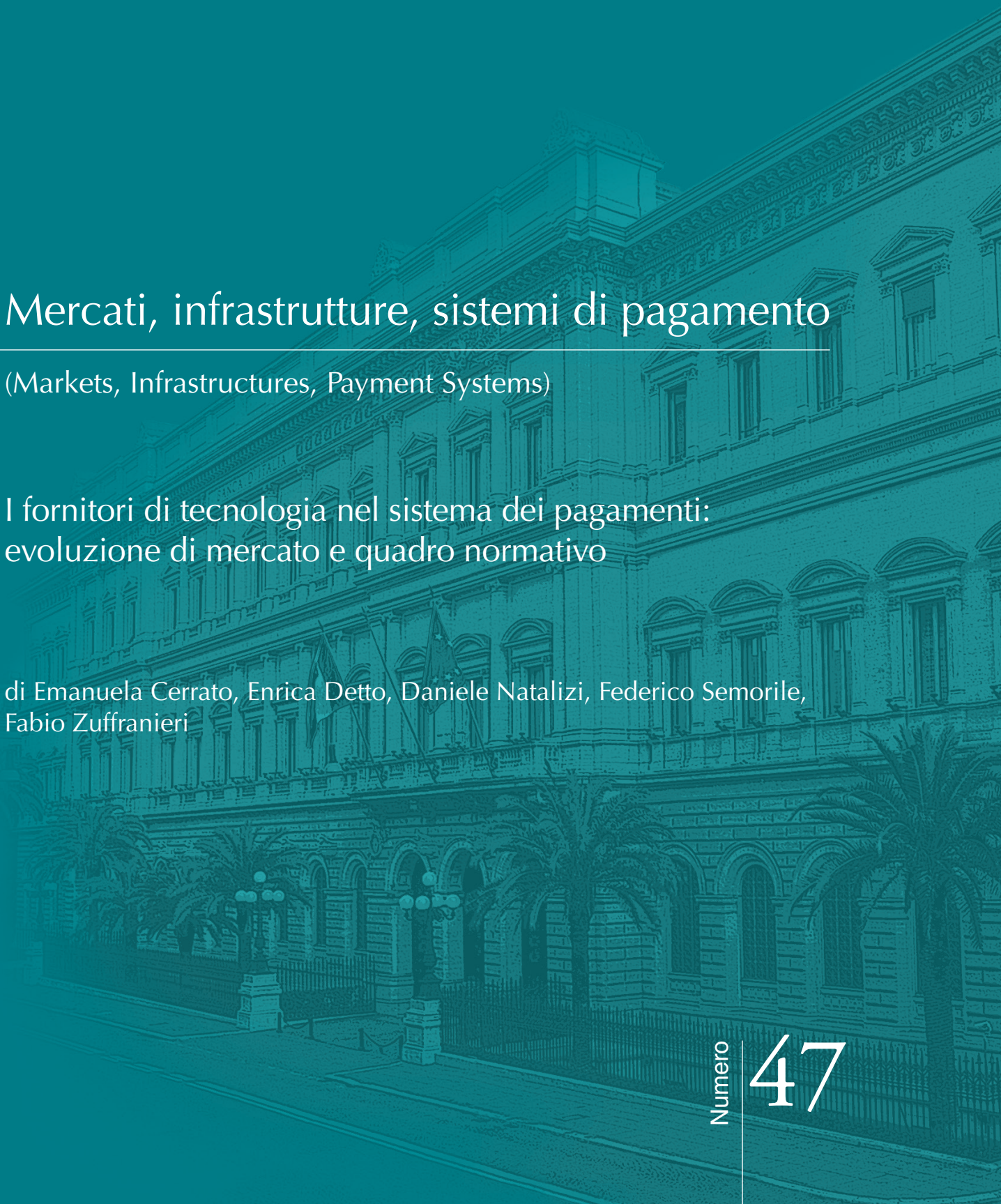
BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

I fornitori di tecnologia nel sistema dei pagamenti: evoluzione di mercato e quadro normativo

di Emanuela Cerrato, Enrica Detto, Daniele Natalizi, Federico Semorile, Fabio Zuffranieri



Marzo 2024

Numero 47

BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

I fornitori di tecnologia nel sistema dei pagamenti: evoluzione di mercato e quadro normativo

di Emanuela Cerrato, Enrica Detto, Daniele Natalizi, Federico Semorile, Fabio Zuffranieri

Numero 47 – Marzo 2024

I lavori pubblicati nella collana "Mercati, infrastrutture, sistemi di pagamento" presentano documentazioni e studi su aspetti rilevanti per i compiti istituzionali della Banca d'Italia in tema di monitoraggio dei mercati finanziari e del sistema dei pagamenti, nonché di sviluppo e gestione delle relative infrastrutture. L'intento è quello di contribuire alla diffusione della conoscenza su questi argomenti e di favorire il dibattito tra le istituzioni, gli operatori economici, i cittadini.

I lavori pubblicati riflettono le opinioni degli autori, senza impegnare la responsabilità dell'Istituto.

La serie è disponibile online sul sito www.bancaditalia.it.

Copie a stampa possono essere richieste alla casella della Biblioteca Paolo Baffi: richieste.pubblicazioni@bancaditalia.it.

ISSN 2724-6418 (online)
ISSN 2724-640X (stampa)

Banca d'Italia
Via Nazionale, 91 - 00184 Roma - Italia
+39 06 47921

Grafica e stampa a cura della Divisione Editoria e stampa della Banca d'Italia

I fornitori di tecnologia nel sistema dei pagamenti: evoluzione di mercato e quadro normativo

di Emanuela Cerrato, Enrica Detto, Daniele Natalizi, Federico Semorile, Fabio Zuffranieri*

Sintesi

I fornitori di tecnologia hanno acquisito un ruolo fondamentale a supporto del settore finanziario, consentendo alle aziende, anche di minori dimensioni, di conseguire guadagni di efficienza e di stare al passo con l'innovazione. Dalle interdipendenze tra questi soggetti e gli operatori finanziari, tuttavia, possono scaturire nuovi rischi sistemici, che richiedono l'attenzione delle autorità di regolamentazione e sorveglianza. Il lavoro illustra il punto di vista delle autorità, con un focus sul sistema dei pagamenti, e mostra come le numerose iniziative intraprese a livello internazionale e nazionale siano caratterizzate da coerenza e dinamicità per la creazione di un quadro regolamentare e di *policy* orientato all'equilibrio tra sicurezza e innovazione.

JEL: E42, G32, G38, O33.
Parole chiave: sistema dei pagamenti, infrastrutture di mercato, terze parti, resilienza operativa digitale, DORA, regolazione, sorveglianza.

* Banca d'Italia, Dipartimento Mercati e sistemi di pagamento.

INDICE

1. Introduzione[1]

Il funzionamento affidabile ed efficiente delle infrastrutture finanziarie di mercato costituisce da sempre una condizione essenziale per lo sviluppo delle economie avanzate, salvaguardando la fiducia nella moneta e favorendo lo scambio delle risorse tra i soggetti economici così come l'allocazione dei rischi tra di loro. In questo contesto, un ruolo fondamentale è svolto dal sistema dei pagamenti (di seguito indicato anche come "ecosistema"), che include tutte quelle componenti del sistema finanziario che consentono di eseguire pagamenti e transazioni in titoli in modo sicuro ed efficiente. I soggetti privati, quali i consumatori e le imprese, gli operatori pubblici e gli stessi intermediari devono disporre di mezzi efficaci e convenienti per inviare e ricevere pagamenti. A tal fine sono di fondamentale importanza gli accordi di scambio, compensazione e regolamento tra operatori finanziari[2]. Le attività svolte nel sistema dei pagamenti non sono tuttavia esenti da rischi, che possono essere in grado di causare anche gravi perturbazioni nel sistema finanziario, con ripercussioni sull'economia reale.

Il buon funzionamento dell'ecosistema dei pagamenti contribuisce quindi ad assicurare la fiducia del pubblico nel sistema economico e finanziario. Per conseguirlo, condizioni essenziali sono l'efficienza, la stabilità e la sicurezza della rete di relazioni tra operatori finanziari, ma anche tra questi e i fornitori di tecnologia. Proprio i servizi e le infrastrutture fornite da soggetti terzi non finanziari hanno acquisito negli ultimi anni una sempre maggiore rilevanza, dovuta al crescente ricorso a soluzioni tecnologiche avanzate, dalle quali dipende in modo significativo il buon fine di una transazione.

Il lavoro analizza dapprima le principali linee evolutive dello scenario che ha accentuato l'importanza di tali "terze parti" (paragrafo 2), per poi presentare le principali iniziative dei regolatori, nelle sedi di cooperazione internazionale (paragrafo 3) e a livello europeo e italiano (paragrafi 4 e 5). Tra queste ricopre un ruolo preminente il Regolamento UE sulla "*digital operational resilience for the financial sector*" (c.d. *Digital Operational Resilience Act* – DORA), per quanto il suo ambito di applicazione non ricomprenda tutti i soggetti attivi nell'ecosistema dei pagamenti (paragrafo 6).

1.1 La terminologia "terza parte"

Da un punto di vista economico appare agevole identificare i meccanismi alla base dell'esternalizzazione (*outsourcing*) di servizi, come del ricorso a fornitori "terzi" in senso più ampio. Da un punto di vista terminologico, tuttavia, la definizione di "terza parte" può divergere tra regolamentazioni, ragion per cui appare utile chiarire l'ambito soggettivo utilizzato nel presente articolo.

In questo lavoro l'utilizzo del termine terza parte si riferisce a un fornitore, non finanziario, di servizi e infrastrutture di supporto al business di operatori finanziari o all'ecosistema finanziario nel suo complesso, con un focus sul comparto dei pagamenti.

[1] Gli autori ringraziano Luca Arciero, Gino Giambelluca, Giuseppe Grande, Claudio Impenna e il revisore anonimo per gli utili suggerimenti.

[2] Si fa riferimento alle definizioni contenute nel Provvedimento della Banca d'Italia del 9 novembre 2021. Per "scambio" si intende l'attività attraverso la quale vengono scambiate fra i partecipanti al sistema le informazioni di pagamento, ossia i messaggi e gli ordini diretti a trasferire fondi o, comunque, ad estinguere obbligazioni tramite compensazione. La successiva fase di "compensazione" prevede la conversione, secondo le regole del sistema, in un'unica posizione - a credito o a debito - dei crediti e dei debiti di uno o più partecipanti nei confronti di uno o più partecipanti. Il "regolamento" estingue le posizioni a credito o a debito di due o più partecipanti.

Questa accezione è ad esempio presente nella normativa secondaria nazionale e nelle linee guida delle Autorità europee di vigilanza che, con il termine "terza parte", fanno in genere riferimento a quei fornitori che svolgono attività per conto dei soggetti finanziari serviti (es. gestori di infrastrutture di mercato, inclusi i sistemi di pagamento, banche, assicurazioni). In caso di esternalizzazione di funzioni essenziali o importanti[3], viene richiesto ai committenti (*outsourcee*) di porre in essere una serie di presidi aggiuntivi a livello contrattuale e organizzativo, che le autorità di vigilanza controllano secondo un approccio di "vigilanza indiretta" sulle terze parti per il tramite del soggetto finanziario vigilato. Un esempio può essere una banca che esternalizza l'archiviazione di dati.

