DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Servizi TIC ed esternalizzazione di funzioni, tra DORA e disciplina AIFMD

25 Agosto 2026

Francesco Silla, DVMA - Della Vecchia Marrocco Associati

Francesco Silla, DVMA - Della Vecchia Marrocco Associati

Studio legale

DVMA - Della Vecchia Marrocco Associati

DVMA | DELLA VECCHIA MARROCCO ASSOCIATI STUDIO LEGALE

1. Premessa

Il Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (c.d. "DORA")[1] ha introdotto un quadro normativo armonizzato in materia di resilienza operativa digitale del settore finanziario, disciplinando la gestione dei rischi connessi all'utilizzo delle tecnologie dell'informazione e della comunicazione ("TIC") da parte delle entità finanziarie[2].

Tra i principali ambiti di intervento del nuovo *framework* assume rilievo la disciplina relativa alla gestione dei rischi derivanti da fornitori terzi di servizi TIC (*ICT third-party risk*), cui è dedicato il Capo V del DORA.

Come risulta dai considerando del DORA, le entità finanziarie sono divenute progressivamente più dipendenti dall'utilizzo di servizi TIC forniti da soggetti terzi[3], con la conseguente necessità di introdurre

1 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, in GUUE L 333 del 27 dicembre 2022, disponibile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022R2554. Il DORA è applicabile dal 17 gennaio 2025 (art. 64, par. 2).

2 Ai sensi dell'art. 2, par. 2, del DORA sono definite collettivamente "*entità finanziarie*" le entità elencate al par. 1, lettere da a) a t), del medesimo articolo, ossia: enti creditizi; istituti di pagamento, compresi gli istituti di pagamento esentati a norma della direttiva (UE) 2015/2366; prestatori di servizi di informazione sui conti; istituti di moneta elettronica, compresi gli istituti di moneta elettronica esentati a norma della direttiva 2009/110/CE; imprese di investimento; fornitori di servizi per le cripto-attività autorizzati a norma del regolamento sui mercati delle cripto-attività ed emittenti di *token* collegati ad attività; depositari centrali di titoli; controparti centrali; sedi di negoziazione; repertori di dati sulle negoziazioni; gestori di fondi di investimento alternativi; società di gestione; fornitori di servizi di comunicazione dati; imprese di assicurazione e di riassicurazione; intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio; enti pensionistici aziendali o professionali; agenzie di rating del credito; amministratori di indici di riferimento critici; fornitori di servizi di crowdfunding; repertori di dati sulle cartolarizzazioni. I fornitori terzi di servizi TIC, ai quali pure il DORA si applica ai sensi dell'art. 2, par. 1, lettera u), non rientrano invece nella nozione di "entità finanziarie".

3 Cfr. i considerando 27 e 28 del DORA, ove si rileva, rispettivamente, che "*la natura e la portata di tale dipendenza ha conosciuto negli ultimi anni un'evoluzione costante*" e che "*tale ampio uso dei servizi TIC è testimoniato dalla complessità degli accordi contrattuali*". Per evidenze quantitative sull'entità e sulla concentrazione del ricorso a fornitori terzi TIC, cfr. Banca d'Italia, *Rischio di terza parte ICT. Principali risultati dell'analisi orizzontale sui Registri delle Informazioni DORA*, *Workshop* sulla Resilienza Operativa Digitale, Roma, 4 febbraio 2026 (perimetro della rilevazione: banche meno significative e intermediari non bancari, oltre 300 segnalanti): 9.861 contratti TIC, di cui 5.283 (54 per cento) a supporto di almeno una FEI; spesa annua di 2,381 miliardi di euro, di cui 1,678 miliardi (70 per cento) per

presidi specifici volti a monitorare e gestire i rischi derivanti da tali rapporti.

La rilevanza sistemica del fenomeno trova riscontro nelle evidenze dell'attività di vigilanza svolta dalla Banca d'Italia. Nelle Considerazioni finali sull'anno 2025, il Governatore ha osservato che "*il crescente ricorso a fornitori esterni amplia le vulnerabilità: catene di fornitura articolate su più livelli e concentrate in pochi operatori possono trasformare criticità circoscritte in problemi di ampia portata*"; pertanto "*agli intermediari compete assicurare la salvaguardia e la continuità dei propri sistemi, anche quando si avvalgono di fornitori esterni*", fermo restando che "*su questi ultimi ricadono analoghe responsabilità*"[4].

