«Il diritto dell'economia» issn 1123-3036, anno 70, n. 115 (3 2024) pp. 247-267

Articoli e saggi

I rapporti tra finanza e settore ICT nella resilienza operativa digitale per il settore finanziario

Matteo Pignatti

Sommario: 1. La digitalizzazione nel settore finanziario. La resilienza del Mercato Unico e le sfide della globalizzazione. – 2. I rischi nell'affidamento a soggetti terzi di servizi ICT nel settore finanziario e la loro gestione. – 3. I contratti con i soggetti terzi fornitori di servizi ICT e l'attività di vigilanza nella resilienza operativa digitale per il settore finanziario. – 4. La resilienza operativa digitale per il settore finanziario nei rapporti di dipendenza con il settore ICT.

1. *La digitalizzazione nel settore finanziario. La resilienza del Mercato Unico e le sfide della globalizzazione*

L'utilizzo diffuso dei servizi ICT nel settore finanziario[1] ha cambiato le caratteristiche dell'attività finanziaria. Si è eliminata la dimensione territoriale dei mercati[2] e i rapporti giuridici sono stati slegati dalla individualità dei soggetti che ne sono parte, consentendo agli operatori del settore di realizzare rapporti giuridici complessi a cui prendono parte più soggetti, alcuni dei quali non entrano in diretto contatto tra loro[3].

[1] Il valore del mercato delle ICT era stimato nel 2019 sopra ai cinquemila miliardi di dollari USA. La sua crescita conferma la sempre maggiore diffusione e importanza della tecnologia nella società odierna e «il settore finanziario rappresenta il principale utilizzatore di ICT al mondo, con una quota pari al 20 % della spesa totale per le TIC». Cfr. 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*, 24 febbraio 2021.

[2] Tale circostanza ha consentito di ampliare i confini delle attività delle organizzazioni finanziarie per competere nel mercato globalizzato e ridurre i costi di gestione. N. Irti, *L'ordine giuridico del mercato*, Bari, 2003, 21. Il mercato, che oggi non coincide con il territorio di uno o più stati, ma risulta come uno spazio slegato da un ambito territoriale definito, estendendo i rapporti giuridici ed economici tra le parti coinvolte.

[3] A. M. Pancallo, *Il digital lending: la* «disumanizzazione» *della filiera del credito*, in *Riv. trim. dir. dell'economia*, 2021, 398 e s., in cui sono analizzati riflessi dell'innovazione tecnologica con particolare riferimento al fenomeno del *digital lending* riprendendo il lavoro di G. Oppo, *Disumanizzazione del contratto?*, in *Riv. dir. civ.*, 1998, I, 525 e s.

La transizione digitale nel settore finanziario si inserisce in un contesto in cui la necessità di adeguare e rendere competitivo il Mercato Unico 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[4]. Si è così creata una co-dipendenza tra settore finanziario e ICT[5] che ha generato differenti fenomeni rilevanti per il diritto dell'economia[6] conferendo al *FinTech* un'autonoma rilevanza[7].

---

[4] 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. A. Bronzetti, *Il diritto europeo della banca e della finanza tra passato e futuribile*, in *Riv. trim. dir. dell'economia*, 2023, 6 e s.; C. Ruocco, *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, 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: F. Capriglione, *Diritto ed economia. La sfida dell'intelligenza artificiale*, in *Riv. trim. dir. eco.*, 2021, 3, 4 e s.; B. Celati, *La sostenibilità della trasformazione digitale: tra tutela della concorrenza e* «sovranità tecnologica europea», in *Riv. trim. dir. eco.*, 2021, 3, 252 e s.; G. Finocchiaro, *La sovranità digitale*, in *Dir. pub.*, 2022, 809 e s.

[5] Già oggi le banche europee dichiarano che il 65% di esse ha *partnership* contrattuale con le aziende *BigTech*. Si v.: J.M. Campa, *Operational resilience in EU financial services*, keynote speech at the 14th Financial meeting organised by Expansion, 10 ottobre 2023, 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. 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 alcune problematiche 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.

[6] 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.

[7] *Ex multis*: V. Lemma, *FinTech Regulation: Exploring New Challenges of the Capital Markets Union*, Palgrave Macmillan, Cham, 2020; Id., *Solidarietà e regolazione dell'innovazione finanziaria*, in *Riv. trim. dir. dell'economia*, 2023, 83 e s.; F. Annunziata, *La disciplina europea del mercato delle cripto-attività (MiCAR)*, in *Riv. Soc.*, 2023, 923 e s.; L. Ammannati, *Regolatori e supervisori nell' era digitale: ripensare la regolazione*, in *Giur. Cost.*, 2023, 1453; F. Annunziata, A. Minto, *Il nuovo Regolamento UE in materia di Distributed Ledger Technology*, in *Riv. Dir. Bancario*, 2022; P. Mazzarisi, A. Ravagnani, P. Deriu, F. Lillo, F. Medda, A. Russo, *Metodi sperimentali di machine learning per supportare le decisioni nella detection degli abusi di mercato*, in *Quaderni FinTech - Consob*, n. 11, 2022; F. Annunziata, *Verso una disciplina europea delle cripto-attività. Riflessioni a margine della recente proposta della Commissione UE*, in *Riv. Dir. Bancario*, 2020; A. Sciarrone Alibrandi, G. Borello, R. Ferretti, F. Lenoci, E. Macchiavello, F. Mattassoglio, F. Panisi, *Marketplace lending Verso nuove forme di intermediazione finanziaria?*, in *Quaderni FinTech - Consob*, n. 5, luglio 2019.

