LUISS

Corso di Laurea in Economia e Finanza

Cattedra di Diritto Dei Mercati E Degli
Intermediari Finanziari

L'esternalizzazione ai TPP: fattore di sviluppo o ostacolo per lo sviluppo dell'Open Banking?

Prof.ssa Pellegrini Mirella — RELATORE

Prof. Di Noia Carmine — CORRELATORE

Matr. 782921 Borsatto Melissa

CANDIDATO

Anno Accademico 2024/2025

INTRODUZIONE 4
CAPITOLO 1 – CONTESTO NORMATIVO E IMPLICAZIONI 4
1.1 L'Open Banking e la PSD2: il ruolo dei TPP e l'obbligo di condivisione dei dati 6
1.1.1 Il principio di *Access-to-Account*: fine del monopolio informativo delle banche 8
1.1.2 I *Third Party Providers* (*TPP*): tipologie e ruolo nel sistema PSD2 10
1.1.3 *API* e standard tecnici: la regolazione dell'interfaccia tra banche e TPP 12
1.1.4 *Strong Customer Authentication* (*SCA*): principio, funzionamento e criticità operative 15
1.2 Dal modello della PSD2 all'Open Finance: l'estensione della condivisione dei dati 16
1.3 L'esternalizzazione come problema di governance e compliance 28
1.3.1 Le nuove sfide della sicurezza informatica nell'ecosistema dell'Open Banking 31
1.3.2 Il *Digital Operational Resilience Act* (*DORA*): verso una resilienza digitale strutturale 35
1.3.3 PSD2 e GDPR: un difficile equilibrio tra innovazione e tutela dei dati 40
1.4 Confronto normativo tra Europa, UK e US 45
1.4.1 Il modello regolatorio del Regno Unito: un framework unitario e centralizzato 45
1.4.2 Il modello statunitense: un approccio frammentato e *market-driven* 56
CAPITOLO 2 – L'IMPATTO ECONOMICO DELL'ESTERNALIZZAZIONE AI TPP 65
2.1 L'esternalizzazione ai TPP: tra necessità normativa e strategia economica 65
2.1.1 I benefici economici diretti ed indiretti dell'esternalizzazione ai TPP 69
2.1.2 I rischi per le banche legati all'esternalizzazione 74
2.2 L'esternalizzazione dal punto di vista dei TPP: tra opportunità e minacce 80
2.2.1 Opportunità economiche e di crescita per i TPP 81
2.2.2 Minacce e criticità per i TPP: tra scarsa monetizzazione e dipendenza dalle banche 85
2.2.3 Minacce e criticità per i TPP (segue): standardizzazione mancata e competizione verticale 88
2.3 Modelli emergenti: *Banking-as-a-Platform* (BaaP) e *Banking-as-a-Service* (BaaS) 92
2.3.1 Banking-as-a-Platform: integrazione e apertura dell'ecosistema 93
2.3.2 Banking-as-a-Service: modularità e infrastruttura come servizio 97
CAPITOLO 3 – REVOLUT E N26: DUE MODELLI DI BANCA DIGITALE NEL CONTESTO DELL'OPEN BANKING 102
3.1 Introduzione all'analisi 102
3.2 Revolut: l'esternalizzazione ai TPP come leva di crescita 104

3.2.1 L'evoluzione del modello di business: tra scelte strategiche e vincoli regolatori 105
3.2.2 TPP e architettura operativa: un modello abilitante tra innovazione e scalabilità . 108
3.2.3 Criticità dell'architettura TPP-centrica: tra lock-in e responsabilità regolatorie .. 112
3.3 N26: la limitata esternalizzazione come presidio di solidità 115
3.3.1 Evoluzione del modello di business: tra crescita ed equilibrio regolatorio..... 115
3.3.2 Ruolo dei TPP e architettura operativa: un modello centrato sul *core banking* 118
3.3.3 Criticità di un modello centrato sul core banking: tra rischio di concentrazione e perdita di autonomia competitiva..... 122
3.4 Sintesi critica del confronto tra i due modelli di esternalizzazione 125
CONCLUSIONI..... 128
BIBLIOGRAFIA..... 130
SITOGRAFIA 130

INTRODUZIONE

Negli ultimi anni stiamo assistendo a una fase di profonda trasformazione del settore bancario. Le banche, da secolari presidi di fiducia e gestione accentrata, stanno progressivamente diventando nodi di una rete molto più articolata. L'accelerazione della digitalizzazione – e in particolare la diffusione capillare degli smartphone – non si è limitata rendere più rapidi ed accessibili i servizi tradizionali, ma ha cambiato radicalmente le regole del gioco, ridefinendo i ruoli, le aspettative e i valori dell'intero ecosistema finanziario.

Al giorno d'oggi, soprattutto a seguito della pandemia e dell'espansione del mobile banking, un numero crescente di utenti non accetta più le lunghe attese, la burocrazia e i vincoli tipici delle banche tradizionali. Al contrario, la maggior parte privilegia soluzioni *fintech* caratterizzate da semplicità d'uso, immediatezza e integrazione nella vita quotidiana, senza rinunciare a sicurezza e trasparenza.

In questo contesto si inserisce l'Open Banking, reso possibile in Europa dall'entrata in vigore della Direttiva PSD2, che ha favorito l'apertura dei sistemi tramite interfacce utente standardizzate (*Application Programming Interface*), consentendo così a soggetti terzi autorizzati (c.d. *Third Party Providers*) di inserirsi in spazi che un tempo erano esclusivo appannaggio delle banche. Il risultato è stato una progressiva disintermediazione bancaria, ovvero funzioni che in passato erano considerate vitali per la banca – come i pagamenti, la gestione dei dati finanziari o persino la relazione con il cliente – vengono oggi esternalizzate, in parte per scelta strategica, in parte per vincoli normativi e pressioni competitive.

L'esternalizzazione ai TPP si configura dunque come uno snodo cruciale. Da un lato, consente alle banche di alleggerirsi, specializzarsi e cogliere le opportunità di un ecosistema più aperto; dall'altro rischia di ridimensionarle, privandole di leve strategiche e lasciando spazio a soggetti non bancari nel controllo della relazione con il cliente. È proprio a partire da tali considerazioni che nasce spontanea la domanda a cui il presente elaborato cerca di rispondere, ovvero se l'esternalizzazione ai TPP rappresenti un vantaggio per lo sviluppo del settore bancario – e più in generale dell'Open Banking – o piuttosto un freno capace di erodere il ruolo delle banche e minare la solidità dell'intero ecosistema finanziario.

Per rispondere a questo interrogativo di fondamentale importanza, la ricerca intreccia profili giuridici e profili economici. In particolare, nel *primo Capitolo* verrà delineato il quadro normativo che ha reso possibile negli anni lo sviluppo dell'Open Banking, a partire dalla PSD2 fino alle più recenti proposte europee – *Payment Services Package* e regolamento *FIDA* –, includendo un confronto con i modelli normativi del Regno Unito e degli Stati Uniti per inquadrare meglio la specificità del contesto europeo e l'evoluzione verso l'Open Finance.

Il *secondo Capitolo*, invece, affronterà le principali implicazioni economiche, mettendo in luce benefici e rischi dell'esternalizzazione tanto per le banche quanto per i TPP. In questa prospettiva, verranno analizzati anche i modelli di business ibridi e *platform-based* che stanno progressivamente emergendo a seguito della diffusione dell'esternalizzazione ai TPP dell'accesso ai dati e ai conti, al fine di comprendere se tali dinamiche possano tradursi effettivamente in un vantaggio competitivo per l'intero ecosistema o, al contrario, in nuove forme di dipendenza e fragilità. Infine, il terzo Capitolo sarà dedicato all'analisi di due casi emblematici – Revolut e N26 – che, pur con strategie differenti, hanno ridefinito il rapporto banca-cliente, dimostrando come l'esternalizzazione ai TPP possa essere al tempo stesso fattore di successo e fonte di vulnerabilità.

Ne emerge così che l'esternalizzazione non è una scelta meramente tecnica od organizzativa, ma il banco di prova su cui si gioca il futuro stesso dell'Open Banking. Capire se l'esternalizzazione rappresenti un'opportunità o una minaccia non significa, quindi, solo valutare i destini dei TPP o delle banche, ma comprendere quale sarà l'architettura futura dei mercati finanziari in Europa.

CAPITOLO 1

CONTESTO NORMATIVO E IMPLICAZIONI

1.1 L'Open Banking e la PSD2: il ruolo dei TPP e l'obbligo di condivisione dei dati

Negli ultimi anni la crescente digitalizzazione e l'ascesa delle realtà FinTech hanno posto le basi per l'avvio di radicali mutamenti all'interno del settore bancario e finanziario[1]. In passato, competere con gli operatori tradizionali, come le banche e i circuiti consolidati di carte di credito e di debito, risultava particolarmente complesso a causa delle modalità di servizio e del rapporto privilegiato con la clientela. Tuttavia, le profonde innovazioni apportate dalla diffusione su larga scala delle tecnologie dell'informazione e comunicazione (o servizi *ICT*[2]) hanno generato nuove opportunità all'interno di tale settore, agevolando l'ingresso nel mercato di operatori non bancari in grado di offrire soluzioni più personalizzate e digitalmente più avanzate rispetto agli intermediari tradizionali[3]. Questa maggiore apertura del mercato si configura, però allo stato attuale, come una concorrenza meramente potenziale, in quanto l'effettiva capacità dei nuovi entranti di incidere in modo significativo sull'assetto competitivo risulta spesso limitata dalla presenza di barriere di natura regolamentare, tecnologica e relazionale, che ne ostacolano l'affermazione e rischiano di attenuare l'impatto innovativo auspicato.

Ad ogni modo, tra i vari comparti del settore finanziario, il settore dei pagamenti è quello che ha subito con maggiore intensità le trasformazioni imposte dalla digitalizzazione e dall'ingresso dei nuovi operatori. Così come accaduto in altri settori, anche in questo ambito l'innovazione tecnologica ha modificato in profondità le modalità di offerta dei servizi, ridefinendone la struttura, le tempistiche e le modalità di fruizione.

---

[1] Sull'evoluzione del FinTech e le sue ricadute sul sistema bancario e finanziario si veda, tra gli altri, Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N., *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, in *New York University Journal of Law & Business*, 2017, vol. 14, pp. 393-446, dove gli autori propongono una distinzione in tre fasi evolutive del fenomeno: (i) FinTech 1.0 (dal 1866 fino al 1967), caratterizzata dai primi utilizzi tecnologici nei servizi finanziari; (ii) FinTech 2.0 (dal 1967 al 2008), segnata dall'automazione bancaria e dall'infrastruttura digitale interna agli istituti; e (iii) FinTech 3.0 (dal 2008 in avanti), in cui emergono nuovi operatori esterni alla banca, basati su piattaforme digitali e innovazioni come l'Open Banking, l'Intelligenza Artificiale e la Blockchain. Per una rassegna più recente e focalizzata sul contesto europeo si veda anche: *European Banking Authority (EBA), Report on the impact of FinTech on incumbent credit institutions' business models*, Luglio 2018; nonché di recente: Gozman, D., Liebenau, J., & Mangan, D., *The Innovation Mechanisms of FinTech Start-Ups: Insights from Open Banking*, in *Journal of Management Information Systems*, 2021.

[2] Per "*servizi ICT*" (ove l'acronimo sta per *Information and Communication Technology*) si intendono quei servizi che utilizzano l'infrastruttura ICT per fornire soluzioni ai problemi e alle esigenze aziendali. Questi includono consulenza, gestione delle reti, e servizi cloud. Questi servizi, spesso personalizzati, permettono alle aziende di concentrarsi sul proprio core business, mentre i fornitori ICT gestiscono gli aspetti tecnologici e di comunicazione. Per ulteriori chiarimenti in merito si veda: Nexsys, "*IT e ICT: cosa sono, definizioni e principali differenze*", https://www.nexsys.it/ict-e-it-significato-e-definizione/

[3] M. Bianco, M. Vangelisti, *Open Banking e inclusione finanziaria*. In "*Dall'Open Banking all'Open Finance. Profili di diritto dell'economia*", a cura di V. Falce & U. Morera, G. Giappichelli, 2024, Torino, p.33-34

Di fatto, sono emersi nuovi strumenti di pagamento alternativi al contante, che – rispetto a quelli inizialmente disciplinati dalla Direttiva 2007/64/CE (c.d. *Payment Service Directive*) – sono progettati per garantire transazioni più rapide, digitalizzate e pienamente conformi agli standard europei in materia di sicurezza ed interoperabilità[4].

Rispetto agli altri settori economici interessati, però, il settore dei pagamenti si caratterizza per un intervento diretto e consapevole del legislatore, il quale non si è limitato a recepire passivamente i cambiamenti in atto, bensì ha scelto di accompagnare ed incentivare il processo innovativo attraverso una revisione organica del quadro normativo di riferimento.

In ragione di ciò, il legislatore si è trovato a dover fronteggiare una sfida cruciale: garantire un equilibrio sostenibile tra innovazione, sicurezza e concorrenza, assicurando allo stesso tempo la protezione dei consumatori e un accesso regolamentato ai dati bancari.

A tal fine, il Parlamento europeo – in collaborazione con il Consiglio europeo – ha promosso una sostanziale revisione del precedente testo normativo, culminata nell'adozione della Direttiva (UE) 2015/2366 (*Seconda Direttiva sui Servizi di Pagamento – PSD2*). Quest'ultima ha non solo aggiornato il contenuto, ma sostituito integralmente la *Prima Direttiva sui Servizi di pagamento* (PSD1)[5], perseguendo a sua volta una moltitudine di obiettivi tra cui: la promozione dello sviluppo digitale dei pagamenti, l'aumento della concorrenza e della trasparenza nel settore bancario, nonché il rafforzamento della protezione dei consumatori e della sicurezza delle transazioni[6]. Tuttavia, la vera novità introdotta consiste nell'obbligo imposto agli istituti bancari di rendere accessibili i dati dei conti dei propri clienti anche a soggetti terzi autorizzati (*Third Party Providers*, *TPP*), tramite *open API* (*Application Programming Interface*) ad essi dedicate. Tale concessione ha avuto riflessi particolarmente importanti non solo per lo sviluppo del settore dei pagamenti, i cui servizi sono stati i destinatari della creazione di notevole valore aggiunto, bensì per l'intero settore bancario.

Per poter cogliere pienamente le implicazioni del modello di Open Banking sviluppatosi a livello europeo, è opportuno a questo punto analizzare separatamente le principali questioni regolamentari emerse a seguito dell'introduzione della PSD2, a partire dal principio di accesso ai conti bancari (*access-to-account* – c.d. *XS2A*), passando per l'identificazione dei nuovi attori di mercato (*TPP*),

[4] E. Cerrato, E. Detto, D. Natalizi, F. Semorile, F. Zuffranieri, *Mercati, infrastrutture e sistemi di pagamento. I fornitori di tecnologia nel sistema dei pagamenti: evoluzione di mercato e quadro normativo,* Quaderni Banca d'Italia, No. 47, Marzo 2024, p.9

[5] La Direttiva 2007/64/CE (*Payment Service Directive – PSD1*) ha rappresentato il primo tentativo organico dell'Unione Europea di armonizzare la disciplina dei servizi di pagamento nl mercato interno. Essa ha introdotto per la prima volta una base normativa comune per l'accesso al mercato da parte dei prestatori di servizi di pagamento (PSP), ponendo le fondamenta per un mercato unico dei pagamenti all'interno dell'UE. In proposito si veda: *European Commission – Fact Sheet*, *Payment Services Directive: frequently asked questions*, Brussels, 12 January 2018

[6] R. Camporeale, *Le asimmetrie della PSD2 e il nuovo Payments Package*. In "*Dall'Open Banking all'Open Finance. Profili di diritto dell'economia*", a cura di V. Falce & U. Morera, G. Giappichelli, 2024, Torino, p.71

fino ad arrivare alle sfide di sicurezza e compliance tecnica poste dagli standard di *Strong Customer Authentication* (SCA) e dalle interfacce di comunicazione.

1.1.1 Il principio di *Access-to-Account*: fine del monopolio informativo delle banche

Tra gli elementi di maggiore discontinuità introdotti dalla Direttiva (UE) 2015/2366 rispetto al precedente quadro regolamentare, spicca l'obbligo per le banche - in qualità di *Account Servicing Payment Providers* (ASPSP) – di consentire la condivisione in tempo reale delle informazioni, previo consenso dell'utente, ai prestatori terzi autorizzati.

Quest'obbligo, noto anche come principio dell'*access-to-account* (XS2A), ha condotto a una sostanziale riformulazione dei rapporti tra le banche e le TPP, senza comportare l'instaurazione di un vero e proprio rapporto contrattuale tra le parti. Si tratta, infatti, non tanto di un accordo negoziale quanto piuttosto di una misura unilaterale imposta alle banche, fondata su un diritto dell'utente e finalizzata ad abbattere le barriere all'ingresso nel mercato dei servizi di pagamento, promuovendo una maggiore concorrenza ed innovazione tramite la disaggregazione dell'offerta bancaria.

In concreto, conformemente a quanto previsto dall'art.36 PSD2, l*'access-to-account rule* ha imposto alle banche di concedere l'accesso ai conti ed ai relativi dati, tramite interfacce dedicate (API), a soggetti terzi autorizzati senza prevedere alcuna forma di remunerazione. Pertanto, esse si sono trovate a dover sostenere integralmente i costi legati allo sviluppo e alla manutenzione delle API, con evidenti ripercussioni sia sul piano economico che organizzativo[7].

Questo nuovo equilibrio ha, peraltro, contribuito a far emergere ulteriori criticità, tra cui significative asimmetrie regolamentari, in quanto, mentre gli istituti bancari sono soggetti ad obblighi normativi rigidi ed onerosi[8], i soggetti terzi con cui sono tenuti a condividere asset strategici – quali i dati – operano spesso secondo regole sensibilmente meno restrittive. A ciò si aggiunga il fatto che la possibilità, per i TPP, di accedere alle informazioni bancarie degli utenti aggirando il *front-end* bancario ha contribuito ad accelerare la disintermediazione digitale, favorendo una riconfigurazione della catena del valore nel settore dei servizi finanziari, in precedenza verticalmente integrato[9].

Dunque, sebbene l'idea originaria alla base dell'apertura dei dati fosse stata quella di favorire la creazione di un ambiente più competitivo, stimolando lo sviluppo di servizi innovativi e centrati sull'utente, tale processo ha finito per accentuare alcune fragilità strutturali. Degne di nota sono, in

[7] CEPS, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, "*A study on the application and impact of Directive (UE) 2015/2366 on Payment Services (PSD2)*", Publications Office of the European Union, 2023, p.14

[8] Con *obblighi normativi e regolamentari* si fa riferimento, ad esempio, ai requisiti patrimoniali, agli obblighi di governance interna, alle norme prudenziali e ai controlli di antiriciclaggio cui le banche sono soggette ai sensi del CRR/CRD IV e delle direttive europee di settore.

[9] Basel Committee on Banking Supervision, "*Report on open banking and application programming interfaces*", Bank for International Settlements, November 2019, p.8

particolare, le nuove vulnerabilità emerse in materia di sicurezza informatica, gestione del rischio e controllo sull'utilizzo delle informazioni condivise; fragilità principalmente riconducibili alla crescente centralità dei dati finanziari, divenuti negli ultimi anni un vero e proprio asset strategico tanto per le banche tradizionali quanto per i nuovi operatori fintech.

Proprio alla luce di queste circostanze, il legislatore europeo ha compreso la necessità di tutelare maggiormente i consumatori, introducendo regole più stringenti per lo scambio di informazioni tra le banche e i *TPP*. Nello specifico, tali regole non giustificano le banche ad ostacolare l'operatività delle terze parti, ad esempio fornendo dati di scarsa rilevanza e qualità, quanto piuttosto mirano a limitare i rischi inerenti alla condivisione di dati sensibili dei clienti migliorandone la *user experience*[10].

Ad ogni modo, per poter comprendere la portata degli effetti rivoluzionari che il meccanismo di accesso ai conti ha determinato, è bene ricordare che, prima dell'entrata in vigore della PSD2 le banche erano effettivamente le uniche detentrici dei dati bancari relativi ai propri clienti, vantando una relazione pressoché esclusiva con i medesimi. Ciò significava che le banche, non avendo alcun obbligo di condividere le informazioni richieste con terze parti, evitavano qualunque forma di intermediazione con le stesse, se non espressamente necessaria [11]. In virtù di ciò, l'adozione del principio del*l'access-to-account* imposto dalla Commissione Europea ha sancito la fine del monopolio informativo delle banche, introducendo un modello di interoperabilità su base non discriminatoria, secondo il quale ogni TPP autorizzato ha il diritto di accedere – alle stesse condizioni – alle informazioni richieste dagli utenti[12].

Questa nuova configurazione del mercato ha imposto significativi cambiamenti strategici alle banche tradizionali, le quali si sono state trovate a dover rivedere il proprio ruolo all'interno dell'ecosistema finanziario, adottando strategie di cooperazione ed integrazione con i TPP, al fine di non essere progressivamente relegate a mere fornitrici di infrastrutture finanziarie[13]. In tal senso, il principio *XS2A* si è rivelato una "*leva di disintermediazione*": se da un lato ha promosso lo sviluppo di servizi innovativi sempre più coerenti con le esigenze dei consumatori, favorendo il superamento dell'approccio "*one-size-fits-all*" che fino ad allora aveva escluso alcune categorie di utenti[14], dall'altro ha accresciuto la complessità nella governance dei dati e ampliato l'esposizione a rischi legati a possibili utilizzi impropri delle informazioni da parte dei TPP.

---

[10] Banca d'Italia, "*PSD2 e Open Banking: nuovi modelli di business e rischi emergenti*", Novembre 2021

[11] R. Porta, "*Banche e PSD2*", https://it.linkedin.com/pulse/banche-e-psd2-riccardo-porta, LinkedIn, Aprile 2018

[12] O. Borgogno e G. Colangelo, "*Data, Innovation and Competition in Finance: The Case of Access to Account Rule*", European Business Law review 31, no.4 (2020), pp. 585-586

[13] C. Asif, T. Olanrewaju, H. Sayama, A. Vijayasrinivasan, "*Financial services unchained: The ongoing rise of open financial data*", McKinsey&Company, Luglio 2021, p.12

[14] OECD, "*Data portability in open banking: Privacy and other cross-cutting issues*", OECD Digital Economy Papers, No. 348, OECD Publishing, Paris, 2023, pp. 11-12

1.1.2 I *Third Party Providers* (*TPP*): tipologie e ruolo nel sistema PSD2

In coerenza con l'obiettivo di apertura del mercato, l'entrata in vigore della PSD2 e del Regolamento Delegato (UE) 2018/389 ha rappresentato – come già evidenziato nel paragrafo introduttivo – un punto di svolta, introducendo e rendendo effettivamente operativi nuovi "attori", i c.d. *Third Party Providers* (*TPP*) [15]. Di fatto, questi nuovi intermediari si caratterizzavano per essere dei "*soggetti terzi rispetto al rapporto intercorrente tra l'utente e il prestatore di servizi (ASPSP) presso il quale il primo [aveva] radicato il conto, [del tutto estranei] alla custodia e alla gestione dei fondi in relazioni ai quali il servizio veniva eseguito*"[16].

È noto che l'introduzione di queste figure, completamente estranee alle precedenti impostazioni della PSD1, si accompagna a un significativo ampliamento del "*novero dei servizi sottoposti a riserva*"[17] sino ad allora mai pienamente definiti né adeguatamente regolamentati.

Nel dettaglio, la Direttiva (UE) 2015/2366 distingue due principali categorie di TPP, ciascuna dotata di una funzione specifica e normativamente definita, ovvero: i prestatori di servizi di disposizione di pagamento (*Payment Initiation Service Providers*, o *PISP*) e i prestatori di servizi di informazioni sui conti (*Account Information Service Providers*, o AISP).

Mentre i PISP svolgono un servizio che – ai sensi dell'art. 4, punto 15, PSD2 – "*consente di impartire un ordine di pagamento su richiesta dell'utente relativamente a un conto detenuto presso un diverso prestatore di servizi, noto anche come prestatore di servizi di radicamento del conto, [senza che sia necessario passare attraverso i tradizionali circuiti bancari o di carte di credito]*", gli AISP forniscono invece un servizio che – secondo l'art. 4, punto 16, PSD2 – "*gli dà la possibilità di accedere alle informazioni relativamente a uno più conti di pagamento dell'utente detenuti presso un diverso prestatore di servizi*".

Tuttavia, oltre a queste due figure, la PSD2 riconosce un ulteriore tipologia di prestatore di servizi, ossia il *Card-based Payment Instrument Issuer* (o CPII). Tale soggetto non accede direttamente ai conti, bensì è chiamato a svolgere un ruolo di mera verifica della disponibilità dei fondi per conto degli emittenti di strumenti di pagamento basati su carta. Detto altrimenti, i CPII rappresentano degli operatori chiamati a svolgere una funziona di "*ponte*" tecnico tra gli emittenti e le banche, gestendo le carte di pagamento (*card issuer*) e consentendo l'avvio delle transazioni, senza tuttavia accedere ai dati personali né disporre di informazioni sui clienti[18].

---

[15] Banca d'Italia, "*PSD2 e Open Banking: nuovi modelli di business e rischi emergenti*", cit., p.10

[16] F. Marasà, "*Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR*", Orizzonti del Diritto Commerciale, Fascicolo 212020, p.634

[17] F. Maimeri, M. Mancini, "*Quaderni di Ricerca Giuridica della consulenza legale. Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*," Banca d'Italia, 2019, p.49

[18] R. Pelletteri, R.Parrini, C. Cafartti, B. A. De Vendictis, *Questioni istituzionali. Mercati, infrastrutture, sistemi di pagamento. L'Open Banking nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza*, no. 31 Marzo 2023, p. 11

Considerato quanto esposto, è opportuno sottolineare che una delle caratteristiche distintive di queste nuove figure – in particolar modo dei prestatori di servizi di disposizione di ordini di pagamento – risiede nel fatto che, a differenza degli istituti di credito o di pagamento tradizionali, essi non possono né detenere né gestire i fondi degli utenti delle prestazioni del servizio[19].

A tal proposito, l'art. 66 PSD2 stabilisce chiaramente che, i PISP possono operare esclusivamente in qualità di intermediario per l'accesso ai dati dei conti ed iniziazione dei pagamenti, trattando solo le informazioni necessarie all'erogazione del servizio nel rispetto del principio di minimizzazione dei dati[20].

Ad ulteriore conferma della distinzione tra i ruoli testé richiamata, la PSD2 precisa che i TPP – siano essi prestatori di servizi AIS (*Account Information Service*) che PIS (*Payment Initiation Service*) – possono accedere alle informazioni finanziarie o avviare pagamenti solamente su mandato dell'utente, il quale deve rilasciare un'esplicita autorizzazione per ciascun accesso od operazione[21].

Al contempo, i prestatori di servizi di radicamento del conto sono "*obbligati ad accettare le richieste di accesso presentate dai soggetti terzi autorizzati, salvo la sussistenza di motivi oggettivi che giustifichino il rifiuto, come, ad esempio, il rischio di frode*"[22].

A ciò si aggiunge che le banche, pur non potendo ostacolare né esercitare alcuna forma di controllo sull'operatività dei TPP autorizzati, restano comunque responsabili della sicurezza dell'infrastruttura tecnica messa a disposizione, nonché della protezione dei dati personali trattati nel contesto dell'accesso da parte dei terzi.

Dunque, questo nuovo assetto regolamentare, se da un lato ha ampliato l'offerta e incentivato la concorrenza, ha anche comportato una maggiore complessità strutturale nei rapporti tra operatori, indebolendo la coesione complessiva del sistema bancario.

---

[19] *Direttiva 2015/2366 del Parlamento europeo e del Consiglio, del 15 novembre 2015, concernente il servizio di pagamento nel mercato interno, che modifica le direttive 2002/65/EC, 2009/110/EC e 2013/36/EU e il regolamento n. 1093/2010 e che abroga la direttiva 2007/64/EC,* art. 66, par. 3: "*Il prestatore di servizi di disposizione di pagamento non detiene in alcun momento i fondi del pagatore in relazione alla prestazione del servizio di disposizione di ordine di pagamento*"

[20] Il *principio di minimizzazione dei dati*, argomento sviluppato già dal D. Lgs 196/2003 (Codice Privacy), rappresenta un concetto chiave del *GDPR* (più precisamente concetto trattato all'art.5 GDPR) ed indica che il trattamento dei dati personali per essere lecito, e quindi consentito, deve essere limitato ai soli dati indispensabili, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono stati raccolti e trattati. Ciò comporta che i titolari del trattamento dati non possono raccogliere più dati di quanti ne siano effettivamente necessari per la finalità del trattamento stesso e che questi dati devono essere mantenuti solo per il tempo necessario per raggiungere tale scopo. Per ulteriori approfondimenti si veda: *Regulation* (EU) 2016/679 *of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulatio*n), art. 5

[21] Si vedano gli articoli 66 e 67 della Direttiva (UE) 2015/2366 per ulteriori dettagli in merito a: le disposizioni per l'accesso ai conti di pagamento in caso di servizi di disposizione di ordini di pagamento e le disposizioni per l'accesso alle informazioni sui conti di pagamento e all'utilizzo delle stesse in caso di servizi di informazione sui conti.

[22] L. Frattini Passi, B. Raganelli, *Open Finance e innovazione finanziaria: opportunità, questioni e sfide*. In "*Dall'Open Banking all'Open Finance. Profili di diritto dell'economia*", a cura di V. Falce & U. Morera, G. Giappichelli, 2024, Torino, p.140

La compresenza di attori tradizionali e TPP, assoggettati a discipline eterogenee, ha reso più complessa la gestione dei flussi informativi e finanziari degli utenti (o *Payment Service Users*, PSU), ponendo sfide inedite in materia di coordinamento, responsabilità e governance.
In particolare, la possibilità per i TPP di operare senza detenere fondi, unita al diritto di accedere ai dati bancari dei clienti in maniera non discriminatoria, ha accentuato la necessità di introdurre standard di sicurezza elevati e meccanismi di autenticazione capaci di garantire un accesso sicuro e conforme alle normative vigenti.
In definitiva, l'integrazione di figure quali i PISP e gli AISP ha segnato una svolta cruciale nel panorama regolamentare europeo, determinando il passaggio da un modello pressoché bancocentrico – fondato sull'esclusività dell'intermediazione bancaria – a un ecosistema digitale interoperabile, in cui l'utente è posto al centro e può delegare ad altri soggetti l'accesso ai propri dati senza che ciò comporti la perdita di controllo o della sicurezza. Tuttavia, la gestione concreta di questi nuovi equilibri ha dimostrato fin da subito le debolezze di un sistema ancora in fase di consolidamento, rendendo evidente la necessità di un intervento del legislatore europeo mediante una serie di standard tecnici vincolanti capaci di tradurre in prassi operativa il nuovo assetto regolatorio delineato dalla PSD2.

1.1.3 *API* e standard tecnici: la regolazione dell'interfaccia tra banche e TPP

Proprio al fine di dare attuazione concreta al principio di *access-to-account*, delineato nel §1.1.1 e reso concretamente operativo con l'introduzione dei TPP, la PSD2 ha imposto agli istituti bancari tradizionali (ASPSP) l'obbligo di predisporre interfacce di comunicazione sicure, accessibili e standardizzate, tramite cui i TPP possano accedere ai conti degli utenti su loro richiesta.
Tali interfacce, comunemente denominate *Application Programming Interface* (API), rappresentano strumenti informatici progettati per consentire ai soggetti autorizzati uno scambio delle informazioni strutturato, tracciabile e in tempo reale.
Rispetto alle pratiche precedenti, come lo *screen scraping*[23] – tecnica largamente utilizzata prima dell'introduzione della PSD2 – l'adozione delle API ha segnato un rilevante passo in avanti in termini di sicurezza, trasparenza e ripartizione delle responsabilità tra soggetti coinvolti. Tuttavia, proprio la

[23] In assenza di una regolamentazione ad hoc, in Europa si sono diffusi prima dell'entrata in vigore della PSD2 servizi di accesso ai conti on-line degli ASPSP basati sul c.d. "screen scraping", che tuttavia in Italia hanno avuto una scarsa diffusione. Lo "*screen scraping*" è una tecnica informatica di estrazione di dati da un sito web per mezzo di programmi software, che simulano la navigazione umana nelle pagine web. Con tali tecniche, prima dell'entrata in vigore della PSD2 che le ha vietate, un operatore, senza un accordo preventivo con l'ASPSP e senza l'obbligo di soddisfare requisiti normativi, è in grado di accedere ai conti on-line dei clienti, simulando il comportamento del cliente stesso. Tale tecnica, ritenuta insicura e non rintracciabile, è stata disincentivata dalla PSD2. Per ulteriori dettagli si veda: Bank Policy Institute, "Screen Scraping: What Is It and How Does It Work?", https://bpi.com/screen-scraping-what-is-it-and-how-does-it-work/, November 2024

necessità di garantire che tali interfacce venissero predisposte e gestite secondo requisiti tecnici minimi ed uniformi tra i vari Paesi dell'UE, nel rispetto dei principi di integrità, disponibilità ed affidabilità dei dati, ha richiesto un ulteriore adeguamento normativo.

In questo contesto, degno di nota è il ruolo svolto dall'Autorità Bancaria Europea (*EBA*), la quale, in forza del mandato conferitole dall'art. 98 della Direttiva 2015/2366 (*PSD2*), ha adottato i *Regulatory Technical Standards* (RTS) finalizzati ad introdurre criteri più stringenti per l'autenticazione dei clienti (*Strong Customer Authentication*, *SCA*), nonché a garantire una comunicazione più efficiente e sicura tra banche e prestatori di servizi di pagamento di terze parti (*TPP*)[24].

Nello specifico, ai sensi dell'art. 98 della Direttiva (UE) 2015/2366 (PSD2), "*l'ABE emana in stretta cooperazione con la BCE, e previa consultazione di tutti i portatori di interessi […], a norma dell'articolo 10 del regolamento (UE) n. 1093/2010, progetti di norme tecniche di regolamentazione indirizzati ai prestatori di servizi di pagamento di cui all'articolo 1, paragrafo 1, della presente direttiva*" volti a: "*a) assicurare un livello adeguato di sicurezza per gli utenti di servizi di pagamento e i prestatori di servizi di pagamento mediante l'adozione di requisiti efficaci e basati sul rischio; b) assicurare la sicurezza dei fondi e dei dati personali degli utenti di servizi di pagamento; c) garantire e mantenere la concorrenza equa tra i prestatori di servizi di pagamento; d) assicurare la neutralità dei modelli tecnologici e commerciali; e)permettere lo sviluppo di mezzi di pagamento accessibili, innovativi e di facile utilizzo*."

Alla luce di quanto esposto, l'adozione dei RTS da parte dell'Autorità Bancaria Europea ha rappresentato uno strumento essenziale non solo per contrastare le criticità legate all'uso indiscriminato delle tecniche di *screen scraping*, attraverso la formalizzazione dell'obbligo di applicazione dell'autenticazione forte del cliente (introdotta all'art. 97 PSD2[25]), ma anche per elevare

[24] Il Parlamento europeo, al fine di garantire un'armonizzazione coerente nei settori specifici di applicazione di alcune disposizioni tecniche più complesse, ha previsto l'adozione dei c.d. *Regulatory Technical Standards* (RTS), atti delegati adottati dalla Commissione Europea su proposta dell'Autorità Bancaria Europea (EBA), in conformità agli artt. 10-15 del Regolamento (UE) n. 1093/2010. A differenza della Direttiva (UE) 2015/2366, la quale ai sensi dell'art. 288 del TFUE vincola la Stato membro cui è rivolta per quanto riguarda il risultato da raggiungere lasciando alle autorità nazionali il potere di scegliere la forma e i mezzi per raggiungere tale scopo, gli RTS sono atti giuridicamente vincolanti e direttamente applicabili in tutti gli Stati membri, senza necessità di recepimento nazionale. Difatti, la loro funzione è quella di integrare e specificare aspetti tecnici delle disposizioni contenute nella direttiva, come nel caso dell'RTS sull'autenticazione forte del cliente e sulla comunicazione sicura (Regolamento Delegato (UE) 2018/389), il quale dettaglia le modalità operative del principio di accesso ai conti (*XS2A*), rendendo effettiva l'interoperabilità tra banche e prestatori terzi.

[25] *Direttiva 2015/2366 del Parlamento europeo e del Consiglio, del 15 novembre 2015, concernente il servizio di pagamento nel mercato interno, che modifica le direttive 2002/65/EC, 2009/110/EC e 2013/36/EU e il regolamento n. 1093/2010 e che abroga la direttiva 2007/64/EC*, art. 97 par. 1: *Gli Stati membri provvedono a che un prestatore di servizi di pagamento applichi l'autenticazione forte del cliente quando il pagatore:*
a) accede al suo conto di pagamento on line;
b) dispone un'operazione di pagamento elettronico;
c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

gli standard di affidabilità operativa dell'intero sistema, imponendo obblighi stringenti tanto agli istituti bancari quanto ai prestatori di servizi di pagamento terzi (TPP).

È bene tener presente, tuttavia, che l'attività dell'EBA non si è limitata all'adozione degli RTS; l'Autorità ha svolto anche una decisiva funzione di indirizzo e vigilanza attraverso l'emanazione di opinioni, chiarimenti interpretativi e documenti di monitoraggio sull'attuazione delle API nei vari Stati membri. Tali strumenti hanno avuto un ruolo cardine nel garantire un'applicazione uniforme del quadro tecnico, contribuendo a risolvere le numerose difficoltà operative emerse nella fase di implementazione.

Ad ogni modo, la previsione di requisiti minimi per la registrazione dei TPP presso le autorità competenti e l'imposizione di metodologie di autenticazione conformi a standard elevati dettati dagli RTS ha contribuito a rafforzare la protezione dei dati e la fiducia degli utenti.

Tali misure hanno senz'altro favorito la creazione di un ambiente più controllato ed affidabile, come dimostrato dall'incremento del numero di licenze concesse ai TPP nei diversi Stati membri dell'Unione Europea, ma hanno anche prodotto un effetto selettivo significativo, determinando la fuoriuscita dal mercato di alcuni operatori minori, incapaci di sostenere sia i costi tecnici che quelli organizzativi richiesti per l'adeguamento ai nuovi standard[26].

In questo scenario, per far fronte alle ingenti criticità emerse sul piano tecnico e di sostenibilità dei costi legati allo sviluppo, alla manutenzione e al testing delle API – già in parte anticipate nel sottoparagrafo 1.1.1 – oltre il 75% delle banche europee ha deciso di adottare il *Framework NextGenPSD2* sviluppato dal *Berlin Group,* il quale si è affermato come una delle soluzioni tecniche più diffuse a livello europeo per l'implementazione delle API conformi alla PSD2[27].

Nello specifico, tale framework ha contribuito ad armonizzare le soluzioni tecniche nei diversi ordinamenti nazionali, riducendo il rischio di implementazione e favorendo un'integrazione più fluida tra le banche e prestatori di servizi terzi.

In definitiva, l'introduzione delle API e l'elaborazione degli RTS da parte dell'EBA hanno fornito le basi tecniche per rendere effettivo l'accesso regolamentato ai conti, cercando di assicurare la presenza di un'infrastruttura sicura, aperta e interoperabile.

Tuttavia, come si avrà modo di approfondire nel successivo paragrafo, l'efficacia di tale sistema dipende in larga misura dall'applicazione di solidi meccanismi di identificazione e autorizzazione degli utenti, centrati sull'autenticazione forte del cliente.

---

[26] CEPS, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, "*A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)*", cit., p.11

[27] The Berling Group, "PSD2 Access to Bank Account", https://www.berlin-group.org/psd2-access-to-bank-accounts

1.1.4 *Strong Customer Authentication* (*SCA*): principio, funzionamento e criticità operative

Nel quadro delineato dalla PSD2, la necessità di rafforzare la fiducia degli utenti nei servizi digitali di pagamento ha condotto all'introduzione di un meccanismo centrale per la protezione delle transazioni elettroniche: la *Strong Customer Authentication* (SCA).

Questo sistema di verifica dell'identità dell'utente si basa sull'impiego combinato di almeno due fattori di autenticazione, ciascuno appartenente a una delle seguenti categorie: conoscenza, possesso ed inerenza.

Più precisamente, la conoscenza si riferisce a quelle informazioni che solo l'utente conosce, come una password o un PIN; il possesso attiene a un oggetto su cui l'utente ha il controllo quasi esclusivo, quale ad esempio un dispositivo mobile o un token di sicurezza; l'inerenza, infine, riguarda caratteristiche biometriche univoche, come l'impronta digitale o il riconoscimento facciale[28].

L'autenticazione forte, quindi, si realizza attraverso la combinazione di questi elementi, i quali integrati nel processo di autorizzazione del pagamento, permettono di generare un codice univoco basato sui dati dell'operazione.

Nella maggior parte dei casi, questo codice si traduce in una *One-Time Password* (OTP), associata all'importo e al beneficiario dell'operazione, non riutilizzabile in caso di intercettazione.

L'introduzione della SCA ha trovato il proprio fondamento nell'art.97 della PSD2, e la sua attuazione tecnica è disciplinata dal Regolamento Delegato (UE) 2018/389, parte integrante degli RTS elaborati dall'EBA, come descritto nel precedente paragrafo.

Sebbene tale strumento sia stato concepito nell'ottica di contenere i rischi di frode connessi alla digitalizzazione finanziaria e fortificare la protezione dei dati personali, è emerso che un'applicazione troppo rigida delle relative misure potrebbe compromettere negativamente la fluidità operativa ed incidere negativamente sulla *user experience*, soprattutto in riferimento a operazioni di basso valore o ricorrenti. Per questa ragione, e al fine di incentivare l'uso di strumenti di pagamento alternativi al contante, il legislatore europeo ha previsto mediante il Regolamento Delegato (UE) 2018/389 specifiche esenzioni all'obbligo di SCA.

Tra le tipologie di operazioni esentate dall'obbligo di autenticazione forte si annoverano i pagamenti effettuati attraverso strumenti di pagamento anonimi, i pagamenti contactless di importo ridotto (solitamente inferiore ai 50 euro) ed i pagamenti ricorrenti con lo stesso importo e beneficiario[29].

---

[28] Banca d'Italia, "*Che cosa è l'autenticazione forte del cliente (Strong Costumer Authentication, SCA)*", https://www.bancaditalia.it/focus/sca/sca-funzione/index.html, 2021

[29] *Regolamento Delegato (UE) 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*, Considerando no. 8 ss.

Nonostante l'implementazione della SCA abbia contribuito a una significativa riduzione delle frodi, stimata intorno al 50% tra il giugno del 2020 e l'aprile del 2021[30], essa non è risultata sufficiente ad eliminare del tutto i rischi connessi alle transazioni elettroniche.

Inoltre, si sono manifestati rapidamente anche effetti collaterali in termini di sostenibilità operativa non solo per gli operatori terzi, i quali hanno subito un incremento dei costi e una riduzione dell'efficienza del servizio, ma anche per i consumatori, costretti ad affrontare procedure sempre più complesse.

Ad ogni modo, uno degli aspetti più controversi emersi in fase applicativa riguarda, in particolare, l'interpretazione – non sempre uniforme – e l'applicazione discrezionale del meccanismo di ri-autenticazione ogni 90 giorni, previsto dall'art.10 degli RTS, il quale dispone che: "*la SCA non è obbligatoria per gli utenti che accedono esclusivamente al saldo del conto e alla cronologia delle transazioni recenti, ma comunque deve essere richiesta al primo accesso e dopo ogni 90 giorni*" (EBA, 2021)[31].

In base a tale disposizione, i prestatori di servizi di radicamento del conto acquisiscono una discrezionalità applicativa tale da generare forti disomogeneità normative a livello europeo. Di fatto, alcuni istituti hanno imposto ri-autenticazioni più frequenti o con modalità complesse, determinando ritardi, interruzioni e una maggiore frizione nell'esperienza utente.

Per i Third Party Providers, in particolare per gli AISP, questa frammentazione regolatoria ha comportato aumenti generalizzati dei costi operativi e un deterioramento sensibile della qualità del servizio offerto, con effetti negativi sulla loro competitività e capacità di offrire soluzioni fluide e scalabili. La conseguenza è stata una perdita generalizzata di fiducia nell'efficienza del quadro normativo, che ha compromesso – almeno in parte – uno degli obiettivi principali della PSD2, ossia quello di semplificare e incentivare l'adozione di servizi finanziari innovativi.

Alla luce di tali considerazioni, è emersa con forza la necessità di una revisione normativa, volta a superare le disomogeneità applicative e migliorare l'interoperabilità tra i diversi operatori coinvolti; obiettivi oggi al centro del dibattito della riforma della PSD2 e sulla futura introduzione del *Payment Service Regulation* (PSR) e della PSD3.

1.2 Dal modello della PSD2 all'Open Finance: l'estensione della condivisione dei dati

[30] Per ulteriori dettagli in merito si veda: EBA, "*Report on the data provided by payment service providers on their readiness to apply strong customer authentication for E-commerce Card-based Payment transaction*", EBA/REP/2021/16, Giugno 2021

[31] *Consultation Paper on Draft Regulatory Technical Standards amending the Commission Delegated Regulation (UE) 2018/389 supplementing Directive (UE) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customers authentication and common and secure open standards of communication*, EBA, Ottobre 2021

A pochi anni dall'entrata in vigore delle PSD2, il panorama finanziario europeo ha registrato un aumento considerevole del numero di nuovi operatori digitali attivi, continuando ad essere caratterizzato da una crescente centralità dei dati. A testimonianza di tale evoluzione, nel secondo semestre del 2023 – a cinque anni dall'entrata in vigore della PSD2 – il numero di *Third Party Providers* (TPP) era salito a 556, considerando sia lo Spazio Economico Europeo (SEE) che il Regno Unito, altrimenti a 355 con riferimento al solo *SEE*[32].

Tuttavia, nonostante a livello globale il mercato dell'Open Banking avesse raggiunto un valore eccezionale circa pari a 24 miliardi di dollari, con l'Europa che continuava a rappresentare uno dei principali motori della crescita, emerge con chiarezza che il suo effettivo utilizzo è rimasto limitato in larga misura a quelle categorie di utenti che già in precedenza avevano effettuato degli acquisti di prodotti finanziari digitali[33].

Sorge, quindi, il dubbio che la PSD2 non sia riuscita a creare le condizioni necessarie e sufficienti per promuovere un'inclusione finanziaria realmente diffusa, ma che, al contrario, sia finita per rafforzare le dinamiche di concentrazione preesistenti del mercato.

A partire da questa riflessione, il presente paragrafo intende esaminare il passaggio del modello delineato dalla PSD2 verso l'Open Finance, inteso come ampliamento strutturale del perimetro della condivisione dei dati e come possibile risposta alle attuali criticità del sistema.

Le elevate aspettative della clientela in merito alla fruibilità dei servizi, l'implementazione di Open API per la condivisione dei dati tra i TPP e le banche, nonché l'introduzione di nuove tecnologie nei sistemi di pagamento – sviluppatesi a seguito dell'entrata in vigore della PSD2 – hanno profondamente alterato l'ecosistema bancario, generando significative opportunità per i nuovi operatori digitali. A tal proposito, è opportuno evidenziare come tali soggetti, se da un lato hanno cooperato con gli istituti bancari tradizionali, dall'altro hanno strutturato modelli di business propri, in grado di intercettare direttamente le esigenze della clientela, ponendosi così in competizione diretta con le banche incumbent.

Questo nuovo assetto ha posto le basi per una vera e propria "distruzione" dei modelli finanziari tradizionali, contribuendo a un progressivo superamento delle logiche di intermediazione verticale che fino ad allora avevano caratterizzato il settore[34].

