per il settore finanziario (Regolamento DORA).

In attuazione della normativa europea, l'Autorità di Vigilanza nazionale ha inoltre chiarito che non devono ritenersi più applicabili i procedimenti amministrativi di divieto dell'esternalizzazione aventi ad oggetto l'*outsourcing* di servizi ICT a supporto di funzione essenziali o importanti[17] previsti dalla normativa secondaria[18], potendosi ritenere assorbiti dall'informativa all'Autorità di Vigilanza richiesta dall'articolo 28 del DORA.

Resta, invece, attuale l'obbligo in capo al Consiglio di Amministrazione di possedere conoscenze e competenze idonee a comprendere e valutare i rischi connessi all'esternalizzazione.

Un ulteriore aspetto centrale del DORA riguarda la soggezione dei fornitori terzi di servizi ICT considerati critici ("*critical third party providers*") alla vigilanza ed al controllo di un'Autorità di Vigilanza capofila ("*lead overseer*"). I *critical third party providers*[19], vale a dire quei soggetti il cui malfunzionamento o interruzione operativa potrebbe avere un impatto rilevante sulla stabilità del sistema finanziario europeo, sono individuati sulla base di elementi qualitativi e quantitativi, ponderati nel loro insieme. In tal senso, in primo luogo, è considerato il potenziale impatto sistemico di un'interruzione dei servizi prestati dal fornitore, in termini di continuità, sicurezza e qualità delle attività finanziarie interessate.

In secondo luogo, si tiene conto del grado di dipendenza funzionale degli intermediari dai servizi del fornitore. A ciò si aggiunge la valutazione della sostituibilità del fornitore, che implica un'analisi della disponibilità di alternative sul mercato, della complessità tecnica dei servizi offerti, della quota di mercato detenuta, nonché dei costi, dei tempi e dei rischi informatici o operativi connessi a una eventuale migrazione verso altri *provider*.

In ultimo, si considera il ruolo sistematico delle entità finanziarie che si affidano a quel fornitore. La combinazione di questi criteri consente alle Autorità europee di Vigilanza di individuare i fornitori la cui operatività assume carattere sistemico per la *resilienza* del mercato finanziario. Le stesse, una volta designato un fornitore come "critico", provvedono a individuare la *lead overseer* competente per la supervisione diretta del soggetto. Ai sensi dell'articolo 31, paragrafo 1, DORA, tale scelta ricade sull'Autorità che vigila sulle entità finanziarie che, nel loro complesso, detengono la quota più elevata delle attività totali tra quelle che si avvalgono dei servizi del fornitore critico[20].

Il DORA ha altresì introdotto il c.d. "registro delle informazioni" (ROI), volto a contenere informazioni dettagliate sulla natura dei servizi, sui rischi associati, sulle funzioni interessate e sulla catena di sub-fornitura.

Sul piano contrattuale, il DORA consolida e rafforza quanto già previsto dagli Orientamenti EBA ICT, elencando in modo dettagliato le clausole obbligatorie da inserire nei contratti con i fornitori ICT, con ulteriori prescrizioni per quelli a supporto di funzioni essenziali o importanti[21].

In ultima analisi, il nuovo quadro delineato dal DORA, introducendo obblighi formali o requisiti tecnici uniformi in tutto il territorio unionale, ridefinisce in senso sostanziale la relazione tra ente finanziario e fornitore ICT, ponendo la gestione del rischio digitale al centro della *governance* complessiva dell'intermediario.

17 Ai sensi dell'art. 3, punto 22 del DORA, per funzione essenziale o importante si intende una funzione la cui interruzione comprometterebbe sostanzialmente i risultati finanziari di un'entità finanziaria o ancora la solidità o la continuità dei suoi servizi e delle sue attività, o la cui esecuzione interrotta, carente o insufficiente comprometterebbe sostanzialmente il costante adempimento, da parte dell'entità finanziaria, delle condizioni e degli obblighi inerenti alla sua autorizzazione o di altri obblighi previsti dalla normativa applicabile in materia di servizi finanziari.