Eventi macroeconomici tra loro interconnessi hanno posto nuovi rischi[8], evidenziando l'importanza della resilienza quale elemento su cui si fonda la fiducia nel settore finanziario europeo (e la sua stabilità)[9].

Ecco come l'utilizzo e la costante evoluzione di strumenti ICT[10] si riflette sugli interessi che l'ordinamento giuridico è chiamato a tutelare mediante la definizione di una disciplina capace di rispondere in maniera efficace alle esigenze del settore finanziario[11].

Le recenti crisi hanno inoltre evidenziato come l'utilizzo di sistemi ICT abbia la capacità di moltiplicare e far propagare gli effetti evolvendosi in una crisi sistemica.

---

[8] Si v. Banca d'Italia, *La cybersicurezza del settore finanziario: ruolo delle autorità e valore della cooperazione*, intervento di apertura di Paolo Angelini - Vice Direttore Generale della Banca d'Italia al convegno "*La cooperazione pubblico-privato per la resilienza cyber del settore finanziario italiano - Le opportunità per gli operatori e il ruolo del CERTFin*", Roma, 4 luglio 2024, in cui si riporta come le segnalazioni inviate alla Banca d'Italia dalle banche e dai prestatori di servizi di pagamento confermano "la forte accelerazione del numero di incidenti cyber l'anno scorso: 30 segnalazioni di attacchi, contro 13 nel 2022. I casi più frequenti hanno riguardato la disponibilità di servizi offerti alla clientela (cosiddetti attacchi *Denial Of Service*), talvolta attuati da soggetti che appaiono riconducibili a governi di paesi Extraeuropei; 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: M. Rabitti, *Le regole di supervisione nel mercato digitale: considerazioni intorno alla comunicazione Banca d'Itlia in materia di tecnologie decentralizzate nella finanza e cripto-attività*, D. Rossano (a cura di) *La supervisione finanziaria dopo due crisi. Quali prospettive*, cit., 345. 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.

[9] Sulla nozione di «resilienza operativa digitale», si v. Regolamento UE, 2554/2022, 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.

[10] «*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*» si v. J. M. Campa, *Operational resilience in EU financial services*, keynote speech at the 14th Financial meeting organised by Expansion, cit.

[11] *Ex multis*: N. Casalino, *La digitalizzazione del settore finanziario*, in M. Pellegrini (a cura di), *Diritto pubblico dell'economia*, Padova, 2023, 337 e s.; R. Baskerville, F. Capriglione, N. Casalino, *Impacts, Challenges and trends of Digital Transformation in the Banking Sector*, in *Law and Economics Yearly Review*, 2020, 341 e s.; G. Alpa, *Fintech: un laboratorio per i giuristi*, in *Contratto e Impresa*, 2019, 377 e s. e quale Premessa in G. Finocchiaro, V. Falce (diretto da), *Fintech: diritti, concorrenza, regole*, Bologna, 2019; A. Miglionico, *Innovazione tecnologica e digitalizzazione dei rapporti finanziari*, in *Contratto e Impresa*, 2019, 1376 e s.

L'esternalizzazione a soggetti terzi di funzioni tecniche e l'interdipendenza dei sistemi ICT incide sulla fiducia nel settore finanziario assumendo rilevanza sotto diversi profili[12]. Se da un lato può consentire di conseguire obiettivi all'interno del mercato (mediante l'acquisizione di un *know-how* specifico), è altresì possibile creare distorsioni (attraverso un erroneo o distorto utilizzo degli strumenti o a causa di interferenze esterne).

La disciplina europea in tema di resilienza operativa digitale per il settore finanziario (*digital operational resilience for the financial sector - DORA*)[13] si inserisce tra le misure volte all'armonizzazione della finanza digitale[14], proponendosi di

[12] Sul tema si v. Basel committee on banking supervision, *The joint forum, outoircung in financial services*, 2005; EBA, *Guidelines on outsourcing*, 14 dicembre 2006; EBA, *Orientamenti in materia di esternalizzazioni*, 25 febbraio 2019; ESMA, *Orientamenti in materia di esternalizzazione dei servizi cloud*, 10 maggio 2021. In dottrina: L. Spitaleri, *L'outsourcing nei servizi bancari e finanziari, profili di governance e prospettive di vigilanza*, in *Riv. trim. dir. dell'economia*, 2023, 111 e s.; A. Sacco Ginevri*, Esternalizzazione (outsourcing),* in Aa.Vv., *Fintech: diritti concorrenza, regole*, a cura di G. Finocchiaro e V. Falce, Bologna, 2019, 205 e s.; G. Falcone, *Profili problematici dell'esternalizzazione di funzioni ed attività «tipiche» da parte degli intermediari del mercato finanziario*, in R. Lener, G. Luchena, C. Robustella (a cura di), *Mercati regolati e nuove filiere di valore*, Torino, 2021, 275 e s.*;* G. Falcone, *Profili problematici del cloud computing nella prestazione di servizi bancari e finanziari: il contratto come strumento «vicario» di regolazione*, in A. Antonucci, M. De Poli, A. Urbani (a cura di), *I luoghi dell'economia. Le dimensioni della sovranità*, Torino, 2019, 229 e s.