Più di recente, il Regolamento europeo n. 2554/2022 sulla resilienza operativa digitale per il settore finanziario (DORA) definisce il fornitore di servizi di tecnologie dell'informazione e della comunicazione come quel soggetto che somministra, su base continuativa, all'entità finanziaria servizi digitali e di dati attraverso sistemi di *Information and Communication Technology* (ICT), inclusa l'assistenza tecnica ed esclusi i servizi telefonici analogici tradizionali.

Il lavoro non considera le "terze parti" introdotte dalla Direttiva europea n. 2366/2015 sui servizi di pagamento nel mercato interno (cd. *Payment Services Directive* 2 – PSD2), ovvero gli operatori specializzati nell'offerta di servizi nell'ambito del cd. *open banking*[4]*,* qualificabili come servizi finanziari a tutti gli effetti.

2. I fornitori "terzi" di tecnologia nel sistema dei pagamenti

2.1 Il ruolo crescente dei fornitori di tecnologia

La nascita di internet e soprattutto la successiva diffusione del Web 2.0, affiancato al rapido sviluppo di altre tecnologie digitali quali la telefonia mobile, hanno rivoluzionato la struttura del sistema produttivo e le abitudini degli individui (Marchetti, 2022). Sono stati automatizzati processi che in precedenza richiedevano un'elevata interazione umana; nuovi prodotti e servizi sono divenuti di uso corrente anche grazie a una progressiva capacità degli utenti di avvalersi di strumenti digitali. Lavorare attraverso un computer, comunicare con uno *smartphone*, ma anche disporre un bonifico online sono solo alcuni esempi di come la vita delle persone sia cambiata grazie alla tecnologia.

[3] Si vedano, ad es. le Linee guida dell'Autorità bancaria europea in tema di *outsourcing* e la Circolare n. 285 della Banca d'Italia.

[4] Per *open banking* si intende un modello di utilizzo di dati finanziari inerenti ai conti di pagamento dei clienti detenuti presso prestatori di servizi di pagamento, da parte di prestatori di servizi "terzi", tramite l'uso di apposite interfacce tecnologiche via web per realizzare nuovi servizi e applicazioni. Per una descrizione di questo comparto dell'industria, con riferimento all'esperienza italiana, si veda Pellitteri et al. (2023).
La PSD2 introduce due nuove tipologie di prestatori di servizi, spesso indicati come *Third-Party Provider* (TPP): gli *Account Information Service Provider*, che offrono ai clienti la possibilità di accedere attraverso un'unica interfaccia alle informazioni consolidate relative a uno o più conti di pagamento di cui siano intestatari e detenuti presso altri intermediari; i *Payment Initiation Service Provider*, che permettono di effettuare un'operazione di pagamento a valere sui conti detenuti presso altri intermediari. Inoltre, viene introdotta la possibilità per un *provider* di emettere carte di pagamento legate a conti accesi presso un altro istituto. I servizi citati non comportano la diretta detenzione di fondi, ma richiedono che il *provider* sia autorizzato a verificare le disponibilità su conti esterni, in maniera funzionale all'offerta dei propri servizi.
A differenza dei fornitori di tecnologia oggetto di questo lavoro, la cui operatività non è soggetta a specifici regimi normativi di "riserva di attività", i TPP di cui alla PSD2 possono operare all'interno dell'Unione solo con apposita licenza e offrono servizi direttamente all'utenza finale.

La digitalizzazione ha rimodellato in primis il settore bancario e finanziario, facilitando l'affermarsi di nuovi modelli di business, nuovi concorrenti e nuove forme di competizione, attraverso un progressivo passaggio dai canali fisici a quelli virtuali.

L'ecosistema dei pagamenti non è stato risparmiato da tali cambiamenti, anzi è stato spesso un ambito di sperimentazione precoce. In passato era molto più difficile entrare in competizione con gli operatori tradizionali, come le banche e i più consolidati circuiti di pagamento con carta di credito o di debito, dove le modalità di erogazione dei servizi e il conseguente rapporto privilegiato con la clientela costituivano le principali barriere all'entrata. L'innovazione ha consentito agli utilizzatori di scegliere tra diverse modalità di pagamento alternative al contante, armonizzate a livello europeo e orientate all'istantaneità delle interazioni digitali[5]. Oggi *BigTech*[6] e *start up* del settore fintech[7] possono sfruttare economie di rete e nicchie di mercato non adeguatamente servite per attrarre clienti grazie al valore aggiunto dei propri servizi, espandendo o disegnando agilmente la propria offerta. Buona parte delle *BigTech* ha già sviluppato servizi di pagamento come borsellini (*wallet*) digitali (ad es. Apple Pay, Google Pay e Samsung Pay) e fa leva su partnership con istituzioni finanziarie per introdurne di nuovi in ambito bancario e finanziario (EBA, 2021). Alcune di esse operano già nel settore, ad esempio attraverso la presenza all'interno del proprio gruppo di società registrate o autorizzate dalle rispettive autorità per la prestazione di servizi di pagamento (Crisanto et al., 2021; Feyen et al., 2021).

Anche i meccanismi che sono "dietro le quinte", le infrastrutture, sono stati oggetto di una profonda trasformazione: i sistemi di pagamento nazionali sono oggi profondamente interconnessi e si sono consolidate soluzioni paneuropee, con una trama di relazioni dirette e indirette a livello transfrontaliero. Ne sono conseguiti vantaggi in termini sia di flessibilità ed efficacia nell'esecuzione delle transazioni, sia di contenimento dei costi.

In questo mutato contesto tecnologico e industriale, la necessità e l'opportunità per gli operatori finanziari di ricorrere a soluzioni offerte da terze parti è cresciuta nel tempo. I servizi esternalizzati, in particolare, possono riguardare alcune funzioni tradizionali, come i sistemi informativo-contabili, ma soprattutto lo sviluppo di prodotti innovativi, le connessioni di rete, l'elaborazione di pagamenti commerciali, etc.

Le principali ragioni economiche che spingono gli operatori del sistema finanziario a esternalizzare servizi, soprattutto in ambito ICT, sono indicate in letteratura (cfr. ad esempio McFarlan & Nolan, 1995; Currie et al., 2008; González et al., 2016; Könning et al., 2019) e possono riguardare gli obiettivi di: i) contenere i costi; ii) focalizzarsi sul *core business* aziendale e su attività strategiche; iii) acquisire *know-how* e professionalità non presenti internamente; iv) ampliare la propria offerta commerciale con prodotti innovativi; v) attivare tempestivamente nuovi servizi in segmenti in rapido sviluppo; vi) arrivare a una struttura patrimoniale relativamente snella.

[5] Basti pensare all'introduzione, nell'area unica dei pagamenti in euro (*Single Euro Payments Area* – SEPA), di regole comuni per effettuare bonifici *instant*, con immediato riconoscimento dei fondi al beneficiario, oppure alla dematerializzazione delle carte di pagamento, che fa sì che la loro emissione non presupponga necessariamente un supporto fisico.

[6] Le società tecnologiche di grandi dimensioni Amazon, Apple, Google, Meta (già Facebook) e Microsoft.

[7] Il Financial Stability Board definisce fintech come: "*technologically enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services*".

Il ricorso a servizi forniti da terzi agevola soprattutto l'operatività dei soggetti di minori dimensioni che, con una minore disponibilità di risorse per investimenti tecnologici, sono in grado di contenere i costi e restare competitivi sul mercato. Ciò si traduce in potenziali esternalità positive sotto forma di una maggiore contendibilità del mercato.

Anche in Italia il cambiamento è stato particolarmente pronunciato, in un contesto in cui le banche assicuravano storicamente una capillare diffusione di sportelli, caratterizzandosi per uno stretto legame con il territorio e per canali di promozione e distribuzione tradizionali. Il percorso di digitalizzazione è stato intrapreso proprio a partire dai servizi di pagamento (Arnaudo et al., 2022)[8], che ha visto gli intermediari fare crescente ricorso a soggetti specializzati al fine di fare evolvere la propria offerta. Esempi di queste tendenze possono essere individuati nello sviluppo di soluzioni "di sistema" per i servizi introdotti dalla PSD2 (al riguardo, cfr. piattaforme multi-operatore di cui al paragrafo 5.2); discorso simile sul fronte dell'accettazione dei pagamenti, dove il ricorso a soggetti terzi, le c.d. *Paytech*, è imprescindibile per lo sviluppo di soluzioni per l'*e-commerce* o i POS evoluti (ECB, 2021b)[9].

2.2 I rischi connessi con il ricorso a fornitori di tecnologia e la regolazione

Accanto ai vantaggi appena descritti, gli investimenti in tecnologia e le partnership con fornitori terzi hanno tuttavia determinato nel tempo il manifestarsi di una forte dipendenza degli operatori del sistema finanziario da tali fornitori e la necessità di presidiare adeguatamente i rischi correlati.

Gli operatori dell'industria finanziaria dispongono sempre più raramente delle capacità tecniche ed economiche necessarie per sviluppare nuove soluzioni *in-house*, per adeguarsi all'innovazione del mercato o per re-internalizzare servizi. Tale condizione determina una forte dipendenza economica verso i fornitori, con effetti di *lock-in*. La crescente dipendenza da fornitori esterni ha attirato l'attenzione dei regolatori sulle conseguenze che i rischi cosiddetti "di terze parti" possono causare sia in prospettiva "micro" a livello di singolo operatore, sia "macro" per il sistema nel suo complesso.

L'intervento delle autorità è inoltre giustificato dal fatto che da un punto di vista operativo l'esternalizzazione può rappresentare un ponte in grado di trasferire rischi tra un settore regolamentato, quale quello del soggetto finanziario servito, e un settore non regolamentato, quello del fornitore (BCBS, 2005)[10]. Diventa necessario adottare un assetto di gestione delle attività e allocazione delle responsabilità tale da non creare una breccia nell'efficacia della supervisione. In questo senso, la regolamentazione è stata finalizzata da un lato ad assicurare un adeguato presidio dei rischi da parte dei soggetti che si affidano a fornitori terzi, anche per evitare possibili ripercussioni sugli utenti finali; dall'altro, a istituire nuovi assetti di sorveglianza sui provider tecnologici, non assoggettati alla regolamentazione settoriale finanziaria.

[8] Alcuni studi (es. Coletti et al., 2022) confermano tale trend, mostrando come l'utilizzo del contante sia in costante declino dal 2016, sebbene esso resti ancora il mezzo di pagamento più utilizzato; di converso, i pagamenti effettuati tramite strumenti elettronici sono in continua crescita: dal 2017 al 2021 il numero di bonifici effettuati in Italia è cresciuto come nel resto dell'Area Euro ad un tasso del 6%, mentre il numero di pagamenti con carta ha registrato una crescita del 17%, superiore alla media dell'Area (12%). È probabile che nel prossimo futuro tali strumenti saliranno in cima alle preferenze degli utilizzatori in tutta Europa.