Nella stessa direzione depongono, inoltre, i dati segnaletici: nell'analisi orizzontale sui gravi incidenti TIC relativa al 2025, la Banca d'Italia ha rilevato che "*in oltre la metà delle segnalazioni è coinvolto un fornitore o subfornitore di servizi*" e che "*il ruolo delle terze parti si conferma centrale nella gestione del rischio ICT*"[5].

2. La nozione di servizio TIC e il regime del Capo V

La nozione di "*servizio TIC*", costituisce il presupposto per l'applicazione del regime previsto dal Capo V del DORA.

Ai sensi dell'art. 3, punto 21) del DORA, sono servizi TIC i "*servizi digitali e di dati forniti attraverso sistemi di TIC a uno o più utenti interni o esterni su base continuativa, inclusi l'hardware come servizio e i servizi hardware, comprendenti la fornitura di assistenza tecnica mediante aggiornamenti di software e firmware da parte del fornitore dell'hardware, esclusi i servizi telefonici analogici tradizionali*".

La definizione richiede pertanto la compresenza di più elementi qualificanti: *(i)* la natura del servizio, che deve avere contenuto digitale o di dati; *(ii)* la modalità di erogazione, che deve avvenire "*attraverso sistemi di TIC*"; *(iii)* la destinazione della prestazione, che deve essere erogata "*a uno o più utenti interni o esterni*"; *(iv)* la continuità, essendo richiesta un'erogazione "*su base continuativa*".

In presenza di servizi così definiti, l'art. 28 del DORA richiede alle entità finanziarie di gestire i rischi informatici derivanti da terzi quali componenti integranti dei rischi informatici nel contesto del proprio quadro per la gestione di detti rischi, prevedendo specifici obblighi relativi alla valutazione, gestione e monitoraggio dei relativi rapporti contrattuali[6].

La disciplina si articola con intensità variabile a seconda della rilevanza funzionale del servizio, prevedendo un sistema di presidi organizzativi e contrattuali che si intensifica laddove i servizi TIC siano destinati a supportare funzioni essenziali o importanti (c.d. "FEI")[7].

Agli accordi relativi a quest'ultima categoria si applicano particolari presidi, quali la politica per l'utilizzo dei servizi TIC a supporto di FEI, l'obbligo di predisporre strategie di uscita e un contenuto contrattuale minimo ampliato[8].

FEI; incidenza della componente extra-gruppo pari al 95 per cento dei contratti e al 91 per cento della spesa; primi cinque fornitori di servizi TIC pari a circa il 40 per cento del costo dei contratti, primi dieci pari al 52 per cento. Su base più ampia, cfr. Banca d'Italia, *Relazione annuale. Anno 2025 – centotrentaduesimo esercizio*, Roma, 29 maggio 2026, cap. 12, ove si segnala che "*i primi cinque fornitori diretti rappresentano circa il 52 per cento della spesa totale*" e che "*Oltre la metà delle segnalazioni complessive ha interessato l'interruzione di servizi da parte di fornitori, nella maggior parte dei casi non superiore alle otto ore*".

4 Cfr. Banca d'Italia, *Considerazioni finali del Governatore. Relazione annuale. Anno 2025 – centotrentaduesimo esercizio*, Roma, 29 maggio 2026, pp. 26-27 (par. "La tecnologia e i rischi cibernetici" ove viene anche rilevato che, nel periodo 2023-25, gli incidenti che hanno coinvolto intermediari italiani "*sono aumentati dell'80 per cento rispetto al triennio precedente*" e che "*quelli di natura cibernetica sono raddoppiati*").

5 Banca d'Italia, *Quadro segnaletico di Vigilanza dei gravi incidenti ICT. Analisi orizzontale 2025*, luglio 2026, p. 6. Il documento precisa che "*Nel 56% delle segnalazioni risulta coinvolto un fornitore di servizi, con una proporzione sostanzialmente analoga tra segnalazioni operative e di cybersicurezza*" e che "*Nel caso delle banche meno significative, il fornitore è all'origine dell'evento nella quasi totalità delle segnalazioni relative a incidenti operativi*" (p. 9).