[13] La disciplina del regolamento UE, 2554/2022 troverà applicazione dal 17 gennaio 2025. Si v.: 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, definisce la «resilienza operativa digitale» come la «capacità delle imprese di garantire di poter resistere ad ogni tipo di perturbazione e minaccia collegata alle tecnologie dell'informazione e della comunicazione (TIC). La dipendenza sempre più elevata del settore finanziario dai software e dai processi digitali comporta che i rischi collegati alle TIC siano ormai intrinseci all'attività delle imprese del settore. Le imprese finanziarie sono diventate il bersaglio di attacchi informatici che possono causare gravi danni finanziari o alla reputazione per i consumatori e le imprese. Tali rischi devono essere ben compresi e gestiti, soprattutto in periodi di stress». Sullo stato di implementazione del regolamento DORA, cfr.: European Banking Autority, in https://tools.eba.europa.eu/interactive-tools/2024/powerbi/dora_visualisation.html.

[14] 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 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: F. Capriglione, *Industria finanziaria, innovazione tecnologica, mercato*, in *Riv. trim. dir. dell'economia*, 2019, 374 e s.;

regolare in maniera uniforme e integrata le misure per la prevenzione e gestione dei rischi relativi all'interconnessione tra settore finanziario e ICT[15].

In questo contesto, la necessità, per gli operatori del mercato finanziario, di ricorrere a soggetti esterni per lo sviluppo e la gestione dei servizi ICT (da cui ormai dipende o co-dipende il settore) è individuata come una autonoma categoria di rischio[16]. La disciplina europea si propone di 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].

M. Sepe, *Innovazione tecnologica, algoritmi e Intelligenza Artificiale nella prestazione dei servizi finanziari*, in *Riv. trim. dir. dell'economia*, 2021, 186 e s.; A. Canepa, *Big tech e mercati finanziari:* «sbarco pacifico» o «invasione»? Analisi di un «*approdo*» con offerta «à la carte», in *Riv. trim. dir. dell'economia*, 2021, 465 e s.; F. Urbani, *Rassegna dei principali interventi legislativi, istituzionali e di policy a livello europeo in ambito societario, bancario e dei mercati finanziari*, in *Riv. delle società*, 2022, 985 ss. 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*.

[15] 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).

[16] Regolamento UE, 2554/2022, artt. 28-45.

[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.

L'articolo si propone di analizzare la disciplina europea sulla resilienza operativa digitale per il settore finanziario, approfondendo i rischi nei rapporti con i fornitori terzi che prestano servizi ICT e la loro gestione mediante previsioni che incidono sulle relazioni contrattuali e sull'attività di sorveglianza.

L'analisi intende evidenziare le criticità connesse a tali rapporti giuridici valutando l'idoneità e l'efficacia delle misure previste in tema di resilienza operativa digitale a bilanciare i rapporti di forza tra operatori finanziari e fornitori di servizi ICT, in considerazione della dipendenza che i primi hanno dall'utilizzo di strumenti tecnologici e degli sviluppi che la transizione digitale può comportare nel Mercato Unico. Il testo cercherà altresì di proporre alcune possibili soluzioni evolutive della disciplina, volte a favorire l'integrazione europea dell'attività di sorveglianza.

2. *I rischi nell'affidamento a soggetti terzi di servizi ICT nel settore finanziario e la loro gestione*

La dipendenza del settore finanziario da quello tecnologico ha portato la disciplina europea a prevedere strumenti per riequilibrare esternamente tale rapporto.

Sulla scorta delle esperienze di altri settori (es. in relazione alla disciplina sulla responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica[20]), l'attività di analisi dei rischi (*risk based approach*)[21] è volta a ridurre l'asimmetria informativa tra le parti, cercando di prevenire la possibilità che questa influisca sull'equilibrio contrattuale (comportando un *lock in* tecnologico ed una «cattura» dei soggetti che svolgono la propria attività nel settore finanziario) e prevedere preliminarmente, mediante la gestione dei rischi, i meccanismi e le misure (organizzative e gestionali) da adottare per ridurre i l'incidenza di un rischio informatico sull'attività finanziaria.

In questo risulta peculiare rilevare come tali rischi risiedano o trovino il proprio fondamento al di fuori dell'ambito finanziario e richiedano professionalità specifiche.

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

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 in un quadro economico in cui il «Mercato Uni-

[20] D.lgs. 8 giugno 2001, n. 231.

[21] Regolamento UE, 2554/2022, artt. 5-16.

co» è solo uno degli attori coinvolti nel più ampio mercato globale e all'interno di una pluralità di ordinamenti giuridici. 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*[22]), 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)[23].