Sebbene in alcuni contesti nazionali la diffusione del fenomeno dell'Open Banking abbia spinto le banche tradizionali (o *incumbent*) a collaborare con imprese FinTech – in particolare piccole e medie imprese con requisiti tecnici indispensabili allo sviluppo di nuovi prodotti –, nella maggior parte dei

[32] Konsentus, "*Tracker Open Banking di terze parti di Konsentus del secondo trimestre del 2023*", https://www.konsentus.com/tpp-trackers/q2-2023/, Luglio 2023
[33] Crif, "*La nuova frontiera dell'Open Finance: AI ed evoluzione normativa*", 2024, p.4
[34] OECD, "*Shifting from Open Banking to Open Finance*", 2023, pp.37-38

casi si è assistito a un abbandono del modello integrato a favore di strategie di business più flessibili, modellate a seconda delle necessità da soddisfare della clientela[35].

È proprio in considerazione di queste importanti trasformazioni digitali che i dati vengono ad assumere (nuovamente) un ruolo centrale all'interno del mercato finanziario. Ciononostante, mentre con la PSD2 il focus normativo era rivolto principalmente all'accesso ai conti di pagamento (*XS2A*) e alla condivisione dei dati finanziari funzionali all'iniziazione dei pagamenti, le nuove esigenze di mercato hanno progressivamente esteso il perimetro anche a dati relativi a prestiti, depositi, assicurazioni e forme di risparmio pensionistico[36].

La possibilità di accedere, scambiare e utilizzare dati anche non finanziari garantirebbe al legislatore di soddisfare le esigenze di una platea più ampia di utenti, ponendo sostanzialmente le basi per una possibile transazione dal fenomeno dell'Open Banking a quello dell'Open Finance. Un simile ampliamento, inoltre, potrebbe generare effetti positivi in tema di fiducia e partecipazione della clientela, specialmente in un contesto segnato dagli effetti di lungo periodo della pandemia Covid-19, la quale ha inciso in maniera rilevante sulle abitudini digitali e sulla percezione della stabilità finanziaria[37].

A tal proposito, è opportuno soffermarsi brevemente sul concetto di "fiducia" all'interno del mercato finanziario, la quale - come specificato dalla Commissione europea nell'*Impact Assessment Report* che accompagna la proposta di sviluppo del *Financial Data Access* - è "*uno dei requisiti fondamentali per garantire l'accessibilità e lo scambio dei dati tra i vari operatori del sistema finanziario*". Tuttavia, già a pochi anni dall'adozione della Direttiva (UE) 2015/2366, si è osservata una diffusa diffidenza da parte dei consumatori circa la condivisione dei loro dati con gli operatori del sistema finanziario. Una delle principali cause legate a questo fenomeno è riconducibile a una "*mancanza di controllo effettivo dei clienti sui dati nell'ambito della prestazione di servizi di pagamento*"[38]. Di conseguenza, molti utenti del servizio di pagamento, non essendo in grado di comprendere chiaramente a chi venivano affidati i propri dati né in quale misura, hanno preferito astenersi completamente dal condividerli, limitando così l'effettiva adozione dei servizi di Open Banking.

Alla luce di ciò, e soprattutto a seguito delle numerose criticità correlate all'applicazione della PSD2 all'interno dello Spazio Economico Europeo, è apparso evidente il bisogno di un ulteriore intervento

[35] PwC's Digital Service, "*Platform Banking & Digital Ecosystems*", pp. 22-25, Marzo 2019

[36] M. Bianco, M. Vangelisti, *Open Banking e inclusione finanziaria*. In "*Dall'Open Banking all'Open Finance. Profili di diritto dell'economia*", cit., pp.47-48

[37] C. Asif, T. Olanrewaju, H. Sayama and A. Vijayasrinivasan, "*The ongoing rise of open financial data*", McKinsey & Company, Luglio 2021, p.10

[38] *Commission Staff Working Document del 28 giugno 2023 Impact Assessment Report Accompanyng the document Proposal for a Regulation of the European Parliament and of the Council on a framework of Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554*, *Bruxelles, SWD(2023) 224 final*, pp. 12-14

regolatorio. Se da un lato è indubbio che la PSD2 stava apportando importanti benefici in termini di innovazione, concorrenza e apertura di mercato, dall'altro essa ha mostrato limiti strutturali significativi, tra i quali si ricorda: l'eccessiva frammentazione normativa tra gli Stati membri, l'eterogeneità nell'implementazione della *Strong Customer Authentication* (SCA) e la mancanza di standard comuni ed interoperabili per l'accesso ai conti da parte dei TPP.

Per porre rimedio a queste incongruenze, pur sempre "*[mantenendo] viva l'idea sottesa alla PSD2 di aprire il mercato finanziario a nuovi soggetti*"[39], la Commissione europea, nell'ambito della Strategia digitale per la finanza[40], propose il c.d. *Payment Package*, il quale rappresenta un pacchetto normativo composto da un regolamento (*Payment Service Regulation*, o *PSR*) e una Direttiva sui Servizi di Pagamento (*PSD3*).

Mentre il *Payment Service Regulation* (PSR) punta a superare la frammentazione normativa, armonizzando le regole sui servizi di pagamento mediante disposizioni uniformi e immediatamente vincolanti, la PSD3, invece, mira a definire un quadro armonizzato per il rilascio delle licenze e l'attività di vigilanza sui prestatori di servizi di pagamento[41], integrando al tempo stesso la normativa sulla moneta elettronica (*Electronic Money Directive* - EMD) fin ad allora oggetto di distinta applicazione.

In questo senso, la distinzione chiave tra i ruoli dei due strumenti normativi è finalizzata a colmare una delle principali lacune lasciate irrisolte dalla PSD2, ossia la frammentazione normativa all'interno dell'UE. Infatti, se da un lato la PSD3, in quanto direttiva, dovrà essere recepita da ciascuno Stato membro – lasciando un certo margine di interpretazione a livello nazionale – dall'altro il regolamento, in quanto strumento di armonizzazione massima, troverà applicazione diretta in tutti gli ordinamenti nazionali, contribuendo a rimuovere le incongruenze emerse con la PSD2, soprattutto in materia di accesso ai dati e tutela dei consumatori[42].

Oltre al pacchetto normativo rappresentato dalla PSD3 e dal PSR, la Commissione europea ha presentato un'ulteriore proposta legislativa, volta ad estendere l'accesso e la condivisione dei dati ben

---

[39] P. Stanzione, *Open Banking, Open Finance e protezione dei dati personali*. In "*Dall'Open Banking all'Open Finance. Profili di diritto dell'economia*", a cura di V. Falce & U. Morera, G. Giappichelli, 2024, Torino, p.67

[40] Per ulteriori dettagli si veda: *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, COM/2020/592 final* e *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, COM/2020/591 final*, entrambe contenute nel *Digital Financial Package*, pubblicato dalla Commissione europea il 24 settembre 2020

[41] Con fornitori di servizi di pagamento è da intendersi, d'ora in avanti, sia gli Istituti di Pagamento (IP) che gli Istituti di Moneta Elettronica (IMEL)

[42] S. Dahiwelkar, "*PSD3: An evolution of the EU payments framework and enabling Open Finance*", https://www.deltacapita.com/insights/psd3-an-evolution-of-the-eu-payments-framework-and-enabling-open-finance, Delta Capita, Ottobre 2023

oltre l'ambito dei soli servizi di pagamento, includendo anche prodotti finanziari come prestiti, assicurazioni ed investimenti.

Tale proposta, meglio nota come *Financial Data Access Framework* (FiDA), si proponeva di rappresentare un punto di svolta per il settore, attraverso l'introduzione di un sistema di "*data-sharing* obbligatorio" finalizzato ad accrescere la concorrenza, stimolare l'innovazione finanziaria e migliorare la qualità dei servizi offerti[43].

In questo scenario, la Commissione europea intendeva avviare una transizione regolata verso *l'Open Finance*, aprendo il mercato anche ad altri operatori non bancari, con l'obiettivo di incentivare la diffusione di servizi digitali più personalizzati, interoperabili e rispondenti alle mutevoli esigenze della clientela[44]. Tuttavia, nonostante le potenzialità riconosciute a tale iniziativa, la proposta ha recentemente incontrato forti resistenze, specialmente da parte degli operatori tradizionali, e ad oggi il suo iter legislativo rimane incerto e ancora oggetto di dibattiti politici.

Ad ogni modo, per comprendere appieno la portata degli effetti legati alla possibile introduzione della nuova Direttiva e del PSR, è anzitutto opportuno sottolineare che il legislatore europeo, nel delineare il nuovo pacchetto normativo, ha tenuto conto dell'esperienza maturata in precedenza con la PSD2, cercando al contempo di superarne i limiti in un'ottica di maggiore innovazione e armonizzazione del mercato finanziario. Oltre a ciò, anche la complessità del quadro normativo europeo preesistente ha inciso in modo preponderante sulla scelta del legislatore di adottare una soluzione normativa più coerente, capace non solo di eliminare le incongruenze tra i diversi ordinamenti, ma anche di ridurre gli oneri operativi per gli attori del sistema.

In risposta a tale esigenza, una delle principali novità contenute nella proposta di Direttiva PSD3 riguarda proprio l'integrazione dell'attuale disciplina sui servizi di pagamento con la Direttiva sulla Moneta Elettronica (EMD2[45]). A tal proposito, il legislatore europeo, riconoscendo "*la crescente difficoltà di distinguere i servizi di moneta elettronica da quelli di pagamento*", ha espresso l'intenzione di unificare i quadri regolamentari[46]. In parallelo, però, tale proposta chiarisce anche che verrebbero comunque mantenute distinte le figure degli Istituti di Pagamento (IP) e degli Istituti di Moneta Elettronica (IMEL), con riferimento alle loro specifiche funzioni e caratteristiche[47].

---

[43] *Commissione europea proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un quadro per l'accesso ai dati finanziari e che modifica i regolamenti (UE) n. 1093/2010, (UE) 1094/2010, (UE) n. 1095/2010 e (UE) 2022/2554, COM/2023/360 final*

[44] OECD, "*Open Finance Policy Consideration*", 2023, pp.8-9

[45] Per ulteriori dettagli si veda: *Direttiva 2009/110/CE del Parlamento europeo e del Consiglio, del 16 settembre 2009 concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 200/46/CE*", Gazzetta Ufficiale dell'Unione Europea

[46] *Risoluzione legislativa del Parlamento europeo del 23 aprile 2024 sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo ai servizi di pagamento nel mercato interno e che modifica il regolamento (UE) n. 1093/2010 (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)), Considerando n.5*

[47] *Ibid.*

In quest'ottica, quindi, l'integrazione normativa proposta risponderebbe alle esigenze tanto di semplificazione del quadro normativo, quanto di riduzione degli oneri amministrativi a carico degli operatori del settore. Difatti, rendendo gli IMEL una sottocategoria degli IP, il legislatore mira a garantire una maggiore coerenza ed omogeneità nell'applicazione delle regole comuni ai prestatori di servizi di pagamento[48].

Ciononostante, la proposta di pacchetto PSD3/PSR presenta ancora criticità rilevanti sul piano della coerenza sistemica, specie in relazione ad altri strumenti normativi europei già in vigore – come il GDPR, il *Data Act* e il MiCAR – rispetto ai quali sarà necessario intervenire per assicurare un'integrazione efficace e un'effettiva interoperabilità a livello di mercato.

È plausibile ritenere che il passaggio dalla PSD2 alla PSD3 comporterebbe sì benefici per i nuovi attori che entreranno nel mercato, anche se sta sollevando forti preoccupazioni da parte degli operatori già autorizzati ad operare dalla disciplina vigente. Per tale ragione, la nuova Direttiva prevede la possibilità per coloro che sono già in possesso dell'autorizzazione a prestare servizi di pagamento di continuare ad operare, a condizione che si sottopongano, entro un termine massimo di 24 mesi dall'entrata in vigore della PSD3, a una nuova verifica da parte delle Autorità competenti, volta ad accertare la conformità ai requisiti normativi aggiornati[49]. Così facendo, le disposizioni transitorie proposte avrebbero l'obiettivo di evitare discontinuità operative nel mercato, pur sempre imponendo a tutti gli operatori un necessario riallineamento ai nuovi standard di sicurezza e governance[50].

Un ulteriore punto critico, cui il legislatore ha inteso ovviare mediante il nuovo quadro regolatorio delineato dalla PSD3 e dal *Payment Services Regulation* (PSR), concerne le difficoltà di accesso ai conti riscontrate dai TPP. A riprova di ciò, dallo studio condotto nel 2021 dalla Commissione europea sugli effetti derivanti dall'applicazione della PSD2 emerge che uno dei principali ostacoli allo sviluppo del fenomeno dell'Open Banking risiedeva proprio nell'atteggiamento ostruzionistico di alcuni ASPSP nei confronti dei prestatori terzi, concretizzato sia mediante la predisposizione di interfacce API di scarsa qualità, sia attraverso rifiuti immotivati di autorizzazione all'accesso.

In considerazione di quanto sopra, il PSR prevede una serie di misure finalizzate a garantire condizioni di accesso più eque per i prestatori di servizi AIS e PIS, rimuovendo parte delle barriere che avevano finora limitato l'evoluzione del settore. In particolare, ai sensi dell'art. 35, paragrafo 3, della proposta di PSR, sarebbe imposto agli ASPSP l'obbligo di fornire interfacce dedicate di alta

---

[48] R. Garavaglia, "*PSD3 e Fida, ecco il nuovo corso europeo su pagamenti e finanza digitali*", https://www.agendadigitale.eu/cittadinanza-digitale/psd3-ecco-il-nuovo-corso-europeo-su-pagamenti-e-finanza-digitali/, Agenda Digitale, Giugno 2023

[49] R. Garavaglia, "*PSD3 e PSR: il 2025 dei servizi di pagamento in Europa*", https://www.agendadigitale.eu/cittadinanza-digitale/pagamenti-digitali/psd3-e-psr-il-2025-dei-servizi-di-pagamento-in-europa/, Agenda Digitale, Gennaio 2025

[50] In proposito parliamo di clausole di "*grandfathering*", che in termini giuridici sottintendono alle clausole di salvaguardia

qualità, "*impiegando standard di comunicazione emessi da organizzazioni di normazione europee o internazionali*", al fine di garantire "*l'interoperabilità dei loro software con quelli dei prestatori di servizi di disposizione di ordini di pagamento e di informazione sui conti*"[51]. Inoltre, la proposta di Regolamento prevede anche che l'interfaccia dedicata offerta dagli ASPSP ai TPP debba garantire tempi di risposta e livelli di servizio equivalenti a quelli forniti direttamente ai propri clienti diretti, eliminando così la possibilità per le banche di fornire interfacce scadenti o di qualità inferiore rispetto a quelle destinate alla propria clientela[52].

In definitiva, se da un lato il *Payment Services Regulation* mirerebbe a definire condizioni più eque tra gli operatori, dall'altro non sembrerebbe in grado – almeno allo stato attuale della proposta – di risolvere in modo definitivo le problematiche connesse all'implementazione tecnica delle suddette interfacce per le banche. Queste ultime, come già evidenziato nel §1.1.1, hanno fin da subito manifestato la loro insoddisfazione per gli elevati costi sostenuti per sviluppare e adeguare le API agli standard imposti dalla PSD2, soprattutto in assenza della possibilità di trasferire tali oneri sui TPP; di qui una delle principali ragioni della bassa qualità di molte interfacce offerte dagli ASPSP.

Comunque, a prescindere da tali problematiche, il legislatore europeo ha inteso mantenere nella proposta di PSR l'impostazione originaria della PSD2, vincolando le banche a garantire l'accesso gratuito ai conti da parte dei TPP. Tale scelta risponde all'esigenza di evitare che eventuali costi imposti ai TPP possano ostacolare la continuità dei servizi regolamentati di accesso ai dati, compromettendo così la concorrenza e l'innovazione nel mercato dei servizi di pagamento.

Come chiarito nel Considerando n.55 del PSR, "*se i servizi regolamentati di accesso ai dati fossero stati soggetti a spese finora non addebitate, l'impatto sulla continuità della prestazione di tali servizi, e quindi sulla concorrenza e sull'innovazione nei mercati dei pagamenti avrebbe potuto essere molto significativo*", creando delle possibili ostruzioni. In quest'ottica, il legislatore ha ritenuto opportuno mantenere un certo *fil rouge* con la disciplina previgente, escludendo l'introduzione di qualsiasi meccanismo di compensazione economica a favore delle banche.

---

[51] Commissione Europea, *Payment Services Regulation*, art. 35 paragrafo 3: "*I prestatori di servizi di pagamento di radicamento del conto assicurano che le loro interfacce dedicate di cui al paragrafo 1 utilizzino standard di comunicazione emessi da organizzazioni di normazione europee o internazionali, tra cui il Comitato europeo di normazione (CEN) o l'Organizzazione internazionale per la standardizzazione (ISO). I prestatori di servizi di pagamento di radicamento del conto assicurano inoltre che le specifiche tecniche delle interfacce dedicate di cui al paragrafo 1 siano documentate specificando una serie di routine, protocolli e strumenti di cui necessitano i prestatori di servizi di disposizione di ordine di pagamento e i prestatori di servizi di informazione sui conti per consentire l'interoperabilità del loro software e delle loro applicazioni con i sistemi dei prestatori di servizi di pagamento di radicamento del conto. I prestatori di servizi di pagamento di radicamento del conto mettono a disposizione, senza spese e senza indugio, su richiesta dei prestatori di servizi di disposizione di ordine di pagamento autorizzati, dei prestatori di servizi di informazione sui conti autorizzati o dei prestatori di servizi di pagamento che hanno chiesto alle loro autorità competenti l'autorizzazione pertinente, la documentazione relativa alle specifiche tecniche delle loro interfacce dedicate di cui al paragrafo 1 e mettono a disposizione del pubblico una sintesi di tale documentazione sul loro sito web.*"

[52] Commissione Europea, *Payment Services Regulation*, art. 37

Contestualmente, però, per tener conto delle esigenze operative ed economiche di alcuni ASPSP, il Regolamento prevede anche la possibilità per le autorità competenti di esentare, su richiesta motivata, tali soggetti dall'obbligo di predisporre un'interfaccia dedicata, altrimenti previsto all'art. 35[53]. Nel dettaglio, ai sensi dell'art. 39 par. 1, PSR, viene stabilito che "*su richiesta dei prestatori di servizio di radicamento del conto, l'autorità competente può esentare il prestatore richiedente dall'obbligo di disporre di un'interfaccia dedicata e consentire a quest'ultimo di offrire, come interfaccia per lo scambio sicuro di dati, una delle interfacce che il prestatore di servizi di radicamento del conto utilizza per l'autenticazione e la comunicazione con i propri utenti di servizi di pagamento o, ove giustificato, di non offrire alcuna interfaccia per lo scambio sicuro dei dati*"[54].

Questa concessione, pur non rappresentando una soluzione definitiva al problema relativo ai costi di sviluppo, assicurerebbe maggiore flessibilità a quegli ASPSP in grado di garantire un livello di accesso ed interoperabilità equivalente a quello che sarebbe stato offerto tramite API dedicate.

Tuttavia, la semplificazione dell'accesso ai conti da parte dei TPP e il rafforzamento dell'interoperabilità nel mercato dei pagamenti renderebbero indispensabile l'istituzione di un meccanismo di bilanciamento, tale da consentire agli utenti un maggiore controllo sull'accesso ai propri dati. A questo riguardo, la proposta di Regolamento prevede l'introduzione di specifiche misure finalizzate ad accrescere la consapevolezza degli utenti in merito agli strumenti di pagamento, consentendo così anche ai soggetti più deboli e meno informati di poter decidere per i propri conti.

Più precisamente, il PSR richiederebbe agli ASPSP di sviluppare delle vere e proprie *dashboard* digitali mediante le quali gli utenti possano monitorare in modo semplice e immediato tutte le autorizzazioni concesse ai TPP per l'accesso ai propri dati[55]. In tal modo, il legislatore mira a risolvere un altro limite emerso nell'applicazione della PSD2, ovvero la scarsa trasparenza nella gestione dei consensi, che aveva contribuito ad alimentare la diffidenza degli utenti verso i servizi di Open Banking. infatti, l'impiego di tali strumenti migliorerebbe non solo il rapporto banca-utente, ma anche quello tra ASPSP e operatori terzi, favorendo un ecosistema digitale più trasparente, sicuro ed inclusivo.

---

[53] L'obbligo di disporre di un'interfaccia dedicata è specificato sinteticamente all'art. 35 paragrafo 1 Payment Services Regulation, ove si specifica che: "*I prestatori di servizi di pagamento di radicamento del conto che offrono a un pagatore un conto di pagamento accessibile online dispongono di almeno un'interfaccia dedicata ai fini dello scambio di dati con i prestatori di servizi di informazione sui conti e di disposizione di ordine di pagamento.*"

[54] Commissione Europea, *Payment Services Regulation*, art. 39 paragrafo 1: "*In deroga all'articolo 35, paragrafo 1, su richiesta di un prestatore di servizi di pagamento di radicamento del conto, l'autorità competente può esentare il prestatore di servizi di pagamento di radicamento del conto richiedente dall'obbligo di disporre di un'interfaccia dedicata e consentire a quest'ultimo di offrire, come interfaccia per lo scambio sicuro di dati, una delle interfacce che il prestatore di servizi di pagamento di radicamento del conto utilizza per l'autenticazione e la comunicazione con i propri utenti di servizi di pagamento o, ove giustificato, di non offrire alcuna interfaccia per lo scambio sicuro di dati*."

[55] Commissione europea, *Payment Services Regulation*, art. 43

In questo quadro, segnato dall'evoluzione tecnologica e dalla crescente centralità dei dati, è emersa con forza la necessità di sviluppare ulteriori strumenti normativi in grado di garantire non solo una maggiore inclusione finanziaria, ma anche un più elevato livello di protezione contro l'uso improprio dei dati da parte dei TPP. Nello specifico, come già anticipato nei §1.1.3 e §1.1.4 con riferimento agli standard tecnici di accesso ai dati e all'obbligo di *Strong Customer Authentication* (SCA), il crescente ricorso ai canali digitali nei pagamenti ha reso indispensabile il rafforzamento dei presidi di sicurezza a tutela degli utenti, soprattutto al fine di contrastare le nuove forme di frode emergenti nel contesto della transazione tecnologica in atto. Se da un lato l'introduzione della SCA ad opera della PSD2 – come delineato nel paragrafo 1.1.4 – ha prodotto effetti positivi, specialmente nel contrasto alle frodi sulle carte, ridotte fino al 60% nel solo 2021, dall'altro non si è rivelata sufficiente ad affrontare le forme di attacco più recenti e sofisticate[56].

La rapida digitalizzazione del settore ha favorito la diffusione di nuove tecniche fraudolente, in particolare nel contesto dei bonifici istantanei e delle transazioni transfrontaliere[57], le quali, secondo quanto riportato dalla BCE, solo nel 2019 hanno rappresentato circa il 65% del totale delle frodi su carta[58].

Dunque, sebbene la PSD2 abbia cercato di prevenire il problema, la diffusione di tecniche informatiche di *social engineering* – tra cui *phishing* avanzato e attacchi basati sull'intelligenza artificiale – ha originato una nuova tipologia particolarmente insidiosa di frode nota come *Authorised Push Payment fraud* (APP *fraud*), nella quale sono gli stessi utenti, ingannati, ad autorizzare inconsapevolmente la transazione.

In risposta a quest'emergenza, la proposta di riforma avanzata con il pacchetto PSD3/PSR prevede un rafforzamento significativo del sistema di sicurezza, ponendo l'attenzione principalmente sulla condivisione tempestiva delle informazioni tra gli operatori, sull'efficienza della SCA e sull'identificazione degli utenti.

Più nel dettaglio, l'art. 83 del PSR stabilisce che i prestatori di servizi di pagamento saranno tenuti a monitorare, rilevare e condividere sollecitamente le informazioni relative ad operazioni sospette o fraudolente, sia con le autorità competenti che tra di loro. A tal fine, è prevista l'istituzione – da parte dell'Autorità Bancaria Europea – di "*una piattaforma informatica dedicata per consentire ai prestatori di servizi di pagamento di scambiare informazioni sugli identificativi univoci fraudolenti e altre informazioni pertinenti […] con altri prestatori di servizi di pagamento*" [59]; tutto ciò con lo scopo di creare un sistema di allerta precoce e prevenzione coordinata.

---

[56] G. Azzelini, "*Parere dell'EBA sulle nuove tipologie di frode*", https://www.antiriciclaggiocompliance.it/parere-delleba-sulle-nuove-tipologie-di-frode/, AntiriciclaggioeCompliance, Maggio 2024

[57] *EBA Opinion on new types of payment fraud and possible mitigants*, EBA-Op/2024/01, 29 aprile 2024

[58] BCE, "*Il rapporto della BCE mostra che le frodi sulle carte sono diminuite nel 2019*", 29 Aprile 2021

[59] Commissione europea, *Payment Services Regulation*, art. 83, paragrafo 4bis

A integrazione di tali misure tecniche, il legislatore ha introdotto altresì la figura del prestatore di servizi di comunicazione elettronica, il quale – in base all'art. 59, paragrafo 5bis, PSR – ha il dovere di mettere in atto "*tutte le misure educative necessarie, tra cui avvertimenti ai loro clienti con tutti i mezzi e i supporti opportuni, qualora emergano nuove forme di truffe online, tenendo conto delle esigenze dei gruppi di clienti più vulnerabili*".

Proprio con riguardo a quest'ultima categoria di utenti, spesso esclusa dai servizi digitali per ragioni tecniche o culturali, il legislatore ha ritenuto opportuno imporre ai prestatori di servizi di pagamento di rendere disponibili strumenti di autenticazione più accessibili, progettati per garantire l'uso anche a coloro che hanno limitate competenze digitali o con disabilità[60].

Affinché tali misure potessero essere adeguatamente introdotte, però, era necessario che gli utenti e gli operatori fossero sufficientemente liberi nella loro adozione, così da non costituire esse stesse un ostacolo. Per questo motivo, in linea con l'approccio già adottato per il Regolamento Delegato (UE) 2018/389, viene attribuito all'EBA il compito di definire quali tipologie di operazioni fossero effettivamente soggette all'obbligo di autenticazione forte, nonché l'intensità e la frequenza della sua applicazione, così da evitare margini interpretativi e abusi potenzialmente lesivi degli interessi degli utenti.

Eppure, la richiesta di adottare misure più incisive contro le frodi, contenuta nella proposta di PSR, assieme all'introduzione dell'obbligo di verifica dell'identificativo previsto dal regolamento (UE) 260/2012 (c.d. *SEPA Regulation*), successivamente aggiornato dal regolamento (UE) 2024/886 sui trasferimenti di denaro istantanei, si è rivelata insufficiente a contrastare in modo efficace la crescita esponenziale del fenomeno.

Difatti, come segnalato nel recente parere dell'EBA, le misure previste dal PSR in materia di monitoraggio e condivisione dei dati tra i PSP, o quelle volte a bloccare l'uso degli strumenti di pagamento una volta verificata la presenza di attività fraudolenta, appaiono ancora troppo deboli rispetto alle complessità degli attacchi informatici odierni.

Consapevoli di tali limiti, il Parlamento europeo e il Consiglio hanno affiancato al *Payment Package* una nuova proposta normativa, il c.d. *Financial Data Access Framework* (FiDA[61]), il quale – come anticipato all'inizio del suddetto paragrafo – si presta ad ampliare l'accesso e la condivisione dei dati anche oltre l'ambito dei conti di pagamento, includendo informazioni su prestiti, assicurazioni, investimenti e fondi pensione.

[60] Commissione europea, *Payment Services Regulation*, art. 88

[61] *Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) no 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554, COM(2023) 360 fina*l, Brussels, 28 giugno 2023

In questa prospettiva, il FiDA avrebbe potuto giocare un ruolo chiave nel contrasto alle frodi, prevedendo – diversamente dal PSR – che l'accesso ai dati non fosse più gratuito, bensì soggetto a un meccanismo di compensazione economica tra i soggetti coinvolti[62]. In altri termini, il costo dell'implementazione delle interfacce sarebbe ricaduto non solo sui "*data holders*[63]", ma anche sui "*data users*[64]", ovvero su quei soggetti autorizzati all'accesso, garantendo un accesso più equo e sostenibile e scoraggiando eventuali accessi indesiderati.

Inoltre, sempre in questo ambito, la proposta stabilisce regole molto più stringenti in materia di accesso ai dati degli utenti, stabilendo che solo determinati *data users*, preventivamente autorizzati dalle autorità competenti, possano accedervi. Più specificatamente, l'accesso ai dati dei conti sarebbe stato riservato esclusivamente agli istituti finanziari regolamentati e alle imprese soggette a un'autorizzazione specifica, anche noti come fornitori di servizi di informazione finanziaria (*Financial Information Service Providers, c.d*. FISP).

Come chiarito nei considerando della proposta, l'autorizzazione richiesta ai FISP per poter operare risulta necessaria cosicché possa essere garantita la stabilità del mercato e la protezione dei consumatori, considerata la sensibilità e il valore strategico dei dati messi a disposizione.

Un ulteriore elemento centrale del FiDA riguarda, poi, l'introduzione di un'unica *dashboard* tramite cui l'utente possa gestire in modo semplice e trasparente l'accesso ai propri dati finanziari. Inizialmente pensata per offrire maggiore visibilità sulle informazioni patrimoniali, tale strumento si propone anche quale mezzo per rafforzare la capacità di identificare attività sospette e prevenire frodi, promuovendo al contempo una maggiore inclusione finanziaria.

Nel tentativo di misurare le concrete ricadute che il FiDA avrebbe potuto produrre, è necessario specificare che a differenza dell'impostazione originale della PSD2, tale proposta mantiene fermo il principio del controllo dei dati in capo ai clienti delle istituzioni finanziarie, riconoscendo loro il diritto di decidere se, a chi e per quali finalità condividere le proprie informazioni[65]. Pertanto, "*l'iniziativa FiDA intendeva estendere il quadro regolamentare Open Banking della PSD2 all'Open Finance poggiandosi sul medesimo approccio customer-centric, ma traendo insegnamento da alcune lezioni apprese da tale direttiva*"[66].

---

[62] *Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) no 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554, COM(2023) 360 final, Brussels*, 28 giugno 2023, art. 10 par. 1 lett. h)

[63] Ai sensi dell'art. 3(5) FiDA, si definisce *data holder* "un ente finanziario diverso da un prestatore di servizi di informazione sui conti che raccoglie, conserva e altrimenti tratta i dati di cui all'articolo 2, paragrafo 1;"

[64] Ai sensi dell'art. 3 (6) FiDA, si definisce *data user* "una delle entità di cui all'articolo 2, paragrafo 2, che, previa autorizzazione di un cliente, ha accesso legittimo ai dati del cliente di cui all'articolo 2, paragrafo 1;"

[65] *Ibid*., Considerando n. 2

[66] G. Colangelo, *Open Banking e Open Finance: sfide, opportunità e rischi per la regolazione*. In "*Dall'Open Banking all'Open Finance. Profili di diritto dell'economia*", a cure di V. Falce e U. Morera, G. Giappichelli, 2024, Torino, p.62

Malgrado ciò, come inizialmente accennato, la proposta ha incontrato svariate resistenze da parte sia dell'industria bancaria che di alcuni Stati membri. Le critiche si sono concentrate non solo sugli elevati costi di implementazione e sui dubbi circa la sostenibilità economica del modello proposto, ma anche sulle preoccupazioni legate alla protezione dei dati personali. In particolare, secondo quanto emerso da una dichiarazione congiunta di sei associazioni di categoria rappresentative del settore bancario, assicurativo e della gestione patrimoniale [(67)], il testo della proposta di regolamento non valutava adeguatamente il rapporto tra i costi previsti e la reale domanda di mercato dei clienti[68]. Se da un lato l'introduzione di un modello di accesso ai dati a pagamento avrebbe potuto correggere gli squilibri tra i *data holders* e i *data users*, dall'altro rischiava di disincentivare gli operatori meno strutturati, favorendo un ritorno a modalità operative alternative a quelle digitali e, di conseguenza, frenando anziché accelerando l'evoluzione dell'Open Finance. A queste perplessità si sono sommate, poi, serie preoccupazioni in materia di privacy, principalmente legate al rischio di un'eccessiva concentrazione del controllo dei dati nelle mani di pochi grandi attori, con potenziali effetti distorsivi sulla concorrenza e sulla neutralità del mercato.

Nella realtà dei fatti, però, la ragione che ha portato gli Stati membri a rinviare l'adozione del FiDA sembra risiedere nella mancanza di evidenze consolidate circa l'effettiva utilità di garantire un accesso così ampio e profondo ai dati finanziari.

Tuttavia, l'interesse crescente verso i modelli di Open Finance mostra come l'estensione della condivisione dei dati non rappresenti solo un'opportunità per la personalizzazione dei servizi, ma anche un'occasione strategica per le terze parti, che potrebbero beneficiare dalla definizione di un quadro normativo più chiaro, coerente e flessibile.

Sebbene il FiDA non abbia trovato ancora piena attuazione, è ragionevole ipotizzare che il tema dell'accesso ai dati finanziari tornerà al centro del dibattito normativo nei prossimi anni, con un focus sempre più orientato a bilanciare innovazione, concorrenza e tutela dei consumatori.

A questo punto è doveroso precisare che questo scenario, per quanto ancora in fase evolutiva, solleva inevitabilmente sfide in materia di governance, compliance e gestione dei rischi, specialmente in un contesto in cui l'esternalizzazione di funzioni e servizi si va facendo sempre più centrale per gli operatori di mercato.

---

[67] Le sei associazioni di settore che hanno condotto alla bocciatura della proposta di Regolamento sull'accesso ai dati finanziari sono le seguenti: Association for Financial Markets in Europe (AFME), European Association of Cooperative Banks (EACB), European Banking Federation (EBF), European Fund and Asset Management Association (EFAMA), European Savings and Retail Banking Group (ESBG), Insurance Europe.

[68] *Joint Statement – Financial Data Sharing: Finding a sound approach for an effective Open Finance Framework*, https://www.wsbi-esbg.org/wp-content/uploads/2024/12/Final_Joint-Statement-FiDA_03.12.24_v3_clean.pdf, Brussel, 9 December 2024

1.3 L'esternalizzazione come problema di governance e compliance

La digitalizzazione del settore bancario, accelerata dall'imminente entrata in vigore della Direttiva (UE) 2015/2366, ha favorito l'integrazione progressiva dei Fornitori di Terze Parti (o TPP) all'interno del sistema finanziario europeo.

Come osservato nei precedenti paragrafi, i progressi tecnologici hanno modificato radicalmente le modalità di accesso ai dati bancari dei clienti, imponendo ai prestatori di servizi di pagamento (PSP) l'adozione di meccanismi di autenticazione più stringenti e di standard tecnici più elevati. Tuttavia, l'apertura obbligatoria dei dati bancari a soggetti terzi ha fin da subito sollevato rilevanti questioni di governance e conformità normativa, soprattutto con riferimento alla supervisione delle informazioni finanziarie condivise e all'attribuzione della responsabilità in caso di abusi o violazioni.

In questo contesto, il legislatore si è trovato a dover rispondere a una questione di fondamentale rilevanza: l'esternalizzazione ai TPP rappresenta una leva di innovazione o una potenziale minaccia per la stabilità e la sicurezza del sistema bancario?

Per poter rispondere a questo interrogativo, però, è prima opportuno chiarire che il concetto di esternalizzazione può riguardare sia la delega di servizi ICT in senso stretto (*outsourcing* tecnologico), sia il trasferimento del controllo operativo sui dati finanziari dei clienti verso soggetti terzi (*data sharing*). Nel primo caso, le banche fanno ricorso a soluzioni come il *cloud computing* per gestire i dati in tempo reale e scalabile o all'affidamento a terzi della gestione infrastrutturale, con lo scopo di ridurre i costi ed aumentare l'efficienza operativa[69]. Nel secondo, invece, si assiste a un vero e proprio trasferimento del rischio, in quanto l'accesso ai dati è concesso a soggetti esterni, con implicazioni dirette in termini di responsabilità e sicurezza.

Alla luce di queste considerazioni, e in linea con l'obiettivo di ricerca della presente tesi, l'analisi si concentrerà prioritariamente su questa seconda forma di esternalizzazione – ossia il trasferimento del controllo operativo sui dati ai TPP – senza però tralasciare i profili rilevanti legati all'*outsourcing ICT*, laddove funzionali a comprendere le sfide di compliance e sicurezza legate all'accesso ai dati.

In questo quadro di profondo mutamento, il settore bancario – e in particolare quello dei servizi di pagamento – è divenuto terreno di sperimentazione avanzata, in cui nuovi attori si sono progressivamente affermati, modificando l'assetto tradizionale della catena del valore. Tuttavia, la frammentazione del controllo sui dati e la moltiplicazione dei soggetti coinvolti hanno prodotto un'asimmetria regolamentare di fondo, in quanto i TPP, pur accedendo a dati sensibili e svolgendo funzioni chiave non sono stati inizialmente sottoposti agli stessi standard di vigilanza delle banche, né agli stessi obblighi patrimoniali o organizzativi. Quest'impossibilità di esercitare alcuna forma di

[69] P. Lucantoni, C. Villani, "*La gestione e supervisione dei rischi ICT e di sicurezza nelle attività finanziarie esternalizzate tra DORA e CRD VI*", https://www.dirittobancario.it/art/la-gestione-e-supervisione-dei-rischi-ict-e-di-sicurezza-nelle-attivita-finanziarie-esternalizzate-tra-dora-e-crd-iv/, Dirittobancario, Gennaio 2025

supervisione e controllo sull'operato dei TPP, sebbene abbia inciso notevolmente sulla capacità delle banche di assicurare ai consumatori il mantenimento di elevati livelli di compliance e sicurezza[70], non è del tutto casuale, bensì coerente con il ruolo attribuito ai TPP all'interno dell'ecosistema finanziario.

L'impossibilità di detenere fondi dei clienti ha permesso a tali operatori di ottenere l'autorizzazione ad operare in modo relativamente più agevolato rispetto agli istituti finanziari tradizionali, i quali, invece, erano soggetti all'applicazione di requisiti stringenti tanto in materia di capitale iniziale minimo, quanto di responsabilità.

In particolare, la PSD2 all'art. 5 prevedeva per i PISP requisiti di autorizzazione simili a quelli degli istituti di pagamento, con alcune differenze significative in merito alla richiesta di un capitale iniziale inferiore e all'obbligo di possedere un'assicurazione sulla responsabilità civile professionale volta a garantire la copertura di eventuali danni derivanti da operazioni non autorizzate[71]. Tali agevolazioni erano, poi, ancora più evidenti nei confronti dei prestatori di servizi di informazione sui conti (*AISP*), i quali, non essendo chiamati ad eseguire transazioni bensì a svolgere una funzione meramente informativa, erano tra l'altro esonerati dall'obbligo di dotarsi di un capitale minimo iniziale e non erano tenuti ad applicare le regole in tema di tutela dei fondi del cliente[72].

Tuttavia, l'evoluzione dell'economia digitale e il crescente valore attribuito ai dati hanno reso il ruolo originariamente accessorio degli AISP sempre più centrale, ponendo in evidenza la necessità di una revisione del quadro normativo e di una maggiore convergenza tra i livelli di responsabilità dei diversi soggetti.

Allo stesso tempo, con riguardo alle condizioni giuridiche alle quali i prestatori di servizi di disposizione di ordine di pagamento e di informazione sui conti erano soggetti, la PSD2 ha esplicitamente stabilito che l'accesso ai conti da parte dei TPP costituiva un diritto per l'utente dei servizi di pagamento, e che le banche non possono opporsi a meno che non vi siano "*motivi obiettivamente giustificati e debitamente comprovati connessi all'accesso non autorizzato o fraudolento al conto di pagamento da parte del prestatore di servizi di informazione sui conti o del prestatore di servizi di disposizione di ordini di pagamento*" (art.68 (5) PSD2)[73]. Come sottolineato

---

[70] Ibid., pp. 15-17

[71] Nello specifico, ai sensi dell'art. 7 par.1 lett. b) della Direttiva (UE) 2015/2366 è stabilito che: "*quando l'istituto di pagamento presta i servizi di pagamento di cui al punto 7 allegato I, il suo capitale non è mai inferiore a 50 000 EUR*". Invece, per quanto concerne la richiesta del possesso dell'assicurazione per responsabilità civile professionale, ai sensi dell'art. 5 par. 2 PSD2, era stabilito che: "*alle imprese che presentano domanda di autorizzazione per prestare i servizi di pagamento di cui al punto 7 dell'allegato I, gli Stati membri impongono, quale condizione per l'autorizzazione, di possedere un'assicurazione per la responsabilità civile professionale valida in tutti i territori in cui offrono i loro servizi, o altra analoga garanzia per la responsabilità a copertura delle responsabilità di cui agli articoli 73, 89, 90 e 92*".

[72] Per ulteriori dettagli in merito alle esenzioni concesse agli AISP si veda l'art. 33 par.1 PSD2

[73] *Direttiva 2015/2366 del Parlamento europeo e del Consiglio, del 15 novembre 2015, concernente il servizio di pagamento nel mercato interno, che modifica le direttive 2002/65/EC, 2009/110/EC e 2013/36/EU e il regolamento n. 1093/2010 e che abroga la direttiva 2007/64/EC*, art. 68 paragrafo 5: "*Un prestatore di servizi di pagamento di*

dall'*European Data Protection Board*, ciò implica che l'utente debba potersi affidare ai TPP in piena sicurezza e trasparenza[74].

Nell'ottica di rafforzare questo diritto, la direttiva ha introdotto una serie di disposizioni finalizzate a regolamentare i rapporti tra gli intermediari rispetto all'esecuzione di operazioni non autorizzate od eseguite in maniera inesatta. Nello specifico, si tratta di un sistema di responsabilità condivisa in cui, nel caso di operazioni non autorizzate svolte da un PISP – ai sensi dell'art. 73, paragrafo 2, PSD2 –, la responsabilità immediata resta in capo alla banca presso cui è radicato il conto, che provvede immediatamente al rimborso dell'importo dell'operazione non autorizzata al cliente. Tuttavia, il PSP di radicamento del conto nell'esatto momento in cui corrisponde il rimborso acquisisce il diritto di rivalersi sul TPP per l'importo corrispondente alla somma risarcita, spetta poi a quest'ultimo l'onere probatorio[75]. In altri termini, l'onere "*di dimostrare che, nell'ambito delle sue competenze, l'operazione di pagamento era stata autenticata, correttamente registrata e non aveva subito […] inconvenienti riguardanti il servizio di pagamento del quale era stato incaricato*" pende sul PISP, che solo dimostrando la liceità dell'operazione è in grado di liberarsi della responsabilità facendola ricadere definitivamente sull'istituto bancario presso cui era radicato il conto[76].

A tal proposito, per poter gestire i rischi connessi alla condivisione dei dati con terze parti ed assicurarsi la fiducia della clientela, le banche hanno reagito stipulando accordi contrattuali dettagliati (*Service Level Agreement*, SLA), conducendo "*operazioni di due diligence sui TPP in modo tale da*

---

radicamento del conto può rifiutare l'accesso a un conto di pagamento a un prestatore di servizi di informazione sui conti o a un prestatore di servizi di disposizione di ordine di pagamento per motivi obiettivamente giustificati e debitamente comprovati connessi all'accesso non autorizzato o fraudolento al conto di pagamento da parte di tale prestatore di servizi di informazione sui conti o del prestatore di servizi di disposizione di ordine di pagamento, compreso un ordine di pagamento non autorizzato o fraudolento. In tali casi il prestatore di servizi di pagamento di radicamento del conto, con le modalità convenute, informa il pagatore del rifiuto di accesso al conto di pagamento e dei relativi motivi. Tale informazione, ove possibile, è fornita al pagatore prima che l'accesso sia rifiutato o, al più tardi, immediatamente dopo, salvo qualora tale informazione non possa essere fornita per motivi di sicurezza obiettivamente giustificati o sia vietata da altre pertinenti disposizioni di diritto dell'Unione o nazionale.

Il prestatore di servizi di pagamento di radicamento del conto consente l'accesso al conto di pagamento una volta cessati i motivi che hanno determinato il rifiuto."

[74] European Data Protection Board, "*Linee guida 06/2020 sull'interazione tra la seconda direttiva sui servizi di pagamento e il GDPR*", Dicembre 2020, p.8

[75] F. Marasà, "*Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR*", cit., p.644

[76] *Direttiva 2015/2366 del Parlamento europeo e del Consiglio, del 15 novembre 2015, concernente il servizio di pagamento nel mercato interno, che modifica le direttive 2002/65/EC, 2009/110/EC e 2013/36/EU e il regolamento n. 1093/2010 e che abroga la direttiva 2007/64/EC*, art. 73 paragrafo 2: "*Se l'operazione di pagamento è disposta mediante un prestatore di servizi di disposizione di ordine di pagamento, il prestatore di servizi di pagamento di radicamento del conto rimborsa immediatamente, e in ogni caso entro la fine della giornata operativa successiva*, *l'importo dell'operazione di pagamento non autorizzata e, se del caso, riporta il conto di pagamento addebitato nello stato in cui si sarebbe trovato se l'operazione di pagamento non autorizzata non avesse avuto luogo.*

Se il prestatore di servizi di disposizione di ordine di pagamento è responsabile dell'operazione di pagamento non autorizzata, risarcisce immediatamente il prestatore di servizi di pagamento di radicamento del conto su richiesta di quest'ultimo per le perdite subite o gli importi pagati in conseguenza del rimborso al pagatore, compreso l'importo dell'operazione di pagamento non autorizzata. Conformemente all'articolo 72, paragrafo 1, spetta al prestatore di servizi di disposizione di ordine di pagamento dimostrare che, nell'ambito delle sue competenze, l'operazione di pagamento è stata autenticata, correttamente registrata e non ha subito le conseguenze di guasti tecnici o altri inconvenienti riguardanti il servizio di pagamento del quale è incaricato."

poter valutare come questi effettuavano i loro controlli sui dati, oltre ad impegnarsi in un processo di revisione etica per poter comprendere le modalità e finalità di utilizzo dei dati" [77].

Considerato quanto sopra, l'aumento dell'interconnessione tra attori eterogenei – banche e TPP – segnala l'avvio di una nuova fase evolutiva dell'ecosistema finanziario, in cui la disponibilità e il trattamento dei dati non costituiscono soltanto un'opportunità di crescita e innovazione, ma anche una potenziale fonte di vulnerabilità sistemica.

Alla luce di tali dinamiche, i rischi legati alla sicurezza informatica e alla resilienza operativa acquisiscono una centralità inedita, ponendo nuove sfide di governance e richiedendo soluzioni tecniche e normative sempre più avanzate.

È proprio a partire da queste trasformazioni che si rende necessario approfondire alcune direttrici critiche del nuovo assetto regolamentare operativo, a cominciare dall'ampliamento della superficie esposta agli attacchi *cyber*, conseguenza diretta dell'architettura aperta dell'Open Banking. Da qui, il discorso si estende all'introduzione di un nuovo approccio sistemico al rischio ICT, reso evidente dal Regolamento DORA, fino ad abbracciare ambiti innovativi come le cripto-attività, disciplinate dal MiCAR. Contestualmente, si pone l'attenzione anche sulle rilevanti criticità nel bilanciamento tra esigenze di innovazione e tutela dei dati personali, in particolare sul delicato rapporto tra PSD2 e GDPR.

1.3.1 - Le nuove sfide della sicurezza informatica nell'ecosistema dell'Open Banking

A partire dalle dinamiche precedentemente descritte, emerge con chiarezza come il progressivo aumento dell'interconnessione tra banche e TPP – reso possibile dall'architettura aperta dell'Open Banking – abbia esposto l'intero ecosistema finanziario a nuove vulnerabilità, in particolare sotto il profilo della sicurezza informatica e della protezione delle informazioni sensibili.

La difficoltà nel prevenire usi impropri dei dati finanziari, unita alla crescente sofisticazione delle minacce digitali, ha infatti reso evidente la necessità di rafforzare i presidi normativi e tecnologici a tutela della privacy degli utenti.

Come già anticipato nel § 1.1.3, uno degli strumenti cardine introdotti per regolare l'accesso dei TPP ai dati bancari è rappresentato dalle API, progettate per superare pratiche rischiose come lo *screen scraping* e per garantire l'applicazione di standard di sicurezza avanzati, basati sull'autenticazione forte e sulla tracciabilità delle operazioni.