18 In particolare, si fa riferimento a: (a) il divieto di esternalizzare funzioni aziendali operative essenziali o importanti, ai sensi dell'articolo 50, comma 3 del Regolamento 5 dicembre 2019; (b) il divieto di esternalizzazione di funzioni aziendali operative essenziali o importanti a fornitori di servizi *cloud*, ai sensi dell'articolo 18, comma 4, del Regolamento 5 dicembre 2019; (c) il divieto di esternalizzare, in tutto o in parte, funzioni operative importanti e di controllo a un soggetto esterno o nell'ambito del gruppo di appartenenza per IP e IMEL, ai sensi delle Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica: Capitolo VI, Sezione II.

19 Si veda l'articolo 3, punto 23 del DORA che a sua volta rinvia all'articolo 31 DORA.

20 Si veda, senza pretesa di esaustività: P. Lucantoni, C. Villani, *La gestione e supervisione dei rischi ICT e di sicurezza nelle attività finanziarie esternalizzate tra DORA e CRD VI*, dirittobancario.it, gennaio 2025.

21 In particolare, il comma 2 dell'art. 30 del DORA individua gli elementi minimi per tutti i contratti: descrizione dei servizi e funzioni ICT, localizzazione di dati e servizi, livelli di servizio misurabili, misure di sicurezza e controllo dei dati adeguate, assistenza in caso di incidenti, cooperazione con le Autorità competenti, diritti di risoluzione e condizione di partecipazione alle attività di formazione. Il comma 3 introduce obblighi rafforzati per i servizi a supporto di FEI: target quantitativi e qualitativi degli SLA, preavvisi e notifiche rafforzate, piani di emergenza testati, cooperazione ai TLPT, ove applicabili all'ente finanziario, monitoraggio continuo con audit illimitati (o alternative di *assurance*) ed *exit strategy* che garantisca la transizione fino alla migrazione o internalizzazione del servizio.
In tal senso, per una compiuta disamina, si veda l'articolo 30 DORA.

vedi l'articolo online

È in questa prospettiva integrata che si ridisegna il paradigma del ciclo di vita del rapporto con il fornitore ICT.

2. Il ciclo di vita del rapporto con il fornitore di servizi ICT: considerazioni e consigli pratici

Dopo aver delineato il quadro regolamentare e di vigilanza, è ora possibile esaminare l'aspetto operativo della relazione con i fornitori, ossia come le prescrizioni del DORA si traducano nella gestione concreta del rapporto di *outsourcing*.

La gestione dei fornitori di servizi ICT[22], pur trovando nel contratto il suo momento centrale, non si esaurisce nella formazione ed esecuzione dell'accordo scritto, ma si intreccia con gli altri ambiti delineati dal DORA e, in particolare, con la gestione degli incidenti, la gestione dei cambiamenti, integrazioni e progetti ICT (c.d. *ICT project and change management*), nonché con le politiche e procedure di continuità operativa digitale.

In questo contesto, principio cardine sancito dal DORA è che, anche a seguito dell'affidamento del servizio ICT a un terzo, l'ente finanziario conserva una responsabilità piena e non delegabile, da esercitare secondo il principio di proporzionalità. Ne deriva un approccio *riskbased* che supera la mera formalizzazione del rapporto contrattuale: la relazione con il fornitore diventa un cantiere di *governance* condivisa, che richiede impegni e forme di collaborazione più mature e trasparenti rispetto alla consueta dinamica "committente-fornitore", divenendo componente strutturale dei presidi organizzativi e di controllo dei rischi ICT dell'entità finanziaria.

In tal senso, il DORA, insieme ai regolamenti delegati ed esecutivi, funge da filo rosso che vincola le parti a un impegno reciproco di tutela dei beni giuridici protetti: i diritti dei consumatori, le attività finanziarie e, più in generale, l'integrità del mercato finanziario europeo.

Il ciclo di vita degli accordi con il fornitore può essere articolato in sei fasi principali[23] - illustrate nel prosieguo - che devono essere disciplinate da un'apposita *policy*, almeno con riferimento alle forniture di servizi ICT a supporto di FEI.