Le differenze tra norme nazionali (di cui il regolamento UE DORA costituisce un primo passo per l'armonizzazione) nella prevenzione e gestione dei rischi informatici rappresenta un ostacolo per il funzionamento del mercato europeo dei servizi finanziari che incide sull'attività transfrontaliera[24]. Se molti dei principi, requisiti e regole tecniche sono già contenuti all'interno di norme, orientamenti e atti di *soft law* di settore[25], risulta tuttavia necessario garantire la loro armonizzazione e la coerenza con concetti definiti in altri settori (quale ad es. quello bancario[26]) 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)[27], al fine di pervenire ad una completa

---

[22] A. Davola, *Bias cognitivi e contrattazione standardizzata: quali tutele per i consumatori?*, in *Contratto e impresa*, 2017, 637 e s.

[23] F. Capriglione, *Le cripto attività tra innovazione tecnologica ed esigenze regolamentari*, in *Riv. trim. dir. eco.*, 2022, 254.

[24] 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., 24 febbraio 2021, p.to 3.7; Comitato economico e sociale europeo, *Parere sulla* «Proposta di regolamento del Parlamento europeo e del Consiglio 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 e (UE) n. 909/2014», 24 febbraio 2021, p.to 4.1.2, in cui per garantire «chiarezza per le imprese, in particolare per quelle attive a livello transfrontaliero» richiede di assicurare «la coerenza delle definizioni e dei termini ed evitando duplicazioni, sovrapposizioni e interpretazioni divergenti su come soddisfare aspettative simili in termini di normative in giurisdizioni diverse». Per questi motivi il Comitato economico e sociale europeo invitava i responsabili politici europei a modificare la definizione di resilienza operativa al fine di garantirne la coerenza con la definizione del Comitato di Basilea per la vigilanza bancaria (CBVB) e di assicurare che tale resilienza operativa costituisca il sistema principale applicabile agli istituti finanziari dell'UE, onde evitare il rischio che entri in contraddizione con altri sistemi.

[25] 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).

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

[27] Proposta di Regolamento UE, *harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Analysis of the final compromise text with a view to agreement*, il testo

armonizzazione (tra settori economici e ordinamenti giuridici) ed evitare comportamenti opportunistici all'interno dell'Unione Europea.

Gli atti che la Commissione UE sarà chiamata ad approvare (nel 2024), possono costituire un importante elemento di armonizzazione di concetti, regole tecniche[28] e documenti[29] 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 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[30] che potrebbero generare ostacoli al funzionamento del mercato unico, a danno degli operatori del mercato e della stabilità finanziaria[31].

La necessità di rendere omogenea l'attività finanziaria mediante strumenti ICT (se non a livello internazionale quantomeno nel Mercato Unico) deve essere bilanciata con l'esigenza di garantire flessibilità ad una disciplina che concerne un settore in continua evoluzione ed in cui il diritto adeguarsi all'utilizzo di applicazioni tecniche nei rapporti economici in cui operano anche soggetti terzi.

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 rispar-

---

approvato dal Parlamento UE nel mese di marzo è accessibile in *https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808_IT.pdf*.

[28] 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).

[29] 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 TIC (entro il 17 gennaio 2024).

[30] G. Schneider, *La proposta di regolamento europeo sull'intelligenza artificiale alla prova dei mercati finanziari: limiti e prospettive (di vigilanza)*, in *Resp. civ. e prev.*, 2023, 1014 e s.; K. Trautmann, *EU-DORA regulation as a result of cloud computing adoption by the financial services industry*, in *Journal of International Banking Law and Regulation*, 2023, 155-161; Arner-Buckley-Zetsche, Open Banking, *Open Data e Open Finance: Lessons from the European Union*, in Jeng (a cura di), *Open Banking*, Oxford, 2022, 147 e s.

[31] Regolamento UE, 2554/2022, considerando n. 9.

mio e garantire la stabilità finanziaria (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 trasforma in dipendenza da soggetti terzi, la cui maggiore conoscenza delle dinamiche tecnologiche può comportare 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 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)[32], 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.

La disciplina europea 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). Sulla base del rapporto soggettivo sono quindi distinti i soggetti terzi fornitori di servizi ICT[33] dai terzi fornitori «critici»[34]. Questi 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[35].

La distinzione assume una ulteriore rilevanza ove il fornitore (o subappaltatore[36]) «critico» sia stabilito in uno Stato esterno all'Unione Europea[37].

---

[32] 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.

[33] Regolamento UE 2554/2022, art. 3, par. I, p.to 19.

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

[35] 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).

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

[37] 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 inte-

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[38] 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[39]. 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 alle misure in materia di sicurezza economica europea).

Le caratteristiche dei singoli mercati di riferimento dei servizi ICT rilevano nella definizione dei rischi[40].

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)[41] che hanno una posizione dominante in alcuni servizi ICT

---

resse 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.

[38] 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.

[39] Regolamento UE 2554/2022, art. 31, par. II.

[40] 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.

