Matteo Pignatti

La cybersecurity nella digitalizzazione del settore finanziario

Abstract: L'innovazione tecnologica costituisce un fattore che incide sull'economia e assume caratteri particolari nel settore finanziario. Il rapporto di co-dipendenza dal settore ICT che si è venuto a creare comporta rischi sulla stabilità finanziaria del sistema europeo e conferisce un ruolo alle Istituzioni UE nella gestione di fenomeni a carattere sovranazionale. Le cripto-attività, la definizione di misure per garantire un livello comune elevato di cybersicurezza nell'UE, la resilienza operativa digitale per il settore finanziario e dei soggetti critici hanno originato un contesto giuridico in cui l'analisi e la gestione rischi, i regimi contrattuali vincolati e l'attività di sorveglianza costituiscono strumenti volti a garantire la sicurezza e l'efficienza nel Mercato Interno. Il contributo intende analizzare i profili giuridici rilevanti nella gestione del rapporto di co-dipendenza tra ICT e finanza, i principali rischi per il settore finanziario e le possibili criticità ad essi connesse.

Keywords: Cybersecurity; Settore bancario e finanziario; Mercato interno; Vigilanza.

1. La digitalizzazione nel settore finanziario

La transizione digitale nel settore finanziario si inserisce in un contesto in cui la necessità di adeguare e rendere competitivo il Mercato Interno a livello internazionale deve essere bilanciata con la sana e prudente gestione nell'attività finanziaria e la tutela del risparmio, contribuendo a definire un mercato unico digitale dei servizi finanziari[1].

1 Circa la necessità di sostenere il progresso tecnologico nell"economia europea nel settore finanziario, si v.: Commissione UE, *Comunicazione relativa a una strategia in materia di finanza digitale per l'UE*, 24 settembre 2020 COM(2020) 591 final. Per una descrizione dell'evoluzione si v. Bronzetti 2023: 6 e s.; Ruocco 2023: 181 e s. In relazione alla sovranità tecnologica si v.: Commissione UE, *Relazione di previsione strategica 2021*, 8 settembre 2021, 4; European Innovation Council, *Statement to accompany the launch of the full EIC*, allegato I, *Statement on Technological Sovereignty*, 18 marzo 2021. In dottrina: Capriglione 2021: 4 e s.; Celati 2021: (3) 252 e s.; Finocchiaro 2022: 809 e s.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760153

Il rapporto tra settore finanziario e ICT[2] ha generato differenti fenomeni rilevanti per il diritto dell'economia[3] conferendo al *FinTech* un'autonoma rilevanza[4] e ponendo in evidenza nuovi rischi[5].

L'adozione di misure per sostenere settori economici rilevanti per la crescita[6] entra in rapporto con quelle connesse alla sicurezza[7], generando un contesto giuridico particolarmente complesso per gli operatori finanziari che sono chiamati a

2 Già oggi le banche europee dichiarano che il 65% di esse ha *partnership* contrattuale con le aziende *BigTech*. Si v.: Campa 2023: 1 e s. Cfr. anche: Financial Stability Board, *FinTech and market structure in financial services: Market developments and potential financial stability implications*, 14 febbraio 2019; Id., *BigTech Firms in Finance in Emerging Market and Developing Economies Market developments and potential financial stability implications*, 12 ottobre 2020. Cfr. anche: European Supervisory Authorities, *ESAs Joint European Supervisory Authority response to the European Commission's February 2021 Call for Advice on digital finance and related issues: regulation and supervision of more fragmented or non-integrated value chains, platforms and bundling of various financial services, and risks of groups combining different activities*, 31 gennaio 2022, ove sono affrontati alcuni profile della digitalizzazione del settore finanziario: catene di valore (*value chains*) sempre più frammentate e non integrate; piattaforme e offerta di prodotti finanziari; rischi per i gruppi che operano in diversi settori integrando differenti attività. Il p. to 4, all'interno della raccomandazione n. 1, pone l'attenzione sui possibili rapporti di dipendenza. Si v. anche European Banking Authority, *Report on the use of digital platforms in the eu banking and payments sector*, 2021, 33 e s., ove ci si riferisce ai rapporti di dipendenza da fornitori terzi di servizi ICT.

3 Tali fenomeni non solo hanno semplificato le attività nel settore finanziario (ove correttamente utilizzati), ma hanno anche inciso sulla diffusione nel mercato degli effetti economici (positivi o negativi) derivanti da essi.

4 *Ex multis*: Lemma 2020: 1 e s.; Lemma 2023: 83 e s.; Annunziata – Minto 2022: 1 e s.; Mazzarisi – Ravagnani – Deriu – Lillo – Medda – Russo 2022: 1-49; Annunziata 2020: 1 e s.; Sciarrone Alibrandi – Borello – Ferretti – Lenoci – Macchiavello – Mattassoglio – Panisi 2019: 1 e s.

5 Si v. Parlamento UE, *Relazione recante raccomandazioni alla Commissione sulla finanza digitale: rischi emergenti legati alle criptoattività – sfide a livello della regolamentazione e della vigilanza nel settore dei servizi, degli istituti e dei mercati finanziari*, 2020; Banca d'Italia, *Comunicazione in materia di tecnologie decentralizzate nella finanza e cripto-attività*, 15 giugno 2022. In dottrina: Rabitti 2023(a): 345 e s.. Cfr. a titolo esemplificativo il caso connesso alla negligenza contabile della società di servizi finanziari *Wirecard*. D. McCrum, *Wirecard made this short seller right but not rich*, in *Financial Times*, 15 luglio 2020.

6 Commissione UE, *The future of European Competitiveness – Part A, A competitiveness strategy for Europe*, 9 settembre 2024, 19 e s., in relazione specificatamente alla digitalizzazione e all'innovazione tecnologica si v. anche *Part B*, 67 e s.

7 Si v. la revisione della disciplina sugli investimenti esteri diretti (Regolamento UE, 2019/452. Si v. anche: Commissione UE, *Proposta di regolamento UE relativo al controllo degli investimenti esteri nell'Unione, che abroga il regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio*, 26 gennaio 2024), le previsioni sulla coercizione economica da paesi terzi (Regolamento UE 2023/2675, *sulla protezione dell'Unione e dei suoi Stati membri dalla coercizione economica da parte di paesi terzi*), le previsioni in materia di sovvenzioni estere alle imprese europee volte a prevenire possibili distorsioni economiche (Regolamento UE 2022/2560, *relativo alle sovvenzioni estere distorsive del Mercato Interno)*, nonché per il sostegno alla ricerca e lo sviluppo su tecnologie potenzialmente a duplice uso e controllo sulle esportazioni di quest'ultime (Regolamento UE 2021/821*, che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso – rifusione –*).

gestire l'evoluzione di strumenti ICT[8] utilizzati nelle proprie attività, garantendo elevati livelli di sicurezza informatica[9] e una resilienza operativa digitale[10] capace di rispondere in maniera efficace alle esigenze del settore finanziario[11].

L'esternalizzazione a soggetti terzi di funzioni tecniche, se da un lato può consentire di conseguire obiettivi all'interno del mercato (mediante l'acquisizione di un *know-how* specifico), è altresì idonea a generare rapporti di co-dipendenza che possono incidere negativamente sulla continuità dell'attività degli operatori finanziari.

Le previsioni europee in tema di cybersicurezza nell'UE (c.d. direttiva NIS2) e di resilienza operativa digitale per il settore finanziario (c.d. regolamento DORA) si inseriscono tra le misure volte all'armonizzazione della finanza digitale[12], propo-

8 Campa 2023, "Around half of EU banks (covering both corporate and retail segments) have reported that most of their customers (75%-100%) primarily use digital channels for daily banking activities. (…) In the area of Artificial Intelligence (AI), more than 70% of EU banks use AI at least in some areas of activities. Its use is more widespread in creditworthiness assessment and credit scoring, fraud detection, commercial profiling and clustering of clients or transactions, AML/CFT being more wide-spread. An increased use of chatbots or similar solutionsis being noticed. We also see that many financial entities focus on optimisation of internal processes and introducing digitalisation in order to increase efficiencies and cut their operating costs".

9 Direttiva UE, 2555/2022, c.d. NIS2, attuata nell'ordinamento giuridico italiano con il d.lgs. 4 settembre 2024, n. 138.