Le indicazioni che seguono hanno carattere pratico, senza pretesa di esaurire le diverse configurazioni applicabili alle entità finanziarie, in quanto mirano ad assicurare coerenza operativa e tracciabilità delle scelte, mantenendo la segregazione tra soggetto promotore, esecutore e approvatore. La separazione dei ruoli, oltre a rispondere a un principio di buona *governance*, previene conflitti d'interesse e garantisce che la decisione sia il risultato di un controllo incrociato effettivo, così da garantire una gestione efficiente ed efficace dei processi che si basano su componenti ICT di terzi, assicurando che siano effettivamente *resilienti* e non ridotti a un mero formalismo contrattuale.

Fase 1 - Decisione sull'utilizzo del servizio ICT

La fase decisionale sull'acquisizione di un servizio ICT richiede una preliminare istruttoria interna volta a chiarire le motivazioni dell'iniziativa, le modalità di approvvigionamento e il perimetro operativo del servizio. Tale accertamento si svolge nel rispetto delle procedure di *ICT project and change management*, per assicurare coerenza metodologica e tracciabilità delle scelte. In questo contesto, vengono definiti, sin dall'inizio, il ruolo della terza parte e gli elementi caratterizzanti il servizio, con l'obiettivo di pervenire a una decisione consapevole e motivata circa l'opportunità di acquisirlo e le relative condizioni contrattuali e operative, ovvero se arrestare il processo di affidamento che, come noto, comporta

22 Elencati nell'Allegato III del Regolamento Esecutivo (UE) 2024/2956.

23 Le fasi qui proposte sono state individuate sulla base dell'art. 4 del Regolamento Delegato (UE) 2024/1773 che sotto la rubrica "*Fasi principali del ciclo di vita degli accordi contrattuali*" stabilisce: "*La politica specifica le prescrizioni, compresi le regole, le responsabilità e i processi, per ciascuna fase principale del ciclo di vita dell'accordo contrattuale, riguardanti almeno gli aspetti seguenti:*
a) le responsabilità dell'organo di gestione, compreso il suo coinvolgimento, se del caso, nel processo decisionale sull'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC;
b) la pianificazione degli accordi contrattuali, tra cui la valutazione dei rischi, la dovuta diligenza di cui agli articoli 5 e 6 e il processo di approvazione di nuovi accordi o di modifiche sostanziali di tali accordi di cui all'articolo 8, paragrafo 4;
c) il coinvolgimento delle unità aziendali, dei controlli interni e di altre unità pertinenti in relazione agli accordi contrattuali;
d) l'attuazione, il monitoraggio e la gestione degli accordi contrattuali di cui agli articoli 7, 8 e 9, anche a livello consolidato e subconsolidato, ove applicabile;
e) la documentazione e la tenuta dei registri, tenendo conto degli obblighi relativi al registro di informazioni di cui all'articolo 28, paragrafo 3, del regolamento (UE) 2022/2554;
f) le strategie di uscita e i processi di risoluzione di cui all'articolo 10."

un impegno significativo e multidisciplinare da parte dell'intermediario.

Cardine di questa fase è la chiara individuazione dell'oggetto della fornitura: occorre precisare le caratteristiche e i requisiti del servizio ICT (funzionali, tecnici, organizzativi e, ove pertinente, di sicurezza e continuità) rispetto agli obiettivi dell'entità finanziaria. Inoltre, con la definizione del servizio ICT vengono identificati i potenziali fornitori in grado di erogarlo secondo i requisiti delineati.

Fase 2 - *Due diligence* e *design* degli accordi

La *due diligence* precontrattuale è il momento in cui si identificano in modo strutturato i rischi ICT connessi al fornitore e lungo l'intera catena di subfornitura[24], così da trasformare l'intenzione di affidare il servizio all'esterno in una decisione effettivamente sostenibile sotto il profilo tecnico, giuridico e organizzativo.

La conduzione delle verifiche è solitamente attribuita alla funzione proponente o, nelle strutture dotate di presidi dedicati, alla funzione *procurement*, con il necessario supporto delle competenze IT (architetture, *cybersecurity* e affini), del *ICT Risk Manager* e, ove richiesto dalla natura del servizio o dagli esiti delle verifiche, con il coinvolgimento delle funzioni di controllo e supervisione - *Risk*, *Compliance* e DPO - per la valutazione tecnica delle evidenze raccolte.