[41] R. Masera, *L'Europa, l'unione europea e l'eurozona: crisi e proposte di soluzione*, in *Riv. trim. dir. dell'economia*, 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 opportuni-*

(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, potrebbero 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[42]. Il ricorso al medesi-

tà per gli emittenti e il risparmio nazionale, 6 luglio 2021. Si v. anche: K. Trautmann, *EU-DORA regulation as a result of cloud computing adoption by the financial services industry*, in *Journal of International Banking Law and Regulation*, 2023, 38(5), 155-161.

[42] 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 and payements sector*, 21 settembre 2021; E. Palmerini, G. Aiello, V. Cappelli, G. Morgante, N. Amore, G. Di Vetta, G. Fiorinelli, M. Galli, *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*, 2018, 35 e s.; J.M. Campa, *Operational resilience in EU financial services*, cit., 4.

mo fornitore 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[43].

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»[44] 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[45]. 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[46].

---

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

[44] 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.

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

[46] 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.

L'analisi e la ponderazione preventiva, equilibrata e precauzionale consentono agli operatori del settore di organizzare e migliorare la propria conoscenza delle attività ICT, è contemperata ed integrata da previsioni contrattuali e di sorveglianza idonee.

3. *I contratti con i soggetti terzi fornitori di servizi ICT e l'attività di sorveglianza nella resilienza operativa digitale per il settore finanziario*

La disciplina europea sulla resilienza operativa digitale nel settore finanziario 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.

Il contratto (inteso quale atto volto a disciplinare l'interazione giuridica tra le parti[47]), di cui è richiesta la forma scritta, in ragione della maggiore capacità di adattamento (rispetto alla norma) è lo strumento a cui è demandata la gestione della condizione di dipendenza del settore finanziario[48]. Al suo interno si individuano le condizioni contrattuali e gli obblighi minimi[49], per garantire la proporzionalità e la ragionevolezza nel bilanciamento tra i differenti interessi in gioco[50].

La definizione delle clausole contrattuali, quale conseguenza dell'analisi dei rischi (e in particolare quello di concentrazione[51]), è limitata dai requisiti

---

[47] 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*, cit., p.to 40, in cui si richiamano le tipologie di atti con cui sono disciplinati i rapporti nella collaborazione tra settore finanziario e ICT: «partnerships, joint ventures, outsourcing and sub-contracting, mergers and acquisitions».

[48] Il contratto trova nella preliminare analisi dei rischi e definizione delle modalità di gestione il momento centrale di definizione di ruoli e attività. In un contesto caratterizzato da rischi esterni all'attività finanziaria e ad una attività di sorveglianza che mette in connessione in maniera diretta i fornitori terzi ICT e le autorità di sorveglianza, le responsabilità si incentrano sul soggetto giuridico che svolge attività finanziaria. La responsabilità dell'organo di gestione dell'operatore finanziario costituisce infatti il «principio guida» (quale valutazione circa l'adeguatezza delle previsioni contenuto nella strategia per i rischi informatici derivanti da terzi e delle clausole contrattuali che disciplinano i rapporti con i terzi fornitori di servizi ICT - Regolamento UE, 2554/2022, considerando n. 45 e art. 5, par. II -) della resilienza operativa digitale per il settore finanziario. 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.

[49] Regolamento UE 2554/2022, art. 30.

[50] M. Rabitti, *Due diligence sulla sostenibilità e digitalizzazione della catena del valore: l'apporto di blockchain e smart contracts*, in *Riv. trim. dir. dell'economia*, 2023, 172.

[51] Regolamento UE 2554/2022, art. 29.

del regolamento DORA[52]. Sulla base del principio di proporzionalità, elementi essenziali minimi del contratto e vincoli prestazionali connessi alla fornitura di servizi a supporto di funzioni essenziali o importanti sono definiti dalla disciplina UE, vincolando l'autonomia contrattuale delle parti[53].

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 la corretta gestione operativa dell'attività finanziaria[54]. Obblighi aggiuntivi sono quindi previsti in relazione ai fornitori che prestano funzioni valutate come essenziali o importanti. L'incidenza di tali attività sui risultati finanziari, e sulla solidità e continuità dei servizi finanziari dell'operatore giustifica un regime «aggravato» che impone previsioni contrattuali volte a rafforzare i vincoli posti in capo al terzo fornitore di servizi ICT, che culminano nell'obbligo di garantire un periodo di transizione nell'ambito della strategia di uscita dal rapporto contrattuale[55].

Un profilo di attenzione concerne il contratto di subappalto che, ove autorizzato e inerente a funzioni essenziali o importanti, richiede un'analisi specifica dei benefici e dei rischi che possono derivare da tale rapporto (in particolare nel caso di un subappaltatore di ICT stabilito in un paese terzo) e da catene di tali contratti[56].

L'attività di sorveglianza interviene a supporto dell'analisi e gestione rischi (in chiave di prevenzione e mitigazione degli eventi)[57] e dell'attività contrattuale con terzi fornitori di servizi ICT (quale strumento istituzionale di garanzia da asimmetrie informative e a tutela del risparmio),

---

[52] Regolamento UE 2554/2022, art. 28, par. IV.

[53] Regolamento UE 2554/2022, art. 30, par. III.

[54] 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).