In questa sede, però, è opportuno soffermarsi non tanto sul funzionamento tecnico delle API, quanto piuttosto sul loro ruolo nella gestione operativa del rischio, evidenziando come la loro

[77]Basel Committee on Banking Supervision,", Bank for International Settlements, May 2024, p. 26

implementazione – seppur fondamentale per rafforzare la protezione dei dati e rendere consapevole il consumatore circa le proprie scelte – non sia bastata ad arginare le criticità sistemiche derivanti dall'esternalizzazione delle funzioni sensibili ai TPP[78].

In questo contesto è bene tener presente anche che, nonostante i progressi fatti grazie alla PSD2 e agli standard tecnici regolamentari dell'EBA (RTS) – che hanno attribuito un effettivo potere decisionale ai titolari dei conti, ridimensionando il tradizionale ruolo di *gatekeeper* delle banche –, la persistente assenza di meccanismi efficaci di monitoraggio e controllo sulla gestione dei dati da parte dei TPP ha continuato a generare opacità, incertezza e rischi, sia per gli intermediari finanziari che per i consumatori.

Un caso emblematico che ha portato alla luce tali criticità è rappresentato da Plaid, una delle più note società fintech nell'ambito dell'Open Banking. Nello specifico, la società è stata oggetto nel 2022 di una *class action* per aver raccolto ed elaborato dati finanziari eccedenti rispetto a quelli per i quali aveva ottenuto l'esplicito consenso dagli utenti, nonché per aver acquisito le credenziali di accesso mediante interfacce grafiche ingannevoli, volutamente simili a quelle delle banche di riferimento, senza comunicare preventivamente agli utenti che non stavano interagendo con la loro banca[79]. Sebbene il caso si sia verificato negli Stati Uniti, ha suscitato ampia risonanza anche in Europa, dove la mancanza di standard tecnici armonizzati e la possibilità per i TPP di riutilizzare i dati per finalità non previste dalla PSD2 avevano già messo in discussione la solidità dell'intero ecosistema finanziario.

In risposta a queste preoccupazioni – acuite dal timore di un ulteriore indebolimento della fiducia degli utenti e degli operatori – il legislatore europeo, nella proposta di PSD3, ha promosso un rafforzamento delle misure di sicurezza, introducendo requisiti più stringenti e presidi di trasparenza più articolati nei processi autorizzativi e di pagamento, pur mantenendosi fedele al modello di condivisione dei dati promosso dalla PSD2[80].

Tuttavia, tali misure contenute nella proposta del *Financial Data Package* – malgrado siano ancora in fase di approvazione – appaiono già oggi non pienamente idonee a colmare le vulnerabilità strutturali insite nell'architettura dell'Open Banking, soprattutto in termini di sicurezza informatica.

Alla luce di ciò, per valutare con maggiore consapevolezza la portata dei rischi connessi all'esternalizzazione dei dati ai TPP, è necessario osservare che alla perdita di controllo diretto sulle

---

[78] L. Brodsky, L. Oakes, "*Data sharing and open banking*", https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking, McKinsey on Payment, July 2017

[79] N. Hanson, "*Judge approves settlement ordering Plaid to pay $58 million for selling customer data*", https://www.courthousenews.com/judge-approves-settlement-ordering-plaid-to-pay-58-million-for-selling-consumer-data/, Courthouse News Service, July 2022

[80] Gedea Data Service, "*La PSD3 e il futuro dell'Open Banking*", https://www.gedeadataservices.it/la-psd3-e-il-futuro-dellopen-banking/, Digital payment, Maggio 2024

informazioni sensibili da parte delle banche si affiancano minacce informatiche sistemiche, strettamente legate alla crescente interconnessione tra piattaforme bancarie e soggetti terzi.

Di fatto la rapida integrazione dei TPP nell'ecosistema finanziario ha ampliato in modo significativo la superficie esposta agli attacchi *cyber*, estendendo i punti di vulnerabilità ben oltre l'infrastruttura bancaria tradizionale e coinvolgendo una pluralità di attori spesso non soggetti ai medesimi requisiti di sicurezza[81]. Di conseguenza, si è registrato un aumento generalizzato dei rischi di accessi non autorizzati, perdite di dati e violazioni della privacy, sollevando interrogativi sempre più urgenti in termini di stabilità, resilienza e conformità dell'intero ecosistema finanziario.

In ragione di ciò, specialmente nell'ultimo decennio, un numero crescente di istituti bancari tradizionali si è trovato nella condizione di dover adottare nuove tecnologie per poter competere con i nuovi operatori bancari e non bancari (c.d. *incumbents*), o persino di esternalizzare a questi ultimi la gestione di determinati servizi perché ritenuti troppo complessi.

Tuttavia, se da un lato l'affidamento dei servizi ai TPP ha consentito alle banche di contenere gli ingenti costi legati allo sviluppo delle infrastrutture e delle tecnologie necessarie per stare al passo con la digitalizzazione del settore bancario, dall'altro ha determinato una maggiore esposizione ai rischi operativi oltre che una maggiore vulnerabilità sul fronte della sicurezza informatica[82]. In particolare, secondo quanto precisato dall*'European Union Agency for Cybersecurity* (ENISA), tra le minacce *cyber* più rilevanti per la sicurezza e trasparenza delle transazioni figurano gli attacchi di tipo *Distributed Denial of Service* (*DDoS*), che solo nel 2024 hanno rappresentato il 12 % del totale degli attacchi subiti dal settore bancario[83]. Tali attacchi, spesso resi possibili dalla presenza di numerose falle nella sicurezza del sistema, mirano a sovraccaricare i servizi di rete attraverso una molteplicità di fonti, provocando una distruzione accidentale o specifica dei dati nel tentativo di renderli inutilizzabili agli utenti legittimi[84].

In parallelo a questi rischi legati alla disponibilità dei dati, le banche hanno dovuto confrontarsi anche con la diffusione sempre più frequente di attacchi *man-in-the-middle* (MITM) e di frodi basate su tecniche di *spoofing*[85].

Mentre nel primo caso si tratta di rischi legati alla presenza di un attore malevolo che intercetta e manipola le comunicazioni tra l'utente e il servizio finanziario, alterando o sottraendo informazioni sensibili, nel secondo, invece, i cybercriminali si fingono entità legittime – come banche o TPP autorizzati – ingannando gli utenti, al fine di carpire le credenziali di accesso o i dati finanziari.

---

[81] Banca d'Italia, "*PSD2 e Open Banking: nuovi modelli di business e rischi emergenti*", cit., p.22
[82] Basel Committee on Banking Supervision, "*Digitalisation of finance*", cit., pp. 17-19
[83] ENISA, "*ENISA Threat Landscape 2024*", September 2024, p. 15
[84] Microsoft, "Cos'è un attacco DDoS?", https://www.microsoft.com/it-it/security/business/security-101/what-is-a-ddos-attack, Microsoft Security,
[85] Banca d'Italia, "*PSD2 e Open Banking: nuovi modelli di business e rischi emergenti*", cit., p.23

A tal proposito, il caso precedentemente citato di Plaid è chiarificatore, poiché mostra come la simulazione di interfacce bancarie possa indurre in errore gli utenti, spingendoli a fornire inconsapevolmente informazioni sensibili.

Queste criticità, unite alla frequente violazione delle interfacce utente sviluppate dalle banche, hanno reso nota l'urgenza di progettare API conformi alle *best practice* di sviluppo dei *software*, fondate su meccanismi di autenticazione ancora più rafforzati per prevenire eventuali intrusioni o frodi informatiche. Tuttavia, come sostenuto anche nel paragrafo 1.1.3, malgrado le API rappresentino uno degli strumenti cardine a disposizione delle banche, la carenza di incentivi concreti per lo sviluppo di tali interfacce hanno rallentato notevolmente il processo di integrazione del mercato avviato con la Direttiva (UE) 2015/2366.

In considerazione di quanto sopra, secondo alcune indagini di mercato condotte da Tink[86], al momento dell'entrata in vigore della suddetta normativa solo il 69% delle API bancarie risultava disponibile e adeguatamente efficiente[87]. Un dato, questo, che testimonia non solo la difficoltà del settore finanziario a adeguarsi agli standard tecnologici richiesti, ma anche una resistenza strategica delle banche, intenzionate a preservare la propria posizione dominante e ad ostacolare i TPP.

Tenendo presente questa condizione allarmante, l'EBA, pur continuando a promuovere lo sviluppo e la diffusione delle API, ha compreso la necessità di instaurare una collaborazione più strutturata con gli istituti finanziari e con le terze parti, affinché i servizi offerti da queste ultime potessero soddisfare gli standard richiesti[88]. Tuttavia, se da un lato l'iniziale flessibilità adottata dall'Autorità Bancaria Europea ha contribuito a scongiurare un possibile scenario di stallo nell'attuazione della PSD2 – evitando così il fallimento di un processo che prometteva innumerevoli benefici per i consumatori –, dall'altro lato ha sollevato una significativa questione di governance.

Infatti, la sicurezza delle API bancarie non poteva più essere considerata una responsabilità esclusiva degli istituti bancari, coinvolgendo sempre più anche i Third Party Providers, i quali spesso non disponevano delle competenze né delle risorse necessarie per garantire un adeguato livello di protezione dei dati.

Oltre all'assenza della menzionata conformità tecnologica, anche l'incapacità degli standard tecnici regolamentari (RTS) di fornire "specifiche dettagliate", chiare e uniformi tra i vari Stati membri ha creato le condizioni tali per cui un numero sempre più ampio di operatori del sistema finanziario

[86] Tink è stata fondata nel 2012 con l'obiettivo di cambiare in meglio il settore bancario. Nel 2022 è diventata parte di Visa, e ad oggi rappresenta una delle piattaforme di open banking più solide d'Europa, con la connettività più ampia e profonda e servizi potenti che creano valore dai dati finanziari. Tale piattaforma offre una serie di strumenti che consentono a chiunque, dalle grandi banche e fintech alle startup, di costruire il futuro dei servizi finanziari in tutta Europa.

[87] Tink, "*Could the poor readiness of APIs put the success of PSD2 in jeopardy*?", https://tink.com/blog/open-banking/status-of-psd2-production-apis/, July 2019

[88] Tink, "*Zero PSD2 APIs are compliant with just weeks left before the deadline*", https://tink.com/blog/open-banking/psd2-status-update/, August 2019

migrino verso ambienti API non conformi, generando disagi per i milioni di utenti che godevano dei loro servizi.

In questo contesto, l'EBA, coadiuvata dalle altre Autorità europee di vigilanza (ESAs), ha rivestito un ruolo chiave introducendo una serie di linee guida specifiche volte a mitigare sia "*i rischi di perdita dovuti a violazione della riservatezza, mancata integrità, inadeguatezza o indisponibilità di sistemi e dati […], [sia] i rischi per la sicurezza derivanti da processi interni inadeguati o da eventi esterni, tra cui attacchi informatici o sicurezza fisica inadeguata*" (EBA, 2019)[89]. In sostanza, lo scopo connesso alla richiesta fatta alle banche e ai TPP di applicare tali misure era quello di mitigare i rischi ICT legati alla condivisione dei dati all'interno del sistema finanziario, come pure di limitare la dipendenza delle banche dalla fornitura di servizi ICT di terze parti.

Nello specifico, tra le principali misure raccomandate si evidenzia:

i. l'adozione di protocolli di sicurezza avanzati per garantire un accesso autenticato e tracciabile, basato sul principio di minimizzazione dei dati, così da prevenire eventuali accessi ingiustificati a grandi quantità di dati sensibili dell'utente (*Payment Service User*)[90];
ii. l'implementazione di strumenti di crittografia *end-to-end* per proteggere la trasmissione delle informazioni tra banche e TPP, parimenti alla riduzione dell'esposizione delle chiavi API sensibili per evitare tentativi di frodi o accessi non autorizzati[91];
iii. lo sviluppo di strumenti necessari per garantire ai *Payment Service User* la comprensione dei rischi insiti al fornire sia il proprio consenso ai prestatori di servizi di pagamento, sia ulteriori dati non necessari per la prestazione nel corso della stessa.

A prescindere dall'importanza di queste raccomandazioni, però, la loro natura non vincolante e l'endemica mancanza di un quadro normativo armonizzato a livello europeo hanno rivelato la necessità di un'azione più incisiva in materia di resilienza operativa digitale. Proprio in tale direzione si inserisce il Regolamento DORA, oggetto di analisi nel paragrafo successivo.

1.3.2 - Il *Digital Operational Resilience Act* (*DORA*): verso una resilienza digitale strutturale

L'aumento della complessità del sistema finanziario digitale, unito alle fragilità emerse dal modello di Open Banking – in primis la frammentazione tecnologica, l'eterogeneità delle API bancarie, la mancanza di standard comuni e l'asimmetria regolamentare tra istituti e TPP – hanno messo in evidenza i limiti di un impianto normativo basato principalmente su strumenti di "*soft law*[92]", come

[89] Definition of ICT and security risk from the *EBA Guidelines on ICT and security risk management* of 29 November 2019 (EBA/GL/2019/04)
[90] *Final Report EBA Guidelines on ICT and security risk management* of 29 November 2019 (EBA/GL/2019/04), p.19
[91] Ibid., pp. 20-22
[92] Secondo quanto riportato dal vocabolario della Treccani per strumenti di *soft law*, nel senso giuridico della parola, si intende un sistema di regole che si connota essenzialmente per il fatto di non essere caratterizzato dai tratti forse più tipici

le linee guida dell'EBA o gli RTS. Sebbene tali strumenti abbiano concorso alla definizione dei principi generali in materia di sicurezza e stabilità del sistema, non si sono rivelati sufficienti a garantire un livello uniforme di resilienza operativa e di accountability condivisa nel trattamento dei dati. A sua volta, anche la crescente interdipendenza tra gli attori del sistema – già approfondita nel §1.3.1 – e la molteplicità dei canali di accesso ai dati sensibili da parte dei soggetti terzi, spesso non soggetti agli stessi obblighi degli istituti bancari, hanno spinto il legislatore a riconoscere la necessità di un approccio normativo più organico, coordinato e vincolante.

In tale contesto si inserisce il *Digital Operational Resilience Act* (DORA), pensato per rivoluzionare la governance del rischio ICT in un'economia sempre più fondata sulla condivisione e circolazione dei dati (*data sharing*).

Ad ogni modo, l'adozione formale del regolamento DORA, datata 16 gennaio 2023, ha rappresentato fin da subito un punto di svolta, introducendo standard operativi comuni e pratiche concrete per assicurare sia la continuità dei servizi finanziari anche in caso di gravi interruzioni operative digitali che la sicurezza delle tecnologie ICT di competenza delle tre ESAs[93].

A dimostrazione della volontà del legislatore di assicurare un impianto normativo efficace ed equo, già all'art. 4 il Regolamento stabilisce esplicitamente che "*le misure di resilienza operativa digitale devono essere commisurate al profilo di rischio, alle dimensioni, alla natura e portata delle attività di ciascun soggetto finanziario coinvolto*"[94].

Nel tentativo di armonizzare il quadro europeo in materia di gestione del rischio ICT, il DORA riunisce coerentemente in un unico atto tutte le disposizioni relative al rischio digitale da *"applicare alle diverse tipologie di entità finanziarie e fornitori di terzi di servizi ICT*", inclusi gli operatori

---

e ricorrenti della norma giuridica: l'essere parte di un ordinamento giuridico e l'essere dotata di una qualche forza vincolante o precettiva. A differenza del termine "*hard law*", comunemente impiegato con riferimento a obblighi giuridici vincolanti per le parti coinvolte, solitamente con il termine "*soft law*" si indicano accordi, raccomandazioni e linee guida non giuridicamente vincolanti.

[93] Si tratta di un'entrata in vigore formale, poiché il regolamento DORA impone alle imprese finanziarie e ai loro fornitori critici di servizi ICT di rispettare una serie di requisiti di sicurezza informatica e di resilienza entro il 17 gennaio 2025. Per ulteriori dettagli si veda: ESMA, "*Digital Operational Resilience Act (DORA)*", https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora#:~:text=The%20Digital%20Operational%20Resilience%20Act,in%20the%20remit%20of%20ESMA.

[94] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, sulla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (Testo rilevante ai fini del SEE), art. 4: "Gli enti finanziari attuano le norme stabilite nel capo II nel rispetto del principio di proporzionalità, tenendo conto delle loro dimensioni e del loro profilo di rischio complessivo, nonché della natura, della portata e della complessità dei loro servizi, attività e operazioni. Inoltre, l'applicazione da parte degli enti finanziari dei capi III, IV e V, sezione I, è proporzionata alle loro dimensioni e al loro profilo di rischio complessivo, nonché alla natura, alla portata e alla complessità dei loro servizi, attività e operazioni, come specificamente previsto nelle norme pertinenti di tali capi. Le autorità competenti prendono in considerazione l'applicazione del principio di proporzionalità da parte delle entità finanziarie quando esaminano la coerenza del quadro di gestione del rischio ICT sulla base delle relazioni presentate su richiesta delle autorità competenti ai sensi dell'articolo 6, paragrafo 5, e dell'articolo 16, paragrafo 2.

coinvolti nella gestione e trasmissione dei dati finanziari condivisi all'interno del sistema Open Banking, quali gli aggregatori di account e i cloud providers[95].

In questo senso, tale regolamento si propone non solo di rafforzare la resilienza operativa dell'interno ecosistema, ma anche di correggere l'asimmetria regolamentare persistente tra banche e TPP, che aveva caratterizzato l'assetto introdotto dalla PSD2.

Quindi, il DORA, integrando il modello di condivisione dei dati promosso dalla PSD2, estende così la responsabilità e la vigilanza anche a soggetti terzi digitali, imponendo obblighi proporzionati al tipo di attività e alla rilevanza sistemica nel trattamento dei dati. In altri termini, rafforza la cornice della responsabilità condivisa nella gestione del rischio ICT e riconosce il ruolo critico anche di soggetti che non rientravano pienamente nel perimetro normativo della PSD2.

Alla luce di quanto sopra, i due strumenti risultano complementari: mentre la PSD2 disciplina prevalentemente il "chi accede ai dati" e "come", il DORA estende l'orizzonte regolamentare imponendo che l'intero ecosistema sia strutturalmente in grado di prevenire, resistere e reagire agli incidenti ICT, indipendentemente dall'attore coinvolto.

La presenza nel perimetro normativo sia di attori tradizionali sia di nuovi operatori fintech – specialmente di quelli responsabili della gestione di funzioni critiche e del trattamento di grandi volumi di informazioni sensibili – ha reso indispensabile l'impiego di un approccio qualitativo, oltre che quantitativo, nel corso del processo di valutazione dei rischi ICT[96]. A tal proposito, è opportuno sottolineare che, proprio a seguito di quest'attenzione alla protezione delle informazioni condivise, e alla responsabilizzazione degli attori digitali coinvolti nella catena del trattamento dei dati, il legislatore ha deciso di articolare il DORA su cinque pilastri fondamentali: (i) gestione interna del rischio ICT; (ii) segnalazione sistemica degli incidenti; (iii) implementazione di test di resilienza operativa basati su scenari reali (*Threat-Led Penetration Testing*); (iv) supervisione rafforzata sui fornitori di servizi ICT, con particolare riguardo a quelli "critici" per la continuità operativa del settore bancario; (v) accordi di condivisione delle informazioni[97].

Una delle principali novità introdotte con il regolamento DORA si riferisce alla valutazione sistemica del rischio derivante dalla catena di fornitura ICT e la relativa supervisione dei fornitori considerati

[95] EIOPA, "*Digital Operational Resilience Act (DORA)*", https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en, 2024

[96] *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational 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, considerando 12

[97] Cerved, "Regolamento DORA: il rischio della fornitura", https://www.cerved.com/ai-innovation/a/tech/regolamento-dora-il-rischio-della-fornitura, Maggio 2025

"*critici*", ossia quegli operatori esterni – spesso estranei al perimetro regolamentare della PSD2 – che risultano essenziali per la continuità operativa delle infrastrutture bancarie[98].

In particolare, il regolamento all'articolo 31 stabilisce la procedura con cui le Autorità di vigilanza europee (ESAs), con il supporto del Joint Committee e dell'Oversight Forum, designano i fornitori ICT ritenuti critici sulla base di criteri oggettivi e qualificati. Tale rilevanza non si circoscrive unicamente alla fornitura di infrastrutture tecniche, ma riguarda direttamente il ruolo centrale che questi soggetti rivestono nel flusso e nella conservazione dei dati finanziari condivisi tra banche, TPP e utenti. È il caso, ad esempio, di cloud providers, aggregatori di dati o API gateway, il cui malfunzionamento può avere grevi ripercussioni a cascata su migliaia di transazioni o processi di trattamento dei dati in tempo reale.

Proprio in virtù del loro potenziale impatto sulla stabilità del sistema finanziario, il DORA ha previsto un regime specifico di vigilanza rafforzata, affidando alle ESAs – in coordinamento con l'Agenzia dell'Unione europea per la cybersicurezza (ENISA) – il compito di elaborare e aggiornare standard tecnici di riferimento per i fornitori ICT, contribuendo così a rafforzare la sicurezza dei servizi digitali e prevenire eventuali minacce sistemiche[99].

Coerentemente con tale impostazione, il regolamento non si limita a stabilire obblighi generici, bensì introduce presidi puntuali di responsabilizzazione, imponendo obblighi di reportistica, di audit e test periodici anche ai fornitori terzi. Per rendere effettive queste responsabilità, il DORA stabilisce, tra

---

[98] *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational 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, art. 31, par.2: "*The designation referred to in paragraph 1, point (a), shall be based on all of the following criteria in relation to ICT services provided by the ICT third-party service provider:*
(a) the systemic impact on the stability, continuity or quality of the provision of financial services in the event that the relevant ICT third-party service provider would face a large scale operational failure to provide its services, taking into account the number of financial entities and the total value of assets of financial entities to which the relevant ICT third-party service provider provides services;
(b) the systemic character or importance of the financial entities that rely on the relevant ICT third-party service provider, assessed in accordance with the following parameters:
(i) the number of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the respective ICT third-party service provider;
(ii) the interdependence between the G-SIIs or O-SIIs referred to in point (i) and other financial entities, including situations where the G-SIIs or O-SIIs provide financial infrastructure services to other financial entities;
(c) the reliance of financial entities on the services provided by the relevant ICT third-party service provider in relation to critical or important functions of financial entities that ultimately involve the same ICT third-party service provider, irrespective of whether financial entities rely on those services directly or indirectly, through subcontracting arrangements;
(d) the degree of substitutability of the ICT third-party service provider, taking into account the following parameters: (i) the lack of real alternatives, even partial, due to the limited number of ICT third-party service providers active on a specific market, or the market share of the relevant ICT third-party service provider, or the technical complexity or sophistication involved, including in relation to any proprietary technology, or the specific features of the ICT third-party service provider's organisation or activity;
(ii) difficulties in relation to partially or fully migrating the relevant data and workloads from the relevant ICT third party service provider to another ICT third-party service provider, due either to significant financial costs, time or other resources that the migration process may entail, or to increased ICT risk or other operational risks to which the financial entity may be exposed through such migration."

[99] Ibid., Art. 15

l'altro, che i soggetti terzi ICT debbano concorrere all'elaborazione e al costante aggiornamento del registro dei servizi ICT critici forniti, collaborare attivamente e senza costi aggiuntivi con le autorità competenti, nonché garantire un accesso illimitato ai propri dati e sistemi ai fini di audit interni ed ispezioni da parte delle medesime autorità e del Lead Overseer[100].

Al contempo, secondo quanto previsto dall'art. 28 DORA, le entità finanziarie che si avvalgono dei servizi ICT restano, in ogni momento, responsabili della conformità ai requisiti normativi previsti dal regolamento[101]. In parallelo, è posto in capo ai soggetti terzi ICT l'obbligo di segnalare tempestivamente all'ente finanziario qualsiasi variazione nelle condizioni contrattuali che possa compromettere la capacità di adempiere alle proprie funzioni in linea con i livelli di servizio concordati (SLA), fino a giustificare, se del caso, la risoluzione immediata del rapporto[102].

Tali obblighi, seppur amplino in modo significativo il perimetro delle responsabilità e della supervisione, non si estendono indiscriminatamente ad ogni ambito dell'ecosistema finanziario digitale. In particolare, è fondamentale rilevare che il campo di applicazione del DORA esclude alcune attività appartenenti a determinate categorie delle cripto-attività, data "*la natura troppo specifica di tali asset e la loro limitata rilevanza per la resilienza operativa digitale del settore finanziario nel suo complesso*", salvo nei casi in cui tali soggetti operino in qualità di fornitori ICT critici[103]. Da ciò deriva la scelta del legislatore di affiancare al DORA altri atti normativi settoriali, come il *Markets in Crypto-Assets Regulation* (MiCAR[104]), il quale mira a disciplinare con maggiore dettaglio i rischi di natura tecnologica e sistemica legati alla gestione e circolazione di cripto-assets.

In proposito, il MiCAR si inserisce in questo disegno normativo come un ulteriore tassello volto a creare le condizioni per un trattamento più uniforme ed equo non solo degli operatori operanti nel campo delle cripto-attività, ma anche per coloro che esercitano attività esterne al perimetro delle banche tradizionali. Pur avendo come obiettivo primario quello di sostenere lo sviluppo di modelli di business legati alle tecnologie a registro distribuito (DLT) e della blockchain, tale regolamento comunque affronta tematiche analoghe a quelle del DORA sul piano della governance del rischio,

---

[100] Ibid., Art. 30, par. 2

[101] Ibid., Art. 28, par. 1, lett. a): "Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework as referred to in Article 6(1), and in accordance with the following principles:
(a) financial entities that have in place contractual arrangements for the use of ICT services to run their business operations shall, at all times, remain fully responsible for compliance with, and the discharge of, all obligations under this Regulation and applicable financial services law"

[102] Ibid., Art. 30, par. 3

[103] Cyberlys, "*Regolamento DORA: cos'è, a chi si applica e quali novità introduce*", https://www.cyberlys.it/blog/regolamento-dora/#:~:text=Regolamento%20DORA:%20testo%20e%20principali,essere%20consultato%20a%20questo%20link, Agosto 2024

[104] Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937 (Testo rilevante ai fini del SEE)

fronteggiando sfide legate alla sicurezza, alla tutela dei consumatori e alla stabilità dei mercati finanziari[105].

Particolarmente significativo, in una prospettiva di contenimento del rischio sistemico, è il fatto che il MiCAR stabilisce misure specifiche in merito a trasparenza, doveri informativi e supervisione prudenziale per gli emittenti e per i fornitori di cripto-servizi – nuova categoria di intermediari a ciò appositamente autorizzati, i c.d. *crypto-asset service providers* (CASP) –, stabilendo requisiti di capitale, obblighi di segregazione dei fondi e controlli sull'adeguatezza operativa delle entità autorizzate, in modo da evitare che la delega di funzioni o la sottovalutazione dei rischi tecnologici minacci la stabilità di mercato[106].

Dunque, pur mantenendo ciascuno la propria autonomia, questi strumenti normativi condividono l'obiettivo di creare un quadro regolatorio armonizzato e coerente, in cui la resilienza operativa e la tutela dei dati vengono garantiti qualunque sia il soggetto coinvolto.

In definitiva, benché la combinazione tra PSD2 e DORA abbia creato un quadro normativo più uniforme e solido per affrontare le sfide della digitalizzazione bancaria e dell'esternalizzazione ai TPP, la piena tutela degli interessi degli utenti non può prescindere da un'efficace disciplina del trattamento dei dati personali. Da qui l'esigenza, che verrà approfondita nel prossimo paragrafo, di un coordinamento ancora più stretto con la disciplina in materia di protezione dei dati personali, ovvero con il Regolamento generale sulla protezione dei dati (Regolamento (UE) 2016/679, GDPR).

1.3.3 – PSD2 e GDPR: un difficile equilibrio tra innovazione e tutela dei dati

Nell'ambito dell'esternalizzazione dei dati ai soggetti terzi – in particolare ai Third Party Providers (TPP) – uno degli aspetti più critici in termini di governance e compliance riguarda l'equilibrio tra l'apertura del mercato e la tutela dei dati personali. In questo contesto, è emerso con chiarezza un disallineamento normativo tra la disciplina settoriale della PSD2, orientata a promuovere l'innovazione e la concorrenza nel mercato dei pagamenti digitali, e il Regolamento generale sulla protezione dei dati (Regolamento (UE) 2016/679, o GDPR), centrato sulla protezione della riservatezza e sull'attribuzione delle responsabilità nel trattamento delle informazioni personali[107].

Questo disallineamento tra i due strumenti regolatori non è si è limitato solo al piano teorico, ma ha anche prodotto rilevanti ricadute pratiche, in particolare per quanto concerne la gestione del consenso

[105] E. Franza, "La Regolamentazione dei Cripto-Asset. MiCA un primo passo.", https://www.dirittobancario.it/art/la-regolamentazione-dei-cripto-asset-mica-un-primo-passo/, DirittoBancario, Settembre 2024

[106] Banca d'Italia, "*Regolamento (UE) 2023/1114 relativo ai mercati delle cripto-attività ("MiCAR"). Comunicazione della Banca d'Italia*", Roma, Luglio 2024

[107] European Data Protection Board, "*Linee guida 06/2020 sull'interazione tra la seconda direttiva sui servizi di pagamento e il GDPR*", cit., p.5

dell'utente, la ripartizione delle responsabilità tra i soggetti che trattano i dati e la definizione dei ruoli (titolare vs. responsabile del trattamento).

Queste incertezze si sono riflesse su tutti gli attori coinvolti, specialmente in uno scenario in cui la condivisione dei dati avviene in assenza di rapporti contrattuali diretti tra banca e TPP, rendendo difficile individuare il soggetto sui cui grava l'onere della conformità normativa.

Per comprendere pienamente le implicazioni di tali contrasti normativi – e soprattutto i rischi di governance associati alla condivisione dei dati con i TPP – è indispensabile soffermarsi brevemente sul valore strategico assunto dai dati sensibili legati ai pagamenti, ovvero "*quei dati ritenuti particolarmente importanti perché la loro [eventuale] appropriazione da parte dei terzi estranei esporrebbe l'utente a un concreto rischio di frode*"[108].

Dopo aver riconosciuto l'urgenza nel tutelare adeguatamente i dati personali, il legislatore ha progressivamente attribuito anche una valenza economica e sistemica, oltre che sociale, ai dati relativi ai servizi di pagamento, imponendo ai TPP precise restrizioni in merito al loro utilizzo. Ne sono prova, ad esempio, le disposizioni dettate agli articoli 66 e 67 della PSD2, che definiscono con rigore sia le finalità di impiego sia le modalità di conservazione dei dati a cui devono attenersi i prestatori di servizi di disposizione di ordini di pagamento (PISP) e di informazione sui conti (AISP).

Ad ogni modo, a prescindere dalle previsioni del Considerando 89 della PSD2 in tema di conformità normativa del trattamento dei dati personali, sono emersi diversi punti di contrasto tra la direttiva e il GDPR – come già affermato in apertura del paragrafo –, non solo per quanto riguarda la liceità del trasferimento dei dati, ma anche per la ripartizione delle responsabilità tra i soggetti coinvolti[109]. In merito, si evidenzia che il GDPR opera una netta distinzione tra titolare e responsabile del trattamento, definendo a priori i rispettivi ruoli e responsabilità nei rapporti interni. In linea generale, se al titolare del trattamento spetta piena autonomia nella determinazione delle modalità e delle finalità di trattamento, al responsabile è richiesto il rispetto di un vincolo di asservimento[110]. In altri termini,

---

[108] F. Marasà, "*Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR*", cit., p.651

[109] *Direttiva 2015/2366 del Parlamento europeo e del Consiglio, del 15 novembre 2015, concernente il servizio di pagamento nel mercato interno, che modifica le direttive 2002/65/EC, 2009/110/EC e 2013/36/EU e il regolamento n. 1093/2010 e che abroga la direttiva 2007/64/EC*, Considerando 89: "*La prestazione di servizi di pagamento da parte dei prestatori di servizi di pagamento può comportare il trattamento di dati personali. La direttiva 95/46/CE del Parlamento europeo e del Consiglio, le norme nazionali che danno attuazione alla direttiva 95/46/CE e il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio si applicano al trattamento dei dati personali ai fini della presente direttiva. In particolare, qualora ai fini della presente direttiva vi sia trattamento di dati personali, è opportuno che sia specificato lo scopo preciso, siano citate le basi giuridiche pertinenti, vi sia conformità con i requisiti di sicurezza pertinenti di cui alla direttiva 95/46/CE e siano rispettati i principi di necessità, proporzionalità, limitazione delle finalità e proporzionalità del periodo di conservazione dei dati. Inoltre, la protezione dei dati fin dalla progettazione e la protezione dei dati di default dovrebbero essere integrati in tutti i sistemi di trattamento dei dati sviluppati e utilizzati nel quadro della presente direttiva*". Tenendo presente che la PSD2 è precedente al GDPR, nel considerando si fa ancora riferimento alla precedente direttiva 95/46/CE che successivamente verrà abrogata e sostituita dal nuovo regolamento generale sulla protezione dei dati (UE) 2016/679.

[110] F. Marasà, "*Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR*", cit, pp. 652-655

quest'ultimo è vincolato a trattare i dati unicamente per conto del titolare, con l'obiettivo di assisterlo nell'espletamento dei suoi obblighi, attenendosi a specifiche istruzioni contenute in un contratto o altro atto giuridico conforme al diritto europeo[111].

Tuttavia, l'applicazione di questa categorizzazione dei soggetti nell'ambito dell'ecosistema designato dalla PSD2 si è rivelata fonte di numerose ambiguità normative, specie con riferimento al ruolo che avrebbero dovuto assumere i Third Party Providers.

Infatti, mentre è chiaro che i prestatori presso cui l'utente ha radicato il conto rivestono il ruolo di titolari del trattamento, non è altrettanto semplice stabilire quale qualifica giuridica assumano i TPP. Tale difficoltà, anche secondo l'interpretazione fornita dall'European Data Protection Board, è per lo più riconducibile al fatto che "*le prestazioni di disposizione di ordini di pagamento e di informazioni sui conti non sono subordinate all'esistenza di un rapporto contrattuale tra il PISP/AISP e il prestatore di servizi di radicamento del conto*", ma è sufficiente una generica autorizzazione dell'utente per l'esecuzione dell'operazione[112].

Questo approccio, di fatto, ha comportato la creazione di una vera e propria "zona grigia", in quanto non era chiaro se i TPP dovessero essere considerati titolari autonomi del trattamento – agendo in maniera indipendente dai PSP di radicamento del conto –, oppure corresponsabili del trattamento, vista la necessaria collaborazione con gli istituti bancari.

In proposito, è opportuno specificare che questa incertezza ha avuto conseguenze dirette sulla ripartizione della responsabilità in caso di trattamento illecito dei dati personali. Nel merito, l'articolo 82, paragrafo 2, del GDPR stabilisce che "*il titolare del trattamento coinvolto risponde per [qualsiasi] danno cagionato dal suo trattamento in violazione delle norme del presente regolamento, [mentre] il responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto agli obblighi specificatamente diretti ai responsabili del trattamento o se ha agito in modo difforme o contrario rispetto alle legittime istruzioni impartite dal titolare del trattamento"* [113].

Ne consegue che, il GDPR impone al titolare una forma di responsabilità oggettiva, anche nel caso in cui l'illecito derivi dall'operato di un responsabile che agisce per suo conto. Al contrario, la PSD2 non fornisce indicazioni altrettanto puntuali sul punto, lasciando irrisolta la questione relativa

---

[111] *Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio* del 27 aprile 2016 *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE* (regolamento generale sulla protezione dei dati), art. 28

[112] European Data Protection Board, "*Linee guida 06/2020 sull'interazione tra la seconda direttiva sui servizi di pagamento e il GDPR*", cit., p.13

[113] *Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio* del 27 aprile 2016 *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE* (regolamento generale sulla protezione dei dati), art. 82 par.2: "*Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento."*

all'individuazione del soggetto responsabile in caso di uso improprio dei dati di violazione della catena del trattamento.

Ciononostante, il disallineamento più rilevante tra i due testi normativi rimane il diverso fondamento giuridico del trattamento dei dati, con riferimento in principal luogo al ruolo e al significato del consenso.

Come già evidenziato nel corso dell'analisi, secondo la PSD2 – in particolar modo secondo quanto stabilito agli articoli 66 e 67 – l'accesso ai dati da parte dei TPP può avvenire in base a una generica autorizzazione dell'utente, necessaria all'esecuzione contrattuale del servizio, escludendo così l'obbligo per le terze parti di ottenere un ulteriore "consenso esplicito" separato. In questo modo, perciò, la direttiva riduceva il ruolo del consenso a un mero elemento tecnico-funzionale.

Di contro, il GDPR – all'art. 6, par.1, lett.a) – prevede che il trattamento dei dati sia lecito solo se l'utente interessato ha espresso un consenso esplicito, libero, specifico, informato ed inequivocabile così come definito all'art. 4 punto 11[114]. Proprio questa differente concezione del consenso era la causa della fonte principale di divergenza tra PSD2 e GDPR, in quanto mentre per la prima il consenso ha una funzione meramente contrattuale, per il secondo costituisce una vera e propria condizione essenziale di legittimità del trattamento.

Tenendo conto sia della complessità di questa interazione, che della necessità di riconoscere maggiore libertà decisionale agli utenti in merito ai prestatori di servizi cui affidare i loro dati, l'*European Data Protection Board* (EDPB) è quindi intervenuto per fornire un'interpretazione più coerente della nozione di "consenso esplicito", cosicché la sua utilità fosse preservata ai sensi di quanto previsto dalla Direttiva (UE) 2015/2366.

Alla luce di ciò, si comprendono le ragioni per cui, nelle sue linee guida, l'EDPB ha attribuito un ruolo accessorio al consenso espresso all'art.94, par.2, PSD2[115] rispetto a quello assunto ai sensi del GDPR, sottolineando che la sua funzione è circoscritta a consentire "*l'accesso ai dati personali per il loro trattamento e la loro successiva conservazione ai fini della prestazione del servizio di pagamento, [senza che ciò costituisca ancora un trattamento autonomo da parte del PSP]"*[116]. In altre parole, il PSP non agisce come titolare autonomo al momento dell'accesso, bensì opera sotto la responsabilità dell'ente titolare dei dati, che rimane formalmente incaricato della loro protezione e conservazione.

---

[114] Ibid., art. 4 punto 11): "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*"

[115] La Direttiva (UE) 2015/2366 parla di consenso esplicito all'art. 94, par.2, ove prevede che: "*I prestatori di servizi di pagamento hanno accesso, trattano e conservano i dati personali necessari alla prestazione dei rispettivi servizi di pagamento, solo dietro consenso esplicito dell'utente dei servizi di pagamento.*"

[116] European Data Protection Board, "*Linee guida 06/2020 sull'interazione tra la seconda direttiva sui servizi di pagamento e il GDPR*", cit., p.15

Sempre nell'ottica del consenso rilevano, poi, anche le divergenze relative alle modalità attraverso cui le due normative disciplinano la revoca dell'autorizzazione da parte dell'utente. Come è noto, la PSD2 riconosce all'utente il diritto di avvalersi – o meno – di una determinata prestazione del servizio di pagamento, garantendo così una certa libertà nel conferimento del consenso all'accesso dei propri dati da parte dei TPP. Tuttavia, la direttiva non chiariva con sufficienza le modalità mediante le quali l'utente potesse revocare selettivamente l'accesso ai dati, senza necessariamente interrompere il servizio di pagamento, rischiando così di compromettere il principio di autodeterminazione dell'interessato. Diversamente, il GDPR – all'art. 7, par.3 – offre una tutela più significativa, stabilendo che il consenso può essere revocato in qualsiasi momento, senza che ciò comprometta la liceità del trattamento fondato sul consenso precedentemente prestato. In tal senso, un sistema pienamente conforme al GDPR avrebbe consentito all'utente di mantenere un pieno controllo dinamico sui propri dati finanziari, ovviando alle conseguenze giuridiche sproporzionate qualora decidesse di non proseguire nella condivisione con i soggetti terzi.

Non essendo però questo il caso, è bene sottolineare che, la scarsa chiarezza della Direttiva europea, unita alle frequenti sovrapposizioni con il Regolamento generale sulla protezione dei dati, ha comportato non solo un indebolimento del ruolo centrale dell'utente nella gestione dei propri dati, ma anche una situazione di estrema incertezza operativa per i TPP – sia nella veste di PISP che di AISP).

Dunque, considerando tali difficoltà, si è resa nuovamente evidente l'esigenza di un più efficace coordinamento, affinché sia i titolari sia i responsabili del trattamento adottino le precauzioni necessarie e trattino unicamente le informazioni strettamente pertinenti all'operazione autorizzata[117].

In conclusione, è possibile quindi ribadire come l'esternalizzazione dei dati ai TPP – oltre che dei servizi ICT – abbia sollevato una molteplicità di incongruenze normative non solo sul piano della sicurezza e della resilienza operativa, ma anche con riguardo alla protezione dei dati personali e alla ripartizione delle responsabilità tra i soggetti coinvolti.

In questo panorama segnato da un evidente frammentazione normativa, la PSD2 – e successivamente il DORA – hanno rappresentato un passo fondamentale per la definizione di un quadro più strutturato in tema di esternalizzazione e per il rafforzamento della gestione del rischio ICT nel settore bancario. Nonostante ciò, il presente disallineamento tra la normativa settoriale della PSD2 e quella orizzontale

[117] In quest'ultimo caso si fa riferimento al *principio di minimizzazione dei dati* sancito dall' art. 25 paragrafo 2 GDPR, il quale sancisce espressamente che: "*Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*"

del GDPR han originato diverse "zone grigie" e sovrapposizioni regolamentari, costringendo gli operatori finanziari ad affrontare continui aggiornamenti normativi e interventi di adeguamento per garantire la tenuta complessiva del sistema finanziario.

Sebbene il legislatore abbia cercato di armonizzare i diversi livelli di regolazione, facendo leva sull'azione delle Autorità europee di vigilanza, permangono comunque criticità rilevanti in termini di governance e compliance. Questa condizione ha reso sempre più urgente per gli intermediari finanziari una revisione profonda dei loro di gestione e controllo, specialmente nel recente contesto di accelerata digitalizzazione, al fine di scongiurare eventuali violazioni ed usi impropri dei dati da parte dei TPP.

A prescindere da quanto detto finora, per poter valutare se e in che misura il fenomeno dell'esternalizzazione possa rappresentare un ostacolo allo sviluppo dell'Open Banking, non basta soffermarsi sulle questioni giuridiche inerenti alla governance e la compliance. È necessario estendere l'analisi alle sue implicazioni economiche e strategiche.

1.4 - Confronto normativo tra Europa, UK e US

L'evoluzione del fenomeno dell'Open Banking in Europa ha richiesto al legislatore di aggiornare continuamente il quadro regolamentare affinché fosse garantita l'efficienza e la sicurezza del sistema finanziario. Il passaggio dalla PSD alla PSD2, seguito dall'elaborazione delle linee guida necessarie per l'implementazione della proposta del nuovo pacchetto normativo PSD3/PSR, ha ribadito nuovamente la difficoltà del legislatore europeo di intervenire in via preventiva rispetto all'insorgere delle problematiche legate alla digitalizzazione attraverso una regolamentazione che sia esaustiva, chiara ed efficiente. Eppure, fin dalle origini del fenomeno dell'Open Banking, l'Europa si è contraddistinta per il un ruolo cruciale rivestito nell'ambito della regolamentazione della condivisione dei dati[118]. Tuttavia, per poter completare il quadro e cogliere effettivamente l'essenza e l'impatto di questo fenomeno, è necessario volgere lo sguardo anche ad altre giurisdizioni e ai loro modelli di business, in particolar modo al Regno Unito e agli Stati Uniti.

1.4.1 – Il modello regolatorio del Regno Unito: un framework unitario e centralizzato

A partire dal 2018 il Regno Unito, grazie allo sviluppo di un modello molto più avanzato e regolamentato rispetto a quello dell'Unione Europea, si è distinto come leader nel contesto dell'Open

[118] L'Europa ha effettivamente svolto un ruolo di guida in ambito della regolamentazione della condivisione dei dati, come dimostrato dall'adozione del Data Governance Act e del Data Act, i quali mirano a facilitare e promuovere lo scambio e l'uso dei dati all'interno del territorio europeo garantendo la sicurezza e protezione degli stessi.

banking, raggiungendo ed oltrepassando solo dopo cinque anni la soglia dei 5 milioni di utenti registrati[119]. Ad ulteriore testimonianza della posizione di leadership vantata dal Regno Unito si segnala la presenza di una rete consolidata di fornitori di terze parti (TPP), oltre al volume significativo di transazioni digitali effettuate tramite i canali Open Banking. In tal senso, secondo recenti indagini, nel gennaio del 2024 si è registrato un numero record di pagamenti effettuati mediante soluzioni Open Banking, per un valore complessivo pari circa a 14,5 milioni di euro, segnando una crescita del 69% rispetto all'anno precedente[120]. Tale crescita, come già evidenziato, risultava principalmente correlata alle prestazioni offerte dalle terze parti, la cui presenza nel territorio britannico si confermava particolarmente significativa. A dimostrazione della rilevanza di tale fenomeno, basti considerare che, già limitando l'analisi ai soli servizi di informazione sui conti (AIS), circa il 48% dei 342 operatori attivi nel territorio dell'Unione Europea risultava registrato nel Regno Unito[121]. Questi dati, quindi, evidenziano un'adozione sempre più ampia e consolidata degli strumenti di Open Banking da parte dei clienti digitali, sollevando però allo stesso tempo un rilevante interrogativo, ossia: come ha fatto il Regno Unito a raggiungere una simile posizione di leadership nel settore dei pagamenti in così poco tempo? In altri termini, quali sono stati gli elementi normativi, tecnologici ed economici che hanno reso possibile lo sviluppo di questo modello di successo? Per rispondere a tale interrogativo, è opportuno analizzare e comprendere più a fondo il ruolo rivestito in questo processo dalla *Competition and Markets Authority* (o CMA) e dall'*Open Banking Implementation Entity* (c.d. OBIE), il quale ha assicurato un'adozione più uniforme delle regole rispetto a quanto stava avvenendo nell'Unione Europea.

Ad ogni modo, prima di entrare nel merito della questione, è opportuno ricordare che il processo di trasformazione, che ha condotto il Regno Unito all'attuale traguardo, ha avuto origine con la pubblicazione del rapporto *Fingleton*, avvenuta nel 2014 ad opera dell'*Open Data Institute*. In particolare, tale documento, attraverso la standardizzazione di interfacce dedicate alle terze parti, riconosceva l'esigenza di garantire maggiore sicurezza e trasparenza nell'accesso ai dati da parte dei consumatori[122]. Inoltre, sempre sulla base delle raccomandazioni ivi contenute, e con l'obiettivo di definire l'ambiente entro cui le *Open API* avrebbero dovuto operare, il Ministero dell'Economia e delle Finanze britannico (HM Treasury) istituì l'*Open Banking Working Group* (OBWG), riservando una specifica attenzione alle esigenze della clientela retail e business.