La *due diligence* comprende una ricognizione puntuale degli elementi tecnici e organizzativi che danno sostanza alla protezione dell'ente e dei suoi clienti: localizzazione di dati e servizi, capacità di *audit* (anche con verifiche *on-site*, se necessario), misure di sicurezza e loro *governance*, certificazioni, gestione degli incidenti e procedure di *escalation*, piani di emergenza con evidenza dei *test*, *reporting* operativo e strategico, nonché livelli di servizio con indicatori e penali.

Un ulteriore elemento chiave è la valutazione del rischio di concentrazione a livello di entità, ossia la dipendenza dal fornitore ICT. Per mitigare tale rischio, è opportuno identificare già in fase di *due diligence* soluzioni alternative e prevedere clausole contrattuali che facilitino l'uscita e la migrazione verso altri fornitori.

Infine, la *due diligence* si estende anche alla verifica della solidità economicofinanziaria del fornitore e della filiera, insieme alla valutazione del quadro assicurativo - in particolare le polizze *cyber* - quale ulteriore elemento di mitigazione del rischio residuale.

Proprio in questa fase si consolida la classificazione del servizio quale supporto o meno a FEI[25].

Il percorso si chiude con l'intervento del *team* legale, che, in base agli *standard* contrattuali dell'organizzazione e agli obblighi normativi, predispone, o revisiona, il contratto di fornitura prevedendo i diritti, obblighi e tutele in modo coerente con il profilo di rischio emerso.

In definitiva, la fase precontrattuale è il momento in cui l'ente individua i rischi, mappa la filiera e definisce controlli e clausole, così da costruire un rapporto di fornitura solido che garantisca *resilienza* e governabilità.

Fase 3 - Negoziazione e formalizzazione degli accordi

Come in ogni pratica negoziale, anche l'acquisizione di servizi ICT prevede una fase di trattativa finalizzata alla formalizzazione dell'accordo di fornitura. Tuttavia, il contesto in cui questa trattativa si svolge è tutt'altro che uniforme: accanto ai tradizionali accordi di fornitura, si sono affermati modelli contrattuali complessi, tipici delle soluzioni *As a Service* (SaaS, PaaS, IaaS), spesso regolati da giurisdizioni straniere e caratterizzati da condizioni standardizzate. In tale scenario, la sfida per l'ente finanziario è duplice: da un lato, garantire il pieno rispetto dei requisiti contrattuali imposti dal DORA; dall'altro, mantenere un margine di flessibilità per gestire le peculiarità dei fornitori, che talvolta non consentono modifiche sostanziali alle proprie clausole per ragioni di scalabilità del prodotto.

24 Per i servizi ICT a supporto di FEI, la disciplina DORA prevede che la subfornitura sia regolata *ex ante*, attraverso una *due diligence* estesa alla filiera, condizioni contrattuali che garantiscano trasparenza, *audit* e rimedi, e un monitoraggio proporzionato lungo tutta la catena.

25 Vi sono poi casi limite che richiedono una qualificazione giuridica più attenta e coerente con i chiarimenti delle ESAs in materia di fornitura di servizi ICT. Come indicato dalle ESAs, quando il fornitore è un'entità finanziaria regolamentata, che eroga a un altro ente servizi finanziari vigilati, il servizio ICT connesso può assumere natura prevalentemente "finanziaria" e, come tale, risultare escluso dal perimetro contrattuale DORA, ferma restando l'applicazione degli altri obblighi che il regolamento pone in capo all'ente.

Quando l'adesione ai requisiti DORA incontra resistenze insormontabili, l'ente finanziario deve assumere una posizione chiara: valutare misure di mitigazione del rischio, ove praticabili, oppure rinunciare all'accordo. La negoziazione non è, dunque, un esercizio di compromesso illimitato, ma un processo orientato alla conformità normativa e alla tutela dell'ente.