6 Cfr. art. 28, par. 1, del DORA, ai sensi del quale "*Le entità finanziarie gestiscono i rischi informatici derivanti da terzi quali componenti integranti dei rischi informatici nel contesto del proprio quadro per la gestione di detti rischi di cui all'articolo 6, paragrafo 1, e conformemente ai principi indicati* [...]".

7 Ai sensi dell'art. 3, punto 22), del DORA, per "*funzione essenziale o importante*" (c.d. "FEI") 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*".

8 Cfr. art. 28, par. 2, del DORA, quanto alla strategia per i rischi informatici derivanti da terzi, che "*comprende una politica per l'utilizzo dei servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi*"; art. 28, par. 8, che prescrive strategie di uscita per i soli "*servizi TIC a supporto di funzioni essenziali o importanti*"; art. 30, par. 3, quanto agli elementi che gli accordi relativi a servizi TIC a supporto di FEI devono comprendere "*in aggiunta*

È prevista altresì la tenuta di un registro delle informazioni avente ad oggetto la totalità degli accordi contrattuali per l'utilizzo di servizi TIC prestati da fornitori terzi, che devono però esservi documentati distinguendo quelli relativi a servizi a supporto di FEI dagli altri[9].

Sul piano degli obblighi informativi, l'art. 28, par. 3, del DORA prevede che le entità finanziarie "*informano tempestivamente l'autorità competente in merito a eventuali accordi contrattuali previsti per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti, nonché del momento in cui una funzione diventa essenziale o importante*".

3. Il rapporto con le discipline settoriali dell'esternalizzazione

La disciplina così delineata interagisce, peraltro, con un quadro regolamentare già caratterizzato dalla presenza di presidi specifici in materia di esternalizzazione di funzioni e attività da parte degli intermediari finanziari, in primis le Linee guida dell'EBA sugli accordi di esternalizzazione allo stato attuale oggetto di revisione[10].

Il DORA, infatti, non è intervenuto in sostituzione delle discipline settoriali già applicabili in materia di esternalizzazione, ma si è posto in termini di complementarità[11].

agli elementi di cui al paragrafo 2". Il contenuto della politica di cui all'art. 28, par. 2, è precisato dal Regolamento Delegato (UE) 2024/1773 della Commissione del 13 marzo 2024 (in GUUE L, 2024/1773, del 25 giugno 2024).

9 Cfr. art. 28, par. 3, del DORA, che impone di mantenere e aggiornare "*un registro di informazioni su tutti gli accordi contrattuali per l'utilizzo di servizi TIC prestati da fornitori terzi*", i quali sono "*opportunamente documentati, distinguendo quelli che si riferiscono a servizi TIC a supporto di funzioni essenziali o importanti dagli altri*".

10 Sul punto, si segnala la recente consultazione, avviata da EBA e conclusasi a ottobre 2025, del progetto di revisione delle proprie linee guida sugli accordi di esternalizzazione emanate nel 2019, con l'obiettivo di stabilire un quadro più armonizzato in materia di gestione del rischio di terze parti e di tenere conto dell'entrata in vigore del Regolamento (UE) 2022/2554 (DORA).

11 Cfr. considerando 29 del DORA: "*Anche se il diritto dell'Unione in materia di servizi finanziari contiene talune norme generali in materia di esternalizzazione, il monitoraggio della dimensione contrattuale non è sempre saldamente radicato nel diritto dell'Unione. In assenza di norme dell'Unione che si applichino in maniera chiara e mirata alle disposizioni contrattuali stipulate con fornitori terzi di servizi TIC, la fonte esterna dei rischi informatici rimane una questione non adeguatamente affrontata. È pertanto necessario stabilire alcuni principi fondamentali che indirizzino la gestione, da parte delle entità finanziarie, dei rischi informatici derivanti da terzi [...]. Tali principi sono complementari alla normativa settoriale applicabile all'esternalizzazione*".