---

[119] Kontomatik, "*Is Open Banking UK only*?", https://www.kontomatik.com/blog/open-banking-uk-only-europe, Febbraio 2024

[120] Open Banking Ltd, "*The Open Banking Impact Report*", https://openbanking.foleon.com/live-publications/the-open-banking-impact-report-2024-march/, Marzo 2024

[121] Tink AB, "*Open banking survey 2020. The use cases driving open banking investments in UK*", 2020

[122] Open Data Institute and Fingleton Associated, "*Data Sharing and Open Data for Banks. A report for HM Treasury and Cabinet Office*", Settembre 2014, pp. 4-5

L'urgenza di creare un sistema capace di garantire il libero scambio dei dati dei clienti, in un quadro caratterizzato da controlli rigidi e strutture troppo complesse per permettere una condivisione veloce e sicura tra clientela e terze parti, spinse il governo britannico ad avviare una profonda revisione delle regole e delle istituzioni poste a tutela dei consumatori e delle piccole e medie imprese (SME). In quest'ottica, l'OBWG propose nel suo rapporto "*The Open Banking Standards*" un modello in grado di favorire una condivisione sicura dei dati finanziari attraverso moderni standard tecnologici, che, a loro volta, assicurassero un elevato livello di interoperabilità, efficienza e protezione dei dati all'interno dell'ecosistema finanziario. A tal proposito, secondo quanto riportato nel rapporto dall'OBWG, l'adozione di questi standard avrebbe consentito alle banche tradizionali e pure agli altri istituti finanziari di mantenere inalterata la proprietà sui dati che detenevano, indipendentemente dalla loro pubblicazione aperta o condivisa, provocando al contempo modifiche rilevanti al meccanismo di concessione "*in licenza*" di tali dati[123]. In ogni caso, poiché l'OBWG aveva un ruolo meramente consultivo, limitato alla definizione delle principali linee guida necessarie per la costruzione del quadro regolatorio, non disponeva di alcun potere che gli consentisse di rendere vincolanti le raccomandazioni formulate nei confronti degli istituti bancari. Consapevole di questo limite, il governo britannico, pur riconoscendo il valore del ruolo svolto dall'*Open Banking Working Group* nel definire le basi per la futura trasformazione del settore bancario, decise di adottare misure normative più stringenti ed incisive, al fine di garantire l'effettiva implementazione di un sistema di Open Banking obbligatorio e standardizzato.

Per valutare con maggiore consapevolezza le implicazioni derivanti dal successivo intervento della *Competition and Markets Authority* è opportuno precisare che, sino a quel momento, il settore bancario britannico si era caratterizzato per una limitata propensione delle banche all'innovazione e all'evoluzione tecnologica. Tali istituti, infatti, erano soliti ad introdurre nuovi prodotti o a ridurne i prezzi solo se minacciati dal possibile ingresso di nuovi operatori nel mercato[124]. Di conseguenza, il consolidamento di questa forma di oligopolio tra le maggiori banche aveva chiaramente contribuito alla creazione di significative barriere all'entrata, limitando così la possibilità per i nuovi operatori di accedere al mercato bancario senza frizioni. Inoltre, pure l'assenza di concorrenza all'interno del settore e l'evidente frammentazione tecnologica avevano ostacolato la capacità della clientela di effettuare delle facili comparazioni dei prezzi tra i prodotti e servizi offerti, contribuendo così a rendere statico l'intero settore bancario. In risposta a queste peculiari criticità, la CMA avviò

[123] Open Data Institute, "*Introducing Open banking Standards. Helping customers, banks and regulators take banking into a truly 21-st century, connected digital economy.", https://theodi.org/documents/239/298568600-Introducing-the-Open-Banking-Standard.pdf,* Gennaio 2016, pp. 5-6

[124] CMA, "*Making banks work harder for you*", https://assets.publishing.service.gov.uk/media/5a800298ed915d74e33f7ea3/overview-of-the-banking-retail-market.pdf, Agosto 2016

un'indagine di mercato nel 2016 avente la finalità di individuare gli strumenti regolatori tali da ricreare le condizioni di equilibrio e stabilità tipiche di un sistema bancario attraente e competitivo. Invero, l'intento principale era quello di favorire un ambiente più dinamico, in cui i clienti fossero maggiormente consapevoli degli strumenti a loro disposizione e avessero maggiore controllo sui propri dati finanziari. In quest'ottica, nel 2017, con la pubblicazione del *Retail Investigation Banking Order* la CMA adottò una serie di misure principalmente volte a superare le barriere strutturali e normative, che fino a quel momento avevano scoraggiato l'ingresso di nuovi operatori nel mercato, stimolando così un'ondata di innovazione in tutto il sistema finanziario. Il cuore di tale riforma, però, era rappresentato dall'introduzione dell'obbligo per le nove maggiori banche inglesi (CMA9[125]) di adottare API standardizzate, cosicché la condivisione di tutti i dati bancari della clientela retail e business con i TPP potesse essere più controllata e sicura[126]. Ebbene, è proprio il significato attribuito alla standardizzazione delle API a rivestire un ruolo chiave in questo contesto. Infatti, come ampiamente discusso all'interno del rapporto Fingleton, prima dell'adozione delle *Open API Standards* ogni istituto finanziario impiegava meccanismi propri per la gestione e condivisione dei dati, impendendo così un accesso uniforme ai conti da parte degli operatori. Da ciò si può dedurre, quindi, che il termine "*standard*" quando si parla di Open Banking non ha un valore puramente tecnico, bensì strategico e competitivo, in quanto implica la possibilità per gli operatori di accedere e utilizzare dati uniformi e facilmente comprensibili in qualsiasi momento[127].

Ma a che cosa ci si riferisce effettivamente quando si parla di API standardizzate? Tenendo presente che il termine API (*Application Programming Interface*) si riferisce "*all'insieme di regole o protocolli che consentono alle applicazioni software di comunicare tra loro per scambiare dati, caratteristiche e funzionalità*"[128] (M. Goodwin, Aprile 2024), si può concludere che, con riguardo al fenomeno dell'Open Banking, esse stabiliscono regole comuni per l'accesso ai dati finanziari, assicurando che le terze parti autorizzate ottengano informazioni dai conti bancari dei clienti in maniera uniforme e regolata. Tuttavia, è bene specificare che la CMA, mediante l'istituzione di interfacce standardizzate, non si è limitata solo a definire un quadro tecnico per la condivisione dei dati con le terze parti, bensì ha rivoluzionato completamente le regole di accesso ai conti ed alle informazioni dei clienti. Secondo quando indicato nell'art. 10[129] del *Retail Investigation Banking Order* il processo di apertura ai dati è

[125] In particolare, per CMA9 si intendono le banche con la maggiore capitalizzazione e quota di mercato presenti sul territorio britannico, ovvero: AIB Group (UK) plc trading as First Trust Bank in Northern Ireland, Bank of Ireland (UK) plc, Barclays Bank plc, HSBC Group, Lloyds Banking Group plc, Nationwide Building Society, Northern Bank Limited, trading as Danske Bank, NatWest Group plc, Santander UK plc (in Great Britain and Northern Ireland).
[126] ODI & Fingleton associated, "*Open Banking, preparing for lift off*", Giugno 2019, pp.5-6
[127] OBWG, "*The Open Banking Standards. Unlocking the potential of open banking to improve competition, efficiency and stimulate innovation*", Chapter 7a, pp. 24-25
[128] M. Goodwin, "*Che cos'è un'API*?", https://www.ibm.com/it-it/topics/api, IBM, Aprile 2024
[129] Per ulteriori approfondimenti in merito all'argomento *Open API standards* e *data sharing* si veda il testo integrale dell'articolo 10 del Retail Market Investigation Banking Order

avvenuto in modo pressoché graduale, partendo inizialmente da un modello di accesso ai dati senza possibilità di modifica (*Read-only Data Standard*) per poi passare alla fase successiva che prevedeva, oltre alla lettura dei dati, anche la possibilità per le terze parti di avviare pagamenti o altre operazioni finanziarie (*Read/Write Data Standard*).

La scelta di consentire inizialmente solo il *Read-only access*, noto anche come *Read-only Data Standard* (artt. 12 e 13), era legata alla volontà delle autorità di permettere alle terze parti autorizzate di consultare unicamente le informazioni finanziarie dei clienti con il loro esplicito consenso, stimolando così sia una maggiore consapevolezza tra i consumatori sia la creazione di nuovi servizi innovativi capaci di mettere in discussione il ruolo privilegiato delle banche tradizionali. Inoltre, l'impossibilità di modificare i dati avrebbe ridotto il tentativo di frodi, dando alle banche il tempo necessario per testare le API e migliorare gli standard di sicurezza. Il passaggio successivo al *Read and Write access*, disciplinato all'art. 14 del provvedimento, divenne ben presto necessario per permettere l'integrazione dei nuovi servizi di pagamento e la creazione di nuovi modelli di business nel settore fintech. L'ampliamento dell'autorizzazione ha avuto implicazioni significative sui costi delle transazioni soprattutto per i PISP, i quali avrebbero così iniziato ad avanzare pagamenti direttamente via API senza dover prima passare per i circuiti tradizionali, offrendo al contempo alle imprese e alla clientela retail strumenti avanzati per la gestione finanziaria. Nonostante ciò, al fine di assicurare la reale applicazione delle regole relative all'adozione delle API standard, la CMA istituì un organismo indipendente, l'*Open Banking Implementation Entity* (OBIE), con il compito di supervisionare l'implementazione dell'*Open Banking Standard* [130].

La consapevolezza di non poter delineare nel dettaglio tutti i requisiti tecnici legati alla progettazione dell'*Open Banking Standard*, secondo cui le API dovevano essere preferibilmente costruite come un sistema a rete federato piuttosto che come un sistema centralizzato, ha indotto la CMA ad affidare la progettazione a un organismo terzo, l'OBIE, che avrebbe dovuto confrontarsi con le parti interessate del settore per garantire un applicazione uniforme ed efficace di questi standard tecnici e di sicurezza[131]. Nello specifico, entro due settimane dall'entrata in vigore dell'ordine della CMA, l'*Implementation Entity*, successivamente strutturato come OBIE, avrebbe dovuto coordinare e garantire l'adozione di regole comuni per la gestione degli accessi (*authorisation and authentication standards*[132]), nonché la creazione di un ambiente di autorizzazioni standardizzato per la concessione dei permessi ai TPP (*standardised permission frameworks*[133]).

[130] CMA, "*The Retail Banking Market Investigation Order 2017*", Part 2, Article 10.1
[131] Open Data Institute, "*Introducing The Open Banking Standards*", 2019, p. 9
[132] CMA, "*The Retail Banking Market Investigation Order 2017*", Part 2, Article 10.2.3 (a)
[133] *Ibid*., Article 10.2.3 (b)

Un altro punto chiave del provvedimento della CMA riguardava, poi, la necessità di fornire ai consumatori gli strumenti necessari per compiere scelte informate al fine di scongiurare l'endemico problema dello "*switching inertia*", ossia la tendenza dei consumatori di rimanere fedeli alla propria banca nonostante gli evidenti vantaggi legati al cambiamento. A dimostrazione di tale fatto, secondo le indagini condotte prima dell'avvio del percorso regolamentare relativo all'Open Banking, "solo il 3% della clientela retail e il 4% di quella business tendevano a cambiare istituto nel corso dell'anno" (CMA, 2016)[134], soprattutto a causa di una combinazione di scarsa informazione, complessità nei processi di migrazione e mancanza di strumenti per confrontare le offerte in modo efficace. Alla luce di quanto sopra, la CMA impose alle banche di fornire, qualora necessario, l'accesso continuo anche ai dati storici delle transazioni, affinché i clienti potessero valutare meglio le proprie abitudini di spesa e confrontare le offerte dei vari operatori, sia bancari che non bancari[135]. A beneficiare di questa iniziativa furono anche le terze parti, le quali, solo previa autorizzazione esplicita dei consumatori, potevano accedere ai dati pregressi dei clienti per sviluppare strumenti finanziari comparativamente più accurati e coerenti con i loro bisogni. A questo proposito, è fondamentale sottolineare che, per assicurare una gestione sicura degli accessi e, dunque, dell'impiego dei dati dei clienti, il CMA *Order* ha previsto due livelli di controllo sui TPP, siano essi AISP che PISP. In particolare, per poter operare all'interno del sistema, i TPP necessitavano innanzitutto della autorizzazione della *Financial Conduct Authority* (FCA), dopodiché dovevano risultare regolarmente iscritti in un apposito elenco, *l'Open Banking Directory,* che consentiva alle banche di identificarli. Di fatto, questa lista permetteva alle banche e agli altri istituti finanziari operanti nel mercato di capire se i TPP richiedenti l'accesso alle loro API soddisfacevano i requisiti necessari per operare, agevolando contestualmente un collegamento rapido e fluido tra le banche e le terze parti[136].

Ad ogni modo, nel definire gli obblighi normativi a cui le nove maggiori banche del paese avrebbero dovuto conformarsi, la CMA stabilì precise tappe temporali entro cui avrebbero dovuto essere attuati[137]. Nella pratica, però, questo percorso non fu esente da ostacoli: solo alcune istituzioni finanziarie riuscirono ad adeguarsi entro i termini stabiliti, costringendo le autorità a concedere delle proroghe al fine di permettere a tutte le banche di adeguarsi ai requisiti normativi. In proposito, è bene soffermarsi sul fatto che, uno dei principali ostacoli a cui l'OBIE dovette far fronte, per consentire il tempestivo raggiungimento degli obiettivi temporali prefissati, era di natura tecnologica ed operativa, giacché la maggior parte delle banche non disponeva delle infrastrutture adeguate ad affrontare tali cambiamenti e conformarsi ai nuovi standard operativi. Di fatto, questa transazione

[134] CMA, "*Making banks work harder for you*", August 2016, p.5
[135] CMA, "*The Retail Banking Market Investigation Order 2017*", Part 2, Article 14
[136] ODI & Fingleton Associated, "*Open Banking, preparing for lift off*", Giugno 2019, p. 24
[137] BBVA, "*The Open Banking Standard*" Digital economy Outlook, Aprile 2016

verso l'Open Banking era stata percepita dalle banche come una minaccia ai loro modelli tradizionali di business, inducendole ad opporre resistenza e a ritardare l'adozione delle *Open API Standard*. Inoltre, nonostante la nuova struttura avesse condotto all'abbandono di tecniche per l'accesso ai dati da parte dei TPP particolarmente pericolose per la privacy dei consumatori, quale ad esempio lo *screen scraping*, la necessità di dover garantire una gestione ed un coordinamento sicuro delle informazioni contenute nei conti ha contribuito ulteriormente a rallentare il processo di affermazione dell'Open Banking. Alla luce di tali criticità, la CMA fu costretta a rivedere due volte la data prevista per il completamento della *Roadmap* rispetto a quanto prefissato nell'iniziale *Retail Investigation Banking Order* del 2017. Sebbene l'obiettivo iniziale fosse quello di raggiungere il completamento del provvedimento prima dell'entrata in vigore della PSD2, così da garantire un allineamento fluido alla normativa europea, tale risultato fu raggiunto soltanto nel tardo settembre del 2024, dopo una prima revisione nel 2018 e una seconda nel 2020[138].

Il raggiungimento di questo traguardo, realizzato con il completamento della *Roadmap* da parte delle ultime tre banche[139] appartenenti al gruppo delle CMA9, è stato definito dal direttore della CMA Dan Turnbull come "*un importante pietra miliare",* poiché *"questo risultato consolidava il passaggio effettivo all'Open Banking del Regno Unito, il quale avrebbe potuto espandere così i benefici legati all'applicazione [di tale fenomeno] oltre a quelli previsti dall'ordine della CMA*"[140].

La menzionata volontà del governo britannico di allineare quanto disposto nel CMA *Orde*r con la PSD2 era per lo più legata alla consapevolezza di dover mantenere una certa compatibilità con il framework europeo, così da ridurre eventuali problematiche regolamentari per le istituzioni finanziarie operanti all'interno del mercato europeo[141]. A tal proposito l'*HM Treasury*, responsabile del recepimento della PSD2 nel diritto nazionale britannico, propose nel suo documento di consultazione sull'attuazione della seconda direttiva sui servizi di pagamento di continuare a basarsi sul quadro normativo previgente, cercando di mantenere contemporaneamente un filo conduttore con le normative europee. Questa scelta, quindi, non avrebbe solo ridotto i costi di adeguamento per le imprese, ma avrebbe altresì consentito ai consumatori di beneficiare della protezione e dei diritti legati all'entrata in vigore della PSD2, lasciando sostanzialmente invariato il regime dei servizi di pagamento all'interno del mercato britannico[142].

---

[138] OBIE, "*Delivering the Roadmap. Open Banking – A UK success story*", https://www.openbanking.org.uk/delivering-the-roadmap/, 2025

[139] Nello specifico le ultime tra banche ad aver completato la Roadmap prevista dal CMA sono state Danske Bank, Bank of Ireland, e Allied Irish Bank

[140] A. Leonards, "*Final UK banks complete Open Banking Roadmap*", https://www.fstech.co.uk/fst/Final_UK_Banks_Complete_Open_Banking_Roadmap.php, Settembre 2024

[141] D. Milanesi, "*A New Banking Paradigm: The State of Open Banking in Europe, the United Kingdom, and the United States*", TTLF Working Paper No.29, 2017, pp.97-98

[142] HM Treasury, "*Implementation of the revised EU Payment Services Directive II: response to the consultation*", Luglio 2017, p.5

Nel definire i ruoli che le Autorità avrebbero dovuto rivestire, l'*HM Treasury* ribadì che la *Financial Conduct Authority* (FCA) avrebbe continuato ad essere responsabile dell'autorizzazione e della registrazione degli istituti di pagamento, nonché delle regole di condotta per la fornitura di servizi di pagamento da parte di tutti i PSP. In quest'ottica, pur riconoscendo che il Regno Unito avesse sviluppato un modello di Open Banking più innovativo ed ambizioso rispetto a quello europeo, la FCA avviò una serie di consultazioni per comprendere quali modifiche fossero necessarie per finalizzare l'approccio alla PSD2. Uno degli aspetti cruciali di questo allineamento normativo riguardava proprio i *Regulatory Technical Standards* (RTS) emanati dall'EBA, che dettavano le linee guida e gli standard di sicurezza per l'accesso ai dati da parte delle terze parti oltre che per l'autenticazione dei clienti. A tal proposito, secondo quanto disposto dalla FCA, qualsiasi istituto bancario e non bancario avrebbe dovuto adeguarsi a tali regolamenti per garantire l'interoperabilità tra i sistemi e facilitare le transazioni transnazionali. Tuttavia, viste le evidenti perplessità espresse dagli operatori in merito alla possibilità di adempiere entro il 14 settembre 2019 agli stringenti obblighi disposti dall'EBA in tema di *Strong Customer Authentication* (SCA), la FCA decise di concedere una proroga per la completa implementazione degli stessi, tenuto conto anche delle palesi difficoltà operative riscontrate dalle banche e dei fornitori di servizi di pagamento[143].

Se sul tema dell'autenticazione la FCA si dimostrò più flessibile rispetto all'EBA, collaborando con gli operatori per garantire un'implementazione graduale ed evitare malfunzionamenti del mercato, sul tema dell'accesso ai dati bancari da parte dei TPP adottò, invece, un approccio molto più rigido. Infatti, mentre gli RTS dell'EBA lasciavano aperta la possibilità per gli istituti finanziari di adottare soluzioni proprietarie senza imporre standard tecnici univoci per le API, la FCA ribadì l'uso esclusivo di API standardizzate per l'accesso ai dati, in linea con quanto previsto nel CMA *Order*, vietando esplicitamente tecniche di *screen scraping*[144]. Contestualmente, però, per evitare che questo disallineamento rispetto alla PSD2 vanificasse i benefici legati all'introduzione degli *Open API Standard*, venne espressamente indicato all'interno del provvedimento finale della CMA che "*né il Read-only Data Standard, né il Read/Write Data Standard potessero contrastare la PSD2*" (art. 10.2 CMA Order). Pertanto, questo quadro normativo avrebbe dovuto assicurare un sistema più sicuro ed interoperabile, a differenza del contesto europeo ove l'assenza di un ente centrale indipendente di coordinamento e controllo (quale era invece l'OBIE) portò a una frammentazione nell'implementazione tra i vari Stati membri.

Sul fronte della protezione dei dati, l'introduzione del regolamento generale per la protezione dei dati (*GDPR*) da parte del legislatore europeo ha modificato profondamente il quadro normativo

[143] FCA, *Approach to final Regulatory Technical Standards and EBA guidelines under the revised Payment Services Directive (PSD2)*, PS18/24, Dicembre 2024, pp.10-11
[144] *Ibid., p.9*

britannico, sostituendo il precedente *Data Protection Act* del 1998 con un nuovo quadro giuridico in grado di conformarsi al regolamento europeo. Nello specifico, il *Data Protection Act* (DPA) del 2018 ha recepito quasi integralmente il GDPR, imponendo alle banche e ai TPP stringenti obblighi sulla gestione e sul trattamento dei dati dei clienti. Ciò ha richiesto un attento bilanciamento tra la necessità di favorire la condivisione delle informazioni e la tutela della privacy degli utenti.

Uno dei principali cambiamenti introdotti dal *Data Protection Act* del 2018 per allinearsi al GDPR riguardava il principio di minimizzazione dei dati. Nello specifico, in conformità con quanto disposto dall'art. 5, lett. c), GDPR[145], il DPA ha imposto ai soggetti coinvolti nella raccolta dei dati di trattare esclusivamente le informazioni "*minime necessarie*" rispetto alle finalità perseguite. Questo cambio di prospettiva era finalizzato, per lo più, ad impedire che le terze parti autorizzate raccogliessero informazioni eccessive, mitigando così i potenziali danni derivanti da violazioni o usi impropri dei dati personali[146]. Successivamente, è stato altresì introdotto anche l'obbligo per gli utilizzatori dei dati - siano essi istituti finanziari o terze parti - di ottenere un consenso esplicito da parte dei soggetti interessati alla condivisione delle informazioni. Spettava, invece, all'autorità competente il compito di verificare *nel continuum* la validità del consenso rilasciato e, qualora ritenuto necessario, accertarne l'eventuale revoca[147].

A sua volta, però, il DPA 2018 ha introdotto disposizioni specifiche che non erano trattate dal GDPR, quale ad esempio l'elaborazione dei dati per scopi di sicurezza nazionale e di applicazione della legge[148]. A tal proposito, è opportuno sottolineare che, nonostante entrambi gli atti avessero lo scopo di proteggere i dati personali, il DPA costituiva una normativa autonoma e specifica del Regno Unito, legittimata, perciò, ad approfondire anche ambiti non espressamente regolati dal regolamento europeo. Inoltre, al fine di garantire un monitoraggio costante dell'applicazione della legge e della sua conformità alla normativa europea, nonché per assicurare l'adozione di misure correttive, il DPA ha istituito un'autorità di regolamentazione per la protezione dei dati, ossia l'*Information Commissioner's Office* (ICO). Tale autorità, data la complessità del quadro normativo delineato dal GDPR, ha svolto un ruolo fondamentale nei confronti sia della clientela retail che di quella business, non solo promuovendo una maggiore consapevolezza riguardo ai rispettivi diritti ed obblighi in materia di protezione dei dati, ma anche garantendo che gli scambi di informazioni con i TPP

[145] In particolare, l'art. 5 (c) del GDPR stabilisce che i dati personali sono: "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

[146] Exabeam, "*Che cos'è l'articolo 5 del GDPR?*", https://www.exabeam.com/explainers/gdpr-compliance/gdpr-article-5-key-principles-and-6-compliance-best-practices/

[147] *Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio*, 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), Capo II, Art. 7

[148] Exabeam, "*GDPR vs. DPA: 6 differenze chiave e best practice di conformità*", https://www.exabeam.com/explainers/gdpr-compliance/gdpr-vs-dpa-6-key-differences-compliance-bestpractices/#:~:text=While%20GDPR%20aims%20for%20uniform,into%20the%20UK's%20legal%20framework

avvenissero in modo equo e sicuro. L'annuncio, e la successiva realizzazione nel 2021, dell'uscita del Regno Unito dall'Unione europea hanno avuto pesanti ripercussioni sulla regolamentazione dell'Open Banking, costringendo il governo britannico ad intraprendere un nuovo percorso normativo. In questo processo, il governo si è trovato a dover bilanciare il mantenimento della leadership del sistema bancario nazionale con la necessità di preservare un certo grado di compatibilità con il framework europeo. Di fatto, l'uscita del Regno Unito dall'UE ha "*implicato l'immediata riclassificazione come paese terzo, sebbene insolita […]. Tuttavia, [da quel momento in poi], nel settore bancario le aziende con sede nel Regno Unito che desideravano fornire servizi nell'UE non erano più in grado di farlo tramite il passaporto, ovvero il diritto di servire i clienti in tutta l'UE dal loro Stato membro di origine, sia tramite la libera fornitura di servizi (transfrontalieri) sia tramite l'istituzione di filiali locali a condizioni preferenziali*" (ECB, Gennaio 2023) [149].

Pertanto, la Brexit ha rappresentato un'arma a doppio taglio per il governo britannico, poiché da un lato ha permesso alle istituzioni di divergere dalle direttive europee e dagli stringenti regolamenti tecnici dell'EBA, ma dall'altro ha permesso la creazione di nuove barriere normative per i TPP e le fintech britanniche che operavano nel mercato europeo. Alla luce dei possibili esiti negativi che una divergenza regolamentare tra UE e Regno Unito avrebbe potuto avere per i soggetti operanti, l'EBA, già precedentemente alla conclusione del periodo di transizione, aveva invitato gli istituti finanziari operanti all'interno del territorio europeo a finalizzare accordi e mettere in atto piani tali da consentire la mitigazione dei rischi e la protezione dei consumatori[150]. Questo invito aveva avuto un'importanza particolare, poiché "*gli istituti di pagamento e di moneta elettronica autorizzati nel Regno Unito che desideravano continuare ad offrire servizi ai clienti con sede nell'UE non avrebbero più potuto farlo, a meno che non fossero stati adeguatamente autorizzati in anticipo da un'autorità competente dell'UE*" (EBA, Luglio 2020)[151]. Questi operatori, senza alcun tipo di accordo, avrebbero dovuto registrarsi in uno degli Stati membri dell'UE per poter continuare a offrire servizi ai clienti europei, generando così un aumento dei costi operativi e burocratici per gli stessi.

Sempre in quest'ottica, l'Autorità bancaria europea, pur consapevole degli ingenti costi che tali azioni avrebbero comportato per gli istituti finanziari coinvolti, richiese che le API bancarie britanniche continuassero ad essere sviluppate secondo standard compatibili a quelli europei, al fine di attenuare la creazione di ulteriori barriere all'accesso ai dati per le istituzioni finanziarie e i TPP operanti a

[149] ECB, "*Brexit and the EU banking sector: from the fundamental freedoms of the Internal Market to third country status*", https://www.bankingsupervision.europa.eu/press/interviews/date/2023/html/ssm.in230130~cd7de9ce0c.en.html, Gennaio 2023

[150] *Opinion of the European Banking Authority on preparations for the withdrawal of the United Kingdom from the European Union*, EBA/Op/2018/05, Giugno 2018, p.2

[151] EBA, "*The EBA calls on financial institutions to finalise preparations for the end of the transitional arrangements between the EU and UK*", Luglio 2020

livello transfrontaliero. Ciononostante, la FCA, tenendo conto delle indicazioni espresse dall'EBA, avviò comunque un processo di revisione della normativa britannica, con l'obiettivo di personalizzare il quadro legislativo alle esigenze del Regno Unito. Un chiaro esempio di tale adattamento fu la decisione della FCA, sentite le terze parti, di modificare la regola di ri-autenticazione entro 90 giorni imposta dagli RTS dell'EBA, considerata da molti TPP un ostacolo incisivo all'adozione nel lungo termine dell'Open Banking[152]. In ogni caso, nel procedere con tali modifiche normative, l'autorità prestò attenzione a bilanciarne i benefici con i costi di implementazione, mantenendo sempre vivo l'interesse di stringere accordi con l'UE, anche in qualità di paese terzo[153].

Tuttavia, uno degli aspetti più critici della regolamentazione post-Brexit ha riguardato lo scambio dei dati finanziari e personali tra istituti finanziari operanti nel Regno Unito e in UE. A tal proposito, l'ICO, con il beneplacito della Commissione Europea, stabilì che il GDPR continuasse ad applicarsi come *UK GDPR* congiuntamente al *Data Protection Act* del 2018[154]. È doveroso sottolineare, però, che questa decisione è stata adottata temporaneamente, vista la possibilità di una futura revoca qualora il Regno Unito apporti modifiche significative al proprio *Data Protection Act*. Comunque, data l'importanza dei principi stabiliti in tale regolamento, il governo britannico sta cercando di mantenere rapporti collaborativi con le Autorità europee, al fine di continuare a trattare i dati dei cittadini europei senza dover adottare meccanismi alternativi, limitando anche le possibili discontinuità che si potrebbero generare per le aziende e i consumatori.

Pertanto, alla luce delle analisi sin qui condotte, emerge chiaramente che il modello di Open Banking britannico si è sviluppato come un sistema più strutturato e dinamico rispetto a quello europeo, principalmente grazie a una regolamentazione chiara, all'adozione di API standardizzate e alla supervisione dell'OBIE. A tal proposito, occorre evidenziare che, proprio l'adozione dell'*Open Banking Standard* ha garantito al Regno Unito di segnare un livello di penetrazione dell'Open Banking nettamente superiore a quello degli altri mercati europei. Secondo l'*Impact Report* dell'OBIE, a gennaio del 2024 la percentuale di clienti che hanno effettuato un pagamento tramite Open Banking è cresciuta al 14%, segnando un traguardo storico[155]. In questo contesto di crescente digitalizzazione dei pagamenti emerge, quindi, che l'esternalizzazione dell'accesso ai dati finanziari ai TPP riveste un ruolo fondamentale per lo sviluppo del settore bancario. A conferma di quanto appena menzionato, il numero crescente di chiamate API mensili registrate nel sistema britannico,

[152] OBIE, "*Annual Report 2020*", 2020, pp.15-16
[153] House of Lords, "*The UK-EU relationship in financial services*", Authority of House of Lords, Giugno 2022, pp. 47-49
[154] ICO, "*Data Protection Impact Assessments (DPIAs)*", https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/
[155] OBIE, "*The Open Banking Impact Report*", https://openbanking.foleon.com/live-publications/the-open-banking-impact-report-2024-march/adoption-analysis, Marzo 2024

che nel gennaio del 2024 ha superato i 10 miliardi[156], evidenzia la capacità delle imprese fintech e dei TPP di sviluppare servizi innovativi e di integrarsi con il sistema bancario tradizionale in modo scalabile ed efficiente, specialmente nell'epoca post-Brexit in cui il Regno Unito stava ridefinendo la propria regolamentazione nei riguardi dell'UE.

In altri termini, l'elevata adozione delle API standardizzate ha dimostrato che, nella maggior parte dei casi, l'esternalizzazione ai TPP non rappresenta un ostacolo, ma piuttosto un acceleratore dell'Open Banking. Se da un lato sono emersi i benefici legati all'espansione dell'offerta di servizi finanziari, oltre a quelli tradizionali, e alla creazione di un ambiente più aperto e competitivo, capace di migliorare la *customer experience*; dall'altro lato, invece, è necessario considerare gli evidenti rischi connessi a un'eccessiva dipendenza dai TPP, soprattutto in termini di sicurezza dei dati e continuità operativa. Pertanto, l'esternalizzazione ai TPP può rappresentare uno dei fattori trainanti del futuro dell'Open Banking nel Regno Unito, ma questo dipenderà dalla capacità delle autorità regolamentari di saper imporre le regole necessarie per limitare la dipendenza del settore da operatori terzi, bilanciando contemporaneamente la nuova autonomia normativa con gli standard dell'UE.

1.4.2 – Il modello statunitense: un approccio frammentato e *market-driven*

A questo punto, potrebbe essere utile esaminare brevemente come viene regolamentato il fenomeno dell'Open Banking negli Stati Uniti, in quanto ciò ci permette di avere una visione più approfondita delle differenti strategie regolamentari adottate. A differenza dell'UE e del Regno Unito, gli Stati Uniti non hanno adottato un quadro normativo vincolante in tema di Open Banking, bensì tale fenomeno è stato principalmente guidato dalle forze di mercato e dalle crescenti aspettative dei consumatori. Negli ultimi anni, però, questo approccio tendenzialmente "*laissez faire*" da parte del governo statunitense ha sollevato vari dubbi tra le istituzioni in merito alla sua capacità di garantire sicurezza, accessibilità e innovazione nel lungo periodo. Una delle possibili spiegazioni legate a quest'incapacità degli U.S. di adottare un modello standardizzato, chiaro ed efficace, come nel Regno Unito, si rinviene principalmente nell'elevata frammentazione interna al mercato bancario. Di fatto, il mercato statunitense si è sempre caratterizzato per un numero elevato di istituzioni finanziarie attive al suo interno, solo nel 2024 si sono registrate oltre 3920[157] banche commerciali, ma anche per la presenza di diverse autorità regolamentari statali oltre che federali con giurisdizione sui dati finanziari

[156] Ibid.

[157] Per maggiori dettagli in merito alla composizione del mercato bancario e finanziario statunitense si rimanda alla banca dati BankFind Suite (https://banks.data.fdic.gov/bankfind-suite/historical), la quale riporta una sintesi annuale dei dati finanziari e strutturali di tutti gli istituti assicurati dalla FDIC. Tali dati, pertanto, possono essere impiegati per identificare e analizzare le tendenze a lungo termine del settore bancario e finanziario statunitense.

dei consumatori[158]. Nondimeno, la protezione dei consumatori non è mai stata al centro dell'interesse di alcuna autorità federale, le quali, data la forte decentralizzazione dell'autonomia legislativa, non disponevano comunque dei mezzi necessari per imporsi sull'intero mercato. Questa mancanza di un effettivo mandato di responsabilità in capo alle autorità, unita alle evidenti lacune nella struttura giuridica statunitense, ha favorito forme di abuso di potere da parte degli istituti finanziari nei confronti dei consumatori, i quali si sono trovati spesso e volentieri a dover fronteggiare l'offerta di prodotti con standard di protezione inferiori a quelli previsti. Il risultato di questa situazione si rivelò ancor più devastante di quanto si potesse prevedere, basti pensare alla crisi finanziaria del 2008 ed alle successive conseguenze.

Ad ogni modo, nel tentativo di porre rimedio a questa situazione di evidente incertezza normativa, nel 2010, venne promulgato il *Dodd–Frank Wall Street Reform e Consumer Protection Act* (c.d. *Dodd-Frank*), il quale aveva l'obiettivo di riorganizzare il sistema di regolamentazione finanziaria non solo mediante l'assegnazione di nuovi compiti alle agenzie federali esistenti, ma anche creandone di nuove, come ad esempio: il *Consumer Financial Protection Bureau* (CFPB), il *Financial Stability Oversight Council* (FSOC) e *l'Office of Financial Research* (OFR)[159]. A fronte delle innumerevoli novità introdotte, il *Dodd-Frank* fu inizialmente visto da alcuni esponenti politici come "*un punto di svolta storico nell'economia americana, in quanto avrebbe assicurato che il sistema finanziario avrebbe agito nell'interesse dei consumatori, promuovendo la crescita economica e la sicurezza dei consumatori piuttosto che l'interesse dei speculatori*" (Heather Booth, March 2010)[160].

Come già accennato in parte, il *Dodd-Frank* istituì nuove agenzie federali, incaricate principalmente di monitorare la stabilità del sistema finanziario e di garantire maggiore protezione ai consumatori nei confronti delle istituzioni finanziarie e delle terze parti. In particolare, secondo quanto disposto nel Titolo I Sec. 112 del *Dodd-Frank*, all'FSCO spettava il compito di identificare eventuali minacce alla stabilità finanziaria degli Stati Uniti, promuovendo la disciplina di mercato ed eliminando i potenziali rischi che avrebbero potuto generare in futuro delle crisi sistemiche. Tale agenzia nell'esercizio delle sue funzioni aveva, tra l'altro, il potere di designare come "*systemically important*" i servizi finanziari da regolare in maniera più stringente. L'OFR, invece, era incaricato di assistere il Consiglio nello svolgimento dei suoi compiti, raccogliendo e fornendo dati, nonché implementando strumenti analitici per il monitoraggio dei rischi, al fine di assicurare nel continuo un

[158] FDATA, "*Opportunities in Open Banking*", FDATA North America, p.9

[159] Wikipedia, "*Dodd–Frank Wall Street Reform and Consumer Protection Act*", https://en.wikipedia.org/wiki/Dodd–Frank_Wall_Street_Reform_and_Consumer_Protection_Actt)

[160] Heather Booth, "*AFR On The Passage Of Historic Financial Reform Legislation*", Americans for Financial Reform https://web.archive.org/web/20100523065059/http://ourfinancialsecurity.org/2010/05/afr-on-the-passage-of-historic-financial-reform-legislation/#, Marzo 2010

certo grado di trasparenza all'interno del settore finanziario[161]. Nonostante la FSCO e l'OFR fossero state istituite con lo scopo di garantire maggiore stabilità e trasparenza all'interno del settore bancario e finanziario statunitense, comparvero ben presto alcune lacune legate al loro operato. In proposito, fin dalle origini era emerso che, mentre l'OFR trascurava il suo compito di monitoraggio del sistema finalizzato alla prevenzione di eventuali crisi, operando per lo più come ufficio di supporto della FSCO; la FSCO, a sua volta, mancava di trasparenza sia nei confronti delle altre agenzie, che del pubblico, minando la sua efficacia ed integrità[162].

A prescindere da ciò, la vera innovazione del *Dodd-Frank* risiedeva nella rinnovata attenzione verso la protezione dei consumatori e l'accesso ai dati finanziari, sia da parte delle banche tradizionali che delle terze parti. A tal proposito, secondo quanto rilasciato da Elisabeth Warren, il governo statunitense cercò di creare condizioni di parità in cui tutti i fornitori di servizi e prodotti bancari fossero soggetti allo stesso controllo, proprio nel tentativo di garantire il rispetto delle regole. Invero, questo significava creare le condizioni affinchè sia il cliente che il finanziatore potessero comprendere i termini dell'accordo, il prezzo e il rischio dei prodotti[163]. Di conseguenza, venne istituita all'interno del sistema della Federal Reserve un'agenzia indipendente, il *Consumer Financial Protection Bureau*, che si rivelò una delle più attive a livello federale nella regolamentazione del fenomeno dell'Open Banking e della protezione dei consumatori[164]. Infatti, secondo quanto specificato nel *Dodd-Frank Wall Street Reform and Consumer Protection Act*, il CFPB era chiamato a mettere in atto una serie di misure volte ad assicurare che tutti i consumatori potessero avere accesso ai prodotti e servizi offerti sul mercato dalle istituzioni finanziarie in modo equo, competitivo e trasparente[165]. Allo stesso tempo, però, la presenza di mercati equi e competitivi era una caratteristica necessaria, ma non sufficiente, per garantire un'adeguata educazione finanziaria e protezione dei consumatori. Di fatto, questi ultimi si erano rivelati poco consapevoli non solo del significato connesso alle operazioni di Open Banking che stavano impiegando, ma anche del potenziale rischio legato agli accessi fraudolenti di terze parti non autorizzate. A conferma di ciò, nel 2023, Visa ha riscontrato che dell'87% dei consumatori americani che impiegavano mezzi di pagamento Open Banking solo il 34% era consapevole di quello che stava facendo[166]. Questo rappresentava una minaccia significativa per la stabilità del sistema finanziario statunitense, soprattutto per il fatto che, differentemente dall'UE e dal Regno Unito,

[161] One Hundred Eleventh Congress of the United States of America, *Dodd-Frank Wall Street Reform And Consumer Protection Act*, Title I, Sub. B, Sec.153 (codified at 12USC 5343)
[162] M. N. Baily & A. D. Klein, "*The Impact of the Dodd-Frank Act on Financial Stability and Economic Growth*", Bipartisan Policy Center & Brookings, Ottobre 2014
[163] CFPB, "*Building the CFPB*", Luglio 2011, pp. 5-6).
[164] One Hundred Eleventh Congress of the United States of America, *Dodd-Frank Wall Street Reform And Consumer Protection Act*, Section 1011(a) (codified at 12 U.S.C. Section 5491)
[165] Ibid., Section 1021(a) (codified at 12 U.S.C. Section 5511
[166] Visa Open Banking, "T*he U.S. Open Banking Movement. How consumers are driving U.S. open banking innovation*", Chapter I, p.5, 2023

l'accesso ai dati finanziari del cliente dipendeva esplicitamente da un suo consenso e non era basato su accordi intercorsi tra banche e TPP. Perciò, nel tentativo di rendere i consumatori maggiormente responsabili delle loro decisioni e di facilitare l'accesso ai dati in tempo reale, il CFPB è stato chiamato principalmente a: (a) identificare e comunicare in modo chiaro tutte le informazioni ritenute necessarie per un corretto funzionamento del sistema bancario; (b) monitorare le pratiche delle banche e delle fintech per garantire che i consumatori avessero accesso a prodotti finanziari sicuri; (c) imporre standard più stringenti per la trasparenza dei dati bancari[167].

Una delle principali peculiarità di questa autorità, però, era legata al fatto che, nel far rispettare le proprie regole, impiegava i suoi poteri nei confronti delle banche e degli istituti finanziari non bancari come fosse un'unica entità regolatoria nel panorama giuridico statunitense, sorvegliando l'intero mercato nel tentativo di assicurare un adeguato livello di protezione ai consumatori[168]. Ciononostante, a seguito dell'avanzamento tecnologico e dell'evolversi degli accordi commerciali alla base della condivisione dei dati finanziari, emersero ben presto evidenti ambiguità in merito alla mancanza di una visione concreta su come raggiungere gli obiettivi di protezione ed educazione finanziaria dei consumatori fissati dal Bureau. Inoltre, l'auspicata concorrenza nel mercato, che avrebbe dovuto costituire la base per lo sviluppo di un ambiente sano ed equo in cui i consumatori guidavano il mercato, veniva ostacolata dalla volontà degli istituti finanziari di limitare la libertà dei consumatori di decidere autonomamente in merito allo scambio dei dati finanziari. Pertanto, queste limitazioni all'accesso ai dati imposte dalle istituzioni finanziarie alle terze parti, anche se in presenza dell'esplicita autorizzazione da parte del cliente, hanno avuto un impatto negativo diretto sulla libertà di scelta dei consumatori e sul livello di concorrenza del mercato, alterandone l'equilibrio[169].

A completamento di quanto trattato fin ora, è opportuno precisare anche che, a prescindere dall'adozione del *Dodd-Frank Act* e dall'istituzione del CFPB, la struttura del mercato statunitense rimase comunque caratterizzata da una forte frammentazione e da dinamiche di accesso ai dati basate prevalentemente su accordi bilaterali tra le banche e i TPP. Allo stesso tempo, fu proprio questa persistenza, in gran parte legata all'evoluzione tecnologica in atto, a spingere il settore verso un radicale passaggio al *digital banking*, inducendo gli istituti bancari già radicati a stipulare accordi privati con fintech e aggregatori di dati per riuscire a contrastare l'ingresso delle "*banche alternative*" (c.d. '*Neobanks'*), oltre che ad offrire prodotti e servizi personalizzati ai consumatori[170].

---

[167] One Hundred Eleventh Congress of the United States of America, *Dodd-Frank Wall Street Reform And Consumer Protection Act*, Section 1021(b) (codified at 12 U.S.C. Section 5511)

[168] D. Milanesi, "*A New Banking Paradigm: The State of Open Banking in Europe, the United Kingdom, and the United States*", TTLF Working Paper No.29, 2017, p.106

[169] FDATA, "*Competition Issues in Data-Driven Consumer and Small Business Financial Services*", Giugno 2020, pp.3-5

[170] FDATA, "*Opportunities in Open Banking*", FDATA North America, pp. 9-10

A sua volta, la mancata imposizione iniziale dell'obbligo per le banche di adottare interfacce dedicate per garantire l'accesso ai dati finanziari ai TPP ha condotto alla diffusione di tecniche di screen scraping, con conseguenti effetti diretti in materia di privacy e sicurezza dei consumatori. Nello specifico, tali tecniche richiedevano che il cliente condividesse le proprie credenziali con terze parti, solitamente aggregatori di dati, e una volta concesse potevano essere impiegate per estrarre qualsiasi tipo di dati senza alcuna possibilità per le banche di esercitare su di essi il pieno controllo. Dunque, consapevoli dei rischi di sicurezza e della vulnerabilità dei propri clienti, molte istituzioni finanziarie hanno cercato di ridurre l'impiego di queste tecniche, favorendo il passaggio a modalità di accesso più sicure. In altri termini, esse hanno cercato di favorire il passaggio da un accesso basato sulla condivisione delle credenziali dei clienti ai TPP a un sistema di autorizzazione mediato da API proprietarie, fornite direttamente dagli istituti finanziari agli aggregatori di dati[171]. Sebbene questa transizione avrebbe dovuto ridurre i rischi associati alla condivisione dei dati sensibili dei clienti con le terze parti, l'assenza dell'imposizione di uno standard uniforme, come era accaduto invece nel Regno Unito con l'OBIE, ha condotto inevitabilmente allo sviluppo di interfacce eterogenee con caratteristiche tecniche differenti, spesso incompatibili tra loro. Tale fatto ha rappresentato un ulteriore ostacolo per i TPP, i quali, trovandosi di fronte ad API non standardizzate, hanno continuato ad affidarsi a tecniche alternative più rischiose per garantirsi un accesso ampio e stabile ai dati finanziari dei consumatori. Pertanto, l'inefficacia di questo tentativo delle banche ha dimostrato che la sola disponibilità di API non era sufficiente a garantire un sistema di Open Banking sicuro ed efficiente, a meno che non fosse accompagnata da una regolamentazione chiara ed uniforme, capace di imporre standard comuni per la gestione dell'accesso ai dati. Principalmente alla luce di questa criticità, il CFPB sentì l'esigenza di riconsiderare il quadro normativo esistente proponendo il *Personal Financial Data Right*, in cui promuoveva l'idea di attivare la *Sezione 1033 del Dodd-Frank Act* rimasta "dormiente" per quasi un decennio.

L'obiettivo di questa riforma era sia quello di stabilire un diritto di accesso completo ai dati finanziari, garantendo ai consumatori coerenza, equità e trasparenza, sia quello di supportare e spingere il settore verso un'infrastruttura chiara basata su API simile a quella adottata nel Regno Unito e in Europa[172]. Nel delineare questa proposta, perciò, il Bureau adottò un approccio che riprendeva a grandi linee la normativa europea e britannica in materia di Open Banking, anche se nel farlo entrò decisamente in contrasto con alcune caratteristiche tipiche della struttura del mercato statunitense.

Nello specifico, a partire dall'ordine esecutivo impartito dall'amministrazione Biden nel 2023, il CFPB spostò l'attenzione dal garantire unicamente un accesso al mercato equo, trasparente e

[171] FDATA, "*Competition Issues in Data-Driven Consumer and Small Business Financial Services*", cit., p.9
[172] B. White, "*Plaid's support for a strong consumer financial data right*", Plaid, Gennaio 2023

competitivo, alle modalità necessarie per facilitare la portabilità dei dati delle transazioni finanziarie dei consumatori. Proprio in questo quadro si collocava la Sezione 1033 del *Dodd-Frank Act*, la quale correttamente specificava che "*fatte salve alcune eccezioni, qualsiasi persona che si fosse impegnata a offrire o fornire un prodotto/servizio finanziario per i consumatori doveva rendere disponibile, su richiesta, le informazioni sotto il suo controllo relative al prodotto/servizio finanziario che il consumatore ha ottenuto da tale persona interessata*"; spettava, poi, al CFPB favorire lo sviluppo e il mantenimento di API standardizzate da parte fornitori dei dati, così da garantire ai TPP di accedere ai dati secondo specifiche modalità e standard di sicurezza[173].

Tutto ciò, secondo quanto affermato dal Direttore del CFPB Chopra, avrebbe consentito ai consumatori di "*poter scegliere tra i vari istituti finanziari sulla base delle informazioni a loro disposizione in merito ai prezzi e ai prodotti servizi offerti*" (CFPB, Ottobre 2023)[174].

Contestualmente, tale proposta richiedeva agli operatori un progressivo abbandono delle tecniche più rischiose di raccolta dati, specialmente quelle che prevedevano la cessione da parte dei clienti delle proprie credenziali a terze parti, affinché fosse consentito un rapido passaggio a un sistema caratterizzato da un maggior controllo dell'accesso ai dati da parte dei consumatori. In questo modo, quindi, il CFPB cercava di limitare il frequente riutilizzo dei dati per fini diversi rispetto a quelli per i quali i TPP venivano autorizzati, permettendo un eventuale utilizzo secondario solo per finalità specifiche legate al contrasto delle frodi o al miglioramento dell'offerta dei prodotti e servizi finanziari[175].