Sul piano contenutistico, la trattativa deve assicurare il rispetto dei requisiti di cui all'art. 30 DORA, meglio descritti nella precedente sezione. A ciò si aggiunge un profilo formale non trascurabile: il DORA, infatti, richiede la forma scritta delle clausole previste dall'art. 30 DORA, con implicazioni che si riflettono sulla validità probatoria[26].

Con la formalizzazione dell'accordo contrattuale per l'utilizzo di servizi ICT a supporto di FEI, l'entità finanziaria è tenuta a informare tempestivamente l'Autorità competente[27].

Fase 4 - Attuazione e monitoraggio *in itinere*

La fase esecutiva del contratto è un processo dinamico che richiede un presidio costante. L'organizzazione deve monitorare il fornitore e l'intera catena del valore attraverso interlocuzioni regolari, *audit* periodici, raccolta di informazioni e verifiche sui KPI e sugli SLA, accompagnate da attività di *remediation* ove emergano scostamenti. L'obiettivo è duplice, da un lato garantire il corretto svolgimento del servizio e, dall'altro, preservare nel tempo le tutele di protezione definite al momento della sottoscrizione del contratto.

Il controllo dei contratti ICT è affidato, salvo deroghe, a un ruolo dedicato o a un dirigente di rango elevato, come previsto dall'art. 5, comma 3, DORA. Tale figura assicura la sorveglianza sugli accordi con i fornitori, sulla relativa esposizione al rischio e sulla documentazione, riferendo all'organo di gestione e coordinandosi con l'ICT *Risk Manager* per monitorare il rischio di concentrazione per fornitore, tecnologia e localizzazione, garantendo informazioni complete e tempestive per decisioni strategiche e conformità normativa[28].

Ai sensi del DORA, pare evidente come il monitoraggio *in itinere* debba essere un presidio permanente che richiede competenza, metodo e capacità di coordinamento: solo un controllo strutturato e proporzionato può rendere la relazione con il fornitore un fattore di *resilienza*, anziché una fonte di vulnerabilità giuridica e operativa.

Fase 5 - Procedure di uscita

La cessazione del rapporto con il fornitore, qualunque ne sia la causa, non può essere affrontata come un evento improvviso, ma, almeno nell'ambito dei servizi ICT a supporto di FEI, deve essere governata attraverso le strategie di uscita previste contrattualmente e integrate nei presidi di continuità operativa.

L'entità finanziaria, in qualità di titolare del processo, è chiamata a dirigere e coordinare tutte le attività necessarie per garantire la migrazione del servizio verso un altro fornitore o la sua internalizzazione, nel rispetto delle procedure di *ICT project and change management*. Tale responsabilità non è delegabile, sebbene il fornitore sia contrattualmente obbligato a cooperare e a non ostacolare la portabilità dei dati e la continuità operativa: la regia dell'operazione resta infatti sempre in capo all'ente[29].

La strategia di uscita è un presidio di *resilienza*, volto a mitigare il rischio sistemico connesso alla cessazione del rapporto contrattuale e a garantire, al contempo, la continuità dei servizi e la protezione

26 A tal riguardo, sebbene la firma olografa resti astrattamente possibile, la prassi si orienta verso firme elettroniche avanzate o qualificate, idonee a garantire autenticità e opponibilità in sede di verifica.

27 In generale, permane l'obbligo di comunicare almeno una volta all'anno il numero di nuovi accordi, le categorie di fornitori terzi, la tipologia dei contratti e le funzioni o i servizi ICT forniti.

28 Tale attività di *reporting* è a tutti gli effetti uno strumento di *governance* che consente all'organo di gestione di esercitare il proprio ruolo di supervisione, in linea con le aspettative crescenti delle Autorità di Vigilanza europee. Il monitoraggio deve essere particolarmente rigoroso in occasione di eventi di *change* o integrazioni ICT, che devono essere gestiti in collaborazione con il fornitore per assicurare la conformità ai requisiti DORA. Nei casi più gravi, come incidenti critici o eventi che minacciano la continuità operativa, la cooperazione tra le parti diventa essenziale per attivare tempestivamente i piani di emergenza, garantire la *resilienza* dei servizi e adempiere agli obblighi di segnalazione verso le Autorità di Vigilanza e di comunicazione agli *stakeholder* nei termini previsti dalla normativa.