Il legislatore europeo, pur evidentemente consapevole dell'esigenza di coordinamento con le discipline settoriali, non ha enunciato una regola applicativa: la sintetica affermazione di complementarità resta infatti confinata ai considerando e non trova migliore delineazione nell'articolato, che non prevede alcun criterio di delimitazione tra i servizi TIC e i servizi di diversa natura né una regola di concorso o esclusione rispetto ai regimi settoriali.

Il coordinamento tra le varie norme è rimasto così affidato:

- per un verso, agli interventi di chiarimento delle Autorità di Vigilanza;
- per altro verso, alla valutazione delle singole entità finanziarie, sulle quali grava l'onere di stabilire, prima della conclusione dell'accordo, la natura del servizio e la relativa disciplina applicabile[12].

Ovviamente, dalla qualificazione dell'accordo dipendono sia il regime organizzativo e contrattuale applicabile, sia il contenuto degli obblighi informativi nei confronti dell'Autorità di Vigilanza.

4. Il coordinamento con la disciplina delle esternalizzazioni degli AIFM

Le considerazioni sin qui svolte possono essere verificate, ad esempio, sul terreno della disciplina applicabile ai gestori di fondi di investimento alternativi (AIFM), recentemente interessata dalla revisione delle fonti normative di riferimento.

In tale contesto, la disciplina delle esternalizzazioni trova il proprio fondamento nella Direttiva 2011/61/UE ("AIFMD") e nel Regolamento Delegato (UE) n. 231/2013, nonché, a livello nazionale, nel Testo Unico della Finanza e nella normativa secondaria di attuazione.

In particolare, il Regolamento della Banca d'Italia del 5 dicembre 2019 – adottato in attuazione degli artt.

12 L'art. 28, par. 4, lettera a), del DORA dispone che "*prima di stipulare un accordo contrattuale per l'utilizzo di servizi TIC, le entità finanziarie* [...] *valutano se l'accordo contrattuale riguardi l'utilizzo di servizi TIC a supporto di una funzione essenziale o importante*"; la disposizione presuppone, dunque, che l'accordo sia già stato qualificato come avente ad oggetto servizi TIC. In termini espressi, la risposta al quesito n. 2999 (DORA030), su cui *infra*, nota 16, precisa che "*financial entities are responsible for undertaking an assessment on this basis to determine whether the services they rely on are ICT services, as defined under Article 3(21) DORA*".

vedi l'articolo online

4-undecies e 6, comma 1, lettere b) e c-bis), del TUF – disciplina in modo dettagliato le condizioni e i presupposti della delega e dell'esternalizzazione di funzioni operative essenziali o importanti da parte dei gestori.

Il quadro così descritto è, tuttavia, in corso di revisione. La direttiva (UE) 2024/927 (c.d. "AIFMD II") ha modificato la direttiva 2011/61/UE per quanto riguarda, tra l'altro, gli accordi di delega; il recepimento nazionale è intervenuto con il d.lgs. 13 marzo 2026, n. 39. Contestualmente, è intervenuto il d.lgs. 27 marzo 2026, n. 47 (c.d. "Riforma del TUF"), di attuazione della delega contenuta nella legge 5 marzo 2024, n. 21 (c.d. "Legge Capitali"); al riguardo, sono previsti vari regolamenti di attuazione.

Un'anticipazione in proposito è pervenuta da parte della Banca d'Italia con la comunicazione del 30 dicembre 2024, nella quale l'Autorità ha affermato che, con l'avvio dell'applicazione del DORA, "*all'utilizzo da parte degli intermediari di servizi ICT prestati da fornitori terzi non troveranno più applicazione le discipline settoriali in materia di esternalizzazione*"; per le restanti ipotesi il *framework* settoriale continua invece a operare.

Il riparto, dunque, può essere così sintetizzato:

- agli accordi contrattuali aventi ad oggetto l'utilizzo di servizi TIC prestati da fornitori terzi si applica il Capo V del DORA, con conseguente disapplicazione delle discipline settoriali in materia di esternalizzazione;
- alle esternalizzazioni di funzioni e attività non qualificabili come servizi TIC continuano ad applicarsi le discipline settoriali, ivi compresi i procedimenti amministrativi di divieto previsti dalle disposizioni di vigilanza della Banca d'Italia[13].