Nell'ulteriore tentativo di unificare il settore finanziario attorno a uno standard comune e sicuro, il CFPB riconobbe il *Financial Data Exchange* (FDX) quale *Standard-Setting Body* per l'Open Banking. Nello specifico, FDX forniva una serie di linee guida per la creazione di API interoperabili, promuovendo così un linguaggio universale per la raccolta e il trattamento dei dati da parte delle banche, delle terze parti e anche degli aggregatori di dati[176].

Nonostante la promessa di un accesso più sicuro e standardizzato ai dati mediante l'implementazione delle API avesse destato maggiore fiducia tra i consumatori, che solo nel 2022 in circa 100 milioni[177] hanno concesso l'autorizzazione ai TPP di accedere ai loro dati, molte istituzioni finanziarie in sede

---

[173] One Hundred Eleventh Congress of the United States of America, *Dodd-Frank Wall Street Reform And Consumer Protection Act*, Section 1033(d) (codified at 12 U.S.C. Section 5533)

[174] CFPB, "*CFPB Proposes Rule to Jumpstart Competition and Accelerate Shift to Open Banking*", https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-jumpstart-competition-and-accelerate-shift-to-open-banking/, Ottobre 2023

[175] Scott Hamilton, "*CFPB's Section 1033: Will US open banking reach its potential*?", https://www.finextra.com/the-long-read/1198/cfpbs-section-1033-will-us-open-banking-reach-its-potential, Finextra, Dicembre 2024

[176] Stripe, "*Che cos'è il Financial Data Exchange (FDX)? Ecco cosa c'è da sapere*", https://stripe.com/it/resources/more/what-is-the-financial-data-exchange-fdx-here-is-what-you-should-know#introduction, Luglio 2024

[177] Per ulteriori approfondimenti si veda: CFPB, "*Notice of Final Rulemaking - Required Rulemaking on Personal Financial Data Rights*", CFPB-2023-0052, p.13

di consultazione hanno criticato tale proposta ritenendola incapace di affrontare realmente i rischi insiti alle pratiche di *screen scraping*. In particolare, secondo il *Bank Policy Institute*, "*il CFPB ha oltrepassato la sua autorità statutaria, finalizzando una norma che mette a repentaglio la privacy dei consumatori, i dati finanziari e la sicurezza dei conti*" (BPI, Ottobre 2024)[178]. In sostanza, ciò che emerge dalle discussioni avanzate da tale istituto è che, sebbene il CFPB abbia sostenuto l'adozione di API standardizzate, il sistema non garantiva comunque un controllo sufficiente sulla gestione dei dati da parte delle terze parti e degli aggregatori di dati. Infatti, le nuove regole imposte dal *Personal Financial Data Right* del Bureau imponevano standard stringenti unicamente in capo alle banche, lasciando gli aggregatori di dati e le terze parti liberi da ogni supervisione. A conferma di tale disparità di trattamento, il Dipartimento del Tesoro statunitense evidenziò che, anche dopo l'introduzione delle API standardizzate, gli aggregatori di dati continuavano a raccogliere e trattare i dati sensibili dei consumatori tramite tecniche di *screen scraping,* estraendoli direttamente da fornitori di dati che non si erano ancora pienamente adeguati al nuovo framework normativo[179]. Tale criticità, unita all'espansione sempre più marcata degli aggregatori di dati nel panorama finanziario statunitense, ha sollevato ulteriori preoccupazioni tra le istituzioni bancarie, le quali vedevano nella regolamentazione proposta dal Bureau un vantaggio unicamente per le fintech e i grandi aggregatori di dati; quali, ad esempio, Plaid e Yodlee.

Un ulteriore punto di forte tensione riguardava, poi, l'impossibilità per gli istituti finanziari di recuperare gli ingenti investimenti effettuati per adeguare le infrastrutture tecnologiche e i sistemi di sicurezza agli standard richiesti dal CFPB per la costituzione delle interfacce. A tal proposito, la Sezione 1033 del *Dodd-Frank Act*, in linea con quanto disposto dalla PSD2 in Europa, vietava alle banche di addebitare commissioni a coloro che richiedevano l'accesso ai dati dei conti bancari. Tuttavia, la mancata previsione di un meccanismo di compensazione a favore delle banche, unitamente all'obbligo di condividere gratuitamente i dati tramite le proprie piattaforme con terze parti e aggregatori, rappresentava un ostacolo particolarmente incisivo, specialmente per gli istituti finanziari di piccole dimensioni, spesso incapaci di sostenere simili oneri. In ragione di ciò, secondo gli esperti, tale situazione rappresentava una minaccia rilevante per la tenuta della concorrenza all'interno del settore finanziario, in quanto, se protratta nel tempo, avrebbe potuto compromettere la realizzazione dell'auspicata della condizione di un *level playing field* [180].

---

[178] BPI, "*Banks Challenge CFPB Rule Jeopardizing Security and Privacy of Consumer Financial Data*", https://bpi.com/banks-challenge-cfpb-rule-jeopardizing-security-and-privacy-of-consumer-financial-data/, Ottobre 2024

[179] U.S. Department of the Treasury Report to the White House Competition Council, "*Assessing the Impact of New Entrant Non-bank Firmson Competition in Consumer Finance Markets*", Novembre 2022, pp. 86-90

[180] G. Colangelo, "*Open Banking goes to Washington: Lessons from the EU on regulatory- driven data sharing regimes*", https://doi.org/10.1016/j.clsr.2024.106018, p. 10

Sempre nell'ottica di segnalare le carenze anticoncorrenziali della proposta del Bureau, anche l'*American Fintech Council* rivestì un ruolo chiave, secondo la quale "*la decisione del CFPB di finalizzare questa norma senza considerare e modificare adeguatamente le disposizioni normative relative all'uso secondario dei dati dei consumatori sarebbe incongruente con i principi identificati dalla norma stessa in materia di rafforzamento della concorrenza e tutela dei consumatori*"[181]. Dunque, l'AFC, se da un lato ha riconosciuto la necessità di tutelare i consumatori, soprattutto dopo che le terze parti entravano in possesso dei loro dati, rendendo più complesso per le banche il successivo controllo; dall'altro, però, ha chiarito l'importanza che l'uso secondario di determinati dati potrebbe rivestire nell'ambito dell'offerta di servizi e prodotti ai consumatori.

Ad ogni modo, le tensioni sorte a seguito della proposta del CFPB, come pure i successivi tentativi vani di porre rimedio alle lacune sottolineate dalle istituzioni finanziarie, fanno comprendere come in realtà il contesto economico e giuridico statunitense ostacolino una facile applicazione di tali principi. Di fatto, la presenza di migliaia di istituti bancari di dimensioni variabili, unita al consolidamento della posizione degli aggregatori di dati, ha reso molto complesso per il CFPB promuovere un'unica strategia normativa chiara e coerente per tutti gli operatori, portando suo malgrado il mercato statunitense ad essere sempre più dipendente dagli accordi tra gli operatori bancari e fintech. Inoltre, se da un lato il CFPB ha previsto una regolamentazione stringente per le banche in tema di condivisione dei dati in linea con quella europea, imponendo loro di sostenere ingenti costi tecnologici per lo sviluppo delle interfacce dedicate alle terze parti e agli aggregatori; dall'altro, l'inesistenza di un ecosistema in cui tutti gli attori fossero supervisionati e sottoposti ai medesimi controlli ha lasciato aperta la possibilità di uno sfruttamento dei dati lesivo per i consumatori. Tutto ciò ha reso evidente agli occhi degli studiosi che, nella pratica, il CFPB non doveva limitarsi unicamente a dettare le regole per un accesso regolamentato ai dati tramite API, bensì avrebbe dovuto creare le basi per sviluppare un sistema coerente con le caratteristiche del mercato statunitense in cui tutti gli operatori fossero incentivati ad agire nell'interesse dei consumatori in modo equo, trasparente e competitivo, oltre che pensare a come sostenerlo.

Pertanto, questo suggerisce che il tentativo di importare direttamente il modello europeo o britannico senza una riforma più ampia della struttura di mercato non era bastato a garantire un equilibrio tra innovazione, sicurezza e competitività.

Per concludere, alla luce dell'analisi sin qui condotta, si evince come una strategia regolatoria chiara e centralizzata, quale quella britannica, possa agevolare l'esternalizzazione ai TPP, la quale, a sua

[181] AFC, "*Statement from American Fintech Council (AFC) on the Consumer Financial Protection Bureau's Personal Financial Data Rights Final Rule*", https://www.fintechcouncil.org/press-releases/statement-from-american-fintech-council-afc-senior-vice-president-head-of-policy-and-regulatory-affairs-ian-p-moloney-on-the-consumer-financial-protection-bureaus-personal-financial-data-rights-final-rule, Ottobre 2024

volta, rappresenta un importante motore di sviluppo ed innovazione nell'ambito dell'Open Banking. Diversamente, come messo in evidenza dal caso statunitense, in assenza di una regolamentazione che assicuri un'adeguata trasparenza ed interoperabilità tra i vari attori del sistema, il ricorso all'esternalizzazione ai TPP potrebbe generare un evidente squilibrio di potere tra banche, aggregatori di dati e TPP. Dunque, la sfida che le autorità saranno chiamate ad affrontare in futuro consisterà, proprio, nell'individuare un punto di equilibrio tra l'innovazione legata all'esternalizzazione ai TPP e la tutela della sicurezza, affinché l'evoluzione dell'Open Banking possa proseguire senza compromettere la stabilità finanziaria e la protezione dei consumatori.

CAPITOLO 2

L'IMPATTO ECONOMICO DELL'ESTERNALIZZAZIONE AI TPP

2.1 – L'esternalizzazione ai TPP: tra necessità normativa e strategia economica

Dopo aver analizzato il quadro normativo che ha favorito – e in parte imposto – l'apertura dei conti bancari ai *Third Party Providers* (TPP), è ora fondamentale interrogarsi sulle motivazioni che spingono le banche ad adottare modelli di esternalizzazione sempre più pervasivi.

Se, da un lato, tale apertura deriva da un impulso regolamentare – avviato con la Direttiva (UE) 2015/2366 (PSD2), che ha trasformato l'accesso ai dati bancari da prerogativa esclusiva degli istituti bancari ad obbligo regolamentare in favore di soggetti terzi autorizzati –, dall'altro risponde anche a logiche economiche, strategiche ed operative che trascendono il mero vincolo normativo.

In questa prospettiva, è essenziale comprendere fino a che punto l'esternalizzazione ai TPP rappresenti una scelta consapevole e strategica da parte degli operatori bancari, e in che misura, invece, si configuri come una risposta passiva alle pressioni esercitate dall'attuale contesto normativo e tecnologico.

Sebbene l'Open Banking ne rappresenti oggi una delle principali declinazioni, il fenomeno dell'esternalizzazione è ben più ampio e trasversale, estendendosi anche ad ambiti non direttamente connessi alla condivisione dei dati, quali: i servizi legati al *cloud computing*, la gestione delle infrastrutture IT, i servizi di *cybersecurity* e le soluzioni basate sull'intelligenza artificiale.

A conferma di questa evoluzione, il Regolamento europeo DORA – analizzato nel §1.3.2 –, pur non riferendosi direttamente all'Open Banking, introduce importanti misure per rafforzare la resilienza digitale del settore finanziario, con un'attenzione specifica ai rischi connessi alla dipendenza da fornitori ICT esterni e, in principal luogo, dai fornitori terzi critici.

Il DORA, dunque, ha avuto ricadute concrete non solo sul piano giuridico – contribuendo a consolidare la legittimità regolamentare della delega verso soggetti terzi (TPP inclusi) – ma anche su quello operativo, imponendo nuovi e più stringenti obblighi di monitoraggio, controllo e compliance, con impatti economici considerevoli per le banche, sia in termini di investimenti tecnologici sia di riorganizzazione interna.

In questo quadro, l'esternalizzazione dei servizi connessi all'accesso ai dati bancari e ai conti dei clienti – così come disciplinata dalla PSD2 e successivamente dal Regolamento PSR – si configura come una strategia *ibrida*, dettata da un impulso regolamentare ma, al contempo, parte integrante di strategie economiche ritenute cruciali per la sopravvivenza e l'innovazione degli istituti bancari tradizionali.

Ad ogni modo, per comprendere appieno la portata di tali dinamiche, è necessario analizzare con sguardo critico il contesto macroeconomico e tecnologico entro cui le banche si trovano ad operare. In particolare, negli ultimi anni, esse hanno dovuto affrontare un panorama economico sempre più instabile e competitivo, segnato da persistenti pressioni inflazionistiche, da politiche monetarie altalenanti e da una marcata volatilità dei tassi di interesse.

Sebbene questi fattori contribuiscano in misura significativa all'accelerazione del cambiamento del settore bancario, è principalmente l'ascesa e la crescente penetrazione dei nuovi attori digitali – quali le *challenger banks*[182] e le Big Tech – a ridefinire le dinamiche concorrenziali e mettere in discussione i modelli di business tradizionali, minando la storica centralità delle istituzioni finanziarie[183].

Di fatto, un chiaro segnale della trasformazione in atto è rappresentato proprio dalla crescita esponenziale del settore FinTech che, soprattutto in seguito alla pandemia Covid-19, ha accelerato la transizione verso soluzioni digitali, proponendo soluzioni modelli più agili e maggiormente rispondenti alle esigenze di una clientela sempre più orientata verso servizi finanziari accessibili, personalizzati e integrabili con altri ecosistemi tecnologici[184].

In questo contesto già fortemente competitivo, nonostante alcune recenti stime pubblicate da Konsentus per il secondo trimestre del 2025 nello Spazio Economico Europeo (EEA[185]) e nel Regno Unito rilevino una flessione nel numero di nuove autorizzazioni normative, il numero complessivo dei TPP attivi sul mercato continua a crescere.

A una prima lettura, appare dunque evidente come il settore si muova su un terreno tutt'altro che stabile. L'ecosistema finanziario europeo, a prescindere dagli esiti – tuttora pendenti – dei triloghi dell'UE relativi alla PSD3, al PSR e al Regolamento FiDA (approfonditi nel §1.2), è oggi interessato da una significativa intensificazione dell'attività di mercato rispetto ai trimestri degli anni precedenti, con una presenza media di oltre 102 TPP attivi in ciascun Paese membro. Nello specifico, circa i due terzi di questi operatori sono PISP, ovvero soggetti abilitati all'avvio di pagamenti per conto dei

[182] Con il termine di *challenger bank* ci si riferisce a quelle entità nate per rispondere a determinate esigenze di un target di clientela *digital oriented*, che richiede servizi bancari semplificati, come un conto di pagamento o un conto corrente, gestibili principalmente – o esclusivamente – tramite dispositivi mobili; tra le principali *challenger banks* si citano: Revolut, Monzo, N26. Per ulteriori approfondimenti in merito: L. Grassi, "*Challenger Bank, cosa sono e diffusione in Italia e UE*", https://www.osservatori.net/blog/fintech-insurtech/challenger-bank-cosa-sono-diffusione-in-italia-ue/, Osservatorio Fintech & Insurtech, aggiornato il 9 Giugno 2025

[183] R. D'Orsi, "La BCE aumenta i tassi. Chi ne paga le conseguenze?", https://fondazionefeltrinelli.it/scopri/la-bce-aumenta-i-tassi-chi-ne-paga-le-conseguenze/, Fondazione Giangiacomo Feltrinelli, Maggio 2023

[184] EY Global, "*How both banks and customers can seize the upside of disruption*", https://www.ey.com/en_nl/insights/banking-capital-markets/how-both-banks-and-customers-can-seize-the-upside-of-disruption, Marzo 2021

[185] Lo Spazio economico europeo (*European Economic Area – EEA*) è composto dagli Stati membri dell'Unione europea e da tre Paesi dell'Associazione europea di libero scambio (European Free Trade Association – EFTA), ovvero Islanda, Liechtenstein e Norvegia, esclusa la Svizzera)

titolari dei conti, e oltre il 58% risulta attivo su scala transfrontaliera, contribuendo così ad accrescere la competizione e a rafforzare l'integrazione a livello paneuropeo[186].

Questi dati confermano che la presenza dei TPP non rappresenta più soltanto una novità regolamentare, bensì un elemento strutturale del nuovo ecosistema finanziario. Di conseguenza, per le banche tradizionali la collaborazione con soggetti terzi abilitati ai servizi di PIS (*Payment Initiation Services*) e AIS (*Account Information Services*) si configura non tanto come una mera risposta tecnica agli obblighi imposti dalla normativa, quanto piuttosto come una scelta strategica, finalizzata a: contrastare la disintermediazione bancaria, migliorare la *customer experience* (UX), diversificare i canali distributivi, ottimizzare i costi operativi e sfruttare le economie di scala in ambito tecnologico e innovativo.

Contestualmente all'integrazione sempre più capillare dei TPP nell'architettura del mercato bancario europeo, gli istituti bancari si sono trovati nella necessità di ripensare in chiave digitale i propri modelli operativi, accelerando i processi di digitalizzazione e rinnovamento infrastrutturale. Tale revisione, lungi dal rappresentare un'opzione strategica accessoria, si impone oggi quale condizione imprescindibile non solo per colmare il gap tecnologico, ma anche per rispondere alle aspettative di una clientela sempre più esigente. Si assiste pertanto a un cambio di paradigma: ciò che un tempo era considerato un vantaggio competitivo, oggi rappresenta un prerequisito imprescindibile per la permanenza sul mercato.

Oltre agli aspetti finora evidenziati, merita particolare attenzione anche la crescente difficoltà, da parte degli istituti bancari, nel differenziare la propria gamma di prodotti e servizi all'interno di un contesto sempre più dominato dalle soluzioni digitali avanzate e flessibili proposte dalle *challenger banks* e FinTech.

Proprio a fronte di questo divario competitivo, che andava progressivamente erodendo un rapporto di fidelizzazione già fragile tra banca e cliente, molti istituti – seppur inizialmente esitanti – hanno scelto di aprirsi alle opportunità offerte dall'ecosistema fintech. Una decisione, questa, dettata non solo dall'esigenza di colmare il gap tecnologico rispetto ai modelli *digital-native* e di rafforzare la *customer retention*, ma anche dalla necessità di contenere i crescenti costi operativi e di innovazione interna, specialmente in un momento storico in cui il controllo delle spese è divenuto per le banche un fattore chiave per garantire una crescita sostenibile nel lungo periodo[187].

Tali esigenze sono emerse con ancora maggiore evidenza nel periodo post-pandemico, durante il quale l'utilizzo dei canali digitali è cresciuto in maniera esponenziale. Difatti, proprio in

[186] Konsentus, "*Q2 2025 Konsentus Third Party Provider Open Banking Tracker*", https://www.konsentus.com/tpp-trackers/q2-2025/, Luglio 2025

[187] M. Wade, M. Gauchat, V. Srinivas, "*2025 banking and capital markets outlook*", https://www.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-outlooks/banking-industry-outlook.html, Deloitte Center for Financial Services, Ottobre 2024

corrispondenza di questo momento storico, secondo stime recenti l'*online banking* ha registrato un incremento superiore al 20%, contribuendo in maniera incisiva all'espansione delle soluzioni digitali promosse dalle neobanche[188]. Ad ulteriore conferma di questo trend, il *Chase Digital Banking Attitudes Survey*, condotto dalla banca statunitense JP Morgan, sottolinea come oltre il 70% dei clienti abbia iniziato a utilizzare esclusivamente soluzioni di *digital banking*, o abbia espresso l'intenzione di farlo nel breve termine[189].

Di fronte a questi profondi mutamenti nei comportamenti di consumo e nelle aspettative degli utenti – specialmente tra le generazioni "*native digitali*" –, le tradizionali strategie standardizzate e transnazionali si sono rivelate sempre meno efficaci nel preservare le quote di mercato detenute dagli operatori *incumbent*. Tale scenario ha imposto, perciò, l'adozione di nuovi modelli operativi fondati su logiche maggiormente incentrate sul principio del *Know Your Customer* (KYC) e sull'interoperabilità tecnologica abilitata dalle API[190].

Alla luce di queste considerazioni si comprende che, la priorità per le banche non risiede più nella mera crescita dimensionale, ma si concentra perlopiù sulla ridefinizione delle proprie logiche operative, orientandosi verso la sperimentazione, la modularità e le infrastrutture nativamente interconnesse[191].

Sebbene, in linea teorica, lo sviluppo di questi nuovi modelli avrebbe potuto condurre gli istituti bancari verso un approccio pressoché *customer-centric* – fondato sull'adozione di tecnologie avanzate, sull'integrazione tramite API, sull'analisi predittiva e sull'impiego di tecniche di AI –, nella pratica la loro realizzazione si è rivelata fortemente condizionata dalla presenza di risorse e competenze interne spesso non disponibili: da qui la necessità, o l'opportunità, di collaborare con i TPP. In tal senso, l'esternalizzazione dell'accesso ai dati e conti – quale forma evoluta di collaborazione con soggetti terzi – ha assunto un rilievo strategico, divenendo un fattore abilitante della trasformazione in atto.

Tuttavia, a questo punto sorge spontanea una domanda: fino a che punto questa esternalizzazione rappresenta un effettivo vantaggio competitivo per le banche tradizionali?

---

[188] T. Brackert, et all., "*Global Retail Banking 2021: The Front-to-Back Digital Retail Bank*", https://www.bcg.com/publications/2021/global-retail-banking-report, Boston Consulting Group, Gennaio 2021

[189] Chase Media Center, "*Consumers Are Using Banking Apps for More Than Transactions, New Chase Study Finds*", https://media.chase.com/news/consumers-are-using-banking-apps-for-more-than-transactions-new-chase-study-finds, Febbraio 2024

[190] N.Moden, "*Five questions about banking in today's digital age, answered*", https://www.ey.com/en_nl/insights/banking-capital-markets/five-questions-about-banking-in-todays-digital-age-answered, Ey Global, Marzo 2021

[191] EY, "*Banking & Capital Markets*", https://www.ey.com/en_lt/industries/banking-capital-markets, Marzo 2022

E ancora: il ricorso all'esternalizzazione ai TPP è realmente in grado di colmare i gap tecnologici e di competenze, generando benefici economici sostenibili nel lungo termine, oppure si limita ad assicurare un'efficienza immediata, ma potenzialmente instabili e reversibile?
Per rispondere a questi quesiti, è necessario analizzare meò dettaglio i benefici – diretti ed indiretti, che l'esternalizzazione ai TPP può offrire agli operatori bancari nell'attuale contesto competitivo e tecnologico.

2.1.1 – I benefici economici diretti ed indiretti dell'esternalizzazione ai TPP

Al fine di fornire una risposta organica ai quesiti testé delineati, è necessario circoscrivere con maggiore precisione l'ambito di esternalizzazione oggetto d'analisi.
In questa sede, l'attenzione non sarà rivolta ai benefici dell'outsourcing ICT tradizionale – basato sulla delega estesa di attività non strategiche a fornitori terzi, come attestano il Regolamento DORA e la vasta letteratura economica – bensì a modelli *data-driven*, fondati su un'esternalizzazione selettiva e strategica.
Tali modelli si concretizzano nella concessione a terze parti dell'autorizzazione ad accedere ai conti e ad elaborare i dati detenuti dagli istituti bancari – come già illustrato nel §1.1.1 –, previo esplicito consenso dell'utente e nel rispetto del principio di *access-to-account* (XS2A) sancito dalla PSD2. In questa prospettiva, le banche mantengono la titolarità della relazione con il cliente, autorizzando però i TPP a utilizzare le informazioni in loro possesso per sviluppare soluzioni digitali avanzate – spesso tramite servizi *cloud*, integrazione API e strumenti di analisi predittiva – necessarie per la digitalizzazione dei processi di *client onboarding*, la creazione di interfacce utente evolute e strumenti di *Personal Finance Management* (PFM), nonché per lo sviluppo di servizi di pagamento digitali.
Si crea così una condizione di reciproco vantaggio, in cui la banca esternalizza il "mezzo" tecnologico necessario all'erogazione dei servizi, preservando il "fine" strategico del controllo sulla relazione con il cliente e sulla direzione complessiva dell'offerta.
Questa dinamica si inserisce in un più ampio processo di trasformazione del settore bancario, contraddistinto da una crescente frammentazione della catena del valore e dall'affermarsi di nuovi modelli di collaborazione quali il *Banking-as-a-Service* (BaaS) e il *Banking-as-a-Platform* (BaaP), che hanno spinto gli istituti bancari tradizionali a riconsiderare la centralità del proprio ruolo.
Di fatto, secondo tali modelli – oggetto di approfondimento nel §2.4 – il baricentro competitivo non dipende più tanto dal possesso dell'infrastruttura tecnologica, quanto piuttosto dalla capacità di gestire e valorizzare la relazione con il cliente finale attraverso servizi di partner terzi[192].

[192] H. Junghanns, M.Niebudek, "*Platform Banking & Digital Ecosystems*", PwC's Study, Marzo 2019, p.22

Si tratta quindi di un radicale cambiamento, che segnala il passaggio da un modello bancario tradizionale, verticalmente integrato e *capital-intensive*, a uno in cui le banche tendono a configurarsi come piattaforme relazionali in grado di orchestrare, in un disegno strategico coerente, servizi selezionati forniti da soggetti terzi.

Alla luce di quanto sopra, l'esternalizzazione selettiva verso i TPP emerge non soltanto come un adattamento a un contesto normativo e tecnologico in evoluzione, ma anche come una scelta strategica capace di rafforzare il posizionamento competitivo delle banche attraverso modelli operativi più flessibili ed operativi. Tale impostazione costituisce il presupposto per il conseguimento di benefici tangibili, che si manifestano sia sottoforma di effetti immediatamente quantificabili, sia come implicazioni di lungo periodo. Pertanto, muovendo da queste considerazioni di carattere perlopiù strategico, ai fini di una più compiuta analisi appare opportuno concentrare l'attenzione sulle ricadute economiche concrete generate dal fenomeno dell'esternalizzazione selettiva, a partire da quelle di più immediata rilevazione. In particolare, tra queste spicca, come già evidenziato in sede introduttiva, la significativa riduzione dei costi infrastrutturali e operativi.

Affidare a soggetti terzi specifiche funzionalità – quali l'aggregazione dei conti, il *budgeting* intelligente, il *risk scoring* e la profilazione dei clienti – consente, secondo l'86% degli istituti bancari intervistati da EY Parthenon, di contenere gli investimenti in infrastrutture IT, sicurezza e sviluppo software, mantenendo comunque un elevata qualità dei servizi e accelerando l'implementazione[193].

Tale aspetto assume particolare rilievo non solo in una fase di congiuntura macroeconomica sfavorevole, ma anche alla luce dell'aumento esponenziale dei costi legati al lancio di modelli di business ad alto impatto innovativo e del contestuale rallentamento della crescita dei ricavi del settore bancario.

In questo contesto, uno studio di Accenture rileva come, per mantenere un ritorno tangibile sui margini di capitale e competere efficacemente con i nuovi attori fintech e le neobanche, gli istituti debbano perseguire una riduzione dei costi compresa tra il 20% e il 25%, senza trascurare la customer expercience[194].

In linea con tali considerazioni, lo sviluppo e la manutenzione interna di soluzioni digitali risultano per molti istituti non solo economicamente gravosi, ma anche caratterizzati da complessità organizzative che rallentano il *time-to-market*. Al contrario, le tecnologie fornite dai TPP – originariamente progettate per gestire grandi volumi di dati in tempo reale – offrono un'alternativa intrinsecamente scalabile, con costi inferiori e spesso commisurati all'effettivo utilizzo.

---

[193] E. T Court, "*How banks can fix broken fintech partnership models*", https://www.ey.com/en_us/insights/strategy-transactions/how-banks-can-fix-broken-fintech-partnership-models, EY Global, Marzo 2023

[194] Accenture, "*Reinvent banking operations with data and AI*", https://www.accenture.com/us-en/industries/banking/banking-operations, 2025

In proposito, i dati raccolti da Capgemini confermano tale vantaggio per le banche, segnalando una riduzione media dei costi operativi circa pari al 33% nel caso in cui gli istituti adottino soluzioni *cloud* fornite dai TPP[195]. Questo risultato è riconducibile, tra l'altro, alla capacità degli *Account Information Service Providers* (AISP) di aggregare in un'unica dashboard dati provenienti da più conti bancari e di elaborarli in profili di spesa personalizzati, sfruttando infrastrutture cloud-native ed API-ready.
Tali caratteristiche permettono ai TPP di erogare servizi su larga scala, mantenendo elevati livelli di adattabilità e rapidità di aggiornamento tanto a livello tecnologico, quanto normativo, traducendosi così in ulteriori benefici economici e competitivi.
Sulla base di quanto finora esposto emerge, altresì, un ulteriore beneficio immediato dell'esternalizzazione dell'accesso ai dati e ai conti, rilevabile nella possibilità delle banche di fare leva sulla specializzazione tecnologica dei TPP.
Infatti, grazie alla capacità di questi ultimi di fornire soluzioni altamente scalabili e pronte all'uso, gli istituti bancari sono in grado di evitare gli ingenti investimenti richiesti per lo sviluppo interno di tecnologie complesse, la cui realizzazione richiederebbe competenze e risorse di cui essi spesso non dispongono[196].
Diversamente dagli istituti bancari tradizionali, i TPP operano in contesti altamente competitivi e *digital-first*, maturando un livello di competenza tecnica notevolmente superiore che, unito all'assenza di gravosi sistemi legacy, consente loro di sviluppare e gestire strumenti innovativi con una velocità e una reattività difficilmente replicabili con pari efficienza *in-house*. Pertanto, le banche – spesso vincolate da strutture organizzative complesse e da costi di adeguamento estremamente elevati – trovano più conveniente affidarsi a fornitori terzi specializzati, liberando al contempo risorse da reinvestire nelle attività *core* a maggiore marginalità strategica.
Un caso emblematico in tal senso è rappresentato dalla collaborazione tra ABN AMRO e Tink, TPP svedese specializzato in soluzioni di aggregazione dei dati e gestione finanziaria personale. Nello specifico, tale partnership ha permesso alla banca di integrare nella propria offerta uno strumento di *budgeting* digitale, sfruttando una tecnologia già testata e conforme alle normative di Tink ed evitando perciò il sostenimento degli oneri e dei rischi legati allo sviluppo interno[197].
In sintesi, questa decisione ha consentito all'istituto di ottimizzare tempi e risorse, determinando un significativo incremento della base utenti e un miglioramento della fidelizzazione. Ciò ha confermato

[195] Capgemini, "*La maggior parte delle banche e delle compagnie assicurative fatica a massimizzare il valore dei propri investimenti nel cloud*", https://www.capgemini.com/it-it/news/comunicati-stampa/la-maggior-parte-delle-banche-e-delle-compagnie-assicurative-fatica-a-massimizzare-il-valore-dei-propri-investimenti-nel-cloud/, Novembre 2024
[196] Gear Inc., "*The Benefits & Risks Of Outsourcing In The Banking Industry"*, https://gearinc.com/outsourcing-banking-industry/#elementor-toc__heading-anchor-0, Settembre 2024
[197] ABN AMRO, "ABN AMRO increases its stake in Tink", https://www.abnamro.com/en/news/abn-amro-increases-its-stake-in-tink, Ottobre 2017

l'efficacia dell'esternalizzazione selettiva ai TPP nel potenziare la *customer retention* e nell'arricchire l'offerta digitale, garantendo tempi di sviluppo più rapidi e costi più contenuti[198].

L'esperienza di ABN AMRO dimostra, inoltre, come l'affidamento a TPP specializzati possa non solo ridurre i costi e migliorare la qualità dei servizi, ma anche velocizzare in maniera significativa i tempi di sviluppo e di rilascio di nuove soluzioni digitali.

Questo aspetto mette in evidenza che la possibilità di ridurre drasticamente il *time-to-market* è un ulteriore fattore da considerare nell'analisi dei benefici immediatamente quantificabili.

Consapevoli della necessità di accelerare il ciclo dell'innovazione, molte banche hanno progressivamente adottato piattaforme di *core banking* flessibili – secondo il modello di *Banking-as-a-Service* precedentemente menzionato – che, sfruttando le licenze bancarie e l'accesso al capitale, consentono di integrare più rapidamente le tecnologie dei TPP.

In particolare, l'adozione di interfacce di programmazione applicativa (API) evolute ha permesso di immettere sul mercato prodotti finanziari digitali altamente adattabili, con tempi di implementazione sensibilmente ridotti rispetto allo sviluppo interno[199].

Queste interfacce, inizialmente introdotte dalla PSD2 come strumenti tecnici-normativi con finalità di sicurezza e standardizzazione dell'accesso ai dati, si sono progressivamente affermate come fulcro operativo dell'integrazione tra banche e TPP. Di fatto, da semplice mezzo di collegamento, esse si sono trasformate in una risorsa strategica, facilitando oltre il 60% dei trasferimenti dei dati nelle moderne operazioni bancarie[200].

Tale dato, quindi, mette in luce come le API stiano assumendo anche la veste di moltiplicatore dei benefici economici legati all'esternalizzazione ai TPP, oltre che rappresentare uno strumento tecnico imprescindibile per l'operatività quotidiana delle banche, in quanto concorrono a ridurre di circa il 40% il tempo di integrazione con le piattaforme di terze parti. Ciò comporta non solo un abbattimento significativo delle spese legate allo sviluppo di interfacce personalizzate, ma anche una riduzione del *time-to-market*, rafforzando così l'efficacia complessiva della collaborazione con i TPP[201].

Non sorprende, quindi, che – secondo Forrester – le banche possono lanciare prodotti digitali con maggiore rapidità grazie all'integrazione di soluzioni già esistenti e operative tramite API, ottenendo un ritorno medio sull'investimento (ROI) superiore al 300% in un arco temporale triennale. Un risultato che conferma come l'esternalizzazione selettiva dell'accesso ai dati e ai conti, unita all'uso

---

[198] Tink, "*How ABN AMRO turned its PFM app bank-agnostic*", https://tink.com/blog/use-cases/abn-amro-grip-app-aggregation/, Novembre 2019

[199] 10x Banking Technology Limited, "*How Banking-as-a-Service helps banks transform*", https://www.10xbanking.com/insights/how-banking-as-a-service-helps-banks-transform, Settembre 2021

[200] S. Lee, "*5 Key API Integrations Boosting Efficiency in Finance 2023*", https://www.numberanalytics.com/blog/api-integrations-efficiency-finance-2023, Numberanalytics, Marzo 2025

[201] FDX, "*Financial Data Exchange Response to Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights Consumer Financial Protection Bureau (CFPB)*", Dicembre 2022

strategico della API, rappresenti una leva decisiva per evitare l'obsolescenza tecnica e mantenere la competitività in un mercato altamente dinamico[202].

Tuttavia, è opportuno ricordare che, oltre ai menzionati vantaggi economici tangibili nel breve periodo, l'esternalizzazione produce anche effetti di lungo periodo di natura più strategica, che contribuiscono in misura rilevante all'efficientamento complessivo e alla crescita degli istituti bancari all'interno dell'ecosistema finanziario.

In tal senso, alcune riflessioni emerse nel corso del Bain Banking Event 2023 evidenziano che la collaborazione con TPP tecnologicamente avanzati consente di migliorare la percezione del brand, soprattutto tra le fasce di clientela più giovani e digitalmente orientate, rafforzando il rapporto di fidelizzazione tra banca e cliente[203]. Inoltre, esternalizzando componenti digitali modulari ai TPP – sfruttandoli in qualità sia di canali di diffusione che di raccolta dati –, le banche possono integrare o dismettere rapidamente servizi in risposta ai mutamenti del mercato o ai nuovi requisiti regolamentari, evitando di rimanere vincolate a infrastrutture legacy rigide.

In questa prospettiva, l'attuale contesto competitivo e macroeconomico sottolinea l'esigenza di promuovere internamente una nuova cultura del business che riconosca nei TPP partner strategici e nei dati dei clienti una risorsa fondamentale per creare valore tramite esperienze d'uso unificate e personalizzate. L'urgenza dettata dalla rapidità d'azione e dalla pressione competitiva dei nuovi player rafforza ulteriormente l'idea che l'esternalizzazione e la collaborazione con i TPP costituiscano una risposta strategica imprescindibile, capace non solo di dare impulso all'innovazione interna, ma anche di generare un effetto di "contaminazione" positivo. Ne deriva, per gli istituti bancari, una spinta concreta verso una maggiore apertura alla sperimentazione e alla revisione critica dei propri processi interni.

In conclusione, sebbene la decisione delle banche di esternalizzare l'accesso ai dati e ai conti non si configuri – come talvolta ipotizzato – quale mero adattamento passivo al dettato normativo, ma piuttosto come una scelta strategica orientata all'efficienza e all'innovazione, è imprescindibile riconoscere che essa non è esente da criticità. Se da un lato consente di accelerare la trasformazione digitale e di generare benefici economici tangibili, dall'altro solleva interrogativi rilevanti in termini di indipendenza strategica, sicurezza dei dati e compliance normativa.

Basti considerare, ad esempio, che la riduzione dei costi potrebbe rivelarsi effimera qualora gli istituti sviluppassero un'eccessiva dipendenza dai fornitori terzi, con possibili ripercussioni anche sul piano reputazionale.

---

[202] S. Lee, "*5 Key API Integrations Boosting Efficiency in Finance 2023*", cit.

[203] M. Valentini, "*Banche e innovazione, raddoppiata la spesa in tecnologia: ecco le sfide future*", https://www.economyup.it/fintech/banche-e-innovazione-raddoppiata-la-spesa-in-tecnologia-ecco-le-sfide-future/#:~:text=Banche%20e%20innovazione%2C%20come%20cambia%20il%20comportamento,di%20servizio%20personalizzato%20e%20di%20alta%20qualit%C3%A0., EconomyUp, Maggio 2023

In definitiva, il ricorso ai TPP quali partner strategici si colloca in un delicato equilibrio tra opportunità di crescita e potenziali profili di vulnerabilità. È in questa zona grigia, in cui le esigenze di innovazione e competitività delle banche si intrecciano con quelle di tutela e controllo, che si definiscono le reali dinamiche competitive del settore bancario contemporaneo. Come si vedrà nel paragrafo successivo, la "posta in gioco" travalica il mero risparmio di costi, investendo aspetti essenziali di autonomia strategica, sicurezza dei dati e conformità regolamentare.

2.1.2 I rischi per le banche legati all'esternalizzazione

Se l'analisi delle motivazioni strategico-economiche e dei benefici legati all'esternalizzazione selettiva ai TPP ha dimostrato chiaramente come questa scelta possa essere per le banche uno stimolo al cambiamento e un'opportunità per aumentare la loro competitività, è altrettanto evidente che i medesimi fattori che generano benefici immediati possono, nel medio-lungo termine, trasformarsi in fragilità strutturali. In altri termini, quei fattori che hanno reso l'outsourcing particolarmente attraente – come la rapidità di integrazione, la specializzazione tecnologica delle terze parti e la riduzione dei costi operativi e di sviluppo interno delle infrastrutture – possono tradursi in forme di dipendenza difficili da invertire, limitando di fatto l'autonomia decisionale delle banche e la loro capacità di mantenere il controllo diretto sui processi critici. Proprio in questo risiede il paradosso dell'esternalizzazione: la leva che oggi genera benefici in termini di efficienza e scalabilità può, se non viene gestita con l'attenzione dovuta, trasformarsi in futuro in una vulnerabilità strutturale capace di erodere i vantaggi che ne avevano giustificato l'adozione.

La vera questione, perciò, non è tanto *se* esternalizzare, quanto piuttosto *a quali condizioni* farlo in modo tale da non pregiudicare l'autonomia strategica, la stabilità operativa e il controllo diretto del rapporto con il cliente.

È in questo quadro che emergono i rischi specifici dell'esternalizzazione selettiva ai TPP, i quali – spesso presentandosi in forme eterogenee e interdipendenti tra di loro – spaziano dal *lock-in* tecnologico e dai costi di switching, alla perdita del *know-how* interno; dalle criticità normative e di governance connesse alla localizzazione geografica dei fornitori e alla supervisione delle attività esternalizzate, fino ai profili reputazionali e strategici legati alla disintermediazione, all'erosione della *brand identity* e alla concorrenza diretta di alcuni TPP nei segmenti *core* dell'offerta bancaria.

Tali rischi, tuttavia, non si manifestano in modo astratto, bensì si inseriscono in un contesto competitivo in continua evoluzione, in cui – come evidenziato nei §§2.1 e 2.1.1 – il settore bancario, sebbene abbia mantenuto un ruolo centrale nella vita quotidiana delle persone, ha progressivamente visto ridursi la capacità degli istituti tradizionali di presidiare i canali e i dati della clientela, complice la rigidità dei sistemi legacy e i vincoli regolamentari.

L'indebolimento della centralità del loro ruolo, unito all'incapacità di valorizzare appieno i dati a disposizione nel miglior interesse dei clienti e della loro esperienza complessiva, ha favorito così l'ingresso di attori più agili e *digital-first*, inducendo le banche a delegare a soggetti terzi un numero crescente di funzioni legate all'accesso ai dati e ai conti, talvolta anche essenziali[204].

Se da un lato questa strategia ha consentito – come esposto nel §2.1.1 – di affinare la *user experience* (*UX*) e di preservare la redditività dei modelli di business, dall'altro ha generato un crescente rischio di dipendenza strutturale dalla fornitura di servizi di terze parti (*vendor lock-in*[205]).

In proposito, le analisi condotte dalla Banca Centrale Europea (BCE) confermano non solo la centralità, ma anche la delicatezza di questo fenomeno, evidenziando come una quota significativa dei contratti attivi di outsourcing bancario riguardi proprio quelle funzionalità che incidono direttamente sulla gestione ed elaborazione dei dati (*Account Information Service*) e sull'avvio delle operazioni di pagamento (*Payment Initiation Service*). Tale dato assume particolare rilievo specialmente se messo in relazione con un'ulteriore evidenza fornita nello stesso rapporto dalla BCE, secondo cui nell'82% dei casi i fornitori terzi coinvolti risultano difficili o impossibili da sostituire in tempi rapidi e a costi contenuti, con il pericolo concreto di generare ricadute sistemiche sull'intero settore[206].

Ne consegue che, laddove le banche decidano di concentrare queste funzioni in pochi TPP – o addirittura in capo a un unico soggetto terzo – esse riducono drasticamente la propria capacità di negoziazione, aumentando l'esposizione al rischio di interruzioni di servizio o di variazioni unilaterali delle condizioni contrattuali[207].

In questo panorama, un esempio emblematico è rappresentato da Solarisbank, che offre una vasta gamma di prodotti modulari facilmente personalizzabili e integrabili nei portafogli per numerosi brand bancari europei e fintech – tra cui Visa, BBVA e ABN AMRO [208]. Tale modello, pur mettendo in luce le potenzialità dell'esternalizzazione in termini di efficienza, velocità e flessibilità, evidenzia al tempo stesso la fragilità di un ecosistema eccessivamente dipendente da un unico TPP, in cui un

---

[204] J. Bellens, "*Five questions about banking in today's digital age, answered*", https://www.ey.com/en_pt/insights/banking-capital-markets/five-questions-about-banking-in-todays-digital-age-answered, Ey Global, Marzo 2021

[205] Con il termine di "*vendor lock-in*" si intende, in gergo economico, "*il rapporto di dipendenza che si instaura tra il cliente (banca) ed un fornitore di beni o servizi (TPP), tale che il cliente si trova nella condizione di non poter acquistare analoghi beni e servizi da un fornitore differente senza dover sostenere rilevanti costi e rischi per effettuare questo passaggio*". Per ulteriori approfondimenti in merito alle possibili condizioni legate ai casi di *vendor lock-in* si veda: Wikipedia, "Vendor lock-in", https://it.wikipedia.org/wiki/Vendor_lock-in

[206] BCE, "*2024 Outsourcing Register – Horizontal Analysis*", https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.outsourcing_horizontal_analysis_202402~2b85022be5.en.pdf, Directorate General Horizontal Line Supervision, pp.4-5

[207] P. Noujeim, "*Unpacking the Financial and Security Implications of Vendor Lock-In*", https://d3security.com/blog/cybersecurity-vendor-lock-in-risks-soar-solution/#:~:text=and%20strategic%20freedom.-,What%20is%20Vendor%2DLock%2DIn?,reconfiguring%20systems%20and%20training%20staff, D3, Novembre 2023

[208] Solaris, "*About us*", https://www.solarisgroup.com/en/about/

eventuale malfunzionamento o una criticità di governance del fornitore potrebbe generare effetti sistemici a catena paralizzando l'intero mercato.

A questa dipendenza strutturale si sommano i costi di *switching*, resi particolarmente gravosi dalla scarsa interoperabilità tra sistemi. Infatti, sebbene l'adozione diffusa di interfacce API evolute rappresenti – come discusso nel §2.1.1 – lo strumento abilitante dell'esternalizzazione selettiva ai TPP, l'assenza di standard tecnici uniformi fa sì che, in caso di migrazione verso un nuovo partner, le banche siano costrette a rivedere i processi interni, formare nuovamente il personale e, soprattutto, ottenere un nuovo consenso da parte degli utenti ai sensi dell'art. 64 PSD2. Di conseguenza, ciò si traduce non solo in un costo economico significativo, ma anche nel rischio di perdita della clientela e in un possibile deterioramento del livello della qualità e della continuità dei servizi offerti[209].

Mentre i costi di switching rappresentano l'effetto più immediato e tangibile del *vendor lock-in*, ancora più rilevante nel medio-lungo termine è la progressiva perdita di know-how interno, che incide direttamente sulla capacità delle banche di innovare e mantenere autonomia strategica.

Molto spesso, infatti, la scelta di esternalizzare in modo sistematico lo sviluppo e la gestione dei servizi AIS e PIS comporta un progressivo impoverimento delle competenze *in-house* degli istituti, rendendoli dipendenti non solo dalla continuità operativa del fornitore, ma anche dal percorso di innovazione tecnologica, accentuando notevolmente le difficoltà di differenziazione nella relazione con il cliente finale.

Accanto a tali profili di natura strettamente operativa ed economica, assumono rilievo anche le criticità di ordine normativo e di governance che l'esternalizzazione selettiva inevitabilmente comporta.

Come già evidenziato nel primo capitolo, il quadro regolamentare europeo si presenta estremamente complesso e in costante revisione – si pensi, ad esempio, alle proposte attualmente pendenti relative al *Payment Packag*e e al *Financial Data Access Regulation* (FiDA). Tenendo presente tali premesse è opportuno sottolineare che, l'affidamento a terze parti determina per le banche un ulteriore onere di conformità, imponendo loro di vigilare affinché i TPP, nello svolgimento dei servizi esternalizzati, rispettino le disposizioni in materia di protezione dei dati personali, sicurezza informatica e continuità operativa[210]. Ciò in quanto, pur essendo formalmente previsto dalla PSD2 un riparto delle responsabilità tra TPP e banche (cfr. §1.1.2), la responsabilità ultima per il mancato rispetto degli obblighi normativi delle terze parti rimane comunque in capo agli istituti bancari, esponendoli non solo a sanzioni amministrative e legali, ma anche a danni reputazionali difficilmente recuperabili[211].

---

[209] Gear Inc., "*The Benefits & Risks Of Outsourcing In The Banking Industry*", https://gearinc.com/outsourcing-banking-industry/#elementor-toc__heading-anchor-1, Settembre 2024

[210] Ibid.