29 Il piano di uscita deve prevedere scenari di interruzione, periodi di transizione, modalità di migrazione e internalizzazione, nonché *test* periodici per verificarne l'efficacia. La definizione dei ruoli e delle responsabilità è cruciale: il fornitore deve garantire supporto tecnico e disponibilità delle risorse necessarie, mentre l'ente deve assicurare la *governance* del processo, la protezione dei dati e la conformità alle norme DORA.

degli interessi giuridici tutelati dal DORA.

Fase 6 - Documentazione e registro delle informazioni (ROI)

Il ciclo di vita del rapporto con il fornitore deve essere documentato in modo continuo e coerente, dalla decisione iniziale fino alla cessazione del rapporto. Tale documentazione - che comprende atti, corrispondenza, *log*, verbali di riunione, *report* di monitoraggio e risultati di *audit* - deve essere archiviata e conservata con modalità idonee a garantirne integrità, autenticità e sicurezza, così da preservarne il valore probatorio nel tempo. Non si tratta di un adempimento meramente amministrativo: l'entità finanziaria, in quanto responsabile dell'operato della propria *supply chain*, deve poter soddisfare l'onere della prova in caso di verifiche dell'Autorità o di contenziosi con terzi. La qualità delle evidenze - completezza, tracciabilità, immodificabilità - diventa quindi il presupposto per dimostrare la diligenza nell'affidamento, nella vigilanza e nella gestione degli avvenimenti avversi.

Accanto al fascicolo istruttorio e operativo del singolo rapporto, il DORA impone la tenuta del registro delle informazioni relativo ai fornitori terzi di servizi ICT. Tale registro deve essere mantenuto e aggiornato a livello di entità, subconsolidato e consolidato, con la chiara distinzione dei contratti che sostengono FEI, e, su richiesta, deve essere esibito all'Autorità competente.

Ne discende un modello di *compliance* sostanziale, in cui la cura delle evidenze e la disciplina del ROI non sono "carta", ma infrastruttura della *resilienza*, la solidità della prova si traduce in certezza del diritto e nella concreta capacità di difesa.