10 Sulla nozione di "resilienza operativa digitale", si v. Regolamento UE, 2554/2022, *Digital operational resilience for the financial sector* – art. 3, par. I, p. to 1), ove è definita come "la capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi TIC, l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza dei sistemi informatici e di rete utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità, anche in occasione di perturbazioni"; Commissione UE, *relazione alla direttiva che modifica le direttive 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341*, COM(2020) 596 final, 24 settembre 2020; Comitato economico e sociale europeo, *Parere sulla 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*, cit., p. to 2.4.

11 *Ex multis*: Casalino 2023: 337 e s.; Baskerville – Capriglione – Casalino 2020: 341 e s.; Alpa 2019: 377 e s.; Miglionico, 2019: 1376 e s.

12 Circa il *Digital Finance Package* si v. Commissione UE, *Comunicazione relativa a una strategia in materia di finanza digitale per l'UE*, 24 settembre 2020; Commissione UE, *Comunicazione relativa a una strategia in materia di pagamenti al dettaglio per l'UE*, 24 settembre 2020. La strategia europea si compone di quattro atti normativi in tema di: cripto-attività (regolamento UE 1114 del 2023, sui mercati delle cripto-attività – MiCA, quali rappresentazioni digitali di valori o di diritti che possono essere trasferiti o memorizzati elettronicamente attraverso una tecnologia che supporta la registrazione distribuita di dati cifrati – tecnologia di registro distribuito, *distributed ledger technology – DLT* su cui si v. Regolamento UE n. 858 del 2022); l'armonizzazione delle principali prescrizioni sulla resilienza operativa digitale (modificando altresì le direttive vigenti in materia di servizi finanziari, per lo più per necessità di adeguare la disciplina concernente i requisiti in materia di rischio operativo e di gestione del rischio al nuovo regolamento DORA, e per aggiornare la definizione di "strumento finanziario" includendo gli strumenti emessi utilizzando la tecnologia DLT (Direttiva UE 2022/2556, che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario). A tali atti si aggiunge la disciplina relativa a mercati equi e contendibili nel

nendosi di regolare in maniera uniforme e integrata le misure per la prevenzione e gestione dei rischi relativi ai rapporti con il settore ICT[13].

La direttiva UE NIS2, entrata in vigore il 17 gennaio 2023 il cui recepimento negli ordinamenti giuridici nazionali era previsto entro il 17 ottobre 2024[14], si propone di realizza un'armonizzazione minima in materia di cybersicurezza nell'UE. La norma supera la distinzione tra "Operatori di Servizi Essenziali" (OSE) e "Fornitori di Servizi Digitali" (FSD) in favore di quella tra "Soggetti Essenziali" e "Soggetti Importanti"[15] che operano all'interno dei settori ad "alta criticità" (all. I, in cui rientra il settore bancario) e degli "altri settori critici" (all. II), e su cui ricade la responsabilità di garantire la sicurezza dei sistemi informatici e di rete che utilizzano nelle loro attività.

Il regolamento UE DORA, applicabile a partire dal 17 gennaio 2025, armonizza le regole di *governance* e di gestione del rischio ICT per le istituzioni finanziarie (definizione che ricomprende non solo gli enti creditizi ma anche le imprese di assicurazione e di riassicurazione, istituti di pagamento e moneta elettronica, imprese di investimento, gestori di fondi alternativi e molti altri operatori del nostro sistema finanziario), sino a oggi frammentate in vari corpi normativi, adottati principalmente dalle Autorità Europee di Vigilanza (EBA, ESMA ed EIOPA).

In questo contesto l'attività di sorveglianza interviene a supporto dell'analisi e gestione rischi (in chiave di prevenzione e mitigazione degli eventi) e dell'attività

settore digitale (Regolamento, n. 1925 del 2022, *Digital Markets Act* – DMA), e la proposta di regole armonizzate sull'intelligenza artificiale (*Artificial Intelligence Act*), di una direttiva relativa sull'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (*AI Liability Directive*), riguardante il regime di responsabilità per danni causati con il coinvolgimento di sistemi di intelligenza artificiale. In dottrina: Capriglione 2019: 374 e s.; Sepe 2021: 186 e s.; Canepa 2021: 465 e s.; Urbani 2022: 985 e s. La Banca Centrale Europea e la Commissione UE stanno inoltre proseguendo le attività dei tavoli di lavoro incaricati dello studio di fattibilità del cd. *digital euro project*, ossia dell'istituzione, regolazione ed emissione di una *central bank digital currency* (CBDC) da parte delle Istituzioni europee. Cfr. BCE, *Progress on the investigation phase of a digital euro, 14 luglio 2023*; BCE, *The case for a digital euro: key objectives and design considerations, luglio 2022*.

13 Mediante ad es.: la definizione e il costante aggiornamento di sistemi, protocolli per gestire rischi informatici (Regolamento UE, 2554/2022, art. 7), l'identificazione dei ruoli e responsabilità nelle funzioni svolte dall'operatore finanziario mediante strumenti ICT (Regolamento UE, 2554/2022, art. 8), il controllo costante la gestione dei dati (per prevenire la loro corruzione, perdita e garantirne la riservatezza, Regolamento UE, 2554/2022, art. 9), l'individuazione di punti di vulnerabilità (Regolamento UE, 2554/2022, art. 10), anche mediante test di resilienza operativa digitale (Regolamento UE, 2554/2022, artt. 24-27) e la gestione di eventi di rischio per garantire la continuità mediante apposite piani e procedure di backup (Regolamento UE, 2554/2022, artt. 11 e 12) è coniugata e collegata con l'attività gestione degli incidenti informatici in collaborazione e coordinamento con le Autorità di Vigilanza (europee e nazionali, Regolamento UE, 2554/2022, artt. 17-23. In ambito europeo il riferimento è all'Autorità europea degli strumenti finanziari e dei mercati – ESMA, all'Autorità europea delle assicurazioni e delle pensioni aziendali o professionali – EIOPA e all'Autorità bancaria europea – EBA).

14 L'attuazione nell'ordinamento giuridico italiano è avvenuta con: d.lgs. 4 settembre 2024, n. 138.

15 Direttiva UE, 2555/2022, art. 4.

contrattuale con terzi fornitori di servizi ICT (quale strumento istituzionale di garanzia da asimmetrie informative e a tutela del risparmio).

In questo contesto, l'ordinamento giuridico europeo si propone di garantire "un livello comune elevato di cibersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno"[16] e bilanciare i differenti interessi e riequilibrare i rapporti di forza tra i due settori mediante la previsione di vincoli contrattuali e in termini di sorveglianza[17], in particolare ove i fornitori di servizi ICT siano qualificati come "critici"[18] o risultino stabiliti in paesi terzi[19].

Il contributo intende analizzare le previsioni in materia di cybersecurity e sulla resilienza operativa digitale per il settore finanziario, approfondendo i rischi connessi alle prestazioni ICT oggetto di esternalizzazione. L'analisi si propone di chiarire i profili giuridici rilevanti nella gestione del rapporto con il settore ICT, i principali rischi per il settore finanziario e le possibili criticità ad essi connesse analizzando il ruolo della vigilanza.

2. La *cybersecurity* e l'affidamento a soggetti terzi di servizi ICT nel settore finanziario

Il rapporto tra il settore ICT e quello finanziario comporta specifici rischi che sovente conseguono ad una asimmetria informativa che può comportare una "cattura" dei soggetti che svolgono la propria attività nel settore finanziario[20].

I rischi connessi alla sicurezza informatica ed alla sua vulnerabilità possono tuttavia assumere differente natura.

16 Direttiva UE, 2555/2022, art. 1.

17 La disciplina europea non impone massimali rigidi o restrizioni rigorose circa il ricorso a fornitori di servizi ICT al fine di non incidere negativamente sull'attività economica del settore limitandone la libertà contrattuale, piuttosto cerca di individuare strumenti, quali l'analisi e gestione dei rischi, la realizzazione di stress test, l'attività di vigilanza, l'attenzione ai contenuti contrattuali con i fornitori terzi di servizi ICT ed i regimi di responsabilità, per equilibrare i rapporti di forza e di dipendenza tra i due settori al fine di tutelare gli interessi degli investitori e del sistema europeo. Tali strumenti, applicati al settore finanziario sulla base di una proporzionalità declinata in termini generali (Regolamento UE, 2554/2022, art. 4, par. I, ove, la disciplina in materia a resilienza operativa digitale per il settore finanziario, trova applicazione "tenendo conto delle (…) dimensioni [degli operatori del settore finanziario] e del loro profilo di rischio complessivo, nonché della natura, della portata e della complessità dei loro servizi, delle loro attività e della loro operatività") e in termini specifici in relazione ai rapporti giuridici con i terzi fornitori di servizi ICT (Regolamento UE, 2554/2022, art. 28, par. I, lett. b), ove la gestione dei rischi informatici derivanti da terzi da parte delle entità finanziarie, tiene conto: "i: della natura, della portata, della complessità e dell'importanza delle dipendenze connesse alle TIC; ii) dei rischi derivanti dagli accordi contrattuali per l'utilizzo di servizi TIC conclusi con fornitori terzi di servizi TIC, tenendo conto della criticità o dell'importanza dei rispettivi servizi, processi o funzioni e del potenziale impatto sulla continuità e la disponibilità delle attività e dei servizi finanziari a livello individuale e di gruppo").