[9] L'ampliamento dell'offerta sul mercato di metodi e strumenti di pagamento sempre più innovativi e digitali è correlato con il cambiamento nelle aspettative di livello di servizio e nelle abitudini di pagamento dei consumatori. Per ulteriori approfondimenti su questo tema si veda Coletti et al. (2022).

[10] A fronte di tali rischi, nonostante il contesto tecnologico di inizio millennio non presentasse il livello di complessità odierna, fu pubblicata una prima serie di principi guida, a testimonianza della crescente importanza che l'outsourcing stava assumendo nel mercato finanziario.

Il ricorso all'*outsourcing*, e più specificamente, la tipologia di servizi affidati e le condizioni economiche delle parti coinvolte, richiedono all'*outsourcee* di gestire una serie di rischi[11]. Tra i principali troviamo: 1) il rischio operativo, nel caso in cui un problema occorso a un fornitore possa ripercuotersi sull'attività dell'entità finanziaria; 2) il rischio *cyber*, laddove l'inadeguatezza delle *policy* di sicurezza di un fornitore possa facilitare attacchi all'entità finanziaria tali da compromettere la disponibilità dei servizi, la riservatezza e l'integrità dei dati; 3) il rischio reputazionale, nel caso in cui un fornitore metta in atto comportamenti che possano danneggiare la reputazione dell'entità finanziaria. Tra gli altri troviamo il rischio di conformità con il quadro normativo e il rischio strategico, legato ad esempio alle scelte di pianificazione, programmazione e controllo.

Da un punto di vista sistemico, il ricorso a terze parti può essere foriero di rischi alla stabilità complessiva del sistema. Per esempio il rischio di interconnessione, che si verifica quando una terza parte fornisce servizi a un gran numero di soggetti. Sono numerose le interdipendenze che si sono create nel tempo tra i diversi sistemi di pagamento e le infrastrutture tecniche di supporto. Specifici fornitori, posti su nodi critici della rete, potrebbero divenire *single points of failure* e causare effetti di *spill-over* nel settore finanziario. Inoltre va considerato che molto spesso la dipendenza dai fornitori critici è dovuta alla particolarità dei servizi offerti. Alcuni di essi, come il *cloud computing*, per loro natura richiedono un'ampia scala dimensionale e sono diffusi a livello intersettoriale. Queste condizioni amplificano di fatto la rischiosità sistemica, poiché gli effetti di un eventuale incidente potrebbero propagarsi su tutti i soggetti serviti, anche al di fuori del settore finanziario.

Le interconnessioni tra operatori finanziari e infrastrutture di supporto possono essere di tipo fisico e ambientale, ma con la crescente digitalizzazione hanno assunto connotazioni ulteriori nello spazio cibernetico. Pertanto, agli operatori sistemici per il mercato finanziario si richiede di diversificare il profilo di rischio delle proprie sedi sia da un punto di vista geografico, per far fronte a catastrofi naturali (ad esempio un'inondazione, un terremoto), sia dal punto di vista tecnologico, apprestando adeguati presidi di resilienza contro il rischio *cyber*, al fine di scongiurare un'interruzione totale o parziale dei servizi (Giannetto e Fazio, 2022).

Questi sono gli elementi sui quali si sono fondati gli interventi dei regolatori degli ultimi 20 anni, che hanno introdotto requisiti e cornici di sorveglianza, coordinando nella misura possibile le iniziative tra i vari livelli istituzionali.

La stessa regolamentazione ha costituito a sua volta un vero e proprio *driver* di cambiamento. La gran parte dei recenti sviluppi tecnologici è stata infatti non solo accompagnata ma anche stimolata da un significativo sviluppo normativo. Un esempio è quello della PSD2, che, oltre ad aver regolamentato importanti innovazioni nei servizi offerti alla clientela[12] e irrobustito la filiera dei pagamenti attraverso la previsione di nuove e più stringenti misure di sicurezza, ha spinto gli operatori a sviluppare soluzioni tecnologiche "di sistema" a supporto

[11] Sin dai primi casi di esternalizzazione di servizi IT, Earl (1996) aveva identificato ben 11 rischi generici derivanti dal processo: i) possibilità di indebolimento del management; ii) staff senza esperienza nel processo; iii) maggiore incertezza del business; iv) obsolescenza delle competenze tecnologiche interne; v) incertezza endemica; vi) costi nascosti; vii) assenza di economie di esperienza; viii) perdita di capacità innovativa; ix) difficoltà di allineamento tra le parti coinvolte; x) indivisibilità e rigidità dell'offerta tecnologica verso la clientela; xi) perdita di pianificazione strategica IT.

[12] Cfr. in particolare European Commission (2017), *Revised rules for payment services in the EU: Summary of Directive (EU) 2015/2366 on EU-wide payment services*.

dell'evoluzione del mercato (cfr. paragrafo 5.2). A testimonianza della costante attenzione del legislatore europeo per l'innovazione nel settore dei pagamenti, la Commissione europea ha svolto consultazioni generalizzate e mirate in vista della revisione della PSD2 e in tale ambito ha posto quesiti anche sul ruolo dei fornitori di tecnologia a supporto di questo mercato[13]. In aggiunta, i lavori in sede europea sui mercati delle cripto-attività e sul regime pilota per le infrastrutture di mercato che utilizzano *la Distributed Ledger Technology* (DLT) stanno contribuendo a delineare la necessaria base giuridica a sostegno di una profonda innovazione, ma anche del presidio del potenziale rischio tecnologico e di terza parte che le soluzioni sviluppate dall'industria potranno rappresentare.

3. Principi e standard internazionali sul rischio di terze parti

L'intervento pubblico nel sistema finanziario, incluso l'ecosistema dei pagamenti, si giustifica in ragione della presenza di carenze nel mercato - esternalità negative, asimmetrie informative e limiti nel grado di sviluppo dell'industria - che non consentono di raggiungere una situazione di equilibrio idonea a garantire un livello ottimale dei servizi.

Fin dai primi anni duemila, nel quadro dei controlli sulla gestione dei rischi degli operatori finanziari, i regolatori hanno sviluppato specifici requisiti in materia di esternalizzazione e ricorso a fornitori esterni. Le cornici regolamentari contengono principi, raccomandazioni e standard per un efficace presidio dei rischi da parte degli operatori finanziari e un efficace controllo da parte delle autorità.

3.1 La cooperazione a livello globale

Nell'ambito dei sistemi di pagamento, i primi accenni al tema delle esternalizzazioni si ritrovano nei *Core Principles for Systemically Important Payment Systems* (di seguito *Core Principles*) pubblicati nel 2001 dal *Committee on Payment and Settlement Systems* (CPSS)[14] della *Bank for International Settlements* (BIS). I *Core Principles* invitavano i gestori di sistemi di pagamento a dotarsi di linee e apparati di telecomunicazione ridondanti e a negoziare opportuni accordi sui livelli di servizio garantiti (*Service Level Agreement*) con i fornitori di servizi di telecomunicazione.

Un ulteriore passo avanti nella definizione del quadro di sorveglianza sulle terze parti è avvenuto nel 2012 quando il CPSS della BIS, insieme al *Technical Committee* della *International Organization of Securities Commissions* (IOSCO), ha aggiornato la cornice per la gestione dei rischi riguardanti le infrastrutture del sistema finanziario (inclusi i *Core Principles*[15]), pubblicando un corpo unitario di principi, i *Principles for Financial Market Infrastructures* (PFMI). Considerata la significativa crescita dell'importanza delle terze parti nel fornire

[13] Per un approfondimento si possono consultare le seguenti pagine web:
https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules_en
https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-psd2-review_en
Da ultimo, il 28 giugno 2023 la Commissione europea ha pubblicato le proposte di revisione della PSD2, oggetto di negoziato.

[14] Oggi *Committee on Payments and Market Infrastructures* (CPMI).

[15] Alle altre infrastrutture del sistema finanziario erano rivolti specifici set di raccomandazioni, elaborati dal CPSS e dal *Technical Committee* della *International Organization of Securities Commissions* (IOSCO), in particolare le *Recommendations for securities settlement systems* e le *Recommendations for central counterparties*.

tecnologia a supporto del sistema finanziario, i PFMI contengono numerosi riferimenti ai fornitori esterni, non solo con riguardo al rischio operativo, ma anche ad altri profili per i quali le terze parti possono avere un ruolo, sia "attivo" sia "passivo", introducendo o subendo rischi nei rapporti con una *Financial Market Infrastructure* (FMI)[16]. In aggiunta, i PFMI sono accompagnati da uno specifico allegato (*Annex F*) che contiene le *Oversight expectations applicable to critical service providers*, in larga misura derivate dalle *High Level Expectations for the oversight of* SWIFT (*Society for Worldwide Interbank Financial Telecommunication*) (cfr. paragrafo 3.2), direttamente rivolte ai fornitori critici. Le nuove *expectations* coprono l'identificazione e la gestione dei rischi, una solida gestione della sicurezza delle informazioni, l'affidabilità e la resilienza, una pianificazione tecnologica efficace e comunicazioni sicure con gli utenti.

I PFMI e i relativi allegati costituiscono una forma di regolamentazione per principi, che si sta dimostrando capace di rimanere attuale e utilizzabile nel tempo, come guida per le autorità e gli operatori. Integrati da successivi documenti di riferimento e interpretati in senso evolutivo, i PFMI sono la base di lavori che mirano a mitigare i rischi emergenti dall'applicazione di nuove tecnologie in campo finanziario, incluse quelle a supporto delle cripto-attività, senza impedire che esse esprimano il proprio potenziale a vantaggio dell'ecosistema, delle sue componenti e dei cittadini quali utilizzatori finali[17].

3.2 Il "caso" di SWIFT

Anche se non direttamente indirizzati alle terze parti, ma solo ai sistemi di pagamento da esse serviti[18], i *Core Principles* hanno costituito la base per la definizione di un quadro di requisiti applicabili a SWIFT, uno dei maggiori fornitori di servizi di messaggistica e di rete del sistema finanziario internazionale, che mette in collegamento tra loro operatori di tutto il mondo per i pagamenti transfrontalieri e lo scambio dei titoli[19].

Il rispetto dei requisiti da parte di SWIFT è monitorato dalle banche centrali, sulla base di quello che ha costituito uno dei primi modelli di sorveglianza cooperativa internazionale, resasi necessaria dalla sua attività "*borderless"*. SWIFT, infatti, dal 2004 è assoggettata alla sorveglianza cooperativa delle banche centrali del G10, con la *National Bank of Belgium* (NBB), banca centrale del paese in cui SWIFT ha stabilito la propria sede legale, nel ruolo di autorità capofila (*Lead Overseer*). La NBB ha siglato con SWIFT un protocollo che regola obiettivi, ambiti e modalità di svolgimento delle attività di sorveglianza, a cui è seguita la stipula di

[16] Secondo i PFMI, un'infrastruttura di mercato può essere definita come un sistema multilaterale tra istituzioni partecipanti, ivi incluso l'operatore del sistema, specializzato nelle attività di compensazione, regolamento o registrazione di pagamenti, transazioni in titoli, derivati o altre transazioni finanziarie. Sono ricomprese nella definizione i sistemi di pagamento, i sistemi di regolamento titoli, i depositari centrali di titoli, le controparti centrali e i repertori di dati sulle negoziazioni (cd. *trade repository*).