[211] SG Analytics, "*The Benefits and Risks of Banking Outsourcing in 2025*", https://writeupcafe.com/the-benefits-and-risks-of-banking-outsourcing-in-2025, Writeupcafe, Luglio 2025

In tal senso il caso Plaid, richiamato al §1.3.1, risulta esplicativo, in quanto dimostra effettivamente come un uso improprio dei dati sensibili a disposizione di un TPP possa tradursi in pesanti conseguenze legali (quali le *class action* promosse dai consumatori) e in rilevanti danni di immagine per tutti gli istituti coinvolti, anche laddove questi non abbiano avuto un ruolo attivo nella violazione. Tale criticità si accentua sensibilmente nei casi di outsourcing transfrontaliero, in cui i fornitori terzi, avendo sede legale al di fuori dell'Unione Europea, operano in ordinamenti giuridici caratterizzati da standard di tutela meno stringenti rispetto a quelli comunitari. In tali circostanze, più che di una vera e propria "asimmetria normativa", è opportuno parlare di una difficoltà di armonizzazione e di enforcement delle regole europee, con potenziali ricadute sulla piena applicazione del GDPR (si veda §1.1.4) e della PSD2, oltre che sulla sicurezza dei dati trattati. In ragione di ciò, le banche sono chiamate a adeguarsi a normative multiple, sostenendo così maggiori costi di compliance, audit e governance.

Sotto il profilo della sicurezza, inoltre, va considerato che l'affidamento a soggetti terzi della gestione dei dati transnazionali e di profilazione riduce considerevolmente la capacità delle banche di esercitare un controllo diretto, esponendole al rischio di violazioni e di utilizzi impropri delle informazioni da parte dei TPP. Questa problematica appare ancor più evidente se si considera che circa il 70% dei contratti di outsourcing riguarda proprio servizi che implicano il trattamento di dati personali e che, in circa il 10% dei casi, tali contratti non risultano conformi alla normativa vigente[212].

Nonostante il profilo normativo rappresenti un aspetto centrale nella valutazione dei rischi, in un settore – quale quello bancario – in cui la fiducia costituisce "*la condizione necessaria affinché le banche possano operare, promuovere la crescita economica e conferire valore aggiunto alla società*", la conseguenza più immediata e insidiosa di una gestione inadeguata dell'esternalizzazione selettiva ai TPP è il rischio reputazionale[213].

Negli ultimi anni, tuttavia, nel tentativo di mantenere la propria competitività a livello globale, gli istituti bancari si sono concentrati prevalentemente sull'ottimizzazione dei costi e sulla mitigazione dei problemi di compliance – specialmente nei rapporti con i fornitori extra-UE – trascurando spesso i rischi indiretti, tra cui quello reputazionale. Eppure, proprio questi ultimi, pur essendo intangibili e difficilmente quantificabili, si rivelano spesso i più insidiosi, in quanto capaci di produrre conseguenze sistemiche e di incidere in misura ancora più significativa sul funzionamento dell'intero sistema economico. Non a caso, secondo quanto riportato da AXA, non sono mancate circostanze in

[212] F. Ninfole, "*La Vigilanza Bce mette in guardia le banche sui rischi legati a cloud e outsourcing di attività critiche*", https://www.milanofinanza.it/news/la-vigilanza-bce-mette-in-guardia-le-banche-sui-rischi-legati-all-outsourcing-di-attivita-critiche-202402211841269565?refresh_cens, Febbraio 2024

[213] ECB Banking Supervision, "*Reintegrating the banking sector into society: earning and re-establishing trust*", https://www.bankingsupervision.europa.eu/press/speeches/date/2015/html/se150928.it.html

cui le disfunzioni dei TPP hanno determinato per le banche coinvolte ripercussioni rilevanti non tanto sotto il profilo strettamente finanziario, quanto piuttosto sul piano reputazionale[214].

In linea con questa evidenza, occorre considerare che un incidente di sicurezza o un malfunzionamento da parte del TPP, pur non essendo direttamente imputabile alla banca, ricade comunque su di essa agli occhi dell'opinione pubblica e delle autorità di vigilanza. Tale rischio risulta ancor più evidente nei casi in cui il controllo dei processi di gestione viene trasferito al TPP oppure quando i servizi vengono erogati "invisibilmente" tramite modelli *white-label*. È proprio in questa prospettiva che la distinzione giuridica tra banca e TPP tende a sfumare, rendendo difficile per l'istituto bancario sia monitorare la qualità del servizio che, al tempo stesso, tracciare con precisione le prestazioni del fornitore[215]. Di qui il motivo per il quale, talvolta, le banche finiscono per essere relegate al mero ruolo di *back-end provider*, perdendo di fatto visibilità sul mercato e, conseguentemente, parte della fiducia della clientela.

Emblematico, a questo riguardo, è l'episodio che colpì NatWest, i cui clienti si trovarono improvvisamente impossibilitati ad accedere ai propri fondi a seguito di un aggiornamento mal gestito della piattaforma esternalizzata[216]. L'accaduto dimostra chiaramente come la crisi di un fornitore terzo non si traduca unicamente in un'interruzione di servizio, ma si configuri primariamente come un danno reputazionale per la banca, poiché, dal punto di vista dell'utente finale, ciò che rileva non è la distinzione formale tra gli attori coinvolti, bensì l'esperienza concreta e immediata del servizio.

Ad ulteriore conferma della centralità del rischio reputazionale, si è espressa anche la Banca d'Italia, sottolineando che, "[sebbene] l'offerta dei nuovi servizi AIS e PIS possa avvenire in maniera integrata nell'offerta commerciale di un altro prestatore di servizi di pagamento, […] l'offerta di un servizio di terzi sull'interfaccia della banca o di un altro PSP con il quale il cliente ha già un rapporto contrattuale, potrebbe rendere non particolarmente chiaro il mero ruolo d'intermediazione svolto dalla propria banca"[217]. Pertanto, in assenza di un'adeguata informativa alla clientela, lo svolgimento di determinati servizi da parte di terze parti all'interno dei canali bacari rischia di accrescere l'esposizione reputazionale degli istituti, con potenziali ricadute in termini di credibilità sul mercato.

Ad accrescere, poi, l'instabilità dello scenario entro cui operano le banche vi è il pericolo che la collaborazione con i TPP sfoci, sul piano più ampio del posizionamento competitivo, in una progressiva disintermediazione degli istituti.

---

[214] A. Defteros, "*Banche: benefici e rischi dell'esternalizzazione*", https://axaxl.com/it/fast-fast-forward/articles/banche-benefici-e-rischi-dell-esternalizzazione, AXA XL, Gennaio 2017

[215] SG Analytics, "*The Benefits and Risks of Banking Outsourcing in 2025*", cit.

[216] K. Makortoff, "*NatWest apologises to millions of customers locked out of app*", https://www.theguardian.com/business/2025/jun/06/natwest-apologises-to-millions-of-customers-locked-out-of-app, The Guardian, Gennaio 2025

[217] Banca d'Italia, "*PSD2 e Open Banking: nuovi modelli di business e rischi emergenti*", cit., p. 27

L'accesso privilegiato ai dati e la gestione delle interfacce digitali – sempre più spesso affidata a soggetti terzi – riducono infatti la capacità di interagire direttamente con la clientela e, con essa, la visibilità del marchio bancario, spostando l'attenzione sull'esperienza fornita dal TPP piuttosto che sull'istituto stesso.

Nonostante ciò, indagini di mercato hanno messo in luce come circa il 40% delle partnership bancarie non riesca a consolidarsi in progetti operativi, o registri tassi di fallimento compresi tra il 20% e il 40% entro i primi anni, a causa di strategie inefficaci, problemi di scalabilità e scarso allineamento strategico[218]. Tali dati segnalano, perciò, che la mancanza di strategie *go-to-market* adeguate e di processi strutturati che definiscano ruoli, responsabilità e modalità di supervisione, inibiscono la corretta gestione dell'esternalizzazione trasformandola in una innovazione di "facciata", incapace di produrre valore durevole.

Sempre sul piano strategico, è noto che l'esternalizzazione di servizi AIS e PIS ha creato le condizioni per cui i TPP riescono a creare legame diretto con i clienti, fornendo servizi tipicamente bancari – quali, ad esempio, pagamenti, prestiti e investimenti – ponendosi così in diretta competizione con gli istituti tradizionali riducendone il ruolo a mero "punto di riferimento" del cliente.

Questo duplice ruolo – partner tecnologico e potenziale concorrente – ha reso particolarmente complesso il disegno strategico di lungo periodo delle banche, alimentando la propensione degli utenti a privilegiare i canali digitali nella gestione delle proprie attività finanziarie e favorendo, contestualmente, la progressiva chiusura delle filiali fisiche.

In definitiva, se l'esternalizzazione selettiva ai TPP ha rappresentato per molte banche uno strumento di mera compliance per adeguarsi agli obblighi introdotti dalla PSD2, non sempre essa è stata accompagnata da una reale strategia di innovazione né da un'attenta valutazione dei rischi connessi. L'averla considerata come una "scorciatoia", più che come una scelta strategica ponderata, ha in alcuni casi esposto gli istituti a fragilità tali da minarne la resilienza nel lungo periodo. Sebbene i benefici derivanti dall'apertura ai TPP restino indubbi, per poterli cogliere le banche sono chiamate a sviluppare capacità di governance adeguate, in grado di bilanciare innovazione e presidio del rischio, delega e mantenimento del controllo. Solo in questo modo l'esternalizzazione può trasformarsi da vulnerabilità potenziale a leva effettiva di competitività.

Tuttavia, per comprendere effettivamente la portata di questo fenomeno è necessario volgere lo sguardo all'altra faccia della medaglia: se per le banche l'esternalizzazione implica un delicato equilibrio tra benefici e rischi, per i TPP essa ha rappresentato allo stesso tempo un'occasione di

[218] E. T. Court "*How banks can fix broken fintech partnership models*", https://www.ey.com/en_us/insights/strategy-transactions/how-banks-can-fix-broken-fintech-partnership-models, EY Parthenon, Marzo 2023

crescita e un banco di prova. Dunque, la vera sfida per questi soggetti sarà dimostrare di saper coniugare crescita e affidabilità, profilo che sarà approfondito nel paragrafo seguente.

2.2 - L'esternalizzazione dal punto di vista dei TPP: tra opportunità e minacce

L'obbligo normativo imposto dalla PSD2 di aprire i dati e i conti bancari a soggetti terzi ha avuto effetti immediati e dirompenti sul settore finanziario, incrinando un assetto storicamente fondato sulla chiusura e sul presidio esclusivo delle informazioni da parte degli istituti bancari[219].

Se dal lato delle banche (cfr. § 2.1) tale apertura si è configurata come un adempimento regolamentare da bilanciare con esigenze di efficienza, controllo e tutela della clientela, dal lato dei TPP essa ha assunto la valenza di condizione abilitante della loro stessa attività economica.

Per questi ultimi, infatti, l'accesso ai dati bancari – reso possibile dall'esternalizzazione selettiva di funzioni un tempo riservate agli intermediari – non rappresentava un vincolo da gestire, bensì il presupposto indispensabile per entrare nel mercato e costruire un'identità imprenditoriale autonoma. In altri termini, ciò che per le banche si traduce in un trasferimento parziale di prerogative e nella necessità di condividere asset strategici con potenziali concorrenti, per i TPP costituisce una risorsa primaria e non sostituibile, da cui dipende la loro stessa sopravvivenza.

Ne deriva un rapporto strutturalmente asimmetrico, in cui i TPP basano la creazione del proprio valore su un asset – i dati e i conti – che non possiedono, ma al quale accedono esclusivamente in virtù di un obbligo regolamentare imposto agli istituti di credito. Tale condizione genera un paradosso: se, da un lato, l'esternalizzazione apre a nuove opportunità di crescita e innovazione, consentendo ai TPP di trovare in questa apertura lo spazio per sviluppare modelli di business scalabili e ad alto potenziale innovativo; dall'altro, essa rappresenta anche la loro più grande vulnerabilità, esponendoli a rischi di dipendenza e di sostenibilità economica.

È proprio su questa ambivalenza che si fonda l'analisi del presente paragrafo, che non si limita a una lettura neutrale delle opportunità offerte ai TPP dall'esternalizzazione, ma prende in esame anche le criticità che rischiano di comprometterne la stabilità nel medio-lungo termine. Solo attraverso tale duplice prospettiva sarà possibile comprendere se l'esternalizzazione selettiva rappresenti un modello *win-win* per banche e TPP, oppure se essa costituisca una soluzione solo transitoria, destinata a ridefinire in modo strutturale il ruolo degli intermediari nel mercato dei dati.

[219] M. S. Desario, Raffaele Croce, "*La nozione di banca nell'evoluzione storica dell'ordinamento del credito*", DB-Non solo Diritto Bancario, Settembre 2024

2.2.1 - Opportunità economiche e di crescita per i TPP

Prima di entrare nel merito delle opportunità economiche e di crescita legate all'esternalizzazione selettiva per i TPP, è opportuno soffermarsi brevemente su uno dei suoi effetti sistemici di più immediata evidenza, ovvero l'abbattimento delle barriere all'ingresso del mercato.

Come rilevato anche nel §1.1, gli operatori non bancari che in origine intendevano offrire servizi di analisi finanziaria o avviare disposizioni operative erano costretti a ricorre a pratiche controverse, come lo *screen scraping*, caratterizzate da costi elevati, rischi giuridici significativi e scarsa affidabilità tecnica. Tuttavia, con l'entrata in vigore della PSD2 – e, in particolare, con il Regolamento delegato (UE) 2018/389 – l'introduzione di un diritto regolato di accesso alle informazioni di conto e ai flussi transazionali tramite API ha reso possibile l'ingresso dei TPP nel mercato secondo basi nuove, certe e standardizzate.

Questo cambiamento, pur configurandosi come un effetto sistemico della Direttiva (UE) 2015/2366, ha avuto per le terze parti una valenza eminentemente opportunistica. In particolare, la riduzione delle barriere, congiuntamente all'avvio operativo dei servizi AIS, PIS e CIS ha rappresentato la condizione abilitante non soltanto per l'ingresso dei TPP in un mercato storicamente caratterizzato dal monopolio informativo delle banche, ma anche per un mutamento della natura economica del dato bancario. Difatti, ciò che in passato costituiva un asset esclusivo, detenuto e sfruttato unicamente dagli istituti di credito, è oggi divenuto un bene condiviso all'interno dell'ecosistema, accessibile – previo consenso del cliente – anche a soggetti terzi[220].

È proprio tale cambio di paradigma che ha reso possibile la progressiva elaborazione di modelli di business innovativi e intrinsecamente scalabili, fondati sulla valorizzazione dei dati bancari e sull'offerta di servizi a valore aggiunto. In altri termini, quello che a livello di sistema rappresentava una "democratizzazione" dell'accesso ai dati, per i TPP si è tradotto, mediante l'esternalizzazione selettiva dell'accesso ai dati e ai conti, in una concreta possibilità di crescita e differenziazione competitiva, aprendo la strada a un'offerta sempre più articolata di servizi e prodotti.

Su queste basi si è progressivamente affermata una varietà di modelli caratterizzati da un impianto fortemente *data-driven* e ad alta componente tecnologica, tra i quali quelli che hanno registrato la maggiore diffusione e consolidamento nel panorama europeo sono i servizi di gestione finanziaria personale (*Personal Financial Management*) e i sistemi di *credit scoring* alternativi.

Nonostante entrambi trovino nel dato bancario esternalizzato la propria leva di sviluppo, essi si distinguono per il diverso ambito applicativo: i primi valorizzano il dato in chiave *consumer*, aiutando i clienti a gestire le proprie finanze e a prevedere esigenze future, mentre i secondi – spesso ricondotti

[220] Stripe, "*Cos'è l'open banking e come funziona*?", https://stripe.com/it/resources/more/open-banking-explained, aprile 2025

al paradigma del *lending-as-a-service* –, ne fanno un uso prevalentemente *business-oriented*, fornendo agli istituti bancari presso cui è radicato il conto strumenti di valutazione più accurati della solvibilità e dell'affidabilità creditizia degli utenti[221].

Oltre a questi modelli, negli ultimi anni si sono diffusi ulteriori approcci tecnologicamente più avanzati – quali, il *Buy Now, Pay Later* (BNPL) e l'*embedded finance* –, caratterizzati dall'integrazione nativa di funzionalità finanziarie all'interno delle piattaforme digitali di *e-commerce* e dei *merchant*[222].

In questo contesto, un esempio emblematico dello sviluppo dei modelli di finanza integrata (*embedded finance*) è rappresentato da Solarisbank, che – come discusso nel §2.1.2 – si è affermata come uno degli attori di riferimento del mercato tedesco ed europeo, offrendo servizi finanziari a valore aggiunto, personalizzabili e facilmente integrabili nell'EEA attraverso una piattaforma tecnologica basata su API[223]. Secondo questo modello, le banche possono incorporare rapidamente nelle loro piattaforme i servizi sviluppati da Solaris, ospitati nel cloud e caratterizzati da tempi di implementazione ridotti, migliorando così la *user experience* e riducendo le complessità legate alla compliance, pur mantenendo il pieno controllo del rapporto con i clienti e sul design del prodotto finale.

Pertanto, questo caso prova come il meccanismo dell'esternalizzazione dell'accesso ai dati costituisca non solo una leva per accelerare l'innovazione, ma anche un'opportunità per i TPP di assumere un ruolo infrastrutturale scalabile, capace di ridefinire le modalità di collaborazione con gli istituti di credito.

Ad incidere ulteriormente su questa dinamica di coopetizione tra banche e TPP è anche l'assetto organizzativo e regolamentare dei soggetti coinvolti. A differenza degli istituti bancari – vincolati da architetture legacy e da stringenti requisiti prudenziali che ne limitano la flessibilità operativa – i TPP, non essendo sottoposti ai medesimi vincoli infrastrutturali e prudenziali[224], hanno potuto concentrare le proprie risorse non tanto su investimenti in infrastrutture proprietarie costose e complesse, quanto

---

[221] M. Navacci, "*Credit scoring: cos'è, come funziona, quali sono i rischi e le tutele*", https://www.agendadigitale.eu/sicurezza/privacy/credit-scoring-cose-come-funziona-quali-sono-i-rischi-e-le-tutele/, Agenda Digitale, febbraio 2020

[222] A. Casagrande, "*Banking as a service e finanza integrata: definizioni e differenze*", https://www.opyn.eu/en/resources/blog/banking-as-a-service-and-embedded-finance-definition-and-differences, OPYN, novembre 2023

[223] ZeroUno, "*Solarisbank, ecco chi è e cosa fa*", https://www.zerounoweb.it/cloud-computing/solarisbank-ecco-chi-e-e-cosa-fa/, Luglio 2021

[224] Nello specifico, si ricorda che gli istituti bancari sono soggetti a una disciplina di vigilanza più stringente e specifica per la raccolta del risparmio tra il pubblico, che all'art. 11 del Testo Unico Bancario viene definita quale attività di acquisizione di fondi con obbligo di rimborso, sia sotto forma di depositi sia sotto altra forma, vietata ai soggetti diversi dalle banche. Inoltre, a differenza dei TPP che sono soggetti a specifici vincoli a seconda dell'attività svolta e ad controllo da parte delle autorità minore, le banche operano sotto l'autorizzazione e la vigilanza della Banca d'Italia, che impone specifici requisiti di solvibilità ed adeguatezza patrimoniale, basti pensare all'obbligo di mantenere costantemente un coefficiente di solvibilità minimo dell'8%.

piuttosto sull'elaborazione dei dati a loro disposizione per sviluppare strategie *go-to-market*, servizi digitali intuitivi e prodotti ad alto valore aggiunto per il consumatore finale.

Alla luce di quanto sopra, è possibile comprendere le ragioni per cui molti TPP sono riusciti a conquistare rapidamente quote di mercato, intercettando segmenti di clientela – quali i *millennials* e le piccole medie imprese digitali (PMI) – tradizionalmente non serviti dagli istituti bancari tradizionali, ma sempre più orientati all'utilizzo di internet e degli *smart device*, influenzandone i comportamenti sociali e di consumo[225]. Tuttavia, come si discuterà nel prosieguo del paragrafo, quest'efficienza operativa legata allo sviluppo di modelli prettamente *digital-first* non sempre si traduce in sostenibilità economica per le terze parti, le quali molto spesso si trovano costrette ad affrontare perdite significative nei primi anni di attività.

Nonostante ciò, il riconoscimento uniforme del diritto di accesso ai dati e ai conti in tutto il territorio dell'Unione europea, parimenti al principio di *passporting*[226] sancito dalla PSD2, ha permesso ai TPP di scalare più rapidamente i propri modelli su diversi mercati, crescendo velocemente senza sostenere i costi tipici degli intermediari tradizionali. In questo modo, le terze parti, sfruttando sia la standardizzazione regolamentare che la loro infrastruttura tecnologica modulare, non necessitano di costruire reti fisiche o di negoziare con ogni singolo istituto bancario, ma replicano unicamente la propria offerta in ciascun mercato. Questa circostanza ha contribuito quindi a rendere ancora più attraenti i TPP, soprattutto agli occhi di investitori istituzionali e del venture capital, i quali hanno visto negli obblighi normativi legati all'apertura dei dati una garanzia di stabilità dei loro modelli di business oltre che di stimolo innovativo per l'intero ecosistema finanziario.

In questa prospettiva si colloca l'esperienza di Tink, originariamente nata come piattaforma di aggregazione dei dati bancari e progressivamente evolutasi fino a divenire uno dei principali API-provider paneuropei, culminando con la sua acquisizione da parte di Visa per 1,8 miliardi di euro. Tale operazione appare particolarmente significativa, poiché evidenzia come l'interesse di Visa non fosse rivolto unicamente alle competenze tecnologiche acquisite dal provider svedese, quanto piuttosto al patrimonio standardizzato di dati bancari da esso gestito. Di fatto, è proprio tale asset

---

[225] KPMG, "Evoluzione dei modelli distributivi bancari. L'impatto del COVID-19 sui modelli di servizio delle banche italiane", pp.9-11, marzo 2021

[226] Ai sensi della Direttiva (UE) 2015/2366 (PSD2), il cosiddetto *passporting* consiste nella possibilità, riconosciuta agli istituti di pagamento debitamente autorizzati nello Stato membro di origine, di prestare servizi sull'intero territorio dell'Unione senza necessità di un'ulteriore autorizzazione nello Stato ospitante. In particolare, l'art. 11, par. 9, stabilisce che: "*l'autorizzazione rilasciata dall'autorità competente di uno Stato membro consente all'istituto di operare in tutta l'Unione sia in regime di libertà di stabilimento, mediante succursali o agenti, sia in regime di libera prestazione di servizi*". Tuttavia, tale facoltà non è incondizionata: l'art. 27 prevede infatti che l'istituto che intenda fornire per la prima volta servizi di pagamento in un altro Stato membro debba darne comunicazione all'autorità competente del proprio Stato d'origine, trasmettendo un insieme di informazioni prescritte dalla direttiva. Sulla base di tali informazioni – e tenuto conto di eventuali osservazioni dell'autorità dello Stato ospitante – l'autorità di origine può rifiutare la registrazione dell'agente o della succursale, ovvero revocarla se già effettuata.
Il *passporting* non si configura dunque come un diritto assoluto, ma come una facoltà subordinata al rispetto di obblighi procedurali e alla valutazione congiunta delle autorità nazionali coinvolte.

informativo ad essersi rivelato indispensabile per consentire a Visa di "*espandere [il proprio raggio di azione oltre] la tradizionale attività di gestione pagamenti con carta, accelerando al contempo l'adozione* dell'Open Banking in Europa *e rafforzando una piattaforma sicura e affidabile*" [227]. Analogo è il caso di Plaid, che, da semplice piattaforma basata sull'esternalizzazione dei dati, si è rapidamente affermata come infrastruttura di riferimento in oltre venti Paesi, connessa a più di 12.000 istituzioni finanziarie – tra cui anche N26. Nello specifico, attraverso i propri servizi, tale piattaforma consente un accesso in tempo reale ai dati, creando le condizioni affinché gli utenti non siano costretti a scegliere tra semplicità di utilizzo e sicurezza, ma possano invece valorizzare il proprio patrimonio informativo mediante esperienze finanziarie rapide, sicure ed intelligenti.[228]

In parallelo, è emersa l'opportunità dei TPP di essere impiegati anche da altri operatori economici – quali, le Big Tech, le imprese e le istituzioni finanziare – come *gateway* per integrare nei loro ecosistemi digitali funzionalità finanziarie, senza dover interfacciarsi direttamente con gli istituti bancari. Tale fatto ha favorito la diversificazione delle modalità di monetizzazione, aspetto particolarmente rilevante in un contesto in cui l'offerta di servizi di aggregazione dei dati e di *personal financial management* (PFM), spesso erogati gratuitamente alla clientela finale, creava significativi problemi di sostenibilità economica. In tal modo, le terze parti si sono progressivamente affermate come abilitatrici tecnologiche in un mercato non più soltanto B2C, ma anche B2B e B2B2C.

A confermarlo è il caso di TrueLayer, provider britannico che ha adottato una strategia di monetizzazione prevalentemente orientata al B2B, offrendo API per i pagamenti e la gestione dei dati a banche ed imprese. In particolare, il successo di questo modello risiede principalmente nella capacità di intercettare le esigenze non solo dei consumatori finali, ma anche di attori istituzionali e corporate, ottimizzando i processi di pagamento attraverso interfacce dedicate e consentendo alle aziende *retail* di integrare soluzioni di *bank payment* tramite appositi plugin[229].

Pertanto, questi esempi – assieme al caso di Solarisbank – confermano con maggiore enfasi nella pratica come l'esternalizzazione dell'accesso ai dati bancari abbia rappresentato non soltanto la condizione che ha consentito l'ingresso dei TPP nell'ecosistema finanziario, ma anche il presupposto per la loro evoluzione in piattaforme abilitanti, scalabili ed attrattive, favorendo così l'erosione dei confini tra settore finanziario e non finanziario. Tuttavia, ad ogni opportunità si affianca una minaccia speculare: la scalabilità può tradursi in vulnerabilità, l'innovazione in difficoltà di monetizzazione, la collaborazione con le banche in dipendenza strategica.

---

[227] E. Prallini, "*Perché Visa ha acquistato la fintech svedese Tink per 1,8 miliardi di euro*", https://forbes.it/2021/06/24/tink-la-fintech-svedese-acquistata-da-visa-per-sbarcare-nell-open-banking, Forbes Italia, giugno 2021

[228] Plaid,"*Abo*ut", https://plaid.com/en-eu/

[229] TrueLayer, https://truelayer.com/it-it/

In questa prospettiva, anche la dimensione tecnologica dell'Open Banking – rappresentata dalle API –, assume un ruolo cruciale sotto il profilo delle vulnerabilità. Se da un lato tali interfacce costituiscono lo strumento abilitante dell'esternalizzazione selettiva (cfr. §2.1.1), garantendo ai TPP l'accesso regolato ai dati e conti bancari, dall'altro esse si rivelano una delle principali fonti di criticità operative, finendo per ostacolare – anziché favorire – l'efficienza e la competitività dei servizi offerti dai TPP.

Quindi, alla luce di tali tensioni sorge spontanea la domanda se il successo finora conseguito dai TPP sia destinato a tradursi in una creazione di valore duratura nel lungo periodo, oppure se l'Open Banking non rischi, paradossalmente, di essere frenato proprio dalle fragilità economiche degli stessi attori che avrebbe dovuto emancipare.

È a partire da questo interrogativo che il § 2.2.2 concentrerà l'attenzione sull'analisi delle principali criticità economiche e operative che rischiano di compromettere la sostenibilità dei modelli di business dei TPP.

2.2.2 - Minacce e criticità per i TPP: tra scarsa monetizzazione e dipendenza dalle banche

Laddove l'esternalizzazione dell'accesso ai dati e conti bancari sembrava garantire ai TPP la chiave per emanciparsi dal monopolio informativo delle banche, la realtà restituisce un quadro più complesso, in cui le stesse caratteristiche che costituiscono la loro principale risorsa si rivelano – al tempo stesso – la loro più grande fragilità.

Ne consegue che l'intero modello si regge su un equilibrio precario, nel quale le promesse di innovazione e scalabilità si intrecciano con criticità strutturali, tecnologiche e regolamentari che rischiano di comprometterne la sostenibilità nel lungo termine.

In questo quadro, le difficoltà di monetizzazione dei servizi di base, la dipendenza dai flussi informativi gestiti dalle banche, le inefficienze delle API e la pressione costante degli investitori configurano un insieme di ostacoli che non si limitano soltanto a rallentare la crescita, ma rischiano addirittura di compromettere la stessa capacità dei TPP di creare valore duraturo e sostenibile nel lungo termine.

Tenendo presente quanto sopra, una delle prime e più evidenti fragilità connesse all'esternalizzazione selettiva riguarda proprio la difficoltà dei TPP di monetizzare i servizi di base. Se da un lato l'accesso regolato ai dati ha consentito alle terze parti di sviluppare soluzioni innovative e attrarre ampi segmenti di clientela, dall'altro non si è tradotto in modelli economici immediatamente redditizi. Non tutti gli operatori, infatti, sono riusciti a convertire l'accesso ai dati esternalizzati in flussi di ricavi sostenibili, soprattutto nel segmento *retail*. Tale circostanza potrebbe essere riconducibile al fatto che, nella maggior parte dei casi, servizi quali la gestione finanziaria personale (PFM) e l'aggregazione

dei conti vengono offerti gratuitamente al consumatore finale, in quanto l'obiettivo dei TPP non è tanto generare margini diretti tramite commissioni o canoni, quanto piuttosto dalla valorizzazione dei dati ceduti dalla clientela[230].

Non a caso – come osservato anche dalla Banca d'Italia –, i servizi di *Account Information Service* (AIS) e di *Payment Initiation Service* (PIS) "*fungono da porta di ingresso per l'erogazione di servizi a maggiore valore aggiunto*", giacché se considerati isolatamente produrrebbero ricavi estremamente irrisori[231]. Si tratta, in altri termini, di servizi *loss leader* o "*gateway*": indispensabili per penetrare nuovi segmenti di mercato e fidelizzare la clientela, ma strutturalmente incapaci di garantire, da soli, la sostenibilità economica dei modelli di business[232].

Tuttavia, per comprendere appieno la portata del problema per i TPP è opportuno osservare come la scarsa monetizzazione dei servizi di base incida in misura diversa sugli istituti bancari. Questi ultimi, grazie a una solida base di clientela e alla possibilità di integrare tali servizi all'interno di strategie di *cross-selling* e *bundling*, riescono infatti ad assorbirne più agevolmente i margini negativi, trasformandoli in strumenti funzionali al rafforzamento della relazione commerciale complessiva[233]. Al contrario, i TPP, non disponendo di economie di scala paragonabili a quelle bancarie e basando gran parte del proprio modello di business su tali attività, rischiano di incorrere in una vera e propria trappola economica. In ragione di ciò, essi sono chiamati a sviluppare rapidamente prodotti a maggiore marginalità o ad individuare forme alternative di monetizzazione – quali abbonamenti *corporate*, modelli B2B o collaborazioni infrastrutturali –, la cui assenza potrebbe confinare servizi a minore redditività al ruolo di *loss leader*, con effetti negativi sulla stabilità complessiva del modello.

Ad ulteriore conferma di tali vulnerabilità, alcuni casi concreti mostrano come l'incapacità di tradurre i servizi *consumer* in ricavi effettivi possa trasformarsi in un ostacolo insormontabile per i TPP. Emblematico in tal senso è il progetto Yolt, piattaforma di *personal financial management* lanciata da ING nel 2016 e chiusa pochi anni dopo a causa dell'impossibilità di raggiungere una scala sufficiente a generare profitti, pur disponendo di una base iniziale di clienti in rapida crescita[234].

---

[230] Banca d'Italia, "*PSD2 e Open Banking: nuovi modelli di business e rischi emergenti*", cit., p.27

[231] Ibid., p.19

[232] Strinkingly, "*La strategia del loss leader: definizione ed esempio*", https://it.strikingly.com/content/blog/loss-leader/, luglio 2022

[233] A. G, "*Un bundle anche per l'offerta digitale*", https://www.aziendabanca.it/notizie/bundle-open-banking-fintech-digitale, Aziendabanca, settembre 2017

[234] Aziendabanca, "Yolt verrà chiusa da ING, fine delle operazioni nell'open banking B2B**",** https://www.aziendabanca.it/notizie/fintech-insurtech/yolt-chiude, agosto 2022

Analoghe difficoltà si riscontrano anche per operatori come TrueLayer e Token.io, i quali, nonostante abbiano consolidato partnership strategiche e raccolto ingenti finanziamenti da investitori istituzionali, non sono ancora riusciti a raggiungere una redditività stabile[235].

In definitiva, queste esperienze dimostrano come l'esternalizzazione dell'accesso ai dati e ai conti spesso non sia sufficiente a garantire sostenibilità economica, malgrado l'attrattiva tecnologica e la capacità di raccogliere capitali delle terze parti.

Pertanto, il rischio è che molti servizi *consumer* si rivelino "utili ma non monetizzabili", rimanendo confinati a funzioni ancillari o *loss leader* e costringendo talvolta gli operatori a una competizione ad alta intensità, caratterizzata da margini ridotti e da una costante pressione sui ricavi, con il pericolo di ridurne l'autonomia strategica e la capacità di costruire modelli duraturi ed indipendenti.

In questo quadro, la difficoltà di monetizzare i servizi di base non rappresenta un limite isolato, ma si intreccia con un'ulteriore criticità di natura sistemica: la dipendenza strutturale dalle banche.

Di fatto, anche se i TPP cercano di rafforzare la propria autonomia imprenditoriale – rivedendo o riconvertendo i propri modelli per ovviare alle note difficoltà di monetizzazione – essi rimangono inevitabilmente vincolati alla disponibilità e alla qualità dei dati messi a disposizione dagli ASPSP, nonché alle condizioni che ne regolano l'utilizzo.

In altri termini, i TPP fondano la creazione del proprio valore su un asset – i dati e i conti – di cui non sono titolari, ma cui possono accedere esclusivamente in virtù di un obbligo normativo imposto agli istituti bancari (cfr. §1.1). In questo senso, l'eventuale decisione delle banche di ridurre la qualità delle interfacce API – ad esempio rallentandone la performance o restringendone l'operatività – rischia di compromettere non solo la stabilità dei modelli di business dei TPP, che si configurano come meri utilizzatori indiretti dei dati, ma anche quella dell'intero settore[236].

Tuttavia, tale dipendenza non si esaurisce alla sola disponibilità dei dati, ma si estende anche alla dimensione tecnologica. Proprio le API, che avrebbero dovuto costituire il veicolo per una relazione trasparente e standardizzata tra banche e TPP, si sono rivelate in più di un'occasione fonte di frizioni e ostacoli, facendo emergere così una chiara contraddizione: lo strumento che abilita l'accesso ai dati è al tempo stesso uno dei principali canali attraverso cui le banche possono condizionare l'operatività delle terze parti.

Nella pratica, infatti, le interfacce sviluppate dagli istituti bancari hanno evidenziato livelli fortemente disomogenei di qualità tecnica, funzionalità e grado di apertura, con ripercussioni dirette sulla

---

[235] G. Donadio, "Open Banking facile con TrueLayer, la fintech di italiani che piace all'Europa", https://startupitalia.eu/economy/economia-digitale/open-banking-facile-con-true-layer-la-fintech-di-italiani-che-piace-alleuropa/, StartupItalia, settembre 2019

[236] Enfuce, "How banks can overcome PSD2 compliance challenges", https://enfuce.com/blog/how-banks-can-overcome-psd2-compliance-challenges/, Settembre 2020

capacità delle terze parti di sfruttare l'accesso regolato ai dati per offrire servizi realmente efficienti e competitivi[237].

A confermarlo è anche la Banca d'Italia, la quale ha sottolineato come interfacce non correttamente implementate dagli ASPSP possano trasformarsi in un ostacolo all'operatività dei prestatori di servizi di informazione sui conti (AISP) e di disposizione di ordini di pagamento (PISP), rendendo la fruizione dei servizi esternalizzati dell'utente più onerosa rispetto a quella garantita dall'accesso diretto tramite l'*online banking* tradizionale[238]. Una affermazione che trova conferma anche nei pareri dell'EBA, i quali hanno chiarito che pratiche apparentemente marginali – quali, ad esempio, richieste eccessive di autenticazione, procedure ridondanti rispetto all'online banking tradizionale, l'impossibilità di utilizzare i dati biometrici per l'identificazione e l'autenticazione del cliente o la mancata attivazione dell'esenzione dalla SCA prevista dalla normativa – finiscono, in realtà, per compromettere in modo sostanziale sia l'efficienza operativa delle terze parti sia la *user experience*[239].

A quest'ultimo riguardo, specialmente nell'ambito dello svolgimento dei servizi di *Account Information Service* (API), riveste un ruolo significativo la mancanza di dettaglio nelle informazioni fornite tramite API dagli istituti bancari alle terze parti. In altri termini, l'impossibilità per i TPP di disporre di informazioni sufficientemente dettagliate nel corso dello svolgimento dei loro servizi può limitare la loro utilità per gli utenti, riducendo notevolmente la *customer retention*[240].

2.2.3 – Minacce e criticità per i TPP (segue): standardizzazione mancata e competizione verticale

È evidente quindi che, nonostante l'EBA abbia imposto agli istituti bancari regole stringenti in merito alla predisposizione delle interfacce di accesso e agli standard aperti e sicuri di comunicazione – tramite i *Regulatory Technical Standards* –, la realtà applicativa si presenti ben più complessa[241].

---

[237] Fabrick, "PSD2: che cos'è e come è cambiata la Direttiva europea sui Servizi di Pagamento", https://www.fabrick.com/it-it/insight/blog/psd2-cos-e/, maggio 2023

[238] Banca d'Italia, "PSD2 e Open Banking: nuovi modelli di business e rischi emergenti", cit., p.13

[239] EBA, *Opinion of the European Banking Authority on obstacles under Article 32(3) of the RTS on SCA and CSC*, EBA/OP/2020/10, giugno 2020

[240] Banca d'Italia, "PSD2 e Open Banking: nuovi modelli di business e rischi emergenti", cit., p.14

[241] Nello specifico, l'art. 32, paragrafo 3, degli RTS dispone che "*I prestatori di servizi di pagamento di radicamento del conto che abbiano predisposto un'interfaccia dedicata provvedono affinché tale interfaccia non crei ostacoli alla prestazione dei servizi di disposizione di ordine di pagamento e di informazione sui conti. Detti ostacoli possono consistere, tra l'altro, nell'impedire l'utilizzo da parte dei prestatori di servizi di pagamento di cui all'articolo 30, paragrafo 1, delle credenziali rilasciate dai prestatori di servizi di pagamento di radicamento del conto ai loro clienti, nell'imporre il reindirizzamento verso l'autenticazione o altre funzioni del prestatore di servizi di pagamento di radicamento del conto, nel richiedere autorizzazioni e registrazioni aggiuntive rispetto a quelle previste dagli articoli 11, 14 e 15 della direttiva (UE) 2015/2366 o nel richiedere ulteriori verifiche del consenso dato dagli utenti dei servizi di pa*gamento ai prestatori di servizi di disposizione di ordine di pagamento e di servizi di informazione sui conti".

A tal proposito, numerosi sono i quesiti e le segnalazioni sollevati dagli operatori terzi ai quali l'EBA è stata chiamata a fornire una risposta, chiarendo per ciascun caso quali comportamenti degli istituti bancari possano ritenersi conformi alla Direttiva sui Servizi di Pagamento e ai relativi RTS e quali, invece, debbano essere qualificati come ostacoli ingiustificati[242].

Questa particolare attenzione rivolta dall'Autorità Bancaria Europea – affiancata dalle frequenti richieste di intervento provenienti non solo dai TPP, ma anche dalle stesse banche e dalle autorità di vigilanza nazionali – testimonia la rilevanza sistemica delle problematiche connesse a tali pratiche di mercato[243]. Invero, nella maggioranza dei casi, tali criticità non si traducono unicamente in un peggioramento della *user experience* e in un aumento dei costi di adeguamento per le terze parti, ma contribuiscono anche ad alimentare una più generale frammentazione del mercato europeo delle API. Ad ulteriore dimostrazione di tale disomogeneità basti pensare alla stessa interpretazione, da parte degli istituti bancari, di cosa debba essere qualificato come un "ostacolo" in relazione alle funzionalità e alle modalità operative delle interfacce di accesso dedicate ai TPP.

Ne consegue che l'assenza di uno standard uniforme a livello europeo costringe i provider a confrontarsi con un mosaico di API eterogenee, la cui configurazione si differenzia da Stato a Stato in base al livello di maturità dei mercati e al numero degli operatori coinvolti. Una condizione, quest'ultima, che non solo limita la scalabilità dei modelli di business a livello paneuropeo, ma rischia altresì di compromettere l'obiettivo stesso perseguito dalla PSD2 di garantire un accesso regolato, paritario e trasparente ai dati e conti bancari (cfr. §2.1.1)[244].

Se dunque il fallimento della standardizzazione delle API rende già di per sé complessa la piena scalabilità dei modelli di business, non meno gravoso per i TPP si rivela il peso della pressione regolatoria conseguente al meccanismo di esternalizzazione.

Dal momento che l'accesso ai dati e conti bancari avviene unicamente in virtù di un obbligo regolamentare – come già ribadito nel corso della trattazione –, le terze parti si trovano inevitabilmente esposte alla continua evoluzione interpretativa e applicativa delle norme, che incidono direttamente sulla sostenibilità dei loro modelli operativi.

A ciò si aggiunge il fatto che i TPP, per poter operare in qualità di *Account Information Service Provider* (AISP) o di *Payment Initiation Service Provider* (PISP), devono ottenere specifiche autorizzazioni nazionali – nel caso italiano rilasciate dalla Banca d'Italia – che vengono

---

[242] A. Di Giorgio, B. Mascagni, "*PSD2: gli ostacoli all'operatività dei TPP alla luce dei chiarimenti dell'EBA*", https://annunziataconso.eu/articolo/psd2-gli-ostacoli-alloperativita-dei-tpp-alla-luce-dei-chiarimenti-delleba/, Annunziata&conso, luglio 2020

[243] Tink, "*The significance of the EBA's opinion on PSD2 API obstacles*", https://tink.com/it/blog/open-banking/opinione-eba-psd2-apis/, luglio 2020

[244] Tink, "*What the EBA putting its foot down on PSD2 API obstacles really means*", https://tink.com/blog/open-banking/eba-opinion-psd2-api-obstacles-fallback-exemptions/, marzo 2021

successivamente riportate e conservate nei registri centralizzati dell'EBA, così da garantirne il riconoscimento reciproco all'interno del mercato unico europeo. Inoltre, per garantire l'instaurazione di canali sicuri di comunicazione con gli istituti finanziari con cui intraprendono rapporti di esternalizzazione, i TPP sono altresì costretti a dotarsi di certificati digitali conformi al Regolamento eiDAS[245], nonché a effettuare i test obbligatori in ambienti sandbox basati su dati fittizi al fine di verificarne l'affidabilità prima dell'avvio operativo[246].

Tenendo conto della particolare sensibilità dei dati su cui si fonda il meccanismo di esternalizzazione selettiva, il legislatore europeo ha ritenuto opportuno estendere anche ai TPP una serie di obblighi che in precedenza gravavano quasi esclusivamente sugli intermediari bancari tradizionali. Ne deriva che, oltre agli adempimenti già menzionati, le terze parti sono oggi chiamate a rispettare stringenti requisiti di resilienza operativa e a implementare procedure avanzate di cybersecurity, così da garantire la protezione dei dati e la continuità dei servizi in linea rispettivamente con il Regolamento DORA e GDPR (cfr. §§1.1.3, 1.1.4).

Per quanto riguarda, invece, la responsabilità del trattamento dei dati personali, sebbene – come discusso nel § 1.1.2 – questa rimanga formalmente in capo agli istituti bancari, ai TPP è comunque richiesto di garantire adeguati presidi di sicurezza per prevenire accessi non autorizzati, violazioni di dati e rischi sistemici connessi alla circolazione delle informazioni finanziarie (cfr. §1.3.1).

In questo contesto, nonostante la relativa leggerezza operativa dei TPP rispetto alle architetture legacy bancarie, i costi di compliance normativa si rivelano tutt'altro che marginali[247]. In proposito, la Direttiva (UE) 2015/2366 – seppur nel tentativo di garantire il rispetto da parte degli operatori di una serie di obblighi in materia di sicurezza, privacy e governance – ha imposto il sostenimento di ingenti investimenti infrastrutturali e tecnologici, talvolta difficilmente sostenibili per start-up di piccole dimensioni o operatori scarsamente capitalizzati.

Ne emerge così un evidente paradosso: l'infrastruttura normativa che avrebbe dovuto abbattere le barriere all'ingresso e garantire un accesso regolato e paritario ai dati e conti bancari finisce, in realtà, per alimentare dinamiche di polarizzazione del mercato. In altri termini, l'imposizione di costi di compliance così elevati ha generato un meccanismo selettivo, secondo il quale soltanto i TPP in grado

---

[245] *Regolamento (UE) N. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 relativa all'identificazione elettronica e ai servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE*. In particolare, esso prevede l'interoperabilità dei sistemi nazionali di identificazione elettronica tra gli Stati membri dell'UE, richiedendo lo sviluppo di un quadro tecnologicamente neutro che non favorisca alcuna particolare soluzione tecnica per l'attuazione dell'identificazione elettronica. A tal fine sono state stabilite norme procedurali e tecniche per facilitare la cooperazione tra i paesi dell'UE, garantire lo scambio senza soluzione di continuità dei dati di identificazione elettronica e promuovere un ecosistema digitale coeso in tutta l'UE.

[246] V. La Vecchia, "*Definizione e differenza tra PISP, AISP e CISP nella PSD2 bancaria*", https://vitolavecchia.altervista.org/definizione-e-differenza-tra-pisp-aisp-e-cisp-nella-psd2-bancaria/

[247] E. Guardati, "*PAYTECH e ML Risk: third party providers obbligati ai sensi del d.lgs. 231/2007*", Osservatorio Normativo, p.15, marzo 2022

di attrarre ingenti capitali e di consolidare rapidamente la propria base clienti riescono a sostenere gli oneri regolatori e a scalare i propri modelli su più giurisdizioni. Al contrario, gli operatori incapaci di differenziarsi o di raggiungere economie di scala adeguate restano confinati in nicchie locali o sono costretti a percorrere strade alternative – fusioni, acquisizioni o, nei casi più estremi, l'uscita dal mercato – come ha dimostrato il caso inizialmente citato di Yolt.

Proprio in questo contesto è possibile stabilire la presenza di una marcata condizione di iper-concorrenza tra gli operatori di mercato, la quale non si limita solo ai TPP, ma si estende anche ai rapporti con le banche tradizionali e le Big Tech.

In proposito, si osserva come molte banche, grazie a una crescente consapevolezza dei costi e delle implicazioni strategiche delle proprie infrastrutture IT, stiano progressivamente rivedendo il grado di dipendenza dai TPP. Come rivelato anche da un recente rapporto McKinsey, i leader del settore bancario si sono rivelati capaci di "*correggere la rotta*", riportando all'interno del loro business quelle risorse e competenze che in una fase iniziale erano state esternalizzate ai TPP, con l'obiettivo di migliorare la redditività e presidiare direttamente la relazione con la clientela[248]. In tal senso, diverse banche hanno avviato processi di "*re-verticalizzazione*", comportandosi esse stesse come provider e sviluppando internamente servizi digitali di gestione finanziaria personale, *credit scoring* alternativo e altre soluzioni un tempo delegate ai TPP.

Emblematico, in tal senso, è il caso delle *challenger banks* Revolut e Monzo, le quali hanno scelto di internalizzare progressivamente servizi inizialmente affidati ai TPP, nel tentativo di recuperare il controllo sulla redditività e di mitigare il rischio di dipendenza strutturale dai soggetti terzi[249].

Parallelamente alla pressione esercitata sui TPP dagli istituti bancari si aggiunge quella delle Big Tech – quali Google, Amazon e Meta – che, forti di una base clienti globale e di risorse tecnologiche e finanziarie difficilmente eguagliabili, hanno iniziato a penetrare con crescente decisione nel settore finanziario, offrendo soluzioni più avanzate rispetto a quelle delle terze parti e spaziando dai pagamenti digitali fino all'erogazione del credito.