L'evoluzione del quadro regolamentare trova significativo riscontro nella disciplina dei servizi *cloud*.

Prima dell'applicazione del DORA, tali servizi erano disciplinati, nell'ambito del *framework* dell'esternalizzazione, dagli Orientamenti ESMA del 10 maggio 2021 (ESMA50-164-4285)[14].

A seguito dell'applicazione del DORA, tali Orientamenti non trovano tuttavia più applicazione nei confronti delle entità finanziarie.

I nuovi Orientamenti ESMA del 30 settembre 2025 hanno confermato espressamente che "*i precedenti orientamenti dell'ESMA sull'esternalizzazione a fornitori di servizi cloud non si applicano più alle entità finanziarie soggette al DORA, come definite all'articolo 2 del medesimo regolamento*" e che, con riferimento agli accordi di esternalizzazione nel *cloud*, le entità finanziarie ivi definite "*sono soggette alle norme specifiche stabilite nel Regolamento DORA e nei regolamenti delegati e di esecuzione della Commissione*"[15].

Su questa linea si colloca quindi la revisione della normativa secondaria nazionale.

Le disposizioni poste in consultazione dalla Banca d'Italia il 27 maggio 2026 indicano fra le proprie finalità quella di "*allineare le disposizioni al regolamento (UE) 2022/2554*" e prospettano, per i gestori, l'abrogazione del procedimento amministrativo di divieto di delega, "*considerato anche che questo stesso procedimento per i servizi ICT a supporto di funzioni operative importanti è già divenuto inapplicabile*" per effetto del DORA[16].

13 Comunicazione della Banca d'Italia del 30 dicembre 2024, par. 2.2, pubblicata sul sito istituzionale della Banca d'Italia (sezione Vigilanza, Avvisi e comunicazioni).

14 Orientamenti ESMA in materia di esternalizzazione a fornitori di servizi *cloud* del 10 maggio 2021 (ESMA50-164-4285), disponibili all'indirizzo https://www.esma.europa.eu/sites/default/files/library/esma_cloud_guidelines_it.pdf.

15 Orientamenti ESMA in materia di esternalizzazione a fornitori di servizi *cloud* del 30 settembre 2025 (ESMA65-294529287-4737), punto 4 e nota 1. I nuovi Orientamenti si applicano ai soli depositari di FIA e di OICVM che non siano entità finanziarie soggette al DORA.

16 Cfr. Banca d'Italia, *Disposizioni Banca d'Italia per recepimento della Direttiva UE 2024/927 e per attuazione di alcune novità del d.lgs. 27 marzo 2026, n. 47*, documento posto in consultazione il 27 maggio 2026 (consultazione aperta fino all'11 luglio 2026) e disponibile all'indirizzo https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2026/2026.05.27-direttiva927/index.html.

5. La qualificazione degli accordi con componente tecnologica: problemi interpretativi e criteri applicativi

Nella prassi, non indifferenti problemi interpretativi sorgono laddove l'entità finanziaria affidi a un soggetto terzo una funzione o attività non avente natura TIC, ma il fornitore utilizzi componenti tecnologiche nell'ambito delle modalità di esecuzione della prestazione.

In tal caso, può non essere agevole la qualificazione degli accordi e l'individuazione del regime regolamentare applicabile.

Ad esempio, è legittimo domandarsi se la presenza di componenti TIC utilizzate nell'esecuzione di una prestazione diversa sia di per sé sufficiente a ricondurre l'intero rapporto nell'ambito degli accordi per l'utilizzo di servizi TIC ai sensi del DORA.

Un elemento di orientamento si ricava dal quesito n. 2999 (DORA030), sottoposto all'EIOPA il 14 febbraio 2024 e riscontrato dalla Commissione europea, avente ad oggetto proprio l'individuazione dei servizi riconducibili alla definizione di cui all'art. 3, punto 21).

In particolare, la Commissione europea ha enunciato un criterio di prevalenza: ove un'entità finanziaria presti ad altra entità finanziaria un servizio TIC connesso a servizi finanziari a loro volta regolamentati, il servizio deve considerarsi prevalentemente finanziario e non deve essere trattato come servizio TIC ai sensi dell'art. 3, punto 21)[17].