18 Regolamento UE, 2554/2022, art. 3, par. I, p. to 23.

19 Regolamento UE, 2554/2022, art. 3, par. I, p. to 24.

20 Regolamento UE, 2554/2022, artt. 5-16.

I rischi legati alla disciplina normativa costituiscono una categoria generale (che va quindi oltre i servizi resi da fornitori terzi e al settore finanziario), ma assumono peculiarità proprie in un contesto in cui interessi economici nazionali si frappongono a quelli europei.

L'armonizzazione di concetti rilevanti e regole tecniche può costituire elemento di sviluppo del mercato europeo e ridurre possibili distorsioni opportunistiche al suo interno (ad es. derivanti da *bias*[21]), anche in relazione alla frammentazione dei servizi finanziari (che rende complessa la *compliance* per gli operatori finanziari), e tutelare i consumatori (nel corretto utilizzo di servizi finanziari digitali)[22]. Se molti dei principi, requisiti e regole tecniche sono già contenuti all'interno di norme, orientamenti e atti di *soft law* di settore[23], risulta tuttavia necessario garantire la loro armonizzazione e la coerenza con concetti definiti in altri settori (quale ad es. quello bancario[24]) o negli atti normativi UE (come ad es. il regolamento UE in materia di Intelligenza artificiale, che individua nel livello di "rischio" un fattore distintivo all'interno della disciplina)[25].

La definizione di molteplici strumenti o atti, a livello sovranazionale[26] e nazionale[27], e l'interazione tra differenti soggetti (pubblici[28] e privati[29]) deve essere accompagnato da un'uniformità di livelli di tutela, regole tecniche e giuridiche per garantire l'efficiente ed efficace funzionamento del Mercato Interno.

21 Davola 2017: 637 e s.

22 Capriglione 2022: 254.

23 Come quelli elaborati dall'ABE e dall'EIOPA, nonché il progetto di orientamenti dell'ESMA, oggetto di consultazione. In materia di esternalizzazione di servizi, si v. la dicotomia, in termini di ambito di applicazione, tra 'esternalizzazione' e 'servizio di terzi'. La resilienza operativa digitale si riferisce unicamente ai "servizi TIC di terzi" per quanto riguarda i principi fondamentali per la gestione corretta dei rischi relativi alle TIC derivanti da terzi (capo V), mentre l'ambito di applicazione degli orientamenti dell'ABE in materia di esternalizzazione si basa su una definizione di esternalizzazione che implica che l'attività sia eseguita in modo ricorrente o continuativo (par. 26). Gli orientamenti dell'ABE forniscono inoltre un elenco di eccezioni che non sono considerate come rientranti nell'ambito dell'esternalizzazione (par. 28).

24 Comitato di Basilea per la vigilanza bancaria, *Principles for operational resilience* (Principi di resilienza operativa), 6 novembre 2020.

25 Regolamento UE 2024/1689, *che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)*.

26 In relazione alla direttiva NIS2, si v., a titolo esemplificativo, direttiva UE, 2555/2022, art. 21, in relazione alla definizione di misure di gestione dei rischi di cybersicurezza ed il d.lgs. 4 settembre 2024, n. 138, art. 24;

27 Direttiva UE, 2555/2022, artt. 1 e 7, in cui si prevede l'obbligo di definire delle strategie nazionali in materia di cybersicurezza. Nell'ordinamento giuridico italiano cfr. d.lgs. 4 settembre 2024, n. 138, art. 9.

28 Si v. le forme di cooperazione previste dalla direttiva NIS2 e dal regolamento DORA.

29 Si v. la definizione del quadro per la gestione dei rischi informatici che deve essere definito dagli operatori finanziari (regolamento UE, 2554/2022, art. 6) ed i sistemi, protocolli e strumenti ICT da utilizzare per "affrontare e gestire i rischi informatici" (regolamento UE, 2554/2022, art. 7).

Gli atti approvati dalla Commissione UE nel 2024 ed in corso di approvazione, possono costituire un importante elemento di armonizzazione di concetti, regole tecniche[30] e documenti[31] nel mercato europeo, che pare assumere carattere di omogeneizzazione dell'attività finanziaria mediante strumenti ICT e di cui oggi si può solo evidenziarne l'opportunità.

Tale auspicio metodologico parrebbe ulteriormente giustificato dai modelli organizzativi fondati sulla cooperazione a livello internazionale, europeo e nazionale previsti dalla direttiva NIS2[32] e dal regolamento DORA[33], nonché dall'approccio orizzontale di gestione dei rischi adottato nella disciplina in materia di resilienza operativa digitale per il settore finanziario e compatibile con la necessità di evitare sovrapposizioni di concetti, duplicazioni e problemi di coordinamento tra norme europee relative a nuove tecnologie rilevanti anche nell'ambito dell'esternalizzazione di prestazioni rilevanti[34] che potrebbero generare ostacoli al funzionamento del mercato unico, a danno degli operatori del mercato e della stabilità finanziaria[35].

La possibile esternalizzazione a "fornitori terzi di servizi ICT", in virtù di ragioni tecniche, contempera la libertà di iniziativa economica (Cost. it., art. 41) con vincoli e controlli di natura pubblica derivanti dalla necessità di tutelare il risparmio e garantire la stabilità (Cost. it., art. 47) e costituisce un elemento di rischio che incide in maniera autonoma e differenziata sul settore finanziario.

La circostanza per cui la dipendenza dallo strumento ICT si riflette nei confronti di soggetti terzi, la cui maggiore conoscenza delle dinamiche tecnologiche può comportare a distorsioni e alterazioni del mercato finanziario, costituisce fondamento dell'analisi e gestione dei rischi.

Ecco come la fase preliminare all'instaurazione di rapporti contrattuali con soggetti terzi diviene fase fondamentale. Una meticolosa analisi precontrattuale

30 Regolamento UE, 2554/2022, art. 15, con riferimento all'armonizzazione di strumenti, metodi, processi e politiche di gestione del rischio informatico (entro il 17 gennaio 2024); art. 18, relativo alla classificazione degli incidenti connessi alle TIC e delle minacce informatiche (entro il 17 gennaio 2024); art. 26, con riferimento ai test avanzati di strumenti, sistemi e processi di TIC basati su test di penetrazione guidati dalla minaccia (entro il 17 luglio 2024); art. 28, in relazione alla politica per l'utilizzo dei servizi ICT a supporto di funzioni essenziali o importanti prestati da fornitori terzi, nell'ambito della strategia per i rischi informatici derivanti da terzi (entro il 17 gennaio 2024); art. 30, par. V, con riferimento alle regole tecniche connesse alle funzioni ICT inserite nei contratti tra operatori del settore finanziario e terzi fornitori di servizi ICT (entro il 17 luglio 2024); art. 41, in relazione all'armonizzazione delle condizioni che consentono lo svolgimento delle attività di sorveglianza (entro il 17 luglio 2024).

31 Regolamento UE, 2554/2022, art. 20, con riferimento all'armonizzazione dei modelli e dei contenuti per la segnalazione (entro il 17 luglio 2024); art. 28, in relazione a modelli standard registro di informazioni sugli accordi contrattuali per l'utilizzo di servizi ICT prestati da fornitori terzi, comprese le informazioni comuni a tutti gli accordi contrattuali per l'utilizzo di servizi ICT (entro il 17 gennaio 2024).

32 Direttiva UE, 2555/2022, artt. 13-19.

33 Regolamento UE, 2554/2022, artt. 28 e s., sulla gestione dei rischi informatici derivanti da terzi.

34 Schneider 2023: 1014 e s.; Arner-Buckley-Zetsche 2022: 147 e s.

35 Regolamento UE, 2554/2022, considerando n. 9.

dovrebbe concentrarsi sui rischi connessi all'utilizzo di strumenti ICT gestiti da fornitori terzi (l'individuazione delle funzioni essenziali o importanti, l'analisi dei rapporti societari di tali soggetti ed i possibili conflitti di interesse, la gestione e la sicurezza dei dati e dei possibili rischi informatici, la realizzazione di test adeguati per verificare la funzionalità e resistenza dei sistemi adottati)[36], che, unitamente alla collaborazione ed al costante rapporto con le autorità di vigilanza costituiscono elementi prodromici e che fondano la diligente gestione dell'attività da parte degli operatori del mercato finanziario e delle loro responsabilità.