[17] Cfr. CPMI-IOSCO (2016), *Guidance on cyber resilience for financial market infrastructures*; CPMI-IOSCO (2022), *Application of the Principles for Financial Market Infrastructures to stablecoin arrangements*.

[18] La maggior parte dei *Core Principles* (6 di 10) si riferiva infatti a profili di rischio di natura finanziaria tipici dei sistemi di pagamento e dei loro partecipanti non riconducibili alle terze parti. Solo alcuni dei *Core Principles*, opportunamente reinterpretati, apparivano applicabili anche alle terze parti, quali l'aspettativa di possedere una solida base legale per la propria operatività, prevedere criteri non discriminatori di accesso ai propri servizi e adeguati assetti di governance. Solo uno dei dieci *Core Principles* sarebbe stato facilmente applicabile anche ai fornitori terzi di servizi tecnologici, quello riguardante il rischio operativo.

[19] SWIFT ha sedi in 28 paesi e conta un organico di oltre 2.800 dipendenti. L'infrastruttura SWIFT connette circa 11.000 operatori finanziari (banche, depositari, istituti di investimento, banche centrali, infrastrutture di mercato e clienti corporate), distribuiti in più di 200 paesi, che nel 2022 si sono scambiati in media 44,8 milioni di messaggi al giorno.

Memorandum of Understanding bilaterali con le banche centrali del G10, che definiscono i rispettivi ambiti di responsabilità e di partecipazione ai lavori[20].

Il caso SWIFT è particolarmente rilevante perché il quadro di controllo sviluppato dal gruppo di sorveglianza cooperativa ha condotto alla formulazione di cinque principi specifici per la gestione del rischio operativo: le *High Level Expectations for the oversight of SWIFT,* già citate nel paragrafo 3.1. Queste hanno costituito la base per la definizione dell'*Annex* F dei PFMI, che al momento costituisce l'insieme di requisiti a cui ogni fornitore critico dovrebbe fare riferimento. Al momento dell'iniziale redazione, per "*expectation*" si intendeva ciascun obiettivo che le autorità si attendevano che SWIFT raggiungesse in termini di resilienza e presidio del rischio operativo. La qualificazione "*high level*" mirava a lasciare un margine di flessibilità a SWIFT nella scelta delle modalità per conseguire gli obiettivi, nonché nell'adozione dei processi di gestione dei rischi e della reportistica con la quale rendicontare le autorità. Non si trattava neanche di seguire *best practices* di settore, perché considerata l'importanza globale di SWIFT, ci si aspettava che la società andasse oltre tali standard.

3.3 Gli "elementi fondamentali" del G7 sul rischio cyber connesso con le terze parti

Una sempre maggiore esposizione al rischio *cyber* è determinata dalla crescente interconnessione tra tecnologia e finanza. Non a caso, i Ministri delle Finanze e i Governatori delle banche centrali del G7 hanno dedicato crescente attenzione ai possibili rischi per il settore finanziario connessi con il ricorso ai servizi di terze parti. A ottobre 2022 è stata pubblicata l'ultima versione del documento "*The G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector*", frutto del continuo aggiornamento di principi adottati nel 2016.

Il documento contiene una serie di elementi chiave per la gestione del rischio informatico di terze parti, tenendo conto del crescente ricorso all'esternalizzazione dei servizi ICT e delle nuove forme di minaccia che interessano la filiera finanziaria. Si tratta di principi di alto livello ai quali le autorità finanziarie delle diverse giurisdizioni possono fare riferimento nelle attività di policy, regolazione e supervisione, relativi a sette ambiti: 1. *governance*; 2. *risk management*; 3. risposta agli incidenti; 4. piani di emergenza e strategie di uscita; 5. monitoraggio del rischio sistemico potenziale; 6. coordinamento intersettoriale; 7. specificità delle terze parti nel settore finanziario.

4. Il quadro europeo di sorveglianza

L'articolo 3 dello Statuto del Sistema europeo delle banche centrali e l'articolo 127 del Trattato sul funzionamento dell'Unione europea assegnano alle banche centrali europee l'obiettivo di promuovere il regolare funzionamento dei sistemi di pagamento. Nell'area dell'euro tale obiettivo è stato trasposto in standard, linee guida e atti normativi che dettano requisiti di sorveglianza sul sistema e sui soggetti che vi operano. I requisiti si inquadrano nello

[20] L'attività di sorveglianza si svolge attraverso le attività di quattro gruppi: 1) *Cooperative Oversight Group* composto dalle banche centrali del G10 che definisce le strategie e politiche di sorveglianza; 2) *Executive Group* composto da rappresentati di NBB, ECB, Federal Reserve Board, Bank of Japan, Bank of England che rappresenta l'*Oversight Group* nelle discussioni e comunicazioni con il Board di SWIFT; 3) *Technical Group* che discute gli aspetti tecnici per la loro discussione nell'*Oversight Group*; 4) *SWIFT Oversight Forum* per la discussione delle strategie globali di SWIFT e l'evoluzione tecnologica dei *provider* dei servizi tecnologico al settore finanziario in un contesto più ampio rispetto al G10. Sono oggetto di sorveglianza gli assetti di governance, le strutture, i processi, le procedure e il sistema dei controlli, con un particolare focus sugli aspetti di rischio operativo e continuità di servizio.

Eurosystem Oversight Policy Framework (ECB, 2016) e sono accompagnati da metodologie comuni tese ad assicurare armonizzazione attuativa e parità di trattamento tra i soggetti sorvegliati delle varie giurisdizioni.

Nel perimetro della sorveglianza – che si modifica nel tempo, in ampiezza e profondità, in relazione al mutamento del contesto di riferimento – rientrano anche i *Critical Service Provider* (CSP), fornitori di servizi e infrastrutture tecnologiche che svolgono un ruolo chiave per l'ecosistema dei pagamenti.

4.1 L'identificazione dei *Critical Service Provider*

L'Eurosistema svolge attività di sorveglianza sui CSP che supportano le FMI che ricadono nella sua sfera di competenza, in linea con la *policy* adottata dal Consiglio direttivo della Banca centrale europea nel 2017[21]. La *policy* si inquadra nel citato *Eurosystem Oversight Policy Framework* e si ispira alle prassi invalse in ambito internazionale sulla scorta, in particolare, dell'*Annex F* dei PFMI.

Sotto il profilo definitorio, la *policy* considera un CSP come "*a service provider that has a direct contractual arrangement with an FMI to provide, on a continuous basis, services to that FMI (and potentially its participants) which are essential for ensuring information confidentiality and integrity and service availability, as well as the smooth functioning of its core operations",* dove sono considerati come servizi essenziali *"data centres, financial messaging/network services, payment processing services, settlement functionality, or other business applications related to payment/clearing/settlement services*"[22].

Da un punto di vista pratico, per identificare i CSP l'Eurosistema conduce un'indagine periodica indirizzata alle FMI dell'area dell'euro. L'indagine riguarda l'ecosistema dei pagamenti in senso lato, un concetto che comprende i sistemi di pagamento di importanza sistemica, i sistemi di pagamento al dettaglio, gli schemi di carte e la piattaforma per il regolamento delle transazioni in titoli TARGET2-*Securities*[23].

I fornitori censiti grazie all'indagine sono valutati sulla base di criteri che consentono di determinarne la criticità per le FMI nell'ecosistema di riferimento, classificarli in base alla tipologia di servizi offerti e adottare il più appropriato approccio di sorveglianza (cfr. paragrafo 4.2).

La *policy* testimonia l'attenzione che le autorità rivolgono alle terze parti che forniscono servizi e infrastrutture strumentali agli attori dell'ecosistema finanziario, alla luce della significativa dipendenza degli operatori dai fornitori esterni di risorse digitali e dell'interdipendenza creata dal ricorso a fornitori comuni. La natura intersettoriale e transnazionale delle tecnologie digitali rende cruciale la cooperazione tra autorità.

4.2 L'approccio di sorveglianza

[21] *Eurosystem policy for the identification and oversight of critical service providers of financial market infrastructures*.

[22] Si veda ECB (2017) Eurosystem oversight report 2016 e ECB (2021a) Eurosystem oversight report 2020.

[23] La *policy* e l'indagine correlata hanno ampia copertura, includendo gli schemi di carte e la piattaforma T2S, che pure non rientrano nella nozione di FMI. Da ultimo, lo *Eurosystem oversight framework for electronic payment instruments, schemes and arrangements* (cd. PISA Framework) esprime l'aspettativa che i gestori degli schemi di carte e degli "*arrangements*" partecipino all'indagine, con un prevedibile ulteriore ampliamento della copertura del sistema dei pagamenti in tale esercizio. Il Framework definisce l'*arrangement* come *"a set of operational functionalities which support the end users of multiple payment service providers in the use of electronic payment instruments. The arrangement is managed by a governance body which, inter alia, issues the relevant rules or terms and conditions"*.

I CSP sono sottoposti a sorveglianza diretta o indiretta o a monitoraggio, in funzione delle loro caratteristiche e di quelle dell'ecosistema che supportano. Tra i CSP si annoverano soggetti stabiliti sia all'interno sia al di fuori dell'Unione europea, che sono attivi in segmenti specifici o forniscono una pluralità di servizi.

L'Eurosistema definisce un approccio di sorveglianza in tre fasi:

i. identificazione dei fornitori che prestano servizi tecnologici a supporto delle FMI rientranti nel proprio mandato di sorveglianza;
ii. individuazione del sottoinsieme dei fornitori considerati critici, sulla base di criteri di alto livello quali l'importanza del fornitore per il soggetto servito e per l'ecosistema in generale e l'assenza di fornitori alternativi;
iii. adozione dell'approccio più appropriato e delle modalità più efficaci per condurre la sorveglianza, tenendo conto di numerosi fattori tra i quali i poteri disponibili in base all'ordinamento nazionale di riferimento, che possono spaziare dalla *moral suasion* all'applicazione di norme cogenti[24].

Tipicamente, se il CSP offre servizi a una pluralità di infrastrutture di mercato, esso viene assoggettato a sorveglianza diretta, che potrà assumere un connotato nazionale o cooperativo, in base al livello di operatività transfrontaliera del CSP.

La sorveglianza sul CSP può essere esercitata anche indirettamente, attraverso requisiti imposti al soggetto sorvegliato servito. In linea con i principi e le prassi comuni in ambito finanziario, il soggetto servito rimane pienamente responsabile per le attività esternalizzate.

Sui CSP per i quali non emerge l'esigenza di una sorveglianza diretta, l'autorità può preferire un'azione di monitoraggio, soprattutto se le caratteristiche dell'operatore richiedono un'attenzione costante all'evoluzione della sua attività (es. se la sua crescita potenziale appare elevata, o se esso è particolarmente rilevante per specifiche FMI).