3. Conclusioni

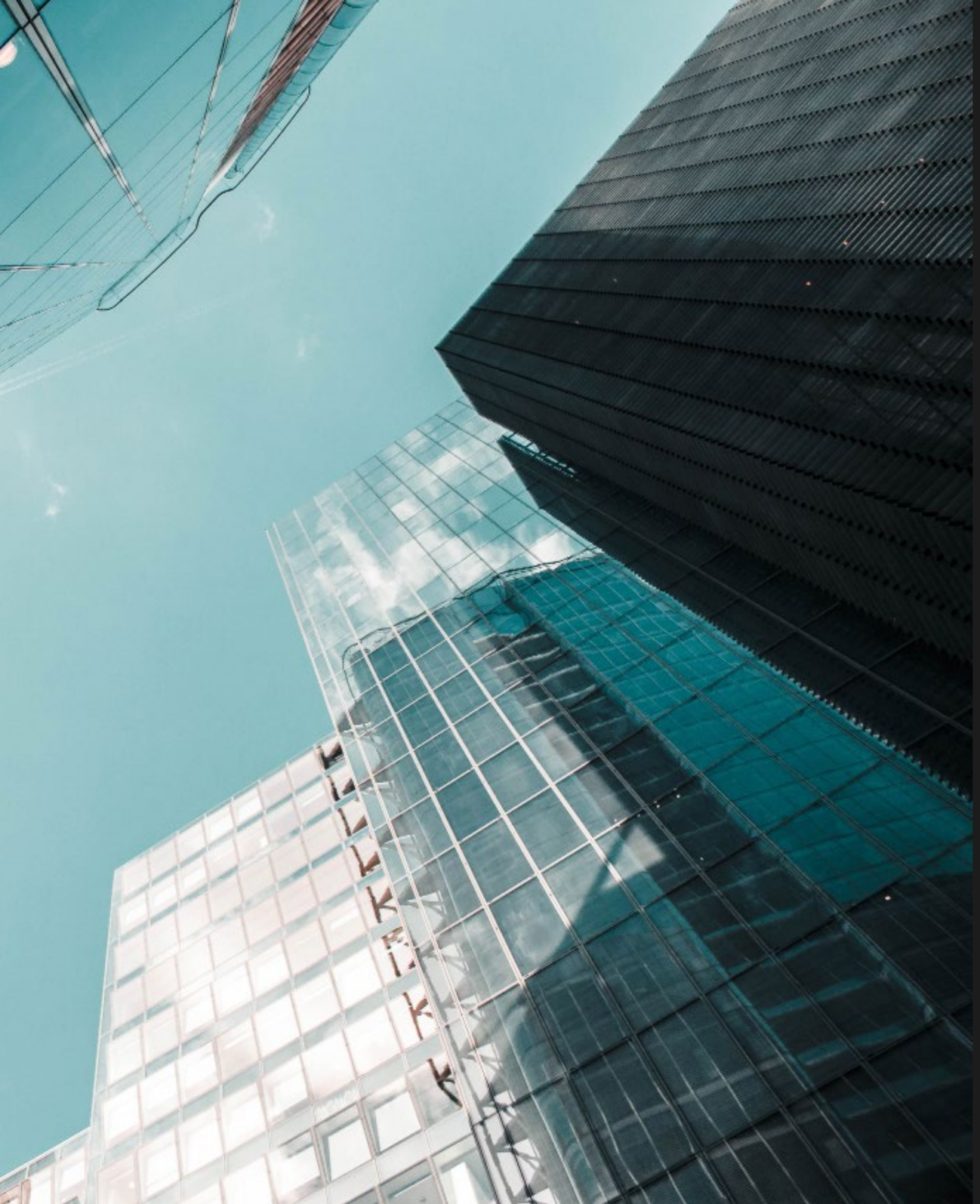
L'evoluzione del quadro regolamentare in materia di *outsourcing* sin qui descritto ha quindi determinato un mutamento del tradizionale rapporto "committente-fornitore", che è stato ridisegnato incrementando gli oneri procedurali a carico dell'intermediario al fine di assicurare un adeguato presidio del rischio connesso alle esternalizzazioni.

In tale contesto, il DORA, introducendo un quadro organico che ha armonizzato la disciplina delle esternalizzazioni in ambito ICT, inserisce nel sistema di *resilienza* operativa dell'ente anche la relazione collaborativa e trasparente con l'*outsourcee*, la quale diviene parte integrante dell'assetto di *governance* e controlli che, *in primis*, l'organo di supervisione strategica deve impostare, approvare e sorvegliare. La "terza parte" non è un soggetto esterno, ma un attore attivo del programma di *resilienza* digitale dell'ente.

Questa impostazione, sul solco delle esternalizzazioni "tradizionali", si traduce in un principio chiave: la responsabilità resta in capo all'ente finanziario. Il quale, adesso e nel futuro, ove intenda esternalizzare servizi ICT, sarà chiamato a rispettare il rigore richiesto dal DORA ed a gestire, così, in modo conforme ai requisiti normativi, gli accordi con tutti i fornitori ICT in perimetro, inclusi quelli che, in virtù della propria posizione di mercato, vantano un forte potere contrattuale nei confronti dell'ente finanziario.

Su tale fronte, il DORA fornisce strumenti concreti per dare sostanza ad un'architettura idonea a garantire la *resilienza* operativa, ma la norma, da sola, non è sufficiente, il resto dipende dalla nuova cultura organizzativa di cui l'ente dovrà diventare promotore, investendo, anche tramite il supporto di professionisti, nella formazione delle risorse interne e nella definizione e strutturazione di processi interni che siano in grado di garantire *resilienza* e conformità in ogni scenario operativo.

Solo affrontando i nuovi obblighi normativi con competenza, metodo e visione strategica sarà possibile trasformare la complessità regolatoria in un *asset* distintivo, capace di generare valore e rafforzare la competitività dell'ente.



DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it