In questo modo, mentre la direttiva UE NIS2, distingue tra "soggetti essenziali" e "soggetti importanti"[37] che operano nei settori ad "alta criticità" (tra cui è ricompreso quello bancario)[38] o in "altri settori critici"[39] per definire l'ambito di applicazione soggettivo delle misure comuni europee in materia di cybersicurezza, il regolamento UE DORA suddivide i rischi connessi ai rapporti contrattuali con soggetti terzi, operando una prima distinzione sulla base delle caratteristiche del fornitore del servizio ICT, dell'oggetto delle prestazioni contrattuali e le modalità con cui sono prestate (per poter valutare altresì gli effetti conseguenti gli automatismi degli strumenti ICT). Tra i soggetti che in generale forniscono servizi ICT ad un operatore finanziario[40], assume carattere rilevante la posizione dei terzi fornitori che specificatamente risultano come "critici"[41]. Questi ultimi sono individuati sulla base di criteri quali: l'impatto sistemico sulla stabilità, la continuità o la qualità della fornitura di servizi finanziari (qualora il fornitore terzo sia interessato da una disfunzione operativa); il carattere sistemico o l'importanza delle entità finanziarie che dipendono da un fornitore terzo; la dipendenza delle entità finanziarie dai servizi prestati ed il grado di sostituibilità del fornitore[42], e risultano ulteriormente classificabili, ove ne ricorrano le condizioni, tra terzi che prestano l'attività nell'ambito di rapporti di controllo societario e in gruppi di imprese[43].

36 Regolamento UE 2554/2022, art. 3, par. I, p. to 5, in cui i "rischi informatici" sono definiti 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 o fisico". Financial Stability Board, *Enhancing Third-Party Risk Management and Oversight. A toolkit for financial institutions and financial authorities*, 4 December 2023, 15.

37 Direttiva UE, 2555/2022, art. 3

38 Direttiva UE, 2555/2022, all. I, p. to 3, ripreso nel d.lgs. 4 settembre 2024, n. 138, all. I, p. to 3.

39 Direttiva UE, 2555/2022, all. II, ripreso nel d.lgs. 4 settembre 2024, n. 138, all. II.

40 Regolamento UE 2554/2022, art. 3, par. I, p. to 19.

41 Regolamento UE 2554/2022, artt. 3, par. I, p. to 23 e 31 e s.

42 Regolamento UE 2554/2022, art. 31, par. II.

43 Regolamento UE 2554/2022, art. 3, par. I, p. ti 25, 26 e 27 in cui si distinguono le nozioni di "impresa figlia" e "impresa madre" e di "gruppo" rimandando alla disciplina relativa ai bilanci d'esercizio, ai bilanci consolidati e alle relative relazioni di talune tipologie di imprese (Direttiva UE 2013/34).

La distinzione assume una ulteriore importanza ove il fornitore (o subappaltatore[44]) "critico" sia stabilito in uno Stato esterno all'Unione Europea[45].

La declinazione data ai criteri individuati per qualificare un fornitore come "critico" è sintomo di una preoccupazione che la dipendenza degli operatori del settore finanziario da imprese ICT sia amplificato da "concentrazioni" di fornitori ICT[46] e che tali situazioni (non consentendo all'organismo che opera nel mercato finanziario di svolgere le proprie funzioni essenziali o assorbire effetti finanziari conseguenti) si riflettano negativamente sulla stabilità del sistema finanziario europeo[47]. L'impatto delle eventuali disfunzioni connesse all'utilizzo di strumenti ICT, il carattere sistemico delle entità finanziarie, il livello di dipendenza dai servizi ICT forniti in relazione alle funzioni essenziali e il grado di sostituibilità del fornitore terzo evidenziano l'attenzione alla continuità delle attività del settore finanziario e alla necessità di particolari accortezze al fine di evitare che disfunzioni di un fornitore si propaghino sull'intero sistema finanziario europeo.

Ecco come la circostanza che un fornitore "critico" sia stabilito presso un paese terzo, e la dipendenza del settore finanziario non sia più solo verso il settore ICT (o un singolo operatore economico) ma verso le economie che controllano quest'ultimo, comporta ulteriori precauzioni insite nella volontà di garantire una autonomia e indipendenza al sistema finanziario europeo da soggetti esterni (in stretta connessione al concetto di sovranità europea che si sta definendo).

Le caratteristiche dei singoli mercati di riferimento dei servizi ICT rilevano nella definizione dei rischi[48].

44 Regolamento UE 2554/2022, art. 3, par. I, p. to 28, in cui viene definito il subappaltatore stabilito in un paese terzo.

45 Regolamento UE 2554/2022, art. 3, par. I, p. to 24. L'attenzione per i fattori che determinano la dipendenza da fornitori terzi ICT stabiliti fuori dall'UE o con evidenti collegamenti societari esteri all'UE non paiono limitati alla tutela di interessi direttamente connessi al settore finanziario, ma pongono l'attenzione sugli ulteriori interventi Europei volti a garantire una sovranità tecnologica europea (che paiono costituire un interesse superiore che va oltre un singolo settore, comunque complementare ad esso). L'evoluzione del progetto Gaia-X (*https://gaia-x.eu/*), volto a realizzare una governance dei dati dell'UE attraverso una rete *cloud* con sede nell'Unione Europea, potrebbe garantire l'indipendenza dai fornitori esterni di servizi *cloud* rafforzando le modalità di gestione dei dati e delle informazioni del settore finanziario, nonché la sovranità economica, tecnologica e politica europea. La realizzazione di una piattaforma dell'UE per i dati potrebbe consentire l'accesso a fornitori di servizi *cloud* alternativi, anche nel settore finanziario. La Commissione ha chiesto all'Agenzia dell'Unione europea per la cibersicurezza (ENISA) di sviluppare un regime di certificazione della cibersicurezza per i servizi *cloud*, in conformità del regolamento sulla cibersicurezza, che contribuirà ad aumentare la fiducia nell'utilizzo del *cloud*, in particolare da parte dei servizi finanziari e degli organismi di regolamentazione. Parere del Comitato economico e sociale europeo sulla 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, 24 febbraio 2021, in cui si ritiene che una rete *cloud* europea faciliterebbe inoltre i flussi di dati tra gli Stati UE.

46 Regolamento UE 2554/2022, art. 3, par. I, p. to 29, in cui si definisce il rischio di concentrazione delle TIC e art. 29, sulla valutazione preliminare del rischio di concentrazione.

47 Regolamento UE 2554/2022, art. 31, par. II.

48 I settori di servizi ICT che comunemente rientrano tra le funzioni critiche e importanti del settore finanziario ricomprendono: i servizi di infrastruttura di rete, i servizi di data center.

La circostanza per cui la maggior parte degli operatori finanziari sistemici europei ricorre ai servizi di tecnologia finanziaria forniti da società di paesi terzi (Stati Uniti e Cina)[49] che hanno una posizione dominante in alcuni servizi ICT (quale il *cloud*) espone il Mercato Unico ad una dipendenza che non è solo più tecnologica, ma che genera effetti sulle operazioni finanziarie e nei rapporti politici. La disciplina europea sulla resilienza operativa digitale (DORA) può rivelarsi insufficiente in situazioni in cui le caratteristiche del mercato dei fornitori di servizi ICT sia tale da vincolare il settore finanziario (es. in caso di un numero limitato fornitori di servizi, esterni all'Unione Europea, in presenza di accordi commerciali, vincoli societari o situazioni di controllo e collegamento tra i possibili fornitori).

L'esternalizzazione di servizi ICT comporta inoltre l'accesso alle informazioni sensibili e dati finanziari da parte di soggetti terzi. Possibili violazioni della sicurezza possono incidere sulla stabilità del settore, anche indirettamente (quale conseguenza della limitata affidabilità del sistema europeo). L'incremento dei rapporti contrattuali tra operatori finanziari e aziende ICT, potrebbe creare un'ulteriore complessità dove i fornitori terzi sfruttino le loro infrastrutture e la superiorità nella raccolta dei dati mediante forme di interconnessione.