4.3 I requisiti e il processo di sorveglianza

Tra gli strumenti di sorveglianza, un ruolo di primo piano viene svolto dal citato *Annex F* dei PFMI (cfr. paragrafo 3.1) che si configura come una guida per il CSP e le autorità e definisce la metodologia di verifica del rispetto delle aspettative contenute nell'allegato sulla base, per ciascuno dei cinque profili di analisi, di una serie di domande chiave.

Di norma, su richiesta dell'autorità veicolata dal soggetto servito, il CSP esegue un esercizio di autovalutazione rispetto alle aspettative. L'*Annex F* nasce infatti come strumento di sorveglianza indiretta, ma costituisce un riferimento fondamentale anche per la sorveglianza diretta. In particolare, nel caso di sorveglianza indiretta l'autorità analizza: i) l'autovalutazione del CSP, fornita alla FMI, rispetto alle aspettative dell'*Annex F*; ii) il rapporto di esternalizzazione tra FMI e CSP in termini di robustezza contrattuale complessiva e di previsioni specifiche (livelli di servizio, indicatori di *performance*, possibilità di *audit* e ispezioni presso la sede del CSP).

[24] Ad esempio, il Testo Unico Bancario attribuisce espressamente alla Banca d'Italia poteri di sorveglianza sui gestori di infrastrutture strumentali tecnologiche o di rete (cfr. paragrafo 5.2).

5. Il quadro italiano di sorveglianza

5.1 Fondamento giuridico

Con l'art. 146 del Decreto legislativo n. 385/1993 (cd. Testo Unico Bancario – TUB) il legislatore italiano ha affidato alla Banca d'Italia l'obiettivo di assicurare il corretto operare del sistema dei pagamenti[25] in termini di affidabilità, efficienza e tutela degli utenti, attribuendole a tal fine poteri regolamentari, informativi, ispettivi e inibitori.

La stessa norma individua le categorie di soggetti nei confronti dei quali la Banca d'Italia può esercitare l'azione di sorveglianza; vi sono ricomprese le infrastrutture strumentali tecnologiche o di rete.

5.2 Normativa attuativa della Banca d'Italia

Nel 2021 la Banca d'Italia ha emanato il Provvedimento recante "Disposizioni in materia di sorveglianza sui sistemi di pagamento e sulle infrastrutture strumentali tecnologiche o di rete", che ha innovato la normativa secondaria di sorveglianza preesistente estendendone – in conformità con l'art. 146 del TUB – l'ambito di applicazione ai gestori di tutti i sistemi di pagamento, anche all'ingrosso, e ai gestori di infrastrutture strumentali tecnologiche o di rete.

L'ampliamento dell'ambito applicativo risponde sia alla progressiva attenuazione della distinzione tra pagamenti all'ingrosso e al dettaglio[26], in termini di velocità di esecuzione delle transazioni[27] e di importi trattati, sia al crescente ruolo nell'industria finanziaria delle infrastrutture strumentali tecnologiche o di rete, il che richiede di rafforzare il presidio dei rischi legati al ricorso a fornitori esterni da parte degli operatori di mercato.

Il ruolo dei fornitori di tecnologia è stato oggetto di particolare attenzione nella revisione della normativa di sorveglianza: come si è già visto, infatti, l'evoluzione tecnologica e la diversificazione dei modelli di business hanno reso più complessa la filiera dei pagamenti e aumentato il novero dei soggetti coinvolti, rendendo necessario disciplinare in maniera più dettagliata non solo le attività di scambio, compensazione e regolamento delle transazioni[28], ma anche attività tecniche strumentali, da cui dipendono sempre più l'affidabilità e l'efficienza dell'ecosistema nel suo complesso.

Il Provvedimento del 2021 dedica quindi una sezione ai fornitori di tecnologia, indicando i principali servizi tecnici funzionali al sistema dei pagamenti, dai più tradizionali servizi di

[25] Esistono significative connessioni tra il regolare funzionamento dei sistemi di pagamento e altri interessi pubblici: l'efficienza e l'affidabilità dei sistemi di pagamento contribuiscono alla corretta trasmissione della politica monetaria e alla stabilità finanziaria.

[26] Ad es., la distinzione tra ingrosso e dettaglio non rileva ai fini della valutazione dell'importanza sistemica di un sistema di pagamento, ai sensi del Regolamento della Banca centrale europea n. 715/2014 sui requisiti di sorveglianza per i sistemi di pagamento di importanza sistemica (e successive modifiche e integrazioni).

[27] I pagamenti istantanei introdotti da alcuni anni consentono di effettuare anche in ambito *retail* trasferimenti immediati di fondi tra conti, un tempo possibili solo a livello interbancario utilizzando sistemi all'ingrosso di regolamento lordo in tempo reale.

[28] L'articolo 1 del Provvedimento del 9 novembre 2021 definisce lo scambio come "*l'attività attraverso la quale vengono scambiate fra i partecipanti al sistema le informazioni di pagamento, ossia i messaggi e gli ordini diretti a trasferire fondi o, comunque, ad estinguere obbligazioni tramite compensazione*", specificando che "*il gestore può disciplinare direttamente l'attività di scambio ovvero fare riferimento a regole definite da soggetti terzi*"; la compensazione come "*la conversione, secondo le regole del sistema, in un'unica posizione – a credito o a debito - dei crediti e dei debiti di uno o più partecipanti nei confronti di uno o più partecipanti e risultanti dallo scambio delle informazioni di pagamento*"; il regolamento come "*l'estinzione delle posizioni a credito o a debito di due o più partecipanti*".

messaggistica e di rete alle piattaforme multi-operatore[29], che abilitano funzionalità di *open banking* (Tavola 1).

Tavola 1: "*Esempi di infrastrutture strumentali tecnologiche o di rete soggette a sorveglianza in Italia"* (1)

- servizi di messaggistica e di rete
- servizi e/o applicazioni di business strumentali a trattamento e scambio di flussi finanziari e informativi, compensazione e/o regolamento di operazioni di pagamento tra prestatori di servizi di pagamento e/o tra prestatori di servizi di pagamento e clienti
- servizi di conservazione e trattamento di dati sensibili relativi ai pagamenti, incluse le credenziali di sicurezza degli utenti e i dati per l'indirizzamento dei pagamenti
- servizi per il trattamento delle operazioni di pagamento (2)
- servizi tecnologici di interfaccia multi-operatore per l'accesso di terze parti ai conti (3)

(1) Cfr. art. 19 del Provvedimento della Banca d'Italia "Disposizioni in materia di sorveglianza sui sistemi di pagamento e sulle infrastrutture strumentali tecnologiche o di rete" del 9 novembre 2021.
(2) Servizi di cui all'art. 2, comma 1, numero 28 del Regolamento (UE) n. 2015/751 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.
(3) Ai sensi del Regolamento delegato (UE) n. 2018/389 della Commissione del 27 novembre 2017 che integra la Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri.

Il Provvedimento prevede per i fornitori l'obbligo di notificare l'inizio dell'operatività con un preavviso non inferiore a 3 mesi. La notifica è funzionale anche alla più ampia attività di monitoraggio del mercato e dei suoi soggetti da parte della Banca d'Italia.

In applicazione del principio di proporzionalità, la Banca d'Italia individua quei fornitori che sono critici per l'ordinato funzionamento del sistema dei pagamenti italiano, che vengono sottoposti a specifici obblighi informativi e requisiti per la gestione dei rischi[30]. La criticità del fornitore è valutata prioritariamente sulla base di alcuni criteri sanciti dal Provvedimento:

i. erogazione di infrastruttura o servizi tecnici essenziali per la confidenzialità, l'integrità e la disponibilità dei dati processati per una quota significativa del mercato italiano;
ii. importanza dei sistemi di pagamento serviti per il mercato italiano; e/o
iii. assenza di fornitori alternativi per l'utenza servita.

La valutazione è svolta nell'ambito di un procedimento amministrativo, che si svolge secondo le modalità descritte nella Guida operativa dei controlli allegata al Provvedimento. La Guida, insieme all'allegato "Misure di continuità operativa", si pone a complemento della normativa secondaria nazionale. In un'ottica di massima trasparenza dell'azione della Banca d'Italia, gli allegati al Provvedimento orientano gli operatori, e tra essi i fornitori, nell'assolvimento dei propri obblighi di sorveglianza: la Guida fornisce un supporto

[29] Si tratta di infrastrutture tecniche per la fornitura di servizi di pagamento mediante l'utilizzo di *Application programming interface (API)*, standard e protocolli informatici che consentono la comunicazione e l'integrazione tra diversi applicativi per lo scambio di flussi informativi tra molteplici anelli in una rinnovata catena del pagamento. Le API consentono ai TPP di connettersi a una pluralità di intermediari attraverso un unico punto di accesso. Per ogni ulteriore approfondimento si rimanda a Pellitteri et al. (2023).

[30] In particolare, l'art. 4 del Provvedimento sull'assetto organizzativo, l'art. 5 sull'efficacia dei controlli, l'art. 6 in tema di esternalizzazione, l'art. 9 sul rischio d'impresa, l'art. 10 sul rischio legale e l'art.11 sui rischi operativi.

metodologico; il secondo allegato, un quadro di riferimento per le misure di continuità operativa da adottare. Il Provvedimento, quale normativa secondaria attuativa dell'art. 146 del TUB, conferisce ulteriore certezza giuridica all'esercizio della sorveglianza nei confronti dei fornitori di tecnologia e rafforza i presidi sul rischio di terze parti nel settore.

Questo approccio garantisce l'allineamento alle prassi sovranazionali, a presidio dei rischi posti da attori critici nel mercato nazionale, evitando sovrapposizioni di competenze o duplicazioni di controlli.

6. Il *Digital Operational Resilience Act*

Il pacchetto per la finanza digitale, pubblicato dalla Commissione europea a settembre 2020, comprende la proposta di una normativa primaria in materia di resilienza operativa digitale del settore finanziario nella forma di un Regolamento dell'Unione (cd. *Digital Operational Resilience Act* – DORA)[31]. Il Regolamento è stato pubblicato il 27 dicembre 2022 (nell'*Official Journal* dell'UE), è entrato in vigore dopo 20 giorni e si applicherà dopo due anni. Tra gli altri aspetti, copre il rischio di terze parti in una duplice prospettiva: indirettamente, attraverso requisiti applicabili alle entità finanziarie nelle loro relazioni con i fornitori di tecnologia, e direttamente, istituendo una nuova cornice di sorveglianza europea sui fornitori considerati critici.

Una premessa sull'ambito oggettivo e soggettivo di DORA è d'aiuto alla schematizzazione della disciplina del rischio di terze parti che essa prevede.