Il criterio è significativo sul piano metodologico: la qualificazione non discende automaticamente dalla presenza di una componente tecnologica, ma richiede di individuare l'oggetto prevalente della prestazione dedotta in contratto.

17 Quesito n. 2999 (DORA030), sottoposto all'EIOPA il 14 febbraio 2024 e pubblicato nel *Q&A database* dell'Autorità: "*The definition of 'ICT services' in Article 3(21) of Regulation (EU) 2022/2554 intentionally maintains a broad scope*"; "*financial entities are responsible for undertaking an assessment on this basis to determine whether the services they rely on are ICT services, as defined under Article 3(21) DORA*"; e, con riguardo ai servizi resi da un'entità finanziaria ad altra entità finanziaria, "*In case both tests are positive, then the related ICT service should be considered to predominantly be a financial service and should not be treated as an ICT service within the meaning of DORA Article 3(21)*".

L'applicabilità della disciplina DORA non dovrebbe dunque essere valutata sulla sola base della presenza di componenti tecnologiche nell'esecuzione della prestazione, ma richiederebbe una valutazione del ruolo assunto dalla componente TIC nell'economia complessiva del rapporto contrattuale.

Si tratterebbe, in altre parole, di condurre una valutazione sostanziale del rapporto, volta a verificare se la componente TIC costituisca il servizio reso dal fornitore ovvero rappresenti uno strumento funzionale all'esecuzione di una diversa prestazione.

Del resto, una lettura fondata sulla mera presenza di strumenti TIC nell'organizzazione del fornitore rischierebbe di attrarre nel perimetro del DORA rapporti nei quali la tecnologia costituisce esclusivamente uno strumento operativo utilizzato per l'esecuzione di una diversa prestazione, con conseguente indebita sovrapposizione tra il regime TIC e le discipline settoriali applicabili alle esternalizzazioni.

In pratica, si potrà ad esempio distinguere le ipotesi nelle quali il fornitore si obbliga a:

(i) erogare ad uno o più utenti interni o esterni dell'entità finanziaria servizi di natura digitale o di trattamento dati attraverso sistemi TIC, con ciò integrando la fattispecie di cui all'art. 3, punto 21), del DORA; ovvero

(ii) eseguire una diversa prestazione – tipicamente di natura gestionale, operativa o professionale – avvalendosi, nella propria organizzazione interna, di sistemi TIC, senza che ciò comporti l'erogazione di servizi TIC.

Tale impostazione appare coerente con l'impianto del DORA, che mira a presidiare i rischi derivanti dall'affidamento a terzi di servizi TIC dei quali l'entità finanziaria fruisce direttamente.

Il coordinamento tra la disciplina del rischio informatico derivante da terzi e quella settoriale delle esternalizzazioni non può dunque essere risolto assimilando a un accordo per l'utilizzo di servizi TIC ogni affidamento a terzi nell'ambito del quale siano impiegati strumenti tecnologici: i due regimi operano su piani distinti ma suscettibili di coordinamento, secondo il rapporto di complementarità espressamente richiamato dal considerando 29 del DORA (v. *supra*, § 3).

vedi l'articolo online

6. Le aspettative di vigilanza

Con la recente Comunicazione al mercato del 17 luglio 2026, la Banca d'Italia ha acceso uno specifico punto di attenzione in merito alla necessità di presidiare i rischi derivanti dall'utilizzo di modelli avanzati di intelligenza artificiale[18].

In particolare, a fronte della capacità dei modelli di ultima generazione di individuare le vulnerabilità dei sistemi software e di generarne contemporaneamente le modalità di sfruttamento "*in tempi estremamente ridotti e senza la necessità di specifiche competenze tecniche*", l'Autorità ha segnalato l'incremento del rischio che le entità finanziarie possano subire attacchi *cyber* efficaci[19].

Di conseguenza, la Comunicazione richiede alle entità finanziarie di analizzare e rappresentare alla Vigilanza, con apposita relazione, il livello di esposizione al rischio e l'adeguatezza dei presidi esistenti, individuando le principali carenze, le relative priorità di intervento e un piano di lavoro recante le azioni, i tempi e gli investimenti necessari.