I rischi operativi, connessi a problemi tecnici o interruzioni nei servizi forniti dai terzi fornitori e la necessità di sostituire un fornitore di servizi ICT, possono incidere direttamente sulle attività delle istituzioni finanziarie (causando ritardi nelle transazioni, perdite di dati o interruzioni dei servizi ai clienti) condizionando la continuità dell'attività. L'allineamento degli strumenti di risposta e recupero dei dati a seguito di incidenti informatici con le previsioni del Consiglio per la stabilità finanziaria (*Cyber Incident Response and Recovery* – CIRR – del *Financial Stability Board* – FSB) pare essenziale per garantire una omogeneità nelle misure.

La costante evoluzione tecnologica e la necessità di correggere, aggiornare strumenti, metodologie e *software* incrementano tali rischi.

I rischi di dipendenza, di concentrazione o di *lock in* da uno (non facilmente sostituibile) o più fornitori terzi (tra loro strettamente connessi) per i servizi rilevanti e per la continuità operativa dell'istituzione finanziaria possono riflettersi negativamente sulla stabilità del sistema finanziario[50]. Il ricorso al medesimo for-

49 Masera 2022: 167, in cui si evidenzia come la Cina, con alcune delle più importanti Fintech Companies del mondo, pone una sfida alla leadership degli US nella Finanza Digitale e al ruolo del dollaro al centro del sistema finanziario internazionale. Per una analisi del contesto italiano: Consob, *FINTECH: Profili di attenzione e opportunità per gli emittenti e il risparmio nazionale*, 6 luglio 2021. Si v. anche: Trautmann 2023: 38(5), 155-161.

50 European Supervisory Authorities, *ESAs Report on the landscape of ICT third-party providers in the EU*, 19 settembre 2023, la cui analisi evidenzia un mercato rilevante composto da circa 15.000 fornitori che prestano servizi ICT a circa 1.600 entità finanziare incluse nel campione d'indagine (tra cui le imprese di assicurazione). Secondo l'analisi, i fornitori più richiesti sono anche quelli che tendono a fornire servizi a supporto del maggior numero di funzioni essenziali o importanti e la difficile sostituibilità dei fornitori ICT che prestano attività in relazione a funzioni essenziali. Si v. anche European Supervisory Authorities, Joint European Supervisory *Authority responsa to a request for technical advice on digital finance and relate issues*, ESA 2022 01, 31 gennaio 2022; European Banking Authority, *Report on the use of digital platforms in the EU banking*

nitore per più tipologie di servizi accresce gli effetti di dipendenza dell'operatore finanziario dal fornitore stesso ponendo quest'ultimo in posizione dominante nel mercato (rendendo altresì possibile, in presenza di un numero limitato di fornitori ICT per specifiche prestazioni contrattuali, la realizzazione di accordi per la suddivisione del mercato rilevante).

Ove più operatori del settore finanziario ricorrano al medesimo fornitore o sussistano interdipendenze societarie tra questi, si possono generare conflitti di interesse riducendo la capacità di prevedere condizioni contrattuali proporzionate alla tipologia di prestazione e rischio. Una particolare attenzione concerne anche la possibile partecipazione di uno o più operatori del settore finanziario al capitale sociale del fornitore di servizi ICT o il ricorso a società che rientrano in gruppi di imprese.

Ulteriori fattori di rischio riguardano i possibili accordi di subappalto e le catene di subappalti, che rendono complessa l'attività di sorveglianza (anche in termini di analisi dei rapporti societari), soprattutto quando siano conclusi con fornitori terzi di servizi ICT stabiliti in un paese terzo[51].

La possibilità che tali eventi si verifichino genera un autonomo rischio che concerne la reputazione dell'operatore finanziario e dell'intero sistema europeo incidendo negativamente sulla fiducia degli investitori. Qualsiasi problema legato alla sicurezza dei dati o alle prestazioni dei servizi ICT da parte di terzi può danneggiare gravemente la reputazione di un'istituzione finanziaria.

L'attività di analisi e gestione del rischio è imputata all'organo di governo dell'operatore finanziario che, nell'ambito dei suoi compiti connessi alla gestione sana e prudente dell'attività, è chiamato ad approvare il "quadro per la gestione dei rischi informatici"[52] che contiene la politica dell'operatore per l'uso di servizi ICT prestati da un fornitore terzo e la predisposizione di canali di comunicazione aziendali idonei ad ottenere informazioni sui rapporti contrattuali con i fornitori terzi e le relative modifiche[53]. Si definisce in questo modo una "strategia per i rischi informatici derivanti da terzi" fondata sulla differenziazione dei fornitori (non solo per ridurre l'incidenza di singoli rischi, ma anche il rapporto di forza sotteso alla dipendenza dall'ICT) e revisioni periodiche dei rischi da parte dell'organo di gestione dell'operatore finanziario[54].

L'analisi e la ponderazione preventiva, equilibrata e precauzionale consente agli operatori del settore di organizzare e migliorare la propria conoscenza

and payements sector, 21 settembre 2021; Palmerini – Aiello – Cappelli – Morgante – Amore – Di Vetta – Fiorinelli – Galli 2018: 35 e s.; Campa 2023.

51 EBA, *Raccomandazioni in materia di esternalizzazione a fornitori di servizi cloud*, 28 marzo 2018, 11 e s.

52 Regolamento UE, 2554/2022, art. 5, par. II. Il quadro per la gestione dei rischi informatici trova disciplina specifica nel successivo art. 6. Nel caso in cui ricorrano le circostanze, si v. anche l'art. 16 relativo al quadro semplificato.

53 Regolamento UE, 2554/2022, art. 5, par. II, lett. h) e i).

54 Regolamento UE 2554/2022, art. 28, par. II. La strategia per i rischi informatici derivanti da terzi comporta, per l'organo di gestione, un controllo costante e periodico rischi individuati in relazione agli accordi contrattuali per l'utilizzo di servizi ICT a supporto di funzioni essenziali o importanti.

delle attività ICT, è contemperata ed integrata da previsioni contrattuali e di sorveglianza idonee.

3. La gestione dei rapporti tra operatori finanziari e fornitori terzi di servizi ICT

La direttiva UE NIS2 definisce un contesto volto a consentire l'efficace gestione di rischi informatici nel Mercato Interno, ed è funzionalmente connessa, con specifica rilevanza per gli operatori finanziari con il regolamento UE DORA. Quest'ultimo individua nel contratto con terzi fornitori di servizi ICT (in relazione a funzioni "essenziali e importanti") e nell'attività di sorveglianza (sull'attività dei fornitori terzi "critici") i due strumenti con cui bilanciare i molteplici interessi in rapporto e riequilibrare la dipendenza del settore finanziario da quello tecnologico.

In un contesto in cui gli operatori finanziari possono avere difficoltà ad imporre determinate clausole all'interno del contratto, rilevano quelli che sono veri e propri obblighi che la disciplina europea pone in capo ai fornitori terzi.

Gli elementi essenziali dei contratti con i fornitori terzi di servizi ICT sono strettamente collegati alla necessità di garantire all'operatore finanziario un controllo sulla sicurezza e sulla corretta gestione operativa dell'attività finanziaria (al fine di tutelare la solidità e la continuità dei servizi finanziari)[55].

Se la previsione normativa di vincoli contrattuali obbligatori per i fornitori terzi di servizi ICT rende ulteriormente percepibile la necessità di tutelare gli operatori finanziari (dalla posizione di forza contrattuale del settore ICT), l'attività delle autorità di vigilanza interviene a supporto dell'analisi e gestione rischi (in chiave di prevenzione e mitigazione degli eventi)[56] e dell'attività contrattuale con terzi fornitori di servizi ICT (quale strumento istituzionale di garanzia da asimmetrie informative e a tutela del risparmio).

Mentre la sorveglianza interna garantisce un livello di autonomia minimo (anche di carattere tecnico) dell'operatore finanziario, rispetto alle altre funzioni interne e ai fornitori ICT[57], la sorveglianza esterna rende i fornitori di servizi ICT (che in linea generale non esercitano attività di natura finanziaria), soggetti alla vigilanza di Autorità che viceversa svolgono il proprio ruolo nell'ambito finanziario, bancario e assicurativo[58]. Tale attività assume un ruolo particolarmente incisivo in relazione ai fornitori terzi "critici"[59], con i quali le Autorità Europee di Vigilanza – AEV (e quella individuata come capofila), istituiscono un rapporto diretto[60].