Sebbene, sotto il profilo sistemico, le Big Tech possano essere ricondotte all'interno della più ampia categoria degli operatori FinTech, di cui fanno parte anche i TPP, esse se ne distinguono per la capacità di scalare i mercati in tempi estremamente ridotti. Tale vantaggio competitivo discende non solo dall'elevato grado di riconoscimento del marchio, ma anche dall'enorme patrimonio informativo

[248] R. Patenge, A. Anand, R. Goel, "*Managing bank IT spending: Five questions for tech leaders*", https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/managing-bank-it-spending-five-questions-for-tech-leaders, ottobre 2024

[249] Revolut, "*Relazione annuale 2022*", https://www.revolut.com/it-IT/annual-report/2022/

accumulato sui comportamenti e sulle preferenze dei propri utenti, che consente loro di integrare rapidamente i servizi finanziari nei propri ecosistemi digitali[250].

Ne consegue che i TPP oggi si trovano esposti a una doppia pressione verticale: dall'alto le banche che, iniziando a sviluppare *in house* i servizi prima esternalizzati, tendono a riappropriarsi del controllo dei dati e della catena del valore; dal basso le Big Tech, la cui capacità di sfruttare economie di scala irraggiungibili per gli operatori indipendenti rischi di ridurre ulteriormente la possibilità di diversificazione delle terze parti.

Alla luce di tali considerazioni, l'esternalizzazione dell'accesso ai dati e ai conti non può essere letta unicamente come un'opportunità di crescita per i TPP né come una mera cessione di prerogative per le banche. Piuttosto, essa rappresenta una fase transitoria, segnata da tensioni latenti che ne limitano la portata e ne rivelano le contraddizioni strutturali.

La difficoltà di monetizzare, la dipendenza dalle banche, le inefficienze tecnologiche e la pressione regolatoria mostrano chiaramente come l'Open Banking, così come oggi configurato, non sia ancora riuscito a tradursi in un equilibrio stabile e sostenibile. Pertanto, il rischio è quello di un ecosistema dominato da pochi grandi player capaci di attrarre capitali e consolidarsi a livello internazionale, mentre una moltitudine di operatori minori sono costretti a reinventarsi per non soccombere.

In questo senso, l'esternalizzazione appare più come un punto di partenza che come un traguardo; un meccanismo abilitante, ma non sufficiente a garantire pluralità, sostenibilità e resilienza. È proprio da questa consapevolezza che prendono forma i modelli emergenti e le strategie ibride analizzati nel §2.3, i quali cercano di superare i limiti dell'attuale paradigma, combinando logiche di esternalizzazione e di controllo diretto per dare vita a forme di cooperazione più stabili e una competizione più equilibrata.

2.3 – Modelli emergenti: *Banking-as-a-Platform* (BaaP) e *Banking-as-a-Service* (BaaS)

L'analisi dei benefici e dei rischi connessi all'esternalizzazione ai TPP, pur evidenziandone tanto le potenzialità quanto le criticità, non consente di ridurre tale fenomeno a una lettura dicotomica, come se si trattasse di una scelta esclusivamente vantaggiosa o, al contrario, intrinsecamente problematica. La realtà dell'Open Banking, ridefinita da una rapida evoluzione guidata da una combinazione di fattori di natura politica, economica e tecnologica, si configura piuttosto come un insieme eterogeneo di modelli organizzativi e di collaborazione, le cui ricadute variano a seconda delle modalità con cui viene strutturato il rapporto banca-TPP.

[250] A. Genovese, V.Falce, *La portabilità dei dati in ambito finanziario. Quaderni FinTech*, No. 8, Consob, aprile 2021, p.189

Questa transizione verso forme più articolate di cooperazione risponde a due dinamiche strettamente intrecciate. Da una parte, le banche tradizionali, progressivamente indebolite dalla pressione concorrenziale di operatori FinTech e Big Tech, guardano ai TPP come a un'occasione per recuperare competitività, accedere a tecnologie più agili e mantenere centralità in un sistema sempre più interconnesso. Dall'altra, i TPP necessitano di trasformare l'accesso alle informazioni bancarie in valore economico, sviluppando soluzioni innovative capaci di intercettare i bisogni dei consumatori e di ritagliarsi un ruolo stabile in un contesto competitivo in rapida trasformazione.

A questo si deve aggiungere anche l'evoluzione del profilo del consumatore, ormai sempre più orientato al digitale e meno incline a sopportare eventuali complessità nelle interazioni finanziarie. In proposito, solo in Italia secondo un'indagine condotta da KPMG, "*circa il 30% dei clienti si dichiara disposto a sostituire una banca tradizionale con un operatore online*" qualora questo garantisca servizi più rapidi, semplici ed innovativi[251]. È dunque evidente che la pressione competitiva non proviene solo dal lato dell'offerta, ma anche da quello della domanda, la quale è sempre più orientata a esperienze bancarie fluide, integrate e facilmente accessibili.

In questo quadro, per valutare se l'esternalizzazione ai TPP rappresenti un vantaggio o un ostacolo alla diffusione dell'Open Banking, è necessario spostare lo sguardo dall'analisi dei singoli attori all'esame dei modelli emergenti di collaborazione, caratterizzati da una crescente centralità del cliente e dall'integrazione di logiche di apertura e controllo. In particolare, tra questi ad aver catalizzato l'attenzione di accademici e professionisti vi sono rispettivamente il *Banking-as-a-Platform* (BaaP) e il *Banking-as-a-Service* (BaaS).

Lo studio di tali modelli consentirà non solo di osservare come l'esternalizzazione venga effettivamente tradotta in prassi operative, ma soprattutto di misurare fino a che punto essa possa rappresentare un fattore abilitante o, al contrario un freno, per la piena affermazione dell'Open Banking.

2.3.1- Banking-as-a-Platform (BaaP): integrazione e apertura dell'ecosistema

Nonostante tra i modelli emergenti il *Banking-as-a-Platform* (BaaP) sia un concetto relativamente recente, esso rappresenta una delle declinazioni più fedeli alla logica originaria dell'Open Banking. Se da una prima lettura potrebbe sembrare semplicemente un modello in cui la banca si limita a fungere da piattaforma di distribuzione di prodotti e servizi, nella realtà il BaaP si traduce in

[251] KPMG, "*Evoluzione dei modelli distributivi bancari. L'impatto del COVID-19 sui modelli di servizio delle banche italiane*", 2021

un'integrazione strutturata delle soluzioni sviluppate dalle terze parti all'interno del sistema bancario[252].

In questo schema la banca assume il ruolo di "orchestratore" dell'ecosistema finanziario, mettendo a disposizione dei TPP un'infrastruttura tecnologica aperta e modulare basata su API standardizzate, stabilendo al contempo regole di collaborazione e precisi livelli di servizio a tutela della clientela. In tal modo, gli istituti bancari riescono a mantenere un rapporto diretto con i propri clienti, preservando così l'elemento che ha storicamente costituito il loro principale vantaggio competitivo nei confronti dei nuovi entranti: la fiducia[253]. Ne consegue che nel modello BaaP l'esternalizzazione si configura come un processo "governato" e strategico, nel quale i TPP non sostituiscono le banche ma, piuttosto, ne completano l'offerta, contribuendo a ridurre i costi e le difficoltà connesse allo sviluppo interno di infrastrutture digitali e consolidando la centralità delle banche nell'ecosistema.

Questa natura di modello "governato" si riflette in particolare nel suo assetto di governance, dal quale emerge chiaramente come il *Banking-as-a-Platform* possa configurarsi quale effettivo vantaggio per l'Open Banking a condizione che la banca definisca regole di accesso trasparenti, adotti standard comuni e garantisca un sistema di responsabilità condivisa. Ne deriva così una situazione di equilibrio tra apertura e controllo, che consente ai clienti di beneficiare di un'offerta più ampia e competitiva di servizi, senza tuttavia rinunciare alle garanzie di tutela derivanti dalla supervisione bancaria[254].

In questo quadro, un ulteriore tratto distintivo risiede anche nella facoltà per gli istituti bancari di selezionare i propri partner e vincolarli al rispetto di requisiti stringenti in materia di protezione dei dati e sicurezza. Una prerogativa che, se da un lato rafforza il legame fiduciario con la clientela e consolida la centralità e la legittimità della banca all'interno dell'ecosistema, dall'altro può ridurre gli spazi di manovra dei TPP, rischiando di limitarne in parte la capacità innovativa.

A prescindere dagli aspetti finora considerati, ciò che realmente distingue il modello BaaP dalle tradizionali pratiche di esternalizzazione è il superamento del paradigma "*vendor-centric*". Difatti, mentre in passato molte banche erano solite affidare funzioni critiche a un numero ristretto di TPP, esponendosi così a forme di *vendor lock-in* (cfr. §2.1.2), oggi il BaaP consente l'onboarding di una pluralità di TPP anche per la medesima funzione – quali i servizi di pagamento, KYC o AML –, riducendo sensibilmente la dipendenza dai singoli partner e rafforzando la posizione contrattuale della banca-orchestratore[255].

---

[252] Tuum, "*Banking as a Service, Banking as a Platform & Open Banking – Knowing the difference*", https://tuum.com/blog/baas-baap-and-open-banking-differences/

[253] R. Coeurderoy, M. Guilhon, "*Why banks are moving towards the banking-as-a-platform model*", https://blogs.lse.ac.uk/businessreview/2023/04/28/why-banks-are-moving-towards-the-banking-as-a-platform-model/, LSE, Aprile 2023

[254] Ibid.

[255] Virtusa, "*Banking-as-a-Platform*", https://www.virtusa.com/digital-themes/banking-as-a-platform

Questo mutamento di prospettiva – reso possibile dalla disponibilità di cataloghi API già collaudati e dall'ampia offerta di *player* presenti sul mercato – ha contribuito quindi a riequilibrare i rischi e i benefici dell'esternalizzazione, offrendo agli istituti bancari una maggiore versatilità nella selezione delle terze parti e riducendo al contempo gli oneri legati alla re-ingegnerizzazione dell'infrastruttura in caso di sostituzione di un TPP.

Eppure, è proprio dietro questa apparente flessibilità che si celano inside tutt'altro che marginali: in assenza di adeguati presidi regolamentari e di governance, l'accesso rischia infatti di essere limitato o condizionato da barriere elevate all'ingresso, con effetti negativi sull'interoperabilità e sulla concorrenza. In uno scenario simile, il modello potrebbe perciò facilmente degenerare in una forma di *platform banking* dominata da pochi *gatekeeper*, capaci di esercitare un potere significativo sull'intero ecosistema.

Proprio per questa sua natura ambivalente, il BaaP deve essere inteso come una forma più matura e strutturata di esternalizzazione, che non si limita a una semplice delega funzionale *one-to-one*, ma implica un processo di co-creazione di valore all'interno di un framework di governance basato su *Service Level Agreement* (SLA), standard tecnici e regole di compliance condivise.

Giunti a questo punto della trattazione, tuttavia, per valutare appieno la portata del modello è necessario considerare che la sua configurazione non si esaurisce nei soli effetti strutturali ed organizzativi, ma produce altresì ricadute tangibili sugli attori dell'ecosistema.

In particolare, esternalizzando a partner esterni funzioni non strettamente core, le banche possono monetizzare le proprie infrastrutture digitali tramite tariffe di accesso alle API o accordi di *revenue-sharing*, trasformando così un obbligo regolamentare – l'accesso ai dati e ai conti bancari – in una nuova fonte di reddito. Parallelamente, grazie al supporto tecnologico ed economico dei TPP, esse hanno l'opportunità di penetrare mercati altrimenti difficilmente accessibili senza dover ricorre a strategie di integrazione verticale particolarmente onerose, di ridurre i costi fissi interni, di accelerare il time-to-market dei nuovi prodotti e, al tempo stesso, di offrire soluzioni modulari e personalizzabili per la clientela[256].

Anche i consumatori e i TPP beneficiano di questa configurazione: i primi accedendo a servizi più efficienti e meglio calibrati sulle proprie esigenze; i secondi ampliando il proprio mercato e moltiplicando le occasioni di profitto[257].

Ciononostante, dietro l'attrattività di tali vantaggi si celano criticità che gli istituti bancari non possono sottovalutare. L'apertura delle proprie piattaforme a soggetti terzi, infatti, introduce

[256] Mia Fintech srl, "Come abilitare il Banking-as-a-Platform con le tecnologie Cloud Native", https://mia-fintech.io/it/blog/banking-as-a-platform-cloud-native/, settembre 2024

[257] Tuum, "Banking as a Service, Banking as a Platform & Open Banking – Knowing the difference", https://tuum.com/blog/baas-baap-and-open-banking-differences/

dinamiche concorrenziali che rischiano di rivelarsi particolarmente controproducenti, generando talvolta rischi concreti di cannibalizzazione. In pratica, i partner cui la banca affida parte del proprio ecosistema possono, al tempo stesso, diventare competitor diretti su linee di business ad alta redditività – quali i prestiti personali, le assicurazioni o i servizi di investimento digitale. Ne consegue una profonda ambivalenza del modello BaaP, in quanto ciò che inizialmente appariva come un'opportunità di arricchimento dell'offerta può tramutarsi in un meccanismo capace di erodere progressivamente i margini delle attività tradizionali.

Accanto a questa vulnerabilità si pone l'ulteriore complessità, spesso sottovalutata, di governare un ecosistema popolato da una pluralità di TPP. Se da un lato tale modello – come già osservato – consente l'integrazione di numerosi partner all'interno della medesima piattaforma, dall'altro impone agli istituti bancari di assicurare la piena compatibilità tecnica delle API e di mantenere standard elevati e uniformi in termini di sicurezza resilienza e qualità del servizio[258]. A ciò si deve poi aggiungere il fatto che, indipendentemente dalla frammentazione dei processi, la responsabilità finale nei confronti del cliente rimane interamente in capo alla banca.

Quindi, queste fragilità dimostrano che il modello BaaP, lungi dall'essere una soluzione univocamente virtuosa, espone gli istituti a nuove tensioni competitive e gestionali che potrebbero, nel lungo periodo, ridimensionarne i benefici iniziali.

Proprio alla luce di tali complessità, appare evidente che il *Banking-as-a-Platform* non possa funzionare senza un adeguato presidio tecnologico. In questo senso, la vera chiave del successo di questo modello risiede nell'adozione di un approccio *API-first*, in cui le interfacce non sono concepite come un mero supporto tecnico, bensì come veri e propri prodotti strategici.

Considerare le API come prodotto implica, infatti, attribuire loro un ciclo di vita definito, standard di qualità e strumenti di monitoraggio, tutti elementi che consentono alla banca di costruire architetture modulari, scalabili e riusabili[259]. Di fatto, un simile approccio permette agli istituti bancari non solo di rispondere con maggiore rapidità all'evoluzione della domanda, ma anche di integrare i TPP in modo più efficiente, riducendo il rischio di dipendenze tecnologiche e favorendo condizioni di effettiva contendibilità del mercato[260]. Al contrario, in assenza di un'implementazione *API-first*, il BaaP rischia di degenerare in una piattaforma monolitica, con l'effetto paradossale di annullare i benefici dell'apertura e trasformare l'esternalizzazione in un ostacolo alla piena realizzazione dell'Open Banking.

---

[258] Mia Fintech srl, "Come abilitare il Banking-as-a-Platform con le tecnologie Cloud Native", cit.
[259] A. Witkowska, "*What is API-first*?", https://tyk.io/blog/res-what-is-api-first/, Tyk, marzo 2023
[260] B. Bhattacharya, "*API-first banking: the future of fintech*", https://tyk.io/blog/api-first-banking-the-future-of-fintech/, Tyk, Agosto 2023

La rilevanza di tale approccio non resta solo sul piano teorico, ma trova riscontro concreto nel caso di Fidor Bank, una tra le prime banche ad adottare una strategia *API-first* tramite lo sviluppo del *Fidor Operating System* (fOS).

Nello specifico, tale piattaforma – fondata proprio sull'integrazione di partner fintech attraverso API aperte – ha permesso a Fidor non solo di ampliare rapidamente la gamma di prodotti e servizi forniti da altri partner e raggiungere la redditività pochi anni dopo il lancio della piattaforma, ma anche di porsi come modello di riferimento per l'intero settore[261].

L'esperienza di Fidor conferma, dunque, come un approccio *API-first* possa tradursi in un vero e proprio vantaggio competitivo, capace di rendere l'esternalizzazione non solo un obbligo regolamentare, bensì un motore di innovazione condivisa e sostenibile. Emblematico, in tal senso, è il successo ottenuto grazie all'integrazione nella propria piattaforma di alcune funzioni sviluppate da *Currencycloud*, che le hanno consentito di diventare una delle prime banche al mondo ad offrire un portafoglio elettronico multivaluta senza dover sostenere ingenti investimenti infrastrutturali[262].

Eppure, sebbene il modello di BaaP sviluppato da Fidor fosse stato concepito per rafforzare la centralità della banca nei rapporti con la clientela, la pressione competitiva e le nuove opportunità di mercato ne hanno progressivamente modificato la traiettoria, riducendone la visibilità. La decisione di abbandonare l'offerta diretta al consumatore in favore della commercializzazione del fOS in modalità *white-label* ha segnato un evidente riposizionamento della banca all'interno dell'ecosistema finanziario, determinando il passaggio da un ruolo di orchestratore di un ecosistema aperto a quello di fornitore infrastrutturale e regolatorio in ottica *Banking-as-a-Service*, imponendole di operare "dietro le quinte" [263].

Proprio a quest'ultimo modello – caratterizzato da una logica di fondo profondamente diversa e da implicazioni specifiche per l'Open Banking – sarà dedicata la successiva analisi.

2.3.2 - Banking-as-a-Service (BaaS): modularità e infrastruttura come servizio

Dal precedente caso di Fidor Bank emerge con chiarezza come l'evoluzione da un modello di *Banking-as-a-Platform* a uno schema di *Banking-as-a-Service* non sia soltanto un cambio operativo, ma risponda a logiche profondamente differenti e si rivolga a target eterogenei nella configurazione dell'ecosistema finanziario. Se, infatti, il *BaaP* appare funzionale soprattutto alle banche tradizionali

[261] A. L'Hostis, "*Banche e Fintech: meglio insieme*", https://www.forrester.com/blogs/16-08-22-banks_and_fintechs_better_together/, Forrester, agosto 2016

[262] Currencycloud, "*I portafogli elettronici multivaluta diventano realtà per Fidor Bank*", https://www.currencycloud.com/it/company/case-study/making-multi-currency-ewallets-possible-fidor-bank/, giugno 2015

[263] A. L'Hostis, "*Banche e Fintech: meglio insieme*", https://www.forrester.com/blogs/16-08-22-banks_and_fintechs_better_together/, Forrester, agosto 2016

che, pur mirando a modernizzare ed arricchire la propria offerta attraverso l'integrazione di servizi di terze parti, mantengono un legame diretto con i propri clienti, il BaaS, al contrario, relega gli istituti bancari a un ruolo secondario di fornitore, spostando la relazione con il cliente verso il TPP, con conseguenze rilevanti sul bilanciamento dei poteri all'interno dell'ecosistema dell'Open Banking[264].
In questa prospettiva, il BaaS si configura come uno schema organizzativo basato su una logica "*back-end*", secondo la quale gli istituti bancari mettono a disposizione la propria infrastruttura regolatoria e i servizi bancari di base in modalità *white-label* a soggetti terzi non bancari – fintech, retailer o persino Big Tech – che, sfruttando le API offerte dalla banca, li integrano nella propria offerta e li distribuiscono sotto il proprio marchio[265]. Ne deriva così una netta separazione tra chi detiene la licenza bancaria e chi, invece, gestisce l'esperienza del cliente, con la conseguente creazione di catene del valore molto più frammentate e orizzontali rispetto a quelle tipiche del BaaP.
Nonostante questa frammentazione della catena del valore tra i diversi attori di mercato renda l'implementazione del *Banking-as-a-Servic*e particolarmente complessa, inducendo talvolta gli operatori a preferire l'approccio del *Banking-as-a-Platform* soprattutto per la sua semplicità e la possibilità di effettuare un passaggio graduale dall'approccio tradizionale a quello collaborativo, il BaaS si è comunque affermato negli ultimi anni come il modello più promettente in termini di valore generato[266]. Secondo recenti indagini di mercato, il comparto del *Banking-as-a-Service* ha raggiunto un valore pari a 24,58 miliardi di dollari nel 2025 e si prevede che raggiungerà i 60,35 miliardi di dollari entro il 2030, con un tasso di crescita annuo composto del 19,68%[267].
Pertanto, tale andamento conferma come tale sistema non rappresenti più una soluzione di nicchia, ma una leva di sviluppo rivoluzionaria, espressione della crescente diffusione dei servizi di *embedded finance*[268].
Promuovendo accordi di partnership e collaborazioni tra istituti bancari e operatori terzi, il modello favorisce la creazione di un ecosistema altamente dinamico in cui, da un lato, le banche possono valorizzare la propria esperienza e sfruttare le infrastrutture tecnologiche già consolidate in ambiti che vanno oltre i soli pagamenti; dall'altro, i TPP non sono più vincolati al canale tradizionale bancario per la distribuzione dei servizi finanziari, ma possono utilizzare diversi canali digitali per

---

[264] Anna, "*Banking-as-a-Service (BaaS): Cos'è, Vantaggi e Differenze con BaaP e Open Banking*", https://www.workinvoice.it/banking-as-a-service/, Workinvoice, settembre 2024
[265] PwC, "*What does Banking-as-a-Service (baaS) mean for a business*?", https://www.pwc.com/gx/en/issues/technology/baas-banking-as-a-service.html, luglio 2024
[266] R. Coerderoy, M. Guilhon, "*Dancing in the dark": Regulatory reforms and incumbent banks' evolution towards new value creation models in the process of open banking*", ESCP Impact Paper No. 2022-24-EN
[267] Mordor Intelligence, "*Banking as a Service Market Size & Share Analysis - Growth Trends & Forecasts (2025 - 2030)",* https://www.mordorintelligence.com/industry-reports/global-banking-as-a-service-market,
[268] L. Grassi, C. Garitta, "*Embedded Finance, Insurance ed erogazione dei servizi in modalità as-a-Service*", https://www.osservatori.net/insight/fintech-insurtech/embedded-finance-insurance-erogazione-servizi-modalita-as-a-service-insight/, Osservatorio Fintech & Insurtech

raggiungere segmenti di clientela tradizionalmente poco serviti, come quelli a basso e medio reddito nei mercati emergenti[269].

Tuttavia, per comprendere le ragioni per cui il modello *Banking-as-a-Service* stia conoscendo una crescita così rapida rispetto al *Banking-as-a-Platform* è necessario soffermarsi sui benefici concreti che ne spiegano l'attrattività. Invero, tali benefici non si esauriscono nel generico ampliamento dell'offerta, ma variano sensibilmente a seconda dei soggetti coinvolti, ridefinendo i rapporti di forza all'interno dell'ecosistema.

Innanzitutto, per gli operatori non bancari e i TPP uno dei vantaggi più rilevanti è l'abbattimento delle barriere all'ingresso. La possibilità di accedere al mercato finanziario senza dover sostenere gli oneri legati all'ottenimento di una licenza o alla costruzione di un'infrastruttura proprietaria –entrambi forniti dalla banca provider in modalità *white-label* – consente di ridurre drasticamente i costi inziali e di trasformarli da fissi a variabili.

Un esempio emblematico in questo senso è rappresentato dal programma lanciato nel 2018 dalla neobanca Starling, noto come "*Starling as a Service*". In questo caso, attraverso l'apertura delle proprie API l'istituto ha permesso a numerose fintech e startup di accedere a servizi bancari di base — dai pagamenti alla gestione dei conti — senza dover costruire da zero un'infrastruttura regolamentata. In questo modo, Starling ha reso possibile per questi operatori sperimentare nuovi prodotti digitali a costi minori e tempi di lancio più rapidi, dimostrando come il BaaS possa fungere da catalizzatore di innovazione[270].

Tale configurazione genera effetti positivi anche per i consumatori, che beneficiano indirettamente della maggiore flessibilità nel pricing, della riduzione dei rischi di investimento e della facoltà di accedere a servizi più personalizzati e meglio integrati nelle esperienze quotidiane[271].

Inoltre, emerge che, nei mercati in cui le banche tradizionali hanno spesso evitato di servire ampie fasce di clientela a basso o medio reddito per via delle loro architetture legacy e degli elevati costi di compliance, il modello BaaS consente invece di offrire servizi sostenibili, distribuiti attraverso canali alternativi a condizioni più flessibili.

Si pensi, ad esempio, alle iniziative di BBVA in Spagna e in America Latina, ove, grazie al lancio della piattaforma *BBVA API Market*, il gruppo ha reso disponibili a operatori esterni servizi bancari integrabili in applicazioni di terzi. Questo ha permesso di ampliare la distribuzione verso fasce di clientela meno servite dal canale tradizionale e di sviluppare soluzioni più aderenti ai bisogni locali,

---

[269] Fabrick, "*Banking as a Service: che cosa significa e come funziona*", https://www.fabrick.com/it-it/insight/blog/banking-as-a-service-cos-e/, agosto 2023

[270] Starling Bank, "*Starling Bank expands Payment Services and Banking-as-a-Service offer*", https://www.starlingbank.com/news/expanding-banking-services/, ottobre 2018

[271] Anna, "*Banking-as-a-Service (BaaS): Cos'è, Vantaggi e Differenze con BaaP e Open Banking*", cit.

riducendo i costi di accesso al credito e ai pagamenti[272]. In tal senso, l'aumento dell'accessibilità non rappresenta un effetto collaterale, bensì uno degli elementi qualificanti del modello.

Infine, per gli istituti bancari assumono il ruolo di fornitori, il BaaS costituisce una fondamentale opportunità per monetizzare asset altrimenti non sfruttati, trasformando infrastrutture costose in una nuova linea di business. In un contesto caratterizzato dal calo dei margini di profitto delle attività tradizionali, la possibilità di generare ricavi tramite la cessione di API, licenze e sistemi di compliance permette agli istituti bancari non solo di diversificare le fonti di reddito, ma anche di acquisire un posizionamento strategico all'interno di ecosistemi non esclusivamente bancari[273].

Alla luce di questi elementi, il *Banking-as-a-Service* si presenta dunque come un modello ad alto potenziale; tuttavia, la mancanza di una chiara definizione concettuale e di un modello giuridico pienamente riconosciuto ha condotto a soluzioni differenziate nelle varie giurisdizioni, generando criticità strutturali che ne ridimensionano l'impatto.

Tenendo presente che, negli schemi di BaaS, l'autorizzazione bancaria viene sostanzialmente trasferita a soggetti non vigilati, i quali assumono il controllo della relazione commerciale, emerge un primo nodo cruciale: l'asimmetria tra responsabilità regolatoria della banca e potere effettivo del TPP. Se, da un lato, questo viene presentato come un modello virtuoso di decentramento, capace di generare efficienza e specializzazione, dall'altro "*rischia di tradursi in una frammentazione elusiva della catena del valore, che aggira il principio della riserva di attività bancaria previsto dal diritto europeo e nazionale (art.8 CRD; art.10TUB)*"[274].

Una tale asimmetria rischia di minare non solo la chiarezza dei rapporti di vigilanza, ma anche la stessa posizione strategica delle banche all'interno del mercato, progressivamente ridotte a meri fornitori di infrastruttura. Ne consegue che lo spostamento del potere contrattuale e relazionale conseguente all'applicazione di questo modello comporta una progressiva perdita della centralità strategica della banca, come pure della sua possibilità di valorizzare la fiducia dei clienti.

A ciò si deve aggiungere che, laddove un TPP costruisce la propria intera offerta su un'unica banca BaaS, ogni migrazione diventa complessa e costosa, generando forme di lock-in che riducono la contendibilità del mercato. In questa prospettiva, quindi, il BaaS tende a riprodurre – in una veste apparentemente più innovativa – lo stesso problema del modello *vendor-centrico* tradizionale che il BaaP aveva tentato di superare.

---

[272] BBVA Spark, "*Four great uses of APIs for high-growth companies*", https://www.bbvaspark.com/en/news/uses-of-apis-for-companies/, dicembre 2024

[273] PwC, "*What does Banking-as-a-Service (baaS) mean for a business*?", https://www.pwc.com/gx/en/issues/technology/baas-banking-as-a-service.html, luglio 2024

[274] E.Rulli, "*Profili critici della banca come servizio (bank as a service)*", https://www.dirittobancario.it/art/profili-critici-della-banca-come-servizio-bank-as-a-service/, Dirittobancario, maggio 2025

Per ulteriori dettagli in merito al *principio di riserva bancaria* sancito dal diritto europeo si veda l'art.8 CRD, mentre per quanto riguarda il diritto nazionale si veda l'art. 10 del Testo Unico Bancario

Dal punto di vista del cliente, infine, emergono ulteriori criticità legate all'opacità regolamentare. A tal riguardo, partendo dal presupposto che il cliente non stipula più il contratto con la banca, bensì con il TPP che utilizza l'infrastruttura bancaria tramite API, emerge che esso può risultare escluso dall'applicazione delle regole previste per gli istituti bancari.
Alla luce di queste considerazioni, il BaaS incarna l'ambivalenza dell'Open Banking, configurandosi come un acceleratore di inclusione e innovazione e al tempo stesso come una fonte di vulnerabilità.
Dunque, dall'analisi del modello *Banking-as-a-Platform* e *Banking-as-a-Service* ciò che appare evidente è che nessuno dei due rappresenta una soluzione "neutra" o priva di contraddizioni. Tanto il BaaP quanto il BaaS mostrano come l'esternalizzazione ai TPP non sia soltanto un'opportunità tecnica, ma una scelta strategica che ridefinisce ruoli, poteri e responsabilità all'interno dell'ecosistema finanziario.
La questione cruciale diventa allora capire non se il modello sia, in astratto, virtuoso o rischioso, bensì in che misura la sua implementazione concreta produca dinamiche di effettiva apertura o, al contrario, di concentrazione e squilibrio.
In questa prospettiva, il passaggio dall'analisi teorica all'osservazione empirica diventa inevitabile. Sono infatti i casi concreti a mostrare come le banche e i nuovi entranti interpretino l'esternalizzazione: se come un'occasione per ampliare la competizione e democratizzare i servizi, o come uno strumento per rafforzare posizioni dominanti. È per questo che il capitolo successivo sarà dedicato all'esame delle esperienze di Revolut e N26, due tra le principali *challenger bank* europee, le cui strategie di crescita consentono di valutare in pratica se l'apertura ai TPP costituisca un vantaggio o un ostacolo per la piena realizzazione dell'Open Banking.

CAPITOLO 3

REVOLUT E N26: DUE MODELLI DI BANCA DIGITALE NEL CONTESTO DELL'OPEN BANKING

3.1 – Introduzione all'analisi

Dall'analisi sin qui condotta emerge chiaramente che il panorama bancario europeo è segnato da un'elevata eterogeneità e da profonde discontinuità, introdotte dai processi di digitalizzazione, che hanno radicalmente trasformato tanto le architetture tecnologiche quanto i modelli di business.

Nei capitoli precedenti si è visto come l'esternalizzazione ai TPP non costituisca un mero dettaglio tecnico, bensì una scelta strategica che incide su governance, innovazione e stabilità. Eppure, nonostante sul piano teorico questa dinamica sia evidente, la sua effettiva portata può essere colta solo attraverso un'analisi empirica di casi concreti.

In questa prospettiva, valutare l'effettivo impatto che l'esternalizzazione ai *Third Party Providers* (TPP) ha avuto per lo sviluppo del fenomeno dell'Open Banking risulta particolarmente complesso, specialmente se si considerano gli istituti bancari tradizionali.

Pur essendo stati i primi a confrontarsi con l'obbligo di apertura imposto dalla PSD2, essi hanno spesso interpretato l'Open Banking come un mero adempimento regolamentare da gestire in chiave difensiva, più che come occasione di crescita e sperimentazione. In tal contesto, l'elevata complessità delle loro infrastrutture legacy, gli assetti di governance articolati e i processi di innovazione perlopiù incrementali contribuiscono ulteriormente a rendere difficoltoso isolare l'effetto specifico dell'esternalizzazione ai TPP, il quale finisce molto spesso per confondersi con altre rigidità strutturali.

Al contrario, le *challenger banks* offrono un terreno d'osservazione privilegiato. La loro struttura nativamente digitale basata su logiche *API-first* le differenzia in modo netto dalle banche tradizionali, consentendo loro di ottenere ampi risparmi di costi fissi operativi e concentrarsi su investimenti in piattaforme digitali, ove l'integrazione con i TPP diventa essenziale per garantire scalabilità e diversificazione[275].

Operando senza sistemi legacy e principalmente via app mobili e piattaforme online, tali banche riescono a cogliere in modo più diretto gli effetti dell'integrazione con terze parti, evitando che questi

[275] P. Rybacki, "*REVOLUT'S REVOLUTION: THE RISE OF A DIGITAL BANK*", University of Chicago, luglio 2022, p.10

vengano attenuati o mascherati da rigidità infrastrutturali[276]. In questo senso, l'esternalizzazione deve essere intesa non tanto come una scelta residuale, quanto piuttosto come leva di crescita e diversificazione, funzionale all'espansione nei mercati, all'ampliamento della gamma di servizi – dai pagamenti al *personal financial management*, dagli investimenti ai crediti *embedded* – e al rafforzamento dei processi di compliance[277]. Inoltre, rispetto agli *incumbent* – spesso penalizzati da interfacce meno intuitive e da politiche di prezzo opache – le *challenger banks* puntano su interfacce *user-friendly* e pricing chiaro. In particolare, questa maggiore trasparenza con cui tali operatori comunicano partnership tecnologiche, *roadmap* di sviluppo e cambiamenti nei prezzi facilita la tracciabilità empirica delle relazioni con le terze parti, offrendo così un terreno di analisi più solido e affidabile.

Alla luce di tali considerazioni emerge che, dove gli *incumbent* privilegiano stabilità e continuità, le *challenger banks* adottano un approccio orientato alla sperimentazione e alla rapidità, condizioni, queste ultime, che hanno portato inevitabilmente a un ampio ricorso all'esternalizzazione.

Ne consegue che esse si configurano come gli intermediari più idonei per permettere l'analisi del rapporto tra esternalizzazione e Open Banking. In questa prospettiva, la scelta di ricorre ai TPP non si limita più a colmare lacune operative, bensì diventa una vera e propria strategia competitiva capace di orientarne la traiettoria di crescita e il posizionamento sul mercato.

Tenendo presente quanto appena esposto, l'analisi si focalizza su due tra le principali *challenger banks* che negli ultimi anni hanno ridefinito il panorama bancario europeo: N26 e Revolut. Tale scelta non è casuale, ma considera il fatto che tali banche, sebbene si siano entrambe distinte negli ultimi anni per l'impiego di tecnologie innovative, interfacce utente intuitive e offerte competitive, rappresentano due modelli contrapposti lungo il continuum dell'esternalizzazione[278]. Se Revolut ha fatto della modularità e della collaborazione con una rete estesa di TPP la leva per scalare rapidamente a livello internazionale e diversificare i propri servizi, N26, invece, ha costruito la propria identità su un modello più integrato e selettivo, che privilegia la governance e la solidità rispetto alla velocità di espansione.

Sulla base di questa contrapposizione si adotta una logica comparativa di tipo *most different system*[279] applicata al grado di esternalizzazione, mantenendo costanti altre variabili rilevanti – come la natura

---

[276] Anna, "*Challenger Banks: Cosa Sono, Come Funzionano e Presenza in Italia/UE*". https://www.workinvoice.it/challenger-banks-cosa-sono/

[277] C. Desando, "*Challenger banks: che cosa sono, come funzionano, le europee e le italiane*", https://www.economyup.it/fintech/challenger-banks-che-cosa-sono-come-funzionano-le-europee-e-le-italiane/, EconomyUp, settembre 2020

[278] A.Matthewson, "*Comparing Revolut, Chime and N26: Neobank Success Stories*", https://fintechmagazine.com/articles/comparing-revolut-chime-and-n26-neobank-success-stories, FinTech Magazine

[279] Per *most different system* si intende "*un metodo di ricerca comparativa che si concentra sul confronto di casi diversi sotto molti aspetti, ma che condividono un risultato o una caratteristica comune. Questo approccio consente ai ricercatori di identificare i fattori che possono influenzare il risultato esaminando casi con contesti e condizioni diversi*." Per ulteriori

digitale e il target retail UE –, così da massimizzare il contrasto utile a testare la validità della tesi. Questo approccio consente quindi di analizzare come due strategie tra loro divergenti affrontino le medesime sfide poste dall'Open Banking e dall'esternalizzazione ai TPP, e di valutare in che misura tali differenze incidano sulla velocità di crescita, sull'ampiezza dei servizi e sulla capacità di mantenere resilienza e compliance.

Tuttavia, occorre precisare che l'analisi non potrà basarsi su un impianto quantitativo pienamente verificabile. Nonostante ripetuti tentativi di ottenere dati granulari direttamente dalle banche oggetto di studio – attraverso richieste formali e sollecitazioni ripetute –, l'accesso a tali informazioni è stato negato data la loro natura altamente sensibile. Di fronte a questa impossibilità, l'analisi ha adottato un approccio prevalentemente qualitativo, basato sull'utilizzo di fonti pubbliche e verificabili – quali bilanci, comunicati ufficiali, documentazione tecnica, rapporti delle autorità di vigilanza –, integrate da indicatori proxy di natura economica e organizzativa. Tale impostazione metodologica, lungi dal costituire un limite, consente di compensare la scarsa disponibilità di dati quantitativi diretti e di osservare in modo critico come l'esternalizzazione[280] ai TPP venga tradotta in strategia competitiva dalle banche digitali.

È in questa prospettiva che trovano fondamento le due ipotesi guida dell'analisi: (i) un crescente ricorso alle terze parti può rappresentare un vantaggio, accelerando il rilascio di nuove funzionalità e favorendo l'ampliamento dell'offerta di Open Banking; (ii) un grado eccessivo di esternalizzazione può generare oneri di controllo e rischi di continuità/*lock-in*, diventando un limite se non sostenuto da un'adeguata struttura di governance.

3.2 – Revolut: l'esternalizzazione ai TPP come leva di crescita

Il caso di Revolut costituisce un esempio paradigmatico di come l'esternalizzazione ai TPP possa trasformarsi da semplice strumento tattico di supporto a vera e propria leva strategica di crescita.

Nata come fintech con l'obiettivo di ridurre i costi dei cambi valuta e dei trasferimenti internazionali, la società ha costruito la propria espansione facendo ampio affidamento su una rete estesa di partner esterni e sullo sviluppo di tecnologie innovative, riuscendo così ad ampliare rapidamente la base

approfondimenti si veda: Business Case Study, "*Comparative Research Methods (Most Similar, Most Different Systems Design)*", https://businesscasestudies.co.uk/comparative-research-methods-most-similar-most-different-systems-design/, agosto 2024

[280] Mentre nei capitoli precedenti l'analisi dell'esternalizzazione ai TPP è stata prevalentemente ricondotta al tema dell'accesso regolamentato ai dati e ai conti, in quanto elemento centrale introdotto dalla PSD2. Nel presente capitolo l'indagine adotta un approccio più ampio, estendendo l'osservazione anche ad altre aree di esternalizzazione – come quelle relative alle infrastrutture tecnologiche, ai servizi di pagamento e alle funzioni di compliance – al fine di restituire una valutazione complessiva più aderente alla complessità dei modelli operativi delle banche digitali.

clienti e a scalare a livello internazionale[281]. Tuttavia, l'evoluzione del suo modello di business non è stata priva di criticità, al contrario l'ampio ricorso all'*outsourcing* ha sollevato significativi interrogativi sulla sostenibilità di lungo periodo, sulla governance e sulla capacità di mantenere un controllo adeguato delle funzioni critiche.

Per indagare questa tensione tra velocità di crescita e solidità regolatoria – in cui il grado di esternalizzazione appare non solo come la principale forza propulsiva, ma anche come fattore di vulnerabilità – si è ritenuto opportuno articolare l'analisi in tre momenti distinti. In primo luogo, verrà ricostruita l'evoluzione del modello di business alla luce delle scelte strategiche e dei vincoli regolamentari; in secondo luogo, si esaminerà il ruolo assunto dai TPP, evidenziando i vantaggi che la loro integrazione ha apportato in termini di innovazione e scalabilità; infine, saranno analizzate le criticità e i rischi connessi a tale impostazione, al fine di valutarne la sostenibilità nel lungo periodo.

3.2.1 – L'evoluzione del modello di business: tra scelte strategiche e vincoli regolatori

Per comprendere le ragioni che hanno spinto Revolut a adottare, sin dall'inizio, un modello fortemente basato sull'esternalizzazione ai TPP, è necessario analizzarne la storia, la mission e le scelte strategiche compiute. Questi fattori, infatti, permettono di chiarire come l'impresa abbia visto nei TPP non un semplice supporto operativo, bensì una leva essenziale di crescita, capace di accelerarne l'espansione e di definire le traiettorie evolutive del modello di business negli anni successivi.

Fondata a Londra nel 2015 da Nikolay Storonsky e Vlad Yatsenko, Revolut nasce con l'obiettivo di superare quelli che lo stesso Storonsky definì "*costi ingiustificati*" legati ai cambi valutari e ai trasferimenti transazionali[282]. Fin dall'inizio, tuttavia, la società non si è limitata a ridurre le commissioni, ma ha cercato di configurarsi come un'alternativa digitale e trasparente al sistema bancario tradizionale, capace di restituire ai clienti un maggiore controllo sulla propria salute finanziaria e di favorire una più ampia inclusione nell'accesso ai servizi[283].

Seguendo una logica tipica delle fasi *early-stage growth*[284], Revolut ha scelto nei primi anni di operare come *Electronic Money Institution* (EMI), concentrandosi soprattutto su servizi a basso

[281] Agenda Digitale, "*Carta Revolut: caratteristiche dei conti e recensione 2025*", https://www.agendadigitale.eu/cittadinanza-digitale/pagamenti-digitali/carta-revolut/, settembre 2025

[282] P. Rybacki, "*REVOLUT'S REVOLUTION: THE RISE OF A DIGITAL BANK*", University of Chicago, luglio 2022, p.16

[283] Revolut LTD, *Annual Report and Financial Statements for the year ended 31 December 2018*, p.4

[284] Per *early-stage growth* si intende la fase iniziale del ciclo di vita di un'impresa caratterizzata da rapida espansione della base clienti e aumento dei ricavi, in genere perseguita attraverso modelli operativi leggeri (*asset light*) e a basso assorbimento di capitale. In questa fase le priorità strategiche sono la scalabilità e la penetrazione del mercato, più che la costruzione di infrastrutture proprietarie e costose. Il modello adottato da Revolut tra il 2015 e il 2018, fondato sul massiccio ricorso a TPP per la gestione di funzioni critiche (pagamenti, onboarding, compliance), rappresenta un esempio

assorbimento di capitale – quali *money transfer*, carte prepagate e cambi in tempo reale – e adottando un modello operativo "*asset light*" basato su un ampio ricorso ai TPP. Questa configurazione le ha consentito non solo di contenere gli investimenti infrastrutturali, ma anche di semplificare l'organizzazione interna e concentrare le risorse sullo sviluppo tecnologico e sull'innovazione di prodotto[285]. Proprio la combinazione tra struttura snella, esternalizzazione delle funzioni critiche e centralità della *user experience* si è rivelata una leva decisiva nella fase di avvio, favorendo un'espansione straordinariamente rapida della base clienti e trasformando in pochi anni l'app da strumento di nicchia per il cambio valuta a piattaforma di riferimento per milioni di utenti[286].

Eppure, l'evoluzione della società non si è limitata alla fase di avvio. Stimolata dall'aumento della base clienti, Revolut ha progressivamente ampliato la propria offerta, andando oltre il perimetro originario dei pagamenti per configurarsi come una piattaforma finanziaria multiprodotto.

Diversamente da N26, che sin dalla sua origine ha intrapreso un percorso più prudente incentrato sul *core banking* e sulla solidità regolatoria, Revolut ha quindi scelto di perseguire una strategia di espansione rapida e diversificata, ampliando costantemente i servizi offerti ben oltre il conto corrente e la carta di pagamento. Difatti, come dichiarato dalla stessa società "*Revolut esiste per rendere la gestione, la spesa, il risparmio, gli investimenti e l'ottenimento di prestiti più economici, semplici e trasparenti. [..] Persone e aziende desiderano un maggiore controllo sulle proprie finanze e noi offriamo ai nostri clienti un'esperienza personalizzata attraverso approfondimenti basati sui dati, consentendo loro di prendere decisioni più consapevoli su come spendere, risparmiare e far crescere il proprio denaro*"[287].

Questa visione ambiziosa, però, non avrebbe potuto consolidarsi senza un rafforzamento sul piano regolatorio e operativo. Proprio in questa prospettiva si colloca la svolta del 2018, anno in cui Revolut ha ottenuto la prima licenza bancaria europea in Lituania, segnando il passaggio da semplice fornitore fintech di servizi finanziari digitali a istituzione bancaria vera e propria.

Alla luce di quanto sopra, l'ottenimento della licenza bancaria europea ha rappresentato un momento di discontinuità decisivo nel percorso di Revolut.

Se fino a quel momento la società aveva potuto scalare rapidamente grazie a un modello fintech basato sull'esternalizzazione e su un ricorso rilevante ai TPP, la licenza ha imposto un ripensamento radicale dell'architettura operativa e della governance, aprendo a una nuova fase di sviluppo.

---

paradigmatico di *early-stage growth* applicato al settore fintech. Per ulteriori approfondimenti in merito si veda: Startup Geeks, "*Le fasi di una startup e il suo ciclo di vita*", https://www.startupgeeks.it/ciclo-vita-startup/

[285] Economy Magazine, "*Aziende e fondi d'investimento accelerano verso il modello "asset light" per una crescita agile*", https://www.economymagazine.it/aziende-modello-asset-light-crescita-agile/, settembre 2024

[286] Nello specifico, dai dati di bilancio emerge un incremento notevole della clientela *retail*, la quale passa da 300.000 utenti nel 2016 a 3,5 milioni nel 2018.

[287] Revolut LTD, 2024 *Annual Report Including Consolidated Financial Statements for the year ended 31 December 2024*, p.16

In qualità di banca autorizzata, Revolut ha acquisito la possibilità di gestire direttamente i depositi dei clienti, di offrire servizi di credito al consumo e di assumere la piena responsabilità in materia di compliance regolatoria. Questo cambiamento di status, quindi, ha comportato un progressivo processo di internalizzazione delle funzioni *core*, riducendo in parte la dipendenza dai partner terzi per le attività più critiche. A confermarlo vi sono anche i dati di bilancio relativi ai costi per *intangible assets*, i quali tra il 2018 e il 2019 – anno in cui la banca ha iniziato effettivamente ad operare in qualità di istituto bancario – sono aumentati del 153,77%[288], a testimonianza degli investimenti destinati allo sviluppo di software e infrastrutture tecnologiche proprietarie, indispensabili per garantire operatività bancaria, resilienza e adeguati standard di governance.

Da ciò ne consegue che, la licenza bancaria non ha solo legittimato Revolut ad operare come attore a pieno titolo nel sistema finanziario europeo, ma ha anche rafforzato la sua capacità di definire strategie autonome e meno vincolate alla rete di TPP su cui si era fondata la fase iniziale della crescita. Parallelamente, l'entrata in vigore della PSD2 in UK e nello Spazio Economico Europeo ha consolidato l'obbligo di condivisione dei dati bancari tramite API (cfr. §§ 1.1.3 e 1.4), creando un ambiente particolarmente favorevole all'operatività di Revolut, che ha potuto così consolidare ulteriormente il proprio modello fondato sull'accesso ai dati e sull'interazione con i TPP. Proprio in questa cornice, la società ha avviato lo sviluppo di API proprietarie, in particolare mediante la piattaforma *Revolut Business*, assumendo così non solo il ruolo di utilizzatore, ma anche di fornitore di soluzioni tecnologiche integrabili da terzi. In modo analogo, ha ampliato l'offerta di prodotti introducendo strumenti coerenti con la mission originaria di semplificare la gestione del denaro, quali Revolut X e Revolut *BillPay*, segnando un'evoluzione verso la costruzione di un'unica piattaforma in grado di integrare funzioni di pagamento, risparmio, investimento e credito.