[55] Regolamento UE 2554/2022, art. 30, si v. il rapporto tra il par. II e il par. III. Ad es. a obblighi di assistenza all'operatore finanziario, di operare con le autorità pubbliche e diritti di risoluzione, si aggiungono obblighi di segnalazione per il fornitore terzo, di attuare e testare piani operativi di emergenza, di partecipare e cooperare con l'operatore finanziario ai test TLPT, di diritti incondizionati di accesso e cooperazione nelle ispezioni e audit e definire contrattualmente strategie di uscita mediante la definizione di un periodo di transizione obbligatorio.

[56] Regolamento UE 2554/2022, art. 29, II, in cui sono individuati quali particolari elementi di attenzione le disposizioni del diritto fallimentare applicabili in caso di fallimento del fornitore terzo di servizi ICT come pure eventuali restrizioni relative all'urgente ripristino dei dati dell'entità finanziaria e, in caso il fornitore o subappaltatore sia stabilito in un paese terzo, del rispetto della disciplina UE sulla protezione dei dati.

[57] M. Rabitti, *Le regole di supervisione nel mercato digitale: considerazioni intorno alla comunicazione Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività*, D. Rossano (a cura di) *La supervisione finanziaria dopo due crisi. Quali prospettive*, cit., 343 e s.

Mentre la sorveglianza interna garantisce un livello di autonomia minimo (anche di carattere tecnico) dell'operatore finanziario, rispetto ai fornitori ICT[58], 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[59]. Tale attività assume un ruolo particolarmente incisivo in relazione ai fornitori terzi «critici»[60], con i quali le Autorità Europee di Vigilanza – AEV (e quella individuata come capofila), istituiscono un rapporto diretto[61]. Le autorità di sorveglianza capofila, individuate direttamente dalle AEV[62] 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)[63], si propongono di acquisire una conoscenza approfondita e completa delle relazioni nei singoli settori della fornitura di servizi ICT[64].

---

[58] Regolamento UE 2554/2022, art. 6, IV.

[59] J.M. Campa, *Operational resilience in EU financial services*, cit., 5.

[60] Regolamento UE 2554/2022, artt. 31-44. Joint European Supervisory Authority, *Discussion paper on the joint ESAs advice to the European Commission on two delegated acts specifying further criteria for critical ICT third-party service providers (CTPPs) and determining oversight fees levied on such providers, under Articles 31 and 43 of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operation resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*, 26 maggio 2023.

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

[62] 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).

[63] 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).

[64] 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.

La cooperazione[65] e il coordinamento[66] 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[67]. La necessità di garantire l'efficacia dell'attività di sorveglianza anche dei fornitori terzi critici con sede in un paese terzo[68] 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»[69].

---

[65] *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.

[66] 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.

[67] 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). G. Schneider, *La proposta di regolamento europeo sull'intelligenza artificiale alla prova dei mercati finanziari: limiti e prospettive (di vigilanza)*, in *Resp. civ. e prev*., 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.

[68] 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.

[69] 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. Sanzioni amministrative di natura economica, si sommano a sanzioni reputazionali (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 -) ed a sanzioni contrattuali imposte dalla disciplina europea (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 – Regolamento UE 2554/2022, art. 42, par. VI. Circa il dovere degli Stati membri di conferire i poteri alle autorità amministrative nazionali si v. l'art. 50 -).

4. *La resilienza operativa digitale per il settore finanziario nei rapporti di dipendenza con il settore ICT*

L'analisi della disciplina sulla resilienza operativa digitale per il settore finanziario rende di interesse valutare quanto le previsioni del regolamento DORA consentano di riequilibrare il rapporto di dipendenza con il settore ICT e quanto possano risultare efficaci nel perseguimento degli obiettivi cui sono preposte.

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. 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), la possibilità di ricorrere a clausole contrattuali standard definite da «autorità pubbliche per servizi specifici»[70] è sintomo di come la dipendenza del settore finanziario dalle imprese ICT possa risultare (in alcune circostanze dettate dalle caratteristiche del mercato) difficilmente gestibile anche contrattualmente da parte deli singoli operatori finanziari[71].

Elementi armonizzati (standard e strumenti tecnici[72], clausole contrattuali, previsioni normative) possono costituire utile strumento comune volto a superare comportamenti opportunistici, ma al contempo non pare possibile escludere che la forza contrattuale delle aziende ICT (specialmente per servizi i cui mercati sono caratterizzati da una ridotta concorrenza) possa riflettersi, più che sulla conclusione dei relativi contratti con gli operatori finanziari, sull'effettiva e corretta esecuzione di prestazioni contrattuali di cui detengono un *know how* specifico. Ecco come la descrizione del dettaglio dei livelli di servizio, termini di preavviso e obblighi di segnalazione possono risultare previsioni non idonee a prevenire

[70] Regolamento UE, 2554/2022, art. 30 par. IV.

[71] Regolamento UE 2554/2022, art. 41.