55 Rilevano quindi la descrizione chiara delle prestazioni oggetto del contratto, i livelli di servizio, ed il luogo della sua esecuzione (anche in un contesto di gestione e conservazione delle informazioni nell'UE), le condizioni di eventuali contratti di subappalto, la gestione delle informazioni e dei dati (anche in relazione ai casi in cui il fornitore terzo risulti impossibilitato a fornire la prestazione).

56 Rabitti 2023(a): 343 e s.

57 Regolamento UE 2554/2022, art. 6, IV.

58 Campa 2023: 5.

59 Regolamento UE 2554/2022, artt. 31-44.

60 Si v.: l'art. 31, par V, in cui si prevede la notifica diretta al fornitore terzo della sua

Le autorità di sorveglianza capofila, individuate direttamente dalle AEV[61] sulla base di criteri aventi ad oggetto i servizi ICT prestati dal fornitore terzo (quali l'impatto sistemico, l'importanza delle entità finanziarie, la dipendenza dai servizi prestati dal fornitore terzo e il grado di sostituibilità)[62], si propongono di acquisire una conoscenza approfondita e completa delle relazioni nei singoli settori della fornitura di servizi ICT[63].

La cooperazione[64] e il coordinamento[65] dell'attività delle Autorità di Vigilanza Europee nell'ambito di una rete comune, costituisce fattore determinante per individuare i possibili soggetti terzi critici e garantire l'effettività della sorveglianza nel Mercato Unico[66].

qualificazione come "critico" (il quale a sua volta deve informare l'operatore finanziario a cui presta servizi ICT); l'art. 31, par. XIII, in cui il fornitore terzo critico è chiamato a notificare direttamente all'autorità di sorveglianza capofila gli eventuali cambiamenti sulla struttura gestionale dell'impresa figlia istituita nell'UE; art. 33, par. I, in relazione ai compiti dell'autorità di sorveglianza capofila, si individua quest'ultima quale "principale punto di contatto per i fornitori terzi critici di servizi ICT"; art. 35, in relazione all'esercizio diretto dei poteri dell'autorità di sorveglianza capofila sul fornitore terzo critico.

61 Su proposta del comitato congiunto delle AEV (per la funzione di coordinamento nell'ambito del Sistema europeo di vigilanza finanziaria) e su raccomandazione del forum di sorveglianza (organo di supporto del comitato congiunto e delle AEV individuate come capofila per il singolo operatore finanziario sulla base della quota principale delle proprie attività).

62 Regolamento UE 2554/2022, art. 31, par. II. Criteri che potranno essere ulteriormente integrati dalla Commissione UE entro il 17 luglio 2024 (si v. il par. VI).

63 In questo contesto sono di interesse (quale anticipazione dei criteri che potranno essere integrati dalla Commissione UE) gli indicatori quantitativi e qualitativi proposti dalle AEV riferiti ad undici criteri di criticità suggeriti ed ai rispettivi livelli di rilevanza. European Supervisory Authorities, *Joint European Supervisory Authorities' Technical Advice to the European Commission's December 2022 Call for Advice on two delegated acts specifying further criteria for critical ICT thirdparty service providers (CTPPs) and determining oversight fees levied on such providers*, 29 settembre 2023, dove, in relazione agli indicatori quantitativi, sono proposte alcune soglie minime di rilevanza. Tali soglie di rilevanza minima costituiscono un requisito minimo al di sopra del quale deve essere effettuata la valutazione sulla criticità.

64 *Ex* art. 16 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010. Cfr. il Regolamento UE 2554/2022, art. 32, c. VII, in cui si prevede il compito per le AEV di formulare (entro il 17 luglio 2024) "orientamenti sulla cooperazione tra le AEV e le autorità competenti concernenti le procedure e le condizioni dettagliate per la ripartizione e l'esecuzione dei compiti tra le autorità competenti e le AEV, nonché forniscono dettagli sugli scambi di informazioni necessari alle autorità competenti per garantire il seguito da dare alle raccomandazioni a norma dell'articolo 35, paragrafo 1, lettera d) rivolte ai fornitori terzi critici di servizi TIC". Si v. anche gli artt. 48 e 49 in relazione, rispettivamente, alla cooperazione tra l'autorità di sorveglianza capofila e le Autorità Europee di Vigilanza con le competenti autorità amministrative indipendenti nazionali.

65 Regolamento UE 2554/2022, art. 34. Cfr. anche art. 35, par. II e IV in relazione al coordinamento dell'autorità di sorveglianza capofila con la rete di sorveglianza comune.

66 Le AEV raccolgono i dati sui contratti conclusi dagli operatori finanziari con fornitori terzi di servizi ICT, potendo anche accedere al registro informazioni completo (art. 28, par. III), li trasmettono al forum di sorveglianza (art. 31, par. X). Schneider 2023: 1014 e s., in cui si prospetta un coordinamento dell'attività di vigilanza anche con IA. In questo contesto sono di interesse (quale anticipazione dei criteri che potranno essere integrati dalla Commissione UE) gli indicatori quantitativi e qualitativi proposti dalle AEV riferiti ad undici criteri di criticità suggeriti ed ai rispettivi livelli di rilevanza. Cfr. il rapporto tra l'art. 33, par. IV e l'art. 34.

La necessità di garantire l'efficacia dell'attività di sorveglianza anche dei fornitori terzi critici con sede in un paese terzo[67] e la possibile assenza di rapporti di cooperazione con le autorità di vigilanza finanziaria nei paesi terzi comporta (per il fornitore terzo) l'obbligo di assicurare una presenza commerciale nell'UE mediante l'istituzione di un'impresa figlia entro 12 mesi dalla sua designazione come "critico"[68].

Tali attività di sorveglianza includono un potere sanzionatorio[69] nei confronti dei fornitori di servizi ICT che si aggiunge alle sanzioni di natura contrattuale previste dalla disciplina europea[70] e che incide sulla gestione del rapporto con gli operatori finanziari.

Nel rapporto tra Autorità di vigilanza e fornitori terzi di servizi ICT si definisce una relazione volta a completare i vincoli contrattuali (previsti direttamente dall'ordinamento giuridico europeo) al fine di vincolare maggiormente i fornitori terzi di servizi ICT. In tale rapporto risulta peculiare come il ruolo della sorveglianza sia chiamato ad intervenire in relazione a rischi esterni all'attività finanziaria, comportando anche la necessità di dotarsi di una specifica conoscenza.

4. Il ruolo della vigilanza nella cybersecurity per il settore bancario e finanziario

La disciplina dei rapporti tra settore finanziario e ICT, inserendosi in un quadro giuridico più ampio, costituisce una presa di coscienza degli interessi coinvolti dal rapporto di dipendenza dal settore ICT e come risultino necessarie specifiche misure volte a rispondere alle specificità del settore finanziario per gestire efficacemente fenomeni a carattere sovranazionale.

67 Rendendo ad es. difficili le attività ispettive e l'irrogazione di eventuali sanzioni (es. in materia di trasparenza e accesso). Si v. il combinato tra Regolamento UE 2554/2022, art. 35, par. I e VI.

68 Regolamento UE 2554/2022, art. 31, par. XII e XIII. Tale misura tuttavia può non essere sufficiente per garantire gli obiettivi dell'attività di sorveglianza richiedendo la conclusione (da parte delle AEV) di appositi accordi di cooperazione con le autorità dei paesi terzi al fine di rendere possibile l'acquisizione di informazioni e l'esercizio delle funzioni ispettive. Sul punto si v. Regolamento UE 2554/2022, art. 36, ove sono altresì disciplinati i limiti dei poteri delle AEV e il contenuto minimo degli accordi di cooperazione amministrativa. Per assolvere alle funzioni previste dal regolamento DORA, le autorità di vigilanza capofila sono dotate di poteri di indagine, ispettivi e di raccomandazione il cui inadempimento può comportare l'adozione di sanzioni amministrative (penalità di mora quantificate su base giornaliera e parametrata al fatturato medio quotidiano realizzato a livello mondiale dal fornitore terzo), anche a seguito di un contradditorio con i rappresentanti del fornitore terzo critico.

69 Regolamento UE 2554/2022, artt. 50-51. Si v. anche art. 52, in relazione alla possibile rilevanza penale nell'ordinamento giuridico nazionale.

70 Regolamento UE 2554/2022, art. 28, par. VII e VIII. Si v. anche l'art. 42, par. VI e 50, secondo cui alle autorità amministrative indipendenti nazionali è riconosciuto il potere di imporre di richiedere ad un operatore finanziario di sospendere temporaneamente o la risoluzione del contratto con un fornitore terzo critico ICT fino a quando non si sia posto rimedio ai rischi individuati nelle raccomandazioni rese ad un fornitore terzo critico.