Guardando all'oggetto di DORA, la "resilienza operativa digitale"[32], meritano attenzione l'uso del termine "resilienza" rispetto al più tradizionale riferimento alla "sicurezza", e le qualificazioni come "operativa" e "digitale". La differenza tra sicurezza e resilienza è relativamente sfumata, con una parziale sovrapposizione. La prima può essere genericamente intesa come presidio dei rischi; la seconda ricomprende la sicurezza e la integra in una più ampia accezione di identificazione, prevenzione, gestione, risposta e ripristino dell'operatività a fronte dei rischi ed eventi avversi. Si associa spesso il concetto di resilienza al rischio cibernetico, qualificandola come "operativa" per la sua strumentalità all'ordinata operatività del soggetto e del settore del mercato interessato, "digitale" per l'utilizzo pervasivo di risorse informatiche. L'obiettivo della resilienza operativa digitale segna quindi un'evoluzione rispetto a quello della continuità operativa, con un focus non solo sull'ininterrotta disponibilità di servizio, ma anche

[31] Da un punto di vista formale, lo strumento normativo scelto per conseguire una disciplina il più possibile armonizzata in materia di resilienza operativa digitale del settore finanziario è stato quello del Regolamento. DORA sarà dunque direttamente applicabile negli Stati Membri dell'Unione, con rilevanza ai fini dello Spazio economico europeo. Specifiche previsioni del Regolamento saranno dettagliate da normativa di secondo livello attraverso *Guidelines, Regulatory Technical Standards* e *Implementing Technical Standards*.
Le negoziazioni sul testo hanno preso avvio nel 2020, durante il semestre di presidenza tedesca del Consiglio dell'Unione. Dopo il raggiungimento di un accordo in Consiglio, dal primo semestre 2022 il negoziato si è svolto in trilogo (Commissione, Parlamento e Consiglio UE). Il testo definitivo è stato pubblicato sotto la presidenza ceca (Regolamento UE 2022/2554). Dalla pubblicazione della proposta, a settembre 2020, le delegazioni nazionali hanno discusso le molteplici tematiche affrontate in DORA, che sono state parallelamente oggetto di dibattito tra operatori e tra questi e le istituzioni. La Banca ha contribuito ai lavori in vari contesti: ha coadiuvato la partecipazione della delegazione italiana al negoziato presso il Consiglio, ha promosso il confronto con il mercato, ha partecipato alla decisione che ha condotto al parere della BCE sulla proposta di Regolamento.

[32] L'art. 3 del Regolamento definisce la resilienza operativa digitale come: "*the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions*".

sull'integrità e la confidenzialità dei dati su cui il servizio si fonda. La resilienza diventa un obiettivo strategico di ogni entità finanziaria, e come tale va integrato in un quadro di *governance* e di controllo interno che assicuri una gestione efficace di tutti i rischi tecnologici. E un contributo sempre più rilevante alla resilienza operativa digitale viene appunto dalla gestione del rischio di terze parti.

Sotto il profilo soggettivo DORA si rivolge, come accennato, al "settore finanziario". La nuova disciplina è diretta a venti tipologie di entità finanziarie, con la finalità di superare la frammentazione sinora esistente tra le diverse normative esistenti sulla materia, eterogenee tra sotto-settori finanziari e, talvolta, caratterizzate da specificità nazionali. L'armonizzazione è molto rilevante per i soggetti attivi in più paesi e sotto-settori. Per i fornitori di servizi critici ICT DORA disegna una cornice di sorveglianza europea, andando quindi al di là del settore finanziario.

I gestori di sistemi di pagamento e gli organismi di governance di schemi di pagamento (ad esempio i circuiti di carte) non sono assoggettati a DORA. Tale scelta, come evidenziato dalla Commissione europea nelle fasi iniziali dei lavori[33] e da ultimo nella relazione al Parlamento e al Consiglio sulla revisione della PSD2[34], tiene conto delle specificità del relativo quadro regolamentare e di sorveglianza, incluse le competenze attribuite alle banche centrali in materia di sistemi di pagamento (ai sensi del Trattato), dalle quali già discende un robusto sistema di requisiti e controlli sulla resilienza operativa digitale. L'opportunità di estendere l'ambito di applicazione di DORA sarà riesaminata in sede di revisione del Regolamento.

Tra gli aspetti più discussi nel corso del negoziato figurano le implicazioni del Regolamento sulla normativa e sull'assetto di competenze vigenti per le autorità nazionali ed europee, in particolare con riguardo alla sorveglianza sui fornitori critici di servizi ICT, e il rapporto con ulteriori proposte di atti normativi europei sulla sicurezza informatica e fisica di settori vitali della vita sociale ed economica.

6.1 Rapporto con altre normative

Per quanto riguarda i requisiti di gestione del rischio di terze parti per le entità finanziarie, DORA prevede tra l'altro la possibilità di usare clausole standard nei contratti di esternalizzazione. La gestione del rischio di terze parti nel contesto delle esternalizzazioni è materia già fortemente regolamentata nel settore finanziario. Basti pensare alle linee guida delle autorità europee di vigilanza in materia di *outsourcing*, incluse quelle specifiche per i servizi in *cloud*[35]. DORA segna in Europa l'innalzamento dei requisiti in materia dalla normativa secondaria a quella primaria.

Inoltre, il tema della resilienza operativa digitale si interseca con quello della sicurezza delle reti e dei sistemi informativi, trattato in una dimensione intersettoriale dalla Direttiva (UE) n. 2016/1148 (cd. *Network Information System Security* – NIS), ora sostituita dalla Direttiva n.

[33] Cfr. *Explanatory Memorandum* che accompagna la proposta della Commissione europea del 24 settembre 2020.

[34] Cfr. clausola di riesame di cui all'art. 58 di DORA, in base alla quale la Commissione avrebbe riportato al Parlamento e al Consiglio sull'opportunità di includere operatori sistemi di pagamento ed entità coinvolte nelle attività di trattamento dei pagamenti nell'ambito di applicazione di DORA; Rapporto dalla Commissione al Parlamento europeo, al Consiglio, alla Banca centrale europea e al Comitato economico e sociale europeo sulla revisione della Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio relativa ai servizi di pagamento nel mercato interno del 28 giugno 2023.

[35] Cfr. EBA (2019), *Final Report on EBA Guidelines on outsourcing arrangements*, EBA/GL/2019/02; ESMA (2020), *Final Report - Guidelines on outsourcing to cloud service providers*, ESMA50-157-2403; EIOPA (2020), *Guidelines on outsourcing to cloud service providers*, EIOPA-BoS-20-002.

2022/2555 (NIS2), rispetto alla quale DORA si pone come *lex specialis* per il settore finanziario. La 'specialità' comporta – nei casi di sovrapposizione di regole sulle medesime fattispecie – la disapplicazione delle norme NIS in favore di quelle stabilite da DORA per il settore finanziario; non fa però venir meno l'esigenza del raccordo tra i due ecosistemi di autorità, in particolare in termini di adeguatezza e tempestività dei flussi di informazioni.

La NIS si applica a tre tipologie di entità finanziarie (banche, gestori di sedi di negoziazione, controparti centrali), prevedendo obblighi in materia di misure di sicurezza e di notifica di incidenti rilevanti a carico degli operatori identificati come essenziali per il mantenimento di attività sociali ed economiche fondamentali. Si tratta di un atto di armonizzazione minima che lascia impregiudicate le misure adottate dagli Stati Membri a tutela della sicurezza nazionale. In Italia la Direttiva ha avuto attuazione attraverso il decreto legislativo 18 maggio 2018, n. 65, modificato dal decreto-legge 14 giugno 2021, n. 82, convertito con legge 4 agosto 2021, n. 109, che ha definito l'architettura nazionale di cybersicurezza e istituito l'Agenzia per la cybersicurezza nazionale (ACN)[36].

Infine, le tematiche della resilienza operativa digitale e della sicurezza delle reti e dei sistemi informativi toccano la sicurezza nazionale, ambito di competenza dei legislatori dei singoli Stati membri. Il legislatore italiano, in linea con la tendenza prevalente in diversi paesi, è sensibile alla tematica della sicurezza cibernetica, oggetto di vari interventi normativi.

Il decreto-legge 21 settembre 2019, n. 105, convertito con legge 18 novembre 2019, n. 133, ha gettato le basi per tracciare il perimetro di sicurezza nazionale cibernetica in cui ricadono soggetti pubblici e privati "aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale". A tali soggetti si è richiesto tra l'altro di adottare specifiche misure di sicurezza, nonché di notificare gli incidenti rilevanti. La legge ha previsto il caso di soggetti ricadenti nel perimetro che siano nel contempo assoggettati alla normativa NIS, evitando duplicazioni e apprestando meccanismi di raccordo tra le normative. L'ACN è investita di competenze per l'applicazione delle norme sul perimetro di sicurezza nazionale cibernetica.

6.2 La cornice di sorveglianza sui fornitori critici di servizi ICT

DORA assegna i nuovi compiti e poteri di sorveglianza ad autorità europee e nazionali, secondo un assetto di governance a più livelli e voci. La definizione di una cornice di sorveglianza sulle terze parti non è di per sé una novità. L'elemento innovativo consiste nella sua dimensione europea, con una normativa primaria armonizzata per il sistema finanziario in senso ampio. È la stessa DORA che riconosce la preesistenza di cornici di sorveglianza, laddove esclude dal proprio ambito di applicazione i fornitori di servizi ICT soggetti a quadri di sorveglianza istituiti a supporto dei compiti di cui all'articolo 127 del Trattato, relativi al buon funzionamento dei sistemi di pagamento. In aggiunta, DORA fa salvi i regimi di sorveglianza nazionali su fornitori che abbiano rilevanza nelle singole giurisdizioni. In Italia, l'assetto di

[36] L'ACN è divenuta l'autorità italiana competente in materia NIS, coadiuvata dai ministeri per gli specifici settori. Ulteriori modifiche potranno discendere dall'abrogazione della Direttiva NIS e dalla trasposizione della Direttiva NIS2 nell'ordinamento nazionale, laddove comunque il carattere di armonizzazione minima e la copertura di entità finanziarie risulta essere confermata nella nuova Direttiva.

sorveglianza di cui al Provvedimento del 9 novembre 2021 della Banca d'Italia presentato nel paragrafo 5.2 coesisterà con quello del Regolamento europeo, in quanto ha ad oggetto fornitori ritenuti critici per la piazza finanziaria nazionale, inquadrandosi nelle competenze attribuite alla banca centrale dal Trattato e dal TUB. Infine, DORA si raccorda con la NIS2 per quanto riguarda i fornitori di servizi digitali assoggettati a entrambe le normative.

Nell'assetto di competenze previsto dalla nuova cornice di sorveglianza le Autorità europee di vigilanza (ESA) giocano un ruolo fondamentale: è ad esse che DORA attribuisce compiti e poteri di sorveglianza sui fornitori critici. È la prima normativa della sua specie ad affidare compiti di sorveglianza a tali Autorità, a suo tempo create con l'obiettivo di rafforzare la stabilità e l'efficienza del sistema finanziario in tutta l'Unione, in particolare attraverso l'emanazione di orientamenti.