[72] European Banking Authority, *Operational resiliance*, accessibile in https://www.eba.europa.eu/regulation-and-policy/operational-resilience; European Supervisory Authorities, *First set of rules under DORA for ICT and third-party risk management and incident classification*, 17 gennaio 2024, accessibili in: *https://www.eba.europa.eu/publications-and-media/press-releases/esas-publish-first-set-rules-under-dora-ict-and-third-party*. Le bozze tecniche finali congiunte comprendono: – standard tecnici di regolamentazione sul quadro di gestione del rischio ICT e sul quadro di gestione del rischio ICT semplificato; criteri standard per la classificazione degli incidenti legati agli strumenti ICT; e stantard tecnici per specificare la politica sui servizi ICT che supportano funzioni critiche o importanti forniti da fornitori di servizi ICT di terze parti; e standard tecnici di attuazione per stabilire i modelli per il registro delle informazioni; European Supervisory Authorities, *Second batch of policy products under DORA*, 17 luglio 2024, accessibile in: https://www.eba.europa.eu/publications-and-media/press-releases/esas-published-second-batch-policy-products-under-dora, le misure intervengono sul sistema di segnalazione degli incidenti legati alle ICT (chiarezza delle segnalazioni, modelli) e sui test basati sulle minacce, introducendo anche alcuni requisiti sulla progettazione del quadro di supervisione, che rafforzano la resilienza operativa digitale del settore finanziario dell'UE, garantendo così anche la continuità operativa dei servizi finanziari ai clienti e la sicurezza dei dati.

in maniera effettiva eventuali rischi ove l'ineffettività delle previsioni contrattuali può realizzarsi nei casi in cui la disciplina europea impone direttamente al fornitore terzo critico obblighi di cooperazione. Esempi in tale senso sono l'obbligo del fornitore di «attuare e testare i piani operativi di emergenza»[73] o i doveri di cooperazione nell'ambito di *audit* o in occasione del periodo di transizione nella gestione della strategia di uscita[74].

La necessità di un'adeguata competenza tecnica da parte degli operatori finanziari, anche mediante un rafforzamento del ruolo della sorveglianza interna, si estende ricomprendendo la gestione dell'evoluzione tecnologica[75]. La costante innovazione delle tecnologie ICT comporta la capacità di pronto adeguamento degli operatori finanziari.

La previsione nel contratto di clausole e procedure che consentano agli operatori finanziari di apportare effettive modifiche alle prestazioni dei fornitori terzi, e garantiscano (al contempo) la corretta e ordinata gestione delle modifiche tecniche, rischia di risultare priva di effetti reali ove non accompagnata da adeguate competenze che devono essere ricercate nell'attività di sorveglianza (interna ed esterna). In questo senso devono essere letti gli obblighi di prestare assistenza («senza costi aggiuntivi o a un costo stabilito *ex ante*») in relazione ad incidenti ICT connessi al servizio prestato, di cooperare («senza riserve») con le Autorità competenti e con quelle di risoluzione dell'operatore finanziario.

Eventuali inadempimenti e violazioni dei vincoli contrattuali da parte di un fornitore terzo critico possono comportare una immediata cessazione dei rapporti contrattuali, ma il possibile impatto negativo che la cessazione del servizio avrebbe per gli operatori finanziari che utilizzano tale specifico fornitore terzo critico[76], richiede di valutare possibili misure correttive, considerando che la possibile mancanza di alternative nel settore ICT limita l'esercizio della risoluzione del contratto.

Nello stesso modo, dato che la definizione di un adeguato livello di sicurezza e la mancanza di alternative reali, costituiscono criteri per la qualificazione di for-

[73] Regolamento UE 2554/2022, art. 30, par. III, lett. c).

[74] Regolamento UE 2554/2022, art. 30, par. III, lett. e), p.to iii; lett. f).

[75] Ecco come la necessità di garantire un'adeguata conoscenza tecnologica al settore finanziario (riducendo asimmetrie informative), si rinviene innanzitutto nella possibilità di ricorrere a revisori (anche esterni) per garantire che la complessità tecnica di alcune prestazioni non vada a detrimento dell'attività finanziaria. Cfr. Regolamento UE 2554/2022, art. 28, par. VI, ove si prevede un dovere dell'entità finanziaria di «verificare» che i revisori siano titolari di competenze e conoscenze adeguate.

[76] Uno dei criteri per designare un fornitore di ICT come fornitore critico sarebbe il grado di sostituibilità, tenendo conto della mancanza di alternative reali o della difficoltà di migrare i servizi, in parte o totalmente (articolo 28, par. II). Se così fosse, sarebbe difficile per gli istituti finanziari trasferire il servizio a un altro fornitore. Inoltre, chiedere che gli istituti finanziari esposti passino a un diverso fornitore di servizi contribuirebbe in ultima analisi a una maggiore concentrazione sul mercato europeo, contraria allo spirito del regolamento in esame.

nitore «critico»[77], 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 previsione di sanzioni quantificate sul fatturato globale e sanzioni reputazionali può altresì comportare una riduzione dell'interesse (per i prestatori internazionali di servizi ICT) dei rapporti contrattuali con operatori finanziari europei. Questo potrebbe ridurre ulteriormente il novero di possibili fornitori di servizi ICT (aumentando i rischi di concentrazione).