L'attività di sorveglianza e la cooperazione tra le autorità di vigilanza risulta strumento essenziale ma non necessariamente sufficiente per prevenire e ridurre eventuali distorsioni in tale settore (che trovano tuttavia origine al di fuori di esso) capaci di incidere negativamente sul rapporto di fiducia con gli investitori.

L'attività di vigilanza è chiamata ad assumere un ruolo centrale a garanzia del corretto funzionamento del settore.

Se, a livello nazionale, la direttiva UE NIS2 prevede un articolato sistema di vigilanza che pone in rapporto l'Agenzia per la cybersicurezza nazionale (individuata quale autorità competente e punto unico di contatto nell'ambito dei rapporti sovranazionali)[71] con il Ministero dell'economia e delle finanze (individuata quale Autorità di settore NIS per i settori bancario e delle infrastrutture finanziarie, "sentite le autorità di vigilanza di settore, Banca d'Italia e Consob")[72], il regolamento UE DORA pone in rapporto diretto i fornitori terzi critici con l'AEV individuata quale autorità capofila[73] (quest'ultima coadiuvata, per quanto concerne i rischi informatici, dal forum di sorveglianza[74] e, in generale, dalle Autorità nazionali competenti[75]).

Si definisce in questo modo un complesso sistema di vigilanza che contempla l'interazione tra soggetti giuridici nazionali ed europei in cui opera un "gruppo di cooperazione" (previsto dalla direttiva UE NIS2[76]) che consente un collegamento con le Autorità competenti ai sensi del regolamento UE DORA[77], rendendo possibile sia uno scambio di informazioni, sia forme di consulenza e assistenza tecnica.

L'utilizzo di poteri impliciti da parte delle autorità di settore (ovvero l'esercizio di competenze che non risultano espressamente da norme giuridiche, ma che si ricavano in via interpretativa per deduzione e che consentono alle autorità di vigilanza il corretto perseguimento dei propri fini istituzionali[78]), oltre ad ampliare il

71 d.lgs. 4 settembre 2024, n. 138, art. 10.

72 d.lgs. 4 settembre 2024, n. 138, art. 11, c. II, lett. b).

73 Regolamento UE, 2554/2022, art 31, par. I, lett. b), individuata tra le AEV sulla base di quella responsabile, "a norma dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010, delle entità finanziarie che possiedono complessivamente la quota maggiore delle attività totali rispetto al valore delle attività totali di tutte le entità finanziarie che utilizzano i servizi del pertinente fornitore terzo critico di servizi TIC, secondo quanto risulta dalla somma dei singoli bilanci di quelle entità finanziarie".

74 Regolamento UE, 2554/2022, art. 32, par. I.

75 Regolamento UE, 2554/2022, art. 40.

76 Direttiva UE, 2555/2022, art. 14.

77 Regolamento UE, 2554/2022, art. 47.

78 Cons. St., VI, 14 dicembre 2020, n. 7972, ove, nell'ambito del contenzioso relativo al caso Telecom S.p.A. e Vivendi S.A., sono ricondotti all'Autorità di settore (Consob) poteri impliciti per garantire il "funzionamento del mercato finanziario e l'interesse generale degli investitori e dei risparmiatori": cfr.: Cons. St., VI, 17 ottobre 2005, n. 5827; Cons. St., VI, 24 maggio 2016, n. 2182, che pur annulla il provvedimento impugnato per non aver perseguito le finalità attribuite all'ARERA. Così anche Cons. St., VI, 1 ottobre 2014, n. 4874 che, pur indicano nei presupposti dell'applicazione del principio di legalità "per obbiettivi" anche l'individuazione di limiti entro cui può esercitarsi l'attività amministrativa, finisce per identificare questi limiti negli stessi obiettivi individuati dalla legge; Cons. St., VI, 20 marzo 2015, n. 1532; VI, 2 maggio 2012, n. 2521; Cons. St., VI, 15 luglio 2019, n. 4993, in cui il Giudice, dopo aver fatto una applicazione ampia della teoria

dibattito sulla compatibilità di tali poteri con il principio di legalità, pone ulteriore indeterminatezza nel corretto adempimento dei vincoli gestionali da parte degli operatori finanziari.

Queste criticità possono risultare tali da non consentire la rapida individuazione di un rischio o incidere sulle tempistiche per la sua efficiente gestione.

Ulteriori elementi previsti dalla direttiva UE NIS2 e dal regolamento UE DORA possono rendere il contesto maggiormente complesso.

Se, nell'ambito del regolamento UE DORA, la definizione di un adeguato livello di sicurezza e la mancanza di alternative reali, costituiscono criteri per la qualificazione di fornitore "critico"[79], un errore di valutazione dell'operatore finanziario sulla criticità di un fornitore può ridurre la sorveglianza delle AEV. Tale circostanza potrebbe risultare anche conseguenza di un tentativo di nascondere alcune criticità per evitare effetti sul mercato finanziario (o ritorsioni commerciali dal settore ICT).

La complessità che consegue a possibili catene di subappalto (che contraddistinguono la fornitura di alcuni servizi ICT)[80] pur comportando la previa valutazione dell'operatore finanziario, rende difficilmente monitorabili i rapporti giuridici tra i subappaltatori (ad es. in relazione a controlli volti ad evitare possibili conflitti di interesse tra i terzi fornitori), contribuendo ad incidere sull'equilibrio contrattuale, sul possibile utilizzo distorto di dati e informazioni e sui rapporti di dipendenza. L'attività di vigilanza è resa ulteriormente complessa dalla collaborazione diretta richiesta al fornitore terzo che, nell'ambito dei propri doveri di buona fede e cooperazione, è tenuto a comunicare determinati eventi all'Autorità di sorveglianza capofila[81] (è questo il caso dei contratti di subappalto, in cui l'Autorità di sorveglianza può raccomandare la rinuncia a stipulare il subcontratto[82]).

Tale rapporto diretto può creare distorsioni anche nei confronti dell'operatore finanziario che, da un lato, ha la "responsabilità finale per la gestione dei rischi informatici dell'entità finanziaria"[83] (dovendosi quindi dotare di specifiche com-

dei poteri impliciti con struttura finalistica, individua un limite all'applicazione di questa soluzione ermeneutica nella previsione di sanzioni amministrative e non nell'adozione di misure amministrative inibitorie. In dottrina, *ex multis*: Marra 2023, 697 e s.; Morbidelli 2007, 703 e s.; Bassi 2001, il quale ritiene che "la funzione predeterminata dalla norma quale scopo da perseguire da parte dell'autorità, cioè, funge qui da semplice criterio di esercizio del potere (attraverso la sanzione del c.d. sviamento), ma non da elemento di attribuzione del potere".

79 Regolamento UE, 2554/2022, art 31, par. 2, lett. c) e d).

80 Rese possibili dalla circostanza che 9000 subappaltatori supportano fornitori terzi critici. Cfr. European Supervisory Authorities, *ESAs Report on the landscape of ICT third-party providers in the EU*, cit., p. to 13.

81 Regolamento UE 2554/2022, art. 35, par. I e V.

82 Regolamento UE 2554/2022, art. 30.

83 Circa la responsabilità dell'organo di gestione dell'operatore finanziario si v.: Regolamento UE, 2554/2022, considerando n. 45 e art. 5, par. II. A questo si aggiungono anche le responsabilità dei collaboratori dell'organo di gestione ed a cui quest'ultimo ha conferito un ruolo nell'ambito della governance di resilienza digitale oltre che le responsabilità di natura contrattuale del soggetto terzo fornitore di servizi ICT.

petenze anche all'interno degli organi di gestione) e, dall'altro, non è parte del dialogo con l'Autorità di vigilanza.

Gli stessi meccanismi di funzionamento dell'attività di sorveglianza e i tempi richiesti per gestire le comunicazioni tra le Autorità (europee e nazionali) coinvolte può non consentire una pronta risposta ad un evento che, attraverso gli strumenti tecnologici, genera effetti considerevoli in un limitato intervallo di tempo.

La possibile irrogazione di sanzioni quantificate sul fatturato globale e di natura reputazionale[84] può incidere negativamente sull'interesse degli operatori economici (per i prestatori internazionali di servizi ICT) di operare nel Mercato Interno e sottoporsi ai vincoli previsti dall'ordinamento giuridico europeo.