Sul piano dell'architettura istituzionale, una tra le tre ESA[37] viene designata l'autorità di sorveglianza capofila (*Lead Overseer*), in base al sotto-settore (bancario, finanziario o assicurativo) prevalentemente servito dal fornitore sottoposto a sorveglianza[38]. L'attività verrà svolta secondo un'organizzazione articolata su vari livelli e facente capo alle ESA: i) il *Joint Committee*, che identifica le terze parti critiche, individua in una delle ESA il *Lead Overseer* competente per ciascuna terza parte e ha compiti di indirizzo e di coordinamento; ii) l'*Oversight Forum*[39], che coadiuva il *Committee* quale braccio operativo incaricato di preparare report e posizioni comuni e di svolgere valutazioni collettive sulle attività di *oversight*; iii) il *Joint Oversight Network*, sede di ulteriore coordinamento operativo tra i *Lead Overseer*. Ai *Lead Overseer* vengono affidati diversi poteri, come: i) richiedere tutte le informazioni e la documentazione necessarie per effettuare il monitoraggio nel continuo dell'operatività del fornitore critico; ii) condurre "*general investigation*" e verifiche on-site[40]; iii) emanare raccomandazioni; iv) imporre sanzioni pecuniarie.

La *governance* prevede un riparto di ruoli tra le ESA responsabili della sorveglianza sulle terze parti e le autorità nazionali competenti per la supervisione dei soggetti finanziari serviti. Alle autorità nazionali è affidato il cd. *follow-up*, ossia il compito di informare i soggetti finanziari supervisionati sui rischi posti dalla terza parte critica e le raccomandazioni a essa indirizzate da parte del *Lead Overseer*, richiedendo, se opportuno, l'adozione di misure specifiche. Valutate le misure intraprese dalle entità finanziarie e l'eventuale perdurare dello stato di *non-compliance* del fornitore critico con le raccomandazioni ricevute, le autorità nazionali possono adottare nei confronti delle entità finanziarie misure cd. *of last resort*, quali la richiesta di sospensione temporanea della fruizione del servizio e, in ultima istanza, di risoluzione del contratto.

Nell'individuazione dei fornitori critici il *Joint Committee* segue quattro criteri non alternativi che riguardano: a) impatto sistemico sulla stabilità, continuità e qualità dei servizi finanziari in caso di interruzione operativa da parte del fornitore; b) rilevanza sistemica dei

[37] L'Autorità bancaria europea (*European Banking Authority* - EBA), l'Autorità europea degli strumenti finanziari e dei mercati (*European Securities and Markets Authority* - ESMA) e l'Autorità europea delle assicurazioni e delle pensioni aziendali o professionali (*European Insurance and Occupational Pensions Authority* - EIOPA).

[38] Nello specifico, viene designata *Lead Overseer* per ogni fornitore di servizi ICT critici la ESA responsabile per le entità finanziarie che hanno insieme la quota maggiore di attività totali sul valore delle attività totali di tutti i soggetti finanziari che utilizzano i servizi di quel fornitore di servizi ICT critici. Questa attribuzione viene basata sui singoli bilanci dei soggetti finanziari.

[39] Al quale è prevista anche la partecipazione di esponenti della BCE e di altre autorità rilevanti.

[40] Per condurre tali attività, i *Lead Overseer* si avvalgono di *Joint examination team*, ossia di gruppi costituiti appositamente per ciascun fornitore critico, con la partecipazione di staff di autorità nazionali.

soggetti serviti; c) affidamento che le entità finanziarie ripongono sulla terza parte per lo svolgimento di funzioni critiche o importanti; d) grado di sostituibilità del fornitore, tenendo in considerazione sia i reali *competitor*, sia la fattibilità della migrazione dei dati e delle attività verso uno di essi. A seguito della *call for advice* rivolta dalla Commissione alle ESAs, sono stati intrapresi lavori tecnici per la declinazione di questi criteri in regole operative di pronto utilizzo per l'individuazione delle terze parti critiche.

In base a tali criteri, potrebbero ricadere nella categoria anche le cd. *BigTech* che offrono servizi di *cloud computing* agli operatori finanziari, considerata la relativa concentrazione e rilevanza per il mercato. Le BigTech rientrerebbero per la prima volta in Europa all'interno di un *framework* di sorveglianza di carattere finanziario[41]. Anche i fornitori di servizi più tradizionali, quali quelli di messaggistica o di rete, potrebbero rientrare in tale cornice.

Sono previste infine specifiche eccezioni per alcune tipologie di fornitori, come ad esempio: i) entità finanziarie che forniscono servizi ICT ad altre entità finanziarie; ii) fornitori infragruppo, che forniscono quindi i propri servizi prevalentemente all'interno del gruppo di appartenenza; iii) terze parti che forniscono i propri servizi in un solo Stato membro e la cui clientela non ha operatività transfrontaliera. Come già accennato, sono infine esclusi dalle nuove regole i fornitori già sotto la sorveglianza dell'Eurosistema ai sensi dell'articolo 127(2) del Trattato.

7. Conclusioni

L'importanza cruciale della tecnologia per l'industria finanziaria e per l'ecosistema dei pagamenti è uno dei tratti distintivi delle economie moderne.

In questo contesto, le strategie di esternalizzazione e in generale il ricorso a fornitori terzi hanno permesso alle aziende, soprattutto a quelle di minori dimensioni e dotate di limitate risorse, di stare al passo con l'innovazione che ha caratterizzato il settore negli ultimi 20 anni. Tali processi però si accompagnano a un aumento di una serie di rischi (operativo, *cyber*, di concentrazione, reputazionale, strategico), che, quando servizi e funzioni sono trasferiti da settori regolati verso soggetti terzi esterni a tale perimetro, possono sfuggire dal campo visivo delle autorità.

Questo è il fondamento, insieme all'affermarsi nel sistema finanziario e dei pagamenti di prodotti sempre più innovativi e digitalizzati, che ha giustificato la crescente attenzione e azione dei regolatori a tutti i livelli, da quello internazionale a quello nazionale.

Le iniziative di autorità, *standard setter* e regolatori analizzate in questo lavoro possono essere ricondotte a due principali ambiti di azione: i) interventi sugli operatori finanziari perché presidino il rischio di terze parti; ii) istituzione di nuovi *framework* di sorveglianza sulle stesse terze parti.

I *Principles for Financial Market Infrastructures* (PFMI) continuano a rappresentare il *benchmark* internazionale e le linee di azione dei regolatori, soprattutto guardando al contesto europeo e italiano, perseguono l'allineamento del quadro normativo alle migliori prassi internazionali.

[41] Le BigTech rientrano in un più ampio quadro di normative europee, delineato tra l'altro dal cd. *Digital Markets Act*, visto il loro ruolo di "*gatekeeper*" o facilitatori dell'accesso a una serie di servizi non finanziari online. L'interazione tra i differenti obblighi in materia di sorveglianza e di concorrenza è un tema di interesse per le varie autorità chiamate ad applicare i nuovi atti normativi.

DORA si pone l'obiettivo di armonizzare le azioni volte ad accrescere la resilienza del settore finanziario, considerandone la forte dipendenza dalle risorse ICT, e attribuisce un nuovo ruolo alle tre autorità europee di supervisione (EBA, EIOPA, ESMA) nell'assetto di sorveglianza sulle terze parti critiche. Ad oggi il Regolamento non ricomprende nell'ambito di applicazione tutti i soggetti dell'ecosistema dei pagamenti; la resilienza di tale ecosistema è comunque assicurata da una consolidata regolamentazione settoriale.

La tematica del rischio di terze parti è trasversale ai diversi ambiti del settore finanziario ed è resa più rilevante dalla sempre più fitta rete di interdipendenze tra soggetti – finanziari e non – che travalicano le giurisdizioni nazionali e modificano le abitudini economiche e sociali dei consumatori.

La mitigazione di questa tipologia di rischi contribuisce ad aumentare la resilienza operativa del settore e dei suoi operatori e, come fine ultimo, la tutela dell'utenza finale di servizi finanziari. Ne viene rinsaldata anche la fiducia nelle autorità, che ricercano da sempre un equilibrio ottimale tra sicurezza e innovazione.

Riferimenti bibliografici

Arnaudo D., Del Prete S., Demma C., Manile M., Orame A., Pagnini M., Rossi C., Rossi P., & Soggia G. (2022), "The digital transformation in the Italian banking sector", *Banca d'Italia - Questioni di Economia e Finanza*, No. 682, April 2022.

BCBS, Basel Committee on Banking Supervision (2005), Outsourcing in Financial Services, February 2005.

Coletti G., Di Iorio A., Pimpini E. & Rocco G. (2022), "Report on the payment attitudes of consumers in Italy: results from ECB surveys", *Banca d'Italia - Mercati, infrastrutture, sistemi di pagamento*, No. 22, March 2022.

CPMI-IOSCO, Committee on Payments and Market Infrastructures - International Organization of Securities Commissions (2012), CPMI-IOSCO Principles for Financial Market Infrastructures, April 2012.

CPMI-IOSCO, Committee on Payments and Market Infrastructures - International Organization of Securities Commissions (2016), Guidance on cyber resilience for financial market infrastructures, June 2016.

CPMI-IOSCO, Committee on Payments and Market Infrastructures - International Organization of Securities Commissions (2022), Application of the Principles for Financial Market Infrastructures to stablecoin arrangements, July 2022.

Crisanto J. C., Ehrentraud J., & and Fabian M. (2021), Big techs in finance: regulatory approaches and policy options, *BIS, Bank for International Settlements – FSI Briefs*, No. 12, March 2021.

Currie W. L., Michell V., & Abanishe O. (2008). Knowledge process outsourcing in financial services: The vendor perspective. *European Management Journal*, 26(2), 94-104.

Earl M. J. (1996). The risks of outsourcing IT. *MIT Sloan Management Review*.

EBA, European Banking Authority (2019), Final Report on EBA Guidelines on outsourcing arrangements, EBA/GL/2019/02, February 2019.

EBA, European Banking Authority (2021), Report on the use of digital platforms in the EU banking and payments sector (EBA/REP/2021/26), September 2021.

EC, European Commission (2017), Revised rules for payment services in the EU: Summary of Directive (EU) 2015/2366 on EU-wide payment services, December 2017.

ECB, European Central Bank (2016), Eurosystem oversight policy framework, July 2016.

ECB, European Central Bank (2017), Eurosystem oversight report 2016, November 2017.

ECB, European Central Bank (2021a), Eurosystem oversight report 2020, April 2021.

ECB, European Central Bank (2021b), Payments and market infrastructure two decades after the start of the European Central Bank, July 2021.

ECB, European Central Bank (2022), Eurosystem oversight framework for electronic payment instruments, schemes and arrangements, November 2021.

EIOPA, European Insurance and Occupational Pensions Authority (2020), Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002), February 2020.

ESMA, European Securities and Markets Authority (2020), Final Report - Guidelines on outsourcing to cloud service providers (ESMA50-157-2403), December 2020.

Feyen E., Frost J., Gambacorta L., Natarajan H., and Saal M. (2021), Fintech and the digital transformation of financial services: implications for market structure and public policy, *BIS, Bank for International Settlements - BIS Papers*, No. 117, July 2021.

Giannetto B. & Fazio A. (2022), "Cyber resilience per la continuità di servizio del sistema finanziario", Banca d'Italia - *Mercati, infrastrutture, sistemi di pagamento*, No. 18, March 2022.

González R., Gascó J., & Llopis J. (2016). Information systems outsourcing reasons and risks: review and evolution. *Journal of Global Information Technology Management*, 19(4), 223-249.

G7 (2022), Fundamental elements for third party cyber risk management in the financial sector, October 2022.