L'aspettativa è puntualmente definita.

Il Consiglio di amministrazione, in seduta congiunta con il Collegio sindacale, è chiamato a esaminare la Comunicazione e ad avviare la predisposizione della relazione. Agli organi con funzione di amministrazione e di gestione spetta definire presidi appropriati per il governo dei fornitori esterni, comprensivi, in particolare, di adeguati requisiti contrattuali e di criteri rigorosi per la loro valutazione *ex ante* e selezione[20].

L'esercizio richiesto non si esaurisce, dunque, in una ricognizione né nella formulazione di una dichiarazione di conformità, ma implica una valutazione effettiva dell'adeguatezza dell'assetto esistente.

Tale valutazione presuppone che i rapporti rilevanti siano stati previamente individuati e correttamente qualificati.

L'attività, peraltro, implica non soltanto un censimento formale dei fornitori o degli accordi contrattuali, ma richiede una considerazione integrata dei profili contrattuali, organizzativi e tecnologici, fondata anche su una lettura coordinata del DORA, della disciplina settoriale applicabile e degli assetti di *governance* dell'entità finanziaria.

Una verifica da condurre caso per caso e in tempo utile affinché i relativi esiti possano confluire nella relazione da trasmettere alla Vigilanza entro il 31 dicembre 2026.

18 Cfr. Banca d'Italia, *Comunicazione al mercato in materia di resilienza operativa digitale e modelli avanzati di Intelligenza Artificiale*, 17 luglio 2026. La Comunicazione è rivolta ai soggetti direttamente vigilati dal Dipartimento Vigilanza Bancaria e Finanziaria, tra i quali banche e gruppi bancari meno significativi, istituti di pagamento, istituti di moneta elettronica, imprese di investimento, gestori di fondi di investimento alternativi e società di gestione.

19 L'iniziativa è in linea con quanto rilevato dalla Banca Centrale Europea: v. *L'Ia Claude Mythos fa paura alle banche, martedì riunione in Bce*, in *Il Sole 24 Ore*, 24 maggio 2026, disponibile all'indirizzo https://www.ilsole24ore.com/art/l-ia-claude-mythos-fa-paura-banche-martedi-riunione-bce-AIz9emGD, e la successiva comunicazione BCE, *Addressing AI-enabled cybersecurity threats*, SSM-2026-0301, 7 luglio 2026, disponibile all'indirizzo https://www.bankingsupervision.europa.eu/press/letterstobanks/shared/pdf/2026/ssm.2026_letter_on_AI_enabled_cybersecurity_threats.en.pdf. Sul punto si segnala anche il recente intervento delle Autorità di vigilanza europee (ESAs) con la dichiarazione congiunta del 31 luglio 2026 in materia https://www.dirittobancario.it/art/le-esas-sui-rischi-derivanti-dai-modelli-di-intelligenza-artificiale-avanzati.

20 Banca d'Italia, *Comunicazione al mercato*, cit., pp. 2 e 4-5. Gli organi con funzione di amministrazione e di gestione "*sono altresì tenuti a definire presidi appropriati per il governo degli eventuali fornitori esterni di servizi informatici; tali presidi comprendono, in particolare, adeguati requisiti contrattuali, volti ad assicurare efficaci misure di monitoraggio della sicurezza e di gestione degli aggiornamenti (patch) da parte del fornitore, nonché criteri rigorosi per la valutazione ex-ante e la selezione dei fornitori*". Quanto alla relazione: "*Ci si attende che il Consiglio di Amministrazione, nel corso di una seduta congiunta con il Collegio Sindacale, esamini il contenuto della presente Comunicazione. Nel corso della medesima seduta, dovrà essere dato avvio ai lavori per la stesura di una Relazione che, distintamente per ciascuna delle aree richiamate, rappresenti il livello attuale di esposizione al rischio e l'adeguatezza dei presidi esistenti, individui le principali carenze e le relative priorità di intervento nonché definisca un piano di lavoro con l'indicazione delle azioni, dei tempi e degli investimenti necessari*"; la Relazione, con allegato il piano di lavoro, "*deve essere trasmessa alla Vigilanza entro il 31 dicembre 2026*".

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it