In tale contesto, una possibile riduzione di tale interesse può riflettersi sul novero di possibili fornitori di servizi ICT (aumentando i rischi di concentrazione) e, nei settori rilevanti in cui opera un numero ristretto di imprese, può generare posizioni 'dominanti' nei singoli mercati di riferimento (riducendo ulteriormente la capacità degli operatori finanziari a inserire vincoli aggiuntivi nei contratti con i fornitori terzi di servizi ICT).

L'ulteriore considerazione per cui, in relazione ai fornitori stabiliti al di fuori dell'UE, sia previsto l'obbligo di costituire un'impresa stabilita nell'UE, è un elemento che non necessariamente pare sufficiente a tutelare gli operatori finanziari o gli investitori, potendo risultare maggiormente opportuna la realizzazione di infrastrutture native nell'Unione Europea.

In questo contesto, permangono tuttavia perplessità sulla efficacia delle misure europee sul settore finanziario, su cui influisce in vario modo il rapporto di dipendenza rispetto al settore ICT.

Bibliografia

Alpa G. 2019, "Fintech: un laboratorio per i giuristi", in *Contratto e Impresa*, 377 e s.

Annunziata F. 2020, "Verso una disciplina europea delle cripto-attività. Riflessioni a margine della recente proposta della Commissione UE", in *Riv. Dir. Bancario*, 1-15.

Annunziata F. – Minto A. 2022, "Il nuovo Regolamento UE in materia di Distributed Ledger Technology", in *Riv. Dir. Bancario*, 1-8.

Arner-Buckley-Zetsche 2022, "Open Banking, Open Data e Open Finance: Lessons from the European Union", in Jeng (a cura di), *Open Banking*, Oxford: Oxford University Press, 147 e s.

84 Sul regolamento UE DORA, si v. la comunicazione al pubblico delle penalità inflitte (Regolamento UE 2554/2022, art. 35, par. X) o nel caso di mancata risposta alle raccomandazioni formulate (Regolamento UE 2554/2022, art. 42, par. II). Sulla direttiva UE NIS2, si v. il regime sanzionatorio che ricade in capo al soggetto essenziale o al soggetto importante in caso di non conformità rispetto agli obblighi previsti (che può arrivare, per i soggetti essenziali, a €10.000.000 o almeno il 2% del fatturato mondiale totale annuo nell'anno fiscale precedente – su cui direttiva UE, 2555/2022, art. 34, par. IV – e, per i soggetti importanti, fino a €7.000.000 o almeno l'1,4% del fatturato mondiale totale annuo nell'anno fiscale precedente della società a cui appartiene l'entità importante per i soggetti importanti – su cui direttiva UE, 2555/2022, art. 34, par. V –).

Baskerville R. – Capriglione F. – Casalino N. 2020, "Impacts, Challenges and trends of Digital Transformation in the Banking Sector", in *Law and Economics Yearly Review*, 341 e s.
Bassi N., "Principio di legalità e poteri amministrativi impliciti", Giuffrè, Milano, 2001.
Bronzetti A. 2023, "Il diritto europeo della banca e della finanza tra passato e futuribile", in *Riv. trim. dir. dell'economia*, 1: 6-60.
Campa J. M. 10 ottobre 2023, "Operational resilience in EU financial services", keynote speech at the *14th Financial meeting* organised by Expansion, accessibile in https://www.eba.europa.eu/sites/default/documents/files/document_library/Calendar/EBA%20Official%20Meetings/2023/Jos%C3%A9%20Manuel%20Campa%20keynote%20speech%20at%20the%2014th%20Financial%20meeting%20organised%20by%20Expansion/1063659/JM%20Campa%20speech%20on%20digitalisation%20and%20DORA%20at%2010-10-2023.pdf.
Canepa A. 2021, "*Big tech* e mercati finanziari: «sbarco pacifico» o «invasione»? Analisi di un «approdo» con offerta «à la carte»", in *Riv. trim. dir. dell'economia*, 465 e s.
Capriglione F. 2019, "Industria finanziaria, innovazione tecnologica, mercato", in *Riv. trim. dir. dell'economia*, 374 e s.
Capriglione F. 2021, "Diritto ed economia. La sfida dell'intelligenza artificiale", in *Riv. trim. dir. eco*., (3) 4 e s.
Capriglione F. 2022, "Le cripto attività tra innovazione tecnologica ed esigenze regolamentari", in *Riv. trim. dir. eco*., 254.
Casalino N. 2023, "La digitalizzazione del settore finanziario", in M. Pellegrini (a cura di), *Diritto pubblico dell'economia*, Vicenza: CEDAM, 337 e s.
Celati B., "La sostenibilità della trasformazione digitale: tra tutela della concorrenza e «sovranità tecnologica europea»", in *Riv. trim. dir. eco*., 2021, 3, 252 e s.;
Davola A. 2017, "*Bias* cognitivi e contrattazione standardizzata: quali tutele per i consumatori?", in *Contratto e impresa*, 637 e s.
Finocchiaro G., "La sovranità digitale", in *Dir. pub.*, 2022, 809 e s.
Lemma V. 2020, "FinTech Regulation: Exploring New Challenges of the Capital Markets Union", Cham: Springer International Publishing.
Lemma V. 2023, "Solidarietà e regolazione dell'innovazione finanziaria", in *Riv. trim. dir. dell'economia*,, 83-100;
Marra A., "I poteri impliciti", in *Dir. amm*., 2023, 697 e s.
Masera R. 2022, "L'Europa, l'unione europea e l'eurozona: crisi e proposte di soluzione", in *Riv. trim. dir. dell'economia*, 151-184.
Mazzarisi p. – Ravagnani A. – Deriu p. – Lillo F. – Medda F. – Russo A. 2022, "Metodi sperimentali di machine learning per supportare le decisioni nella *detection* degli abusi di mercato", in *Quaderni FinTech – Consob*, (11) 1-49.
Miglionico A. 2019, "Innovazione tecnologica e digitalizzazione dei rapporti finanziari", in *Contratto e Impresa*, 1376 e s.
Morbidelli G., "Il principio di legalità e i c.d. poteri impliciti", in *Dir. amm*., 2007, 703 e s.
Palmerini E. – Aiello G. – Cappelli V. – Morgante G. – Amore N. – Di Vetta G. – Fiorinelli G. – Galli M. 2018, "Il FinTech e l'economia dei dati. Considerazioni su alcuni profili civilistici e penalistici. Le soluzioni del diritto vigente ai rischi per la clientela e gli operatori", in *Quaderni FinTech – Consob*, 1-97.
Rabitti M. 2023(a), *Le regole di supervisione nel mercato digitale: considerazioni intorno alla comunicazione Banca d'Itlia in materia di tecnologie decentralizzate nella finanza e cripto-attività*, in D. Rossano (a cura di) *La supervisione finanziaria dopo due crisi. Quali prospettive*, Padova: CEDAM, 345-355.

Rabitti M. 2023(b), "Due diligence sulla sostenibilità e digitalizzazione della catena del valore: l'apporto di blockchain e smart contracts", in *Riv. trim. dir. dell'economia*, 166-185.
Ruocco C. 2023, *"Finanza digitale: opportunità, profili di attenzione e ruolo della supervisione finanziaria"*, in D. Rossano (a cura di) *La supervisione finanziaria dopo due crisi. Quali prospettive*, Padova: CEDAM, 181-187.
Schneider G. 2023, "La proposta di regolamento europeo sull'intelligenza artificiale alla prova dei mercati finanziari: limiti e prospettive (di vigilanza)", in *Resp. civ. e prev*., 1014 e s.
Sciarrone Alibrandi A. – Borello G. – Ferretti R. – Lenoci F. – Macchiavello E. – Mattassoglio F. – Panisi F. 2019, "Marketplace lending Verso nuove forme di intermediazione finanziaria?", in *Quaderni FinTech – Consob*, (5) 1-285.
Schneider G. 2023, "La proposta di regolamento europeo sull'intelligenza artificiale alla prova dei mercati finanziari: limiti e prospettive (di vigilanza)", in *Resp. civ. e prev*., 1014 e s.
Sepe M. 2021, "Innovazione tecnologica, algoritmi e Intelligenza Artificiale nella prestazione dei servizi finanziari", in *Riv. trim. dir. dell'economia*, 186 e s.
Trautmann K. 2022, "EU-DORA regulation as a result of cloud computing adoption by the financial services industry", in *Journal of International Banking Law and Regulation*, 38(5), 155-161.
Urbani F. 2022, "Rassegna dei principali interventi legislativi, istituzionali e di policy a livello europeo in ambito societario, bancario e dei mercati finanziari", in *Riv. delle società*, 985 e s.