Könning M., Westner M., & Strahringer S. (2019). A systematic review of recent developments in IT outsourcing research. *Information Systems Management*, *36*(1), 78-96.

Marchetti S. (2022), "Web3, Blocksplained", *Banca d'Italia - Questioni di Economia e Finanza*, No. 717, October 2022.

McFarlan F. W., & Nolan R. L. (1995). How to manage an IT outsourcing alliance. *MIT Sloan Management Review*, *36*(2), 9.

Pellitteri R., Parrini R., Cafarotti C. & De Vendictis B. A. (2023), "L'Open Banking nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza", *Banca d'Italia - Mercati, infrastrutture, sistemi di pagamento*, No. 31, March 2023.

Pubblicazioni della collana Mercati, infrastrutture, sistemi di pagamento

n. 1 TIPS - TARGET Instant Payment Settlement - Il sistema europeo per il regolamento dei pagamenti istantanei, *di Massimiliano Renzetti, Serena Bernardini, Giuseppe Marino, Luca Mibelli, Laura Ricciardi, Giovanni M. Sabelli (Questioni istituzionali)*

n. 2 Real-Time Gross Settlement systems: breaking the wall of scalability and high availability, *di Mauro Arcese, Domenico Di Giulio, Vitangelo Lasorella* (Approfondimenti)

n. 3 Green Bonds: the Sovereign Issuers' Perspective, *di Raffaele Doronzo, Vittorio Siracusa, Stefano Antonelli* (Approfondimenti)

n. 4 T2S - TARGET2-Securities - La piattaforma paneuropea per il regolamento dei titoli in base monetaria, *di Cristina Mastropasqua, Alessandro Intonti, Michael Jennings, Clara Mandolini, Massimo Maniero, Stefano Vespucci, Diego Toma* (Questioni istituzionali)

n. 5 The carbon footprint of the Target Instant Payment Settlement (TIPS) system: a comparative analysis with Bitcoin and other infrastructures, *di Pietro Tiberi* (Approfondimenti)

n. 6 Proposal for a common categorisation of IT incidents, *di Autorité de Contrôle Prudentiel et de Résolution, Banca d'Italia, Commissione Nazionale per le Società e la Borsa, Deutsche Bundesbank, European Central Bank, Federal Reserve Board, Financial Conduct Authority, Ministero dell'Economia e delle Finanze, Prudential Regulation Authority, U.S. Treasury* (Questioni istituzionali)

n. 7 Inside the black box: tools for understanding cash circulation, *di Luca Baldo, Elisa Bonifacio, Marco Brandi, Michelina Lo Russo, Gianluca Maddaloni, Andrea Nobili, Giorgia Rocco, Gabriele Sene, Massimo Valentini* (Approfondimenti)

n. 8 L'impatto della pandemia sull'uso degli strumenti di pagamento in Italia, *di Guerino Ardizzi, Alessandro Gambini, Andrea Nobili, Emanuele Pimpini, Giorgia Rocco* (Approfondimenti)

n. 9 TARGET2 - Il sistema europeo per il regolamento dei pagamenti di importo rilevante, *di Paolo Bramini, Matteo Coletti, Francesco Di Stasio, Pierfrancesco Molina, Vittorio Schina, Massimo Valentini* (Questioni istituzionali)

n. 10 A digital euro: a contribution to the discussion on technical design choices, *di Emanuele Urbinati, Alessia Belsito, Daniele Cani, Angela Caporrini, Marco Capotosto, Simone Folino, Giuseppe Galano, Giancarlo Goretti, Gabriele Marcelli, Pietro Tiberi, Alessia Vita* (Questioni istituzionali)

n. 11 From SMP to PEPP: A Further Look at the Risk Endogeneity of the Central Bank, *di Marco Fruzzetti, Giulio Gariano, Gerardo Palazzo, Antonio Scalia* (Approfondimenti)

n. 12 Le TLTRO e la disponibilità di garanzie in Italia, *di Annino Agnes, Paola Antilici, Gianluca Mosconi* (Approfondimenti)

n. 13 Overview of central banks' in-house credit assessment systems in the euro area, *di Laura Auria, Markus Bingmer, Carlos Mateo Caicedo Graciano, Clémence Charavel, Sergio Gavilá, Alessandra Iannamorelli, Aviram Levy, Alfredo Maldonado, Florian Resch, Anna Maria Rossi, Stephan Sauer* (Questioni istituzionali)

n. 14 L'allocazione strategica e la sostenibilità degli investimenti della banca centrale, *di Davide Di Zio, Marco Fanari, Simone Letta, Tommaso Perez, Giovanni Secondin* (Approfondimenti)

n. 15 Climate and environmental risks: measuring the exposure of investments, *di Ivan Faiella, Enrico Bernardini, Johnny Di Giampaolo, Marco Fruzzetti, Simone Letta, Raffaele Loffredo, Davide Nasti* (Approfondimenti)

n. 16 Cross-Currency Settlement of Instant Payments in a Multi-Currency Clearing and Settlement Mechanism, *di Massimiliano Renzetti, Fabrizio Dinacci, Ann Börestam* (Approfondimenti)

n. 17 Quale futuro per i benchmark del mercato monetario in euro?, *di Daniela Della Gatta* (Questioni istituzionali)

n. 18 Cyber resilience per la continuità di servizio del sistema finanziario, *di Boris Giannetto, Antonino Fazio* (Questioni istituzionali)

n. 19 Cross-Currency Settlement of Instant Payments in a Cross-Platform Context: a Proof of Concept, *di Massimiliano Renzetti, Andrea Dimartina, Riccardo Mancini, Giovanni Sabelli, Francesco Di Stasio, Carlo Palmers, Faisal Alhijawi, Erol Kaya, Christophe Piccarelle, Stuart Butler, Jwallant Vasani, Giancarlo Esposito, Alberto Tiberino, Manfredi Caracausi* (Approfondimenti)

n. 20 Flash crashes on sovereign bond markets – EU evidence, *di Antoine Bouveret, Martin Haferkorn, Gaetano Marseglia, Onofrio Panzarino* (Approfondimenti)

n. 21 Report on the payment attitudes of consumers in Italy: results from ECB surveys, *di Gabriele Coletti, Alberto Di Iorio, Emanuele Pimpini, Giorgia Rocco* (Questioni istituzionali)

n. 22 When financial innovation and sustainable finance meet: Sustainability-Linked Bonds, *di Paola Antilici, Gianluca Mosconi, Luigi Russo* (Questioni istituzionali)

n. 23 Business models and pricing strategies in the market for ATM withdrawals, *di Guerino Ardizzi, Massimiliano Cologgi* (Approfondimenti)

n. 24 Press news and social media in credit risk assessment: the experience of Banca d'Italia's In-house Credit Assessment System, *di Giulio Gariano, Gianluca Viggiano* (Approfondimenti)

n. 25 The bonfire of banknotes, *di Michele Manna* (Approfondimenti)

n. 26 Integrating DLTs with market infrastructures: analysis and proof-of-concept for secure DvP between TIPS and DLT platforms, *di Rosario La Rocca, Riccardo Mancini, Marco Benedetti, Matteo Caruso, Stefano Cossu, Giuseppe Galano, Simone Mancini, Gabriele Marcelli, Piero Martella, Matteo Nardelli, Ciro Oliviero* (Approfondimenti)

n. 27 Uso statistico e previsivo delle transazioni elettroniche di pagamento: la collaborazione Banca d'Italia-Istat, *di Guerino Ardizzi e Alessandra Righi* (Questioni istituzionali)

n. 28 TIPS: a zero-downtime platform powered by automation, *di Gianluca Caricato, Marco Capotosto, Silvio Orsini, Pietro Tiberi* (Approfondimenti)

n. 29 TARGET2 analytical tools for regulatory compliance, *di Marc Glowka, Alexander Müller, Livia Polo Friz, Sara Testi, Massimo Valentini, Stefano Vespucci* (Questioni istituzionali)

n. 30 The security of retail payment instruments: evidence from supervisory data, *di Massimiliano Cologgi* (Approfondimenti)

n. 31 Open Banking in the payment system: infrastructural evolution, innovation and security, supervisory and oversight practices, *di Roberto Pellitteri, Ravenio Parrini, Carlo Cafarotti, Benedetto Andrea De Vendictis* (Questioni istituzionali)

n. 32 Banks' liquidity transformation rate: determinants and impact on lending, *di Raffaele Lenzi, Stefano Nobili, Filippo Perazzoli, Rosario Romeo* (Approfondimenti)

n. 33 Investor behavior under market stress: evidence from the Italian sovereign bond market, *di Onofrio Panzarino* (Approfondimenti)

n. 34 Reti neurali siamesi per la rilevazione dei difetti di stampa delle banconote, *di Katia Boria, Andrea Luciani, Sabina Marchetti, Marco Viticoli* (Approfondimenti)

n. 35 Quantum safe payment systems, *di Elena Bucciol, Pietro Tiberi*

n. 36 Investigating the determinants of corporate bond credit spreads in the euro area, *di Simone Letta, Pasquale Mirante*

n. 37 Smart Derivative Contracts in DatalogMTL, *di Andrea Colombo, Luigi Bellomarini, Stefano Ceri, Eleonora Laurenza*

n. 38 Making it through the (crypto) winter: facts, figures and policy issues, *di Guerino Ardizzi, Marco Bevilacqua, Emanuela Cerrato, Alberto Di Iorio*

n. 39 Il sistema per lo scambio delle quote di emissione dell'UE (ETS UE), *di Mauro Bufano, Fabio Capasso, Johnny Di Giampaolo, Nicola Pellegrini*

n. 40 La migrazione delle banconote e la stima della circolazione nei paesi dell'area dell'euro: il caso italiano, *di Claudio Doria, Gianluca Maddaloni, Giuseppina Marocchi, Ferdinando Sasso, Luca Serrai, Simonetta Zappa*

n. 41 Assessing credit risk sensitivity to climate and energy shocks, *di Stefano Di Virgilio, Ivan Faiella, Alessandro Mistretta, Simone Narizzano*

n. 42 Report on the payment attitudes of consumers in italy: results from the ecb space 2022 survey, *di Gabriele Coletti, Alberto Di Iorio, Emanuele Pimpini, Giorgia Rocco*

n. 43 A service architecture for an enhanced Cyber Threat Intelligence capability and its value for the cyber resilience of Financial Market Infrastructures, *di Giuseppe Amato, Simone Ciccarone, Pasquale Digregorio, Giuseppe Natalucci*

n. 44 Fine-tuning large language models for financial markets via ontological reasoning, *di Teodoro Baldazzi, Luigi Bellomarini, Stefano Ceri, Andrea Colombo, Andrea Gentili, Emanuel Sallinger*

n. 45 La sostenibilità nelle assemblee societarie in Francia, Germania e Italia, *di Tiziana De Stefano, Giuseppe Buscemi, Marco Fanari*

n. 46 Money market rate stabilization systems over the last 20 years: the role of the minimum reserve requirement, *di Patrizia Ceccacci, Barbara Mazzetta, Stefano Nobili, Filippo Perazzoli, Mattia Persico*