Se quindi la definizione di vincoli contrattuali a livello normativo è sentore di preoccupazione circa la difficoltà per gli operatori finanziari di imporre autonomamente determinate prestazioni, parte del rapporto di dipendenza potrebbe essere colmato mediante le competenze tecniche dell'attività di sorveglianza.

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 nel settore finanziario (che trovano tuttavia origine al di fuori di esso) capaci di incidere negativamente sul rapporto di fiducia con gli investitori.

La complessità che consegue a possibili catene di subappalto (che contraddistinguono la fornitura di alcuni servizi ICT)[78] 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 sorveglianza è resa ulteriormente complessa dalla cooperazione 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[79] (è questo il caso dei contratti di subappalto, in cui l'Autorità di sorveglianza può raccomandare la rinuncia a stipulare il subcontratto[80]).

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 disciplina dei rapporti tra operatori finanziari e fornitori terzi di servizi ICT prevista dal regolamento DORA pare quindi contemplare i principali problemi connessi alla dipendenza del settore finanziario dalla tecnologia e sicuramente,

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

[78] 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.

[79] Regolamento UE 2554/2022, art. 35, par. I e V.

[80] Regolamento UE 2554/2022, art. 30.

inserendosi in un quadro giuridico più ampio, costituisce una presa di coscienza degli interessi coinvolti dal rapporto di dipendenza dell'attività finanziaria dal settore ICT e come solo l'effettività della resilienza operativa digitale per il settore finanziario possa contribuire al perseguimento degli obiettivi prefissati.

La definizione di norme, concetti, infrastrutture e strumenti comuni costituisce un passo importante nella definizione di una più ampia sovranità europea che punta ad assicurare un ruolo al settore finanziario europeo nella globalizzazione economica.

Permangono tuttavia perplessità sulla efficacia delle misure europee sulla resilienza operativa digitale per il settore finanziario, su cui influisce in vario modo il rapporto di dipendenza rispetto al settore ICT. Paiono infatti necessari investimenti infrastrutture ICT UE, volte a superare i limiti derivanti dall'eventuale numero limitato di fornitori terzi nonché dalla circostanza che molti di essi sono stabiliti in paesi terzi (non risultando sufficiente l'obbligo di istituire un'impresa figlia nell'UE entro 12 mesi dalla designazione quale «fornitore critico»[81], rispetto ai possibili rischi connessi all'utilizzo distorto delle informazioni e agli eventuali effetti conseguenti ad inadempimenti contrattuali).

Se infrastrutture ICT realizzate nell'UE possono ridurre la condizione di dipendenza del settore finanziario nella definizione delle condizioni contrattuali con eventuali fornitori terzi, una attenta revisione dell'attività di vigilanza parrebbe necessaria per superare i limiti derivanti dalla conoscenza tecnica (di autorità con specifiche competenze nell'attività bancaria, finanziaria ed assicurativa) e dalla limitata integrazione dei rapporti tra livelli di governo (nazionale ed europeo), indirizzata al perseguimento di una sovranità europea che pare necessaria nei rapporti economici con i mercati internazionali.

[81] Regolamento UE 2554/2022, art. 31, XII.

Matteo Pignatti - Abstract

I rapporti tra finanza e settore ICT nella resilienza operativa digitale per il settore finanziario

L'innovazione tecnologica è un fattore che influenza l'economia e assume caratteristiche particolari nel settore finanziario. Il rapporto di co-dipendenza con il settore delle TIC comporta rischi per la stabilità finanziaria del sistema europeo e per la stessa sovranità europea. La resilienza operativa digitale per il settore finanziario è un mezzo per proteggere gli interessi giuridico-economici sottostanti.
L'analisi e la gestione dei rischi, i regimi contrattuali vincolati e le attività di supervisione mirano a garantire il settore finanziario nelle sue relazioni contrattuali con il settore delle TIC, in particolare in relazione alle funzioni essenziali o importanti e ai fornitori terzi "critici", soprattutto se stabiliti in Paesi terzi.
Il testo si propone di condurre un'analisi del quadro di resilienza operativa digitale per il settore finanziario e di come esso cerchi di bilanciare le relazioni di dipendenza del settore finanziario dal settore ICT. L'analisi mira a verificare l'efficacia delle istituzioni introdotte nel perseguimento degli interessi economici europei, sviluppando alcune considerazioni sulle possibili evoluzioni.

The relationship between finance and ICT in digital operational resilience for the financial sector

Technological innovation is a factor affecting the economy and takes on special characteristics in the financial sector. The co-dependent relationship with the ICT sector entails risks for the financial stability of the European system and for European sovereignty itself. Digital operational resilience for the financial sector is a means of protecting the underlying legal-economic interests.
Risk analysis and risk management, constrained contractual regimes and oversight activities are intended to secure the financial sector in its contractual relationship with the ICT sector, in particular in relation to essential or important functions and 'critical' third-party providers, especially where established in third countries.
The text aims to conduct an analysis of the digital operational resilience framework for the financial sector and how it seeks to balance the dependency relationships of the financial sector on the ICT sector. The analysis aims to verify the effectiveness of the introduced institutions in the pursuit of European economic interests by developing some considerations on possible evolutions.