Inoltre, sempre sul piano regolatorio un traguardo significativo è stato raggiunto nel 2024, quando la *Prudential Regulation Authority* (PRA) ha concesso alla società una licenza provvisoria per lo svolgimento di attività bancaria anche nel Regno Unito; traguardo significativo che testimonia la maturazione del modello e la progressiva riduzione del divario con gli operatori tradizionali[289].

Infine, al consolidamento regolatorio in Europa si è affiancata una marcata strategia di espansione internazionale, che ha condotto al lancio delle versioni beta dell'app dapprima in Australia e Singapore e, successivamente, negli US e in Giappone. Ne è derivato un percorso evolutivo che ha progressivamente trasformato Revolut da fintech focalizzata esclusivamente sui pagamenti a banca digitale globale. Si tratta di un'evoluzione che contrasta – come si vedrà anche nel prosieguo dell'analisi – con quella di N26, la quale, pur avendo intrapreso nello stesso periodo un percorso di

[288] Revolut LTD, *Annual Report and Financial Statements for the year ended 31 December 2019*, p.22

[289] R. Dillet, "*Revolut receives long-awaited UK banking license*", https://techcrunch.com/2024/07/25/revolut-receives-much-awaited-uk-banking-license/, TechCrunch, luglio 2024

crescita analogo come *challenger bank*, ha preferito adottare una strategia più prudente e incentrata sul *core banking*, puntando sulla solidità regolatoria sin dall'inizio.

3.2.2 – TPP e architettura operativa: un modello abilitante tra innovazione e scalabilità

Uno degli elementi che maggiormente contraddistingue Revolut rispetto agli operatori bancari tradizionali è la centralità dei *Third Party Providers* (TPP) nella sua architettura operativa. Fin dai primi anni, la società ha adottato una strategia "*asset light*" e modulare (§cfr. 3.2.1), fondata sull'integrazione di API di partner esterni per presidiare funzioni come i pagamenti, l'onboarding dei clienti e i controlli di AML. In tal senso, i TPP non hanno svolto un mero ruolo accessorio, ma sono diventati veri e propri mattoni infrastrutturali, capaci di ridefinire l'identità e il vantaggio competitivo della fintech.

Questa architettura *plug & play* ha reso possibile ciò che difficilmente sarebbe stato replicabile seguendo il modello di una banca universale, ovvero scalare in tempi rapidissimi, ridurre i costi inziali e concentrare le risorse sul miglioramento della *user experience*. Ne deriva che il ricorso ai TPP non ha rappresentato unicamente una scelta contingente, ma una vera e propria leva di scalabilità che ha accompagnato Revolut anche oltre la fase di avvio.

In questa prospettiva, l'analisi delle principali collaborazioni siglate da Revolut con partner esterni permette di comprendere in che modo l'esternalizzazione sia stata tradotta in vantaggi concreti.

Tra i casi più significativi si colloca la collaborazione con Modulr, avviata nella fase iniziale di sviluppo della società, quando la costruzione di infrastrutture di pagamento proprietarie avrebbe comportato tempi troppo lunghi e costi proibitivi.

Questa partnership ha consentito a Revolut non solo di velocizzare l'apertura dei conti e l'elaborazione delle transazioni, ma anche di integrare in tempi rapidi una piattaforma API *Payment-as-a-Service*, capace di abilitare l'immediata creazione di conti in GBP con *sort code* e *account number* e di garantire l'accesso ai principali sistemi di pagamento britannici (Faster Payments, Bacs e CHAPS) [290].

In quest'ottica, la "*flessibilità, resilienza e scalabilità delle infrastrutture offerte da Modulr hanno giocato un ruolo chiave per la crescita di Revolut*", consentendo alla *challenger bank* di abbattere drasticamente le barriere all'ingresso in un mercato altamente competitivo e di raggiungere in pochi anni quasi 12 milioni di clienti[291]. A confermare ulteriormente l'impatto positivo di questa strategia di esternalizzazione, in termini di crescita e fidelizzazione della clientela è lo stesso CEO Storonsky, secondo il quale *"[Revolut] è entusiasta di avere Modulr al suo fianco mentre prosegue nella sua*

[290] Frog, "*Revolut extend strategic partnership with Modulr*", https://frogcapital.com/think-frog/revolut-extend-strategic-partnership-with-modulr/

[291] Blenheim Chalcot, "*Modulr and Revolut will continue disrupting financial services together*", https://blenheimchalcot.com/blog/modulr-and-revolut-will-continue-disrupting-financial-services-together, luglio 2020

missione di rivoluzionare il settore dei servizi finanziari e lanciare altri prodotti estremamente vantaggiosi per i propri clienti"[292].

Ciononostante, l'esperienza con Modulr rappresenta soltanto un primo tassello della strategia di esternalizzazione implementata da Revolut. In linea con l'iniziale strategia "*asset light*", la società ha fatto ricorso a provider esterni anche per altre funzioni ad alta intensità regolatoria, tra le quali l'*onboarding* della clientela e i controlli AML/KYC. In questo caso, tuttavia, l'esternalizzazione non è rimasta stabile nel tempo, poiché – come si discuterà nel prosieguo – con l'ottenimento della licenza bancaria tali attività sono state progressivamente internalizzate per rafforzare i controlli e la governance.

Nonostante i bilanci societari evidenzino chiaramente il ricorso ai TPP per lo svolgimento di varie attività operative – tra cui appunto i processi di *Know Your Customer* (KYC) & *Anti-Money Laundering* (AML) –, non sono disponibili fonti ufficiali che documentino in modo puntale gli effetti specifici derivanti da tali partnership[293]. La mancanza di evidenze documentali puntuali sugli effetti delle partnership in materia di AML/KYC non impedisce però di formulare alcune considerazioni critiche.

In tal senso, un utile termine di paragone è offerto dal caso Monzo, principale competitor di Revolut nella scena britannica, che ha esternalizzato queste funzioni a Onfido – uno dei TPP più affermati del settore[294]. In particolare, l'esperienza di Monzo mostra come l'esternalizzazione abbia consentito di contenere i costi connessi alla gestione interna di procedure complesse e ad alta intensità normativa, ma soprattutto di ridurre i tempi di *onboarding*, trasformando l'apertura di un conto in un'operazione rapida e accessibile rispetto agli standard delle banche tradizionali[295].

Alla luce di quanto sopra e della forte similitudine tra i due modelli fintech, è ragionevole ipotizzare che anche per Revolut l'esternalizzazione di queste funzioni abbia prodotto benefici analoghi. Ciò spiegherebbe, almeno in parte, la rapidità con cui la società è riuscita ad ampliare la propria base clienti, passata da circa 600.000 utenti nel 2017 a oltre 52 milioni nel 2024[296].

---

[292] Blenheim Chalcot, "*Modulr and Revolut will continue disrupting financial services together*", cit.

[293] Nello specifico, ogni relazione annuale della società riporta sotto la voce "*Third Party Risk*" espressamente che: « *Revolut relies on third parties and outsourcing service providers for the delivery of its business operations across a number of channels, for example, payment processing, customer support, commodity, crypto and stock exchange services, Know Your Customer (KYC) & Anti-Money Laundering (AML) as well as other business services*». Per ulteriori dettagli si veda: Revolut LTD, *Annual Report and Financial Statements for the year ended 31 December 2019*, p.9

[294] L'assunzione dell'esperienza di Monzo quale come *proxy* comparativa risponde a una logica di *analisi per comparables*, in quanto entrambe appartengono allo stesso *peer group* delle *challenger banks* europee e sono caratterizzate da un modello *asset light* e un'architettura operativa fondata sull'integrazione di TPP. Dunque, in assenza di evidenze dirette per Revolut, l'analisi per *comparables* consente di ipotizzare che benefici analoghi – in termini di riduzione dei costi e rapidità di onboarding – possano essersi verificati anche per quest'ultima.

[295] Financial IT, "*Onfido Boosts Identity Verification Solution to Make KYC for Financial Services Even Easier*", https://financialit.net/news/security/onfido-boosts-identity-verification-solution-make-kyc-financial-services-even-easier, ottobre 2016

[296] Revolut LTD, *2024 Annual Report Including Consolidated Financial Statements for the year ended 31 December 2024*

Sebbene tale dinamica sia riconducibile anche ad altre leve – quali la diversificazione dei prodotti, una politica di *pricing* aggressiva e una forte spinta internazionale – l'adozione di processi di onboarding rapidi e sicuri, resi possibili dal ricorso a soluzioni esternalizzate, appare pertanto un fattore decisivo nell'accelerazione del ritmo di acquisizione della clientela.

Eppure, proprio la natura altamente sensibile delle funzioni di AML e KYC e la centralità dei dati trattati hanno reso inevitabile per Revolut un cambio di paradigma.

A partire dall'ottenimento della licenza bancaria nel 2018 – che ha imposto alla società di assumersi direttamente responsabilità fino ad allora delegate ai TPP –, Revolut ha avviato un graduale processo di **internalizzazione, volto a** rafforzare i controlli interni e consolidare la governance. Tale scelta si è concretizzata, successivamente, nello sviluppo interno di un sistema proprietario per l'identificazione dei clienti e nell'investimento in progetti finalizzati a garantire standard elevati di sicurezza delle informazioni[297].

Tuttavia, questo percorso di internalizzazione non ha segnato un arretramento del modello originario fondato sull'esternalizzazione, quanto piuttosto un suo riequilibrio. Se, da un lato, alcune funzioni *core* venivano riportate *in house* per rafforzare la governance, dall'altro altre funzionalità – quali i servizi di aggregazione dei conti, i pagamenti istantanei e l'integrazione di soluzioni verticali – hanno continuato a poggiare su partnership strategiche con TPP specializzati.

In questo contesto la crescente diffusione dell'Open Banking in Europa, accelerata dalla diffusione della PSD2, ha rappresentato per Revolut un terreno particolarmente fertile per consolidare il proprio modello "ibrido". Laddove gli operatori bancari tradizionali hanno spesso faticato a adattarsi a un ecosistema basato sulla condivisione dei dati e sull'integrazione tramite API – come discusso nel §2.1.2 –, Revolut è riuscita a sfruttare le potenzialità dell'Open Banking, esternalizzando a TPP specializzati funzioni innovative per rafforzare la propria posizione competitiva. Alla luce di tali considerazioni, le collaborazioni con TPP specializzati come TrueLayer e Tink hanno così assunto un ruolo centrale, consentendo alla società di rafforzare il proprio posizionamento come piattaforma finanziaria aperta e integrata.

In particolare, la partnership con TrueLayer ha permesso di introdurre servizi di *Account Information Services* (AIS) e *Payment Initiation Services* (PIS), attraverso i quali i clienti possono collegare i propri conti esterni, ottenere una visione unificata delle proprie finanze e ricaricare in tempo reale il conto Revolut senza dover ricorrere a bonifici tradizionali o carte di pagamento[298]. In questo modo, come sottolineato dal *Product Owner Open Banking* di Revolut, la collaborazione con TrueLayer ha

[297] Revolut LTD, *Annual Report & Financial Statements For the year ended 31 December 2020*, p.14

[298] F. Simoneschi, "*Partnering with Revolut to give people greater control over their finances*", https://truelayer.com/blog/financial-services/customer-story-revolut/, TrueLayer

permesso ai clienti retail e business di avere una maggiore visibilità sui conti e godere al tempo stesso di un servizio più efficiente in termini di costi[299].

Parallelamente, la collaborazione avviata con Tink ha rafforzato ulteriormente questo posizionamento. Grazie alla tecnologia PIS sviluppata dalla società svedese, Revolut ha potuto offrire ai propri clienti la possibilità di connettersi direttamente al conto bancario di origine, autorizzare l'operazione e completare un pagamento senza uscire dall'app[300]. Si tratta di un passaggio di rilievo, in quanto, come dichiarato dal responsabile *Retail* di Revolut, "*tali soluzioni consentiranno di espandere i servizi e i prodotti di Open Banking in mercati nuovi in modo più rapido e sostenibile*"[301].

Tenendo presente tali considerazioni, è possibile affermare che l'integrazione con TPP quali TrueLayer e Tink riveli come l'esternalizzazione non rappresenti per Revolut soltanto un supporto operativo, ma il fondamento di un modello che si avvicina sempre più al *Banking-as-a-Service*. Tale logica trova la sua massima espressione in *Revolut Business*, il servizio lanciato nel 2017 per le piccole e medie imprese e i professionisti, attraverso il quale la società è passata dall'essere un utilizzatore di API esterne a fornitore di infrastrutture aperte.

In questo quadro, l'esternalizzazione ai TPP viene trasformata in una vera e propria leva strategica per creare valore anche nel segmento *corporate* attraverso l'*Integration Hub*, concepito come una sorta di marketplace di API capace di collegare il conto aziendale a una pluralità di applicazioni esterne. In questo modo, Revolut non si limita a fornire strumenti finanziari, ma diventa il perno di un ecosistema più ampio, in cui i flussi operativi delle imprese vengono semplificati grazie al ricorso a TPP specializzati. Le integrazioni spaziano dalla contabilità con Xero e FreeAgent, alla gestione HR, fino agli strumenti di produttività con Zapier e alle soluzioni di pagamento per *e-commerce*[302].

Di fatto, attraverso questa architettura modulare, Revolut Business offre alle imprese clienti la possibilità di integrare in un unico ambiente le funzioni critiche del business – conti multivaluta, carte aziendali, funzionalità di gestione dei costi e connessioni con software di contabilità – senza dover sostenere costi di sviluppo proprietari. Non sorprende, dunque, che i clienti business siano passati dai circa 50.000 del 2018 (anno successivo al lancio) a oltre 3,4 milioni nel 2024, con una crescita media annua del 56%, contribuendo per circa il 15% dei ricavi totali del gruppo Revolut[303].

In definitiva, il percorso di Revolut mostra come l'esternalizzazione ai TPP non si limiti a colmare gap tecnologici, ma si configuri come un vero e proprio pilastro della strategia di lungo periodo della società. Se nella fase iniziale l'affidamento a partner esterni ha rappresentato la condizione necessaria

---

[299] TrueLayer, "*Revolut: transforming digital finance*", https://truelayer.com/customers/revolut/

[300] Tink, "*Revolut partners with Tink for European payments*", https://tink.com/press/revolut-partnership/, giugno 2022

[301] Ibid.

[302] Revolut, "*What are Revolut Business integrations?*", https://help.revolut.com/business/help/more/integrating-with-other-accounting-platforms/revolut-connect/what-is-marketplace/

[303] Revolut LTD, *2024 Annual Report Including Consolidated Financial Statements for the year ended 31 December 2024*

per scalare rapidamente e introdurre servizi innovativi, oggi esso costituisce la base su cui la società costruisce il proprio modello di banca digitale globale, aperte e integrata. Tale traiettoria si discosta profondamente da quella di altre *challenger bank*, come N26, che hanno preferito circoscrivere l'esternalizzazione a poche funzioni ancillari (cfr.§3.3.1).

Ciononostante, l'adozione di un modello così fortemente dipendente da TPP non è priva di implicazioni critiche. Ai benefici in termini di velocità, scalabilità e innovazione, si contrappongono infatti rischi e *trade-off* rilevanti, che saranno approfonditi nel prossimo paragrafo al fine di valutare la reale sostenibilità di tale strategia nel lungo periodo.

3.2.3 – Criticità dell'architettura TPP-centrica: tra lock-in e responsabilità regolatorie

Pur essendo un attore relativamente recente, Revolut si è rapidamente imposta come una delle realtà più rilevanti del panorama bancario europeo, mostrando una capacità di crescita che ha pochi precedenti. Tale traiettoria, sostenuta da un modello fortemente orientato alla diversificazione dei ricavi e alla scalabilità internazionale (cfr. 3.2.1), dimostra come il massiccio ricorso ai *Third Party Providers* (TPP) abbia rappresentato un vero fattore abilitante, più che una semplice scelta operativa. Eppure, la stessa architettura *plug & play* che ha consentito a Revolut di scalare rapidamente porta con sé vulnerabilità intrinseche, capaci di mettere in discussione la sostenibilità di tale modello nel lungo periodo. In altri termini, l'esternalizzazione ai TPP non sempre si è tradotta in efficienza lineare, ma sovente ha esposto la società a rischi specifici, primo fra tutti la dipendenza tecnologica.

In proposito, un aspetto critico della dipendenza dai TPP emerge con chiarezza guardando al ruolo di Modulr (approfondito nel §3.2.2), partner strategico per l'infrastruttura dei pagamenti. Se da un lato questa collaborazione ha consentito a Revolut di accedere con rapidità ai principali mercati, abbattendo le barriere all'ingresso e riducendo i costi operativi, dall'altro ha reso evidente come l'operatività di milioni di clienti sia subordinata al corretto funzionamento di un unico operatore terzo. In altre parole, la stessa forza della scalabilità resa possibile dall'esternalizzazione spesso si traduce in un rischio di *lock-in* (cfr. §2.1.2), secondo il quale un'interruzione del servizio o un malfunzionamento del TPP rischierebbe di compromettere immediatamente la continuità dei servizi di Revolut, con effetti diretti sulla clientela.

Un esempio emblematico in tal senso è rappresentato dall'interruzione operativa del servizio verificatasi nel 2017, quando il malfunzionamento di un processore di pagamento di un provider ha determinato il fallimento di numerose transazioni con carta. Tale episodio ha messo in evidenza come un singolo *point-of-failure* possa tradursi in un rischio immediato non solo per l'operatività quotidiana, ma anche per la fiducia della clientela, che percepisce tali inefficienze percepite come responsabilità diretta di Revolut. Lo stesso CEO Storonsky ne ha riconosciuto la portata, ribadendo che, "*pur funzionando nella maggior parte dei casi in maniera "brillante", tali partnership*

comportano sempre una percentuale di rischio legata al possibile fallimento di un punto critico della catena operativa, con conseguenze dirette per i clienti]"[304].

Oltre ai riflessi reputazionali ed operativi, tale episodio ha generato anche rilevanti conseguenze economiche. Difatti, le continue segnalazioni di interruzione del servizio ricevute dagli utenti hanno spinto Revolut a riconoscere la necessità di costruire un processore di pagamento proprietario, così da ridurre la dipendenza dalle terze parti e limitare il rischio di interruzioni future[305]. Una scelta che, sebbene abbia contribuito a rafforzare la resilienza tecnologica dell'istituto, ha mostrato con chiarezza come l'esternalizzazione ai TPP possa tradursi in oneri imprevisti, imponendo investimenti significativi anche nelle fasi più delicate dello sviluppo aziendale.

Alla luce di tali considerazioni, emerge che la dipendenza tecnologica dai TPP, pur garantendo rapidità e scalabilità, espone Revolut a vulnerabilità che travalicano il piano strettamente operativo. I disservizi e i malfunzionamenti, infatti, non si riflettono unicamente sull'esperienza dei clienti, ma pongono anche questioni di natura regolatoria e di governance, giacché la responsabilità ultima rimane sempre in capo all'istituto, indipendentemente dal ruolo del partner esterno.

Proprio in quest'ottica, la disciplina europea in materia di Open Banking ha introdotto regole stringenti volte a disciplinare l'accesso dei TPP ai conti dei clienti. In particolare, gli RTS sull'autenticazione forte emanati dall'EBA, in attuazione della PSD2, stabiliscono che i TPP possano accedere ai conti dei clienti solo se in possesso di un certificato eIDAS, che deve essere verificato obbligatoriamente dalla banca presso cui avviene l'accesso[306]. Tuttavia, se tale strumento garantisce l'identificazione dell'identità del soggetto, non è sufficiente a certificare le effettive autorizzazioni a cui esso è abilitato[307]. Ne deriva che un eventuale affidamento eccessivo di Revolut ai soli certificati qualificati rischierebbe di tradursi in concessioni di accesso improprie, con implicazioni potenzialmente rilevanti sia in termini di conformità regolamentare sia di tutela dei clienti. In questo senso, la dipendenza dai TPP non riduce ma, al contrario, accresce il carico di responsabilità in capo alla società, che deve predisporre sistemi di controllo interni per vigilare su processi che non gestisce direttamente, poiché eventuali controlli insufficienti o verifiche inadeguate non ricadono sul TPP, bensì sulla stessa società[308].

---

[304] N. Storonsky, "*Enough with the excuses. Here's how we're going to stop these outages*.", https://www.revolut.com/blog/post/enough-with-the-excuses-heres-how-were-going-to-stop-these-outages/, Revolut, luglio 2018

[305] T. Andreasyan, "*Revolut to bring processing in-house*", https://www.fintechfutures.com/digital-banking/revolut-to-bring-processing-in-house, FintechFutures, novembre 2018

[306] *Regolamento Delegato (UE) 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,* art.34

[307] Konsentus, "*The Risk of Only Checking eIDAS Certificates*", https://www.konsentus.com/risk-of-only-checking-eidas-certificates/, luglio 2022

[308] Macro Global, "*Open Banking: AISP, PISP & ASPSP Explained*", https://www.macroglobal.co.uk/blog/regulatory-technology/open-banking-psd2/aisp-pisp-aspsp-explained/, Maggio 2022

Non sorprende, dunque, che a partire dall'ottenimento della licenza bancaria la società abbia scelto di internalizzare progressivamente parte dei presidi di AML/KYC, nel tentativo di limitare il rischio di incorrere in sanzioni e rilievi da parte delle autorità di vigilanza.

Ciononostante, permangono criticità rilevanti. In particolare, nel 2023 Revolut è finita sotto osservazione della FCA per presunti trasferimenti sospetti provenienti da conti segnalati dalla *National Crime Agency*, per un valore complessivo di circa 1,7 milioni di sterline[309]. Analogamente, nel 2025 la Banca di Lituania ha comminato una sanzione di 3,5 milioni di euro per "*violazioni e carenze nel monitoraggio delle relazioni commerciali e delle transazion*i", sottolineando le difficoltà della società nel garantire adeguati standard antiriciclaggio[310]. In entrambi i casi, indipendentemente dal ruolo effettivo dei partner esterni, la responsabilità finale è ricaduta su Revolut, a conferma di come la delega a TPP non attenui gli obblighi di vigilanza, ma, anzi, ne accresca la complessità gestionale.

Eppure, l'impatto più critico di queste carenze non si misura solo nelle sanzioni economiche o negli interventi organizzativi necessari per rafforzare i controlli interni, bensì si riflette soprattutto sul danno reputazionale. Ogni rilievo delle autorità o inefficienza riconducibile ai TPP erode il capitale fiduciario di clienti e investitori, che costituisce per una *challenger bank* la principale fonte di legittimazione competitiva.

In definitiva, l'esperienza di Revolut mostra come l'esternalizzazione ai TPP non possa essere valutata in termini assoluti, né come vantaggio univoco né come ostacolo insormontabile. Nella fase iniziale essa ha rappresentato un fattore abilitante decisivo, permettendo alla società di scalare rapidamente, penetrare mercati complessi e diversificare la propria offerta senza dover sostenere costi proibitivi in infrastrutture e risorse interne. Con la maturazione del modello e l'ottenimento della licenza bancaria, invece, è emerso con chiarezza l'altro lato della medaglia: la dipendenza da partner esterni genera rischi tecnologici, normativi e reputazionali che ricadono interamente su Revolut, la quale rimane responsabile ultima anche per processi delegati. La vera sfida consiste, dunque, nel modulare nel tempo l'intensità e la qualità del ricorso ai TPP, così da preservare i benefici senza trasformali in fattori di rischio capaci di compromettere la sostenibilità del modello nel lungo periodo. Un approccio, quest'ultimo, che – come si vedrà in seguito – si contrappone alla strategia più prudente di N26, orientata a limitare l'esternalizzazione a funzioni marginali.

---

[309] A. Fathi, "*FCA indaga su Revolut per aver facilitato transazioni in violazione delle sanzioni*", https://financefeeds.com/it/FCA-indaga-su-Revolut-per-aver-facilitato-le-sanzioni-in-caso-di-violazione-delle-transazioni/, ottobre 2023

[310] Reuters, "*Lithuania fines Revolut 3.5 million euros for money-laundering prevention failures*", https://www.reuters.com/technology/lithuania-fines-revolut-35-million-euros-money-laundering-prevention-failures-2025-04-08/, aprile 2025

3.3 – N26: la limitata esternalizzazione come presidio di solidità

Se Revolut rappresenta l'esempio di una strategia "*asset light*" spinta all'estremo, fondata su un ampio ricorso ai TPP come leva per scalare rapidamente, il caso di N26 evidenzia invece un approccio di natura differente. Pur condividendo con Revolut la natura di *challenger bank* digitale, N26 ha perseguito un modello più vicino a quello tradizionale, orientato a garantire solidità regolatoria e autonomia infrastrutturale. La volontà di limitare l'esternalizzazione ai soli ambiti ancillari e di costruire progressivamente *in house* gran parte delle proprie infrastrutture critiche, dal core banking ai presidi AML/KYC, ha chiarito fin dall'inizio il suo indirizzo strategico.

Questa impostazione ha inevitabilmente ridotto la flessibilità e la capacità di *rollout* su scala internazionale rispetto a Revolut, ma, al contempo, ha consentito a N26 di contenere l'esposizione ai rischi di *lock-in* tecnologico, di mantenere un maggiore controllo sui dati sensibili dei clienti e di rafforzare la propria posizione nei confronti delle autorità di vigilanza.

L'analisi del caso N26, dunque, consente di cogliere gli effetti di una strategia di crescita meno aggressiva, ma più attenta a presidiare governance e compliance dall'interno. Questo rende particolarmente rilevante il confronto tra i due modelli, poiché permette di valutare se – e in quale misura – il ricorso massiccio ai TPP possa configurarsi come un vantaggio competitivo sostenibile nel lungo periodo.

Anche in questo caso, per valutare in maniera sistematica l'impatto dell'esternalizzazione, si è ritenuto opportuno articolare l'analisi in tre momenti distinti. In primo luogo, verrà ricostruita l'evoluzione del modello di business alla luce delle scelte strategiche e dei vincoli regolamentari; in secondo luogo, si esaminerà il ruolo assunto dai TPP, evidenziando i vantaggi che la loro integrazione ha apportato in termini di innovazione e scalabilità; infine, saranno analizzate le criticità e i rischi connessi a tale impostazione, al fine di valutarne la sostenibilità nel lungo periodo.

3.3.1 – Evoluzione del modello di business: tra crescita ed equilibrio regolatorio

L'analisi dell'evoluzione del modello di business di N26 non rappresenta un mero esercizio descrittivo, ma un passaggio essenziale per poter comprendere come le scelte strategiche e regolatorie adottate dall'istituto abbiano inciso sul grado di esternalizzazione ai TPP e, conseguentemente, sulla traiettoria di crescita della banca. Se il caso di Revolut evidenzia come l'affidamento ricorsivo ai TPP possa costituire una leva per scalare rapidamente, N26 si configura fin dall'inizio come un modello opposto: una *challenger bank* che ha preferito costruire la propria espansione su basi regolatorie solide e un ricorso selettivo all'esternalizzazione. La storia e la *mission* non chiariscono soltanto le origini della banca digitale, ma piuttosto spiegano le ragioni per le quali la società abbia preferito un

approccio più prudente, sacrificando in parte la velocità di *rollout* a favore della stabilità e della credibilità istituzionale.

Fondata a Berlino nel 2013 da Valentin Stalf e Maximilian Tayenthal con il nome di *Number26*, la società si è posta l'obiettivo già nella fase iniziale di diventare la "*banca del XXI secolo*", costruita intorno a un'esperienza *mobile-first*, semplice e trasparente.

A differenza di Revolut, N26 non nasce per abbattere i costi dei cambi valutari o per proporre una super-app finanziaria, bensì per replicare in chiave digitale le funzioni essenziali di una banca tradizionale, offrendo un servizio più accessibile, semplice e lineare.

Questa visione si è tradotta fin da subito in scelte operative concrete, trovando una prima applicazione nel lancio ufficiale di Number26: un modello di banca *digital-only* che proponeva un conto corrente gratuito con carta di pagamento integrata, interamente gestibile tramite app. La risposta del mercato fu immediata, in quanto già a pochi mesi dal lancio N26 contava circa 100.000 clienti, a conferma della forte domanda di soluzioni bancarie digitali semplici e intuitive[311].

La scelta di operare sin dalla fase di *early-stage* in qualità di istituto bancario puro – pur non disponendo ancora della licenza bancaria completa e appoggiandosi temporaneamente a un istituto partner per la gestione dei fondi dei clienti – ha rappresentato un elemento distintivo nel panorama fintech dell'epoca[312]. Diversamente da molte *challenger banks*, come Revolut (cfr.§3.2.1), che hanno preferito operare a lungo come *e-money institution*[313] limitandosi a offrire servizi ancillari – quali pagamenti digitali e cambi valuta – in attesa di conseguire una licenza bancaria, N26 ha scelto di presentarsi come una "vera banca", anticipando la successiva autorizzazione.

Il rilascio della licenza bancaria tedesca nel 2016 da parte della *Federal Financial Supervisory Authority* (BaFin) non ha quindi rappresentato una rottura improvvisa, bensì la naturale prosecuzione di un percorso già orientato alla piena integrazione nel sistema finanziario[314]. Tuttavia, sul piano operativo tale autorizzazione ha costituito un vero e proprio punto di svolta, consentendo a N26 non solo di gestire autonomamente i depositi e di rafforzare la propria legittimità istituzionale, ma anche di avviare un percorso di espansione europea più solido e credibile.

Forte della licenza bancaria, N26 ha inizialmente concentrato la propria offerta sui servizi essenziali di *core banking* – conti correnti, carte di pagamento e trasferimenti di denaro internazionali –

---

311 D. Curry, "*N26 Revenue and Usage Statistics (2025)*", BusinessofApps, https://www.businessofapps.com/data/n26-statistics/, gennaio 2025

312 Contrary Research, "*N26*", https://research.contrary.com/company/n26, febbraio 2023

313 Operare in qualità di *e-money institution* significa che la società in questione sfrutta una licenza *e-money*, la quale - a differenza di quella tradizionale - consente alla società di offrire servizi finanziari e di pagamento come bonifici e cambio valuta, ma non di operare come banca o di gestire depositi. Per ulteriori approfondimenti in merito alle licenze bancarie si veda: N26, "*Cos'è una licenza bancaria?*", https://n26.com/it-it/licenza-bancaria

314 N26, "*BaFin order for N26: What it means, what we're doing – and why our customers don't need to worry*", https://n26.com/en-de/blog/bafin-order-what-it-means-and-what-we-are-doing, maggio 2019

integrandoli con alcune funzionalità complementari. Eppure, la diversificazione è rimasta volutamente contenuta e limitata a pochi servizi ancillari – quali strumenti di risparmio, opzioni di investimento e trading di criptovalute –, che, coerentemente con una strategia di esternalizzazione mirata, sono stati affidati a pochi TPP selezionati e specializzati. In tal modo, la banca ha potuto ampliare progressivamente il ventaglio di prodotti senza appesantire la propria infrastruttura interna, garantendo al contempo agli utenti la possibilità di gestire le diverse esigenze finanziarie quotidiane attraverso un'unica applicazione.

Dal punto di vista dell'innovazione, l'obiettivo iniziale di offrire un'esperienza di *mobile banking* interamente fruibile da smartphone si è tradotto nell'introduzione di funzionalità digitali coerenti con il *core business*, pensate per rafforzare la semplicità e la centralità dell'utente. Come sottolineato anche da Schleussner, dirigente di N26, "*creare una banca basata sul cloud in un settore fortemente dipendente dai sistemi IT legacy rappresenta un grande vantaggio, ma ci siamo trovati in una situazione in cui i processi interni non rispecchiavano più l'esperienza bancaria digitale fluida che offrivamo ai clienti tramite la nostra app. Dunque, era assolutamente necessario avere una piattaforma che potesse essere flessibile, scalabile e crescesse con la società*"[315].

In quest'ottica, l'introduzione di *Spaces* costituisce un esempio emblematico di innovazione "interna", che non amplia in modo radicale la gamma dei servizi ma perfeziona la fruibilità del conto, consentendo ai clienti di creare sottoconti personalizzati pur sempre mantenendo fede all'approccio prudente della società[316].

Risulta evidente, alla luce di quanto sopra, come tale impostazione si discosti in maniera sostanziale da quella di Revolut. Mentre quest'ultima – come discusso nel §3.2.1 – ha puntato sin dall'inizio sulla diversificazione rapida dei servizi e sull'esternalizzazione massiccia ai TPP come leva di scalabilità, N26 ha privilegiato un modello lineare e centrato sul *core banking*, in cui le innovazioni interne servono a rafforzare la semplicità d'uso piuttosto che a moltiplicare i servizi[317].

Infine, anche sul piano dell'espansione geografica emergono differenze significative. N26 ha privilegiato la solidità regolatoria e la coerenza operativa, consolidando progressivamente la propria presenza in Europa, dove oggi opera in 23 Paesi. Diversamente da Revolut, che ha puntato su un'espansione rapida verso i mercati extra-UE (cfr. §3.2.1), N26 ha preferito muoversi con maggiore cautela nel panorama internazionale.

---

[315] S. Dunne, "*N26 is revolutionizing the global banking industry through digital transformation*", https://blog.workday.com/it-it/how-n26-delivering-digital-disruption-across-global-banking.html, Workday blog, aprile 2022

[316] N26, "*Simplify your finances with Spaces: our new way to organize your money*", https://n26.com/en-eu/blog/organize-your-way-with-spaces, Agosto 2018

[317] Contrary Research, "*N26*", cit..

Nonostante la visione fosse quella di "*costruire la banca che il mondo ama usare*", i tentativi di ingresso nel Regno Unito e negli Stati Uniti – pensati per rafforzare la *user experience* e a integrare i servizi bancari personali nella vita quotidiana dei clienti – si sono rivelati insostenibili e hanno portato in pochi anni al ritiro dai due mercati[318].

Una decisione che riflette non solo una valutazione di sostenibilità economica, ma anche le complessità regolatorie incontrate in contesti caratterizzati da regimi normativi stringenti e diversi da quelli europeo (cfr. §1.4). Non a caso, l'uscita dal mercato statunitense è coicisa proprio "*con una fase in cui la banca ha scelto di contrarre le proprie risorse sul business europeo e di ampliare progressivamente l'offerta, [andando] oltre i conti correnti tradizionali per rispondere alla domanda crescente di nuovi prodotti e servizi*".[319]

In definitiva, il percorso di N26 mette in luce un modello diametralmente opposto a quello di Revolut, in cui l'esternalizzazione ai TPP viene confinata a poche aree complementari quali risparmio, investimenti e pagamenti transnazionali, mentre le funzioni più sensibili rimangono sotto stretto presidio interno. Una decisione, dettata dalla volontà di ridurre la dipendenza da fornitori esterni e rafforzare la credibilità verso le autorità di vigilanza, che ha configurato l'esternalizzazione non tanto come una leva di crescita, quanto piuttosto come un supporto secondario al *core business*, coerente con una strategia di consolidamento prudente e regolata.

3.3.2 – Ruolo dei TPP e architettura operativa: un modello centrato sul *core banking*

Uno degli elementi che distinguono N26 dalle altre *challenger banks*, e in particolare da Revolut, è l'approccio prudente e selettivo adottato nei confronti dell'esternalizzazione ai TPP.

Nonostante nella fase iniziale si sia appoggiata a Wirecard per il *back-end* bancario – scelta che, in attesa della licenza bancaria, le ha consentito di attrarre rapidamente oltre 200.000 utenti e ottenere consistenti finanziamenti[320] –, N26 si è presto orientata verso un modello fondato sul controllo diretto delle funzioni *core*, ponendosi come banca pienamente regolata sotto la stretta sorveglianza della BaFin. In coerenza con questa scelta strategica, la società ha preferito sviluppare il proprio modello prevalentemente su API proprietarie, progettate e gestite internamente, al fine di garantire continuità operativa e conformità regolamentare. Emerge così una differente configurazione operativa di N26, la quale, anziché frammentare i servizi tra una molteplicità di partner – come accaduto con Revolut

[318] N26, "*N26 interrompe le operazioni negli Stati Uniti*" https://n26.com/it-it/stampa/comunicato-stampa/n26-interrompe-le-operazioni-negli-stati-uniti, novembre 2021

[319] Ibid.

[320] R. Dillet, "*Number26 is now a true bank as it now has a full banking license*", https://techcrunch.com/2016/07/21/number26-is-now-a-true-bank-as-it-now-has-a-full-banking-license/, TechCrunch, luglio 2016

(cfr. §3.2.2) –, ha preferito centralizzare il *core banking* e affidarsi a collaborazioni verticali con fornitori specializzati in alcune aree marginali. In quest'ottica, l'esternalizzazione non viene interpretata come leva aggressiva di scalabilità, bensì come strumento complementare per ampliare la *value proposition,* senza compromettere la solidità regolatoria né la coerenza operativa del modello. Alla luce delle considerazioni testè richiamate, risulta evidente come la logica di questo approccio emerga chiaramente osservando le principali partnership siglate da N26 nel corso degli anni.

A tal proposito, uno dei casi più significativi di collaborazione riguarda TransferWise (oggi Wise), avviata già nel 2016 e fondata sulla comune visione di offrire ai clienti "*un'esperienza bancaria equa e trasparente, priva di costi inutili e delle complicazioni tipiche delle banche tradizionali*"[321].

Tale partnership si è rivelata fin da subito strategica, poiché ha consentito a N26 di colmare – almeno in parte – un gap strutturale rispetto a Revolut: l'impossibilità per gli utenti di detenere fondi in valuta estera direttamente sul conto. In particolare, grazie all'integrazione con Wise, i clienti hanno potuto effettuare transazioni *cross-border* a costi contenuti e senza markup, restando sempre all'interno della piattaforma N26[322]. Questa impostazione ha rappresentato un progresso rilevante per la società, poiché ha reso possibile la gestione dei trasferimenti globali in un ambiente unico e integrato, rafforzando la semplicità d'uso che ne costituisce il tratto distintivo.

Oltre ai benefici in termini di *user experience*, l'integrazione delle API di Wise ha generato anche vantaggi significativi sotto il profilo operativo, consentendo a N26 di evitare la costruzione di un'infrastruttura proprietaria complessa e costosa per i pagamenti *cross-border*. In questo modo, la banca ha potuto concentrare le proprie risorse sullo sviluppo di funzionalità più distintive – quali MoneyBeam e Spaces – rimanendo coerente con la propria *mission* di "banca mobile del XXI secolo". Questa capacità di integrare servizi a valore aggiunto, senza appesantire l'infrastruttura interna, ha contribuito a rendere l'offerta di N26 particolarmente attrattiva nel panorama delle *challenger banks* europee. Non sorprende, infatti, che nel giro di pochi anni la società sia passata dai 100.000 utenti iniziali a oltre 1 milione[323]. Un risultato che, sebbene non possa essere attribuito unicamente alla collaborazione con Wise, può essere interpretato anche come effetto indiretto della possibilità di offrire trasferimenti internazionali rapidi, trasparenti e perfettamente integrati nell'app.

L'esternalizzazione, in questo caso, non si è limitata a colmare un gap strutturale e tecnico, ma ha inciso direttamente sul posizionamento competitivo della banca. Come sottolineato anche dal *Product Manager* di TransferWise, la partnership ha "rafforzato ulteriormente la posizione di mercato di N26

[321] Wise, "*N26 and TransferWise join forces*", https://wise.com/us/blog/number26-and-transferwise-join-forces, luglio 2016
[322] N26, "*International money transfers with N26*", https://n26.com/en-eu/international-money-transfer
[323] N26, "*2018: un'ottima annata*", https://n26.com/it-it/blog/n26-nel-2018, dicembre 2018

in tutta Europa, trasformandola in una delle banche di riferimento per chi desidera trasferire denaro a livello internazionale"[324].

Su questa stessa linea, anche l'evoluzione del quadro regolatorio europeo ha contribuito a mettere in luce la peculiarità dell'approccio di N26.

Con l'entrata in vigore della PSD2, che ha imposto l'apertura dell'accesso ai dati e conti bancari a TPP autorizzati, la società ha confermato la propria strategia selettiva, scegliendo di affidarsi esclusivamente a Token.io per la gestione dei collegamenti con i conti esterni, così da garantire al contempo piena conformità agli standard europei di Open Banking e senza rinunciare al controllo diretto sulle proprie funzioni *core*[325]. In particolare, la collaborazione con Token.io mostra chiaramente come N26 – a differenza di Revolut, che ha costruito gran parte della propria scalabilità su un'ampia rete di TPP (cfr. §3.2.2) – circoscriva l'esternalizzazione a un ambito strettamente regolato, utilizzandola principalmente come strumento funzionale per soddisfare gli obblighi di legge e arricchire la propria offerta con un accesso semplificato a conti detenuti presso altre banche. Ne deriva così un modello che privilegia la compliance e la coerenza operativa, rafforzando la credibilità della banca agli occhi delle autorità di vigilanza.

Ciononostante, accanto a queste esigenze regolatorie l'esternalizzazione ha svolto un ruolo abilitante anche nel migliorare il *customer journey*. Un esempio emblematico in questo senso è rappresentato dalla partnership con Stripe, avviata per semplificare la ricarica del conto, considerato come uno degli snodi più delicati dell'esperienza bancaria. Se tradizionalmente N26 consentiva l'aggiunta di fondi tramite bonifico SEPA, non sempre tale soluzione si è dimostrata affidabile, flessibile e immediata. Quindi, in un contesto in cui i clienti sono sempre meno propensi a voler affrontare procedure di iscrizione complesse, l'integrazione con Stripe ha permesso alla società di introdurre un'alternativa rapida e intuitiva, che prevedeva nuove modalità di ricarica – tramite carta di credito, carte di debito e wallet digitali – direttamente all'interno della piattaforma N26[326]. In questo modo, secondo quanto dichiarato dal Business Operations Associate di N26 Hellebuyck, "*Stripe [ha consentito] di gestire un passaggio critico della fase di attivazione e di acquisire nuovi clienti in modo semplice e rapido*"[327]. L'impatto di questa integrazione è testimoniato ulteriormente della crescita tangibile della

[324] N26, "*N26 extends its partnership with TransferWise to offer money transfers in over 30 currencies*", https://n26.com/en-eu/press/press-release/n26-extends-its-partnership-with-transferwise-to-offer-money-transfers-in-over-30-currencies, giugno 2020

[325] N26, "*What is PSD2 and what does it mean for me?*", https://n26.com/en-it/blog/what-is-psd2, settembre 2019

[326] Stripe, "*N26 collabora con Stripe per semplificare ulteriormente le procedure di ricarica dei conti bancari per oltre 7 milioni di clienti*", https://stripe.com/it/customers/n26

[327] Stripe, "*Operazioni bancarie in tutta sicurezza con N26*", https://stripe.com/it-ch/newsroom/stories/n26-and-stripe, giugno 2022

base clienti, passata da circa 1 milione nel 2018 a oltre 7 milioni nel 2024, segnale di come abbia contribuito a trasformare molti nuovi iscritti in utenti attivi e fidelizzati[328].

In parallelo a questa espansione, per rispondere alle esigenze di una clientela sempre più *tech-savy* – principale segmento a cui si rivolge N26 – la banca ha progressivamente ampliato la propria suite di prodotti finanziari, pur mantenendo sempre l'obiettivo di garantire una crescita sostenibile e profittevole tramite la centralità d'uso del conto corrente e la sua integrazione nella vita quotidiana dei clienti.

In questa prospettiva, N26 ha scelto di estendere l'offerta anche al mondo degli investimenti, in particolare alle criptovalute e alle azioni ed ETF. Dopo aver introdotto nel 2022 N26 Crypto, una funzionalità che consente di acquistare e vendere valute digitali direttamente dall'app, la società ha scelto di affidarsi alla piattaforma Bitpanda per la gestione ed esecuzione delle negoziazioni e la custodia degli asset[329]. In tal modo, la scelta di non sviluppare un motore di trading proprietario le ha consentito di ridurre i rischi operativi legati a un settore altamente volatile, offrendo altresì ai propri clienti l'accesso a questi strumenti in modalità *white-label* senza compromettere il proprio profilo di banca regolata[330].

Coerentemente con questa logica, la banca ha introdotto successivamente un servizio di trading di azioni e ETF, sviluppato in collaborazione con Upvest, consentendo agli utenti di negoziare frazioni di titoli direttamente dall'app, accedendo così a strumenti di investimento tradizionali in maniera semplice e immediata. Anche in questo caso, l'esternalizzazione è stata utilizzata in modo mirato, comportando non solo il rafforzamento della *value proposition* della banca, ma decretando riflessi tangibili sui comportamenti di utilizzo dei clienti. Secondo i dati societari, infatti, ciò avrebbe comportato un aumento del volume annuo delle transazioni del 23% nel 2024, per un totale di 140 miliardi di euro, con una crescita del 16% rispetto a quanto registrato l'anno precedente[331].

In definitiva, tali dinamiche evidenziano come un uso selettivo e specifico dei TPP possa rafforzare l'offerta senza snaturare il modello di una banca centrato sul *core banking*.

L'esternalizzazione, limitata a servizi accessori e innovativi, ha consentito alla società di arricchire la *customer experience* e di aumentare i volumi transazionali, preservando al contempo solidità regolatoria e coerenza operativa. Tuttavia, a differenza di Revolut, la crescita della base clienti è risultata molto più contenuta. Lo stesso CFO di N26 ha sottolineato come, negli ultimi anni, la banca

---

[328] Ibid.
[329] Contrary Research, "*N26*", cit.
[330] Bitpanda, "*Bitpanda e N26 insieme per gli investimenti in cripto*", https://blog.bitpanda.com/it/bitpanda-e-n26-insieme-gli-investimenti-cripto
[331] N26, "*Il Gruppo N26 registra il primo utile trimestrale con una crescita del numero clienti in forte accelerazione*", https://n26.com/it-it/stampa/comunicato-stampa/il-gruppo-n26-registra-il-primo-utile-trimestrale-con-una-crescita-del-numero-clienti-in-forte-accelerazione, novembre 2024

si sia concentrata sulla costruzione di relazioni proficue, stabili e durature con i clienti, che li garantiscano al contempo una gestione operativa dei costi solida e sostenibile nel tempo[332].

Eppure, questa strategia più prudente di esternalizzazione ai TPP, non implica un modello privo di vulnerabilità. Nonostante il ricorso selettivo ai TPP sia coerente con l'idea di modello ideato dai fondatori, espone comunque la banca a criticità operative, strategiche e regolatorie che non possono essere ignorate. In altre parole, muoversi in una "zona di comfort" rispetto a Revolut non significa essere al riparo dai rischi: al contrario, questi assumono forme diverse e meritano di essere analizzati in profondità, come si vedrà nel paragrafo successivo.

3.3.3 – Criticità di un modello centrato sul *core banking*: tra rischio di concentrazione e perdita di autonomia competitiva

In un panorama bancario sempre più orientato al digitale, in cui i volumi delle transazioni via smartphone hanno ormai più che raddoppiato quelli dell'*internet banking* tradizionale, N26 si è affermata come una delle realtà pioniere del *mobile banking* europeo[333].

La scelta di esternalizzare ai TPP funzioni *non-core* ha certamente contribuito a sostenere tale percorso, consentendole di ampliare l'offerta con prodotti innovativi in ambito di risparmio e investimento, ma ha anche amplificato i rischi connessi alla sua architettura tecnologica.

Se, da un lato, l'affidamento di N26 a un numero ristretto di partner per funzioni specifiche ha ridotto l'esposizione al rischio di *lock-in* tecnologico tipico dei modelli come Revolut, che hanno costruito gran parte della propria scalabilità su una rete estesa e frammentata di TPP (cfr.§3.2.3). Dall'altro lato, però, ha concentrato la continuità operativa su un numero limitato di nodi esterni, generando un significativo rischio di concentrazione tecnologica, in cui ogni partner diventa un potenziale "*single point of failure*" per l'intero servizio[334]. In questo scenario, eventuali problemi tecnici o regolatori di uno dei fornitori rischiano di tradursi immediatamente in un disservizio percepito dal cliente finale, con effetti diretti tanto sulla *user experience* quanto sulla reputazione della banca.

Un caso emblematico è rappresentato dal malfunzionamento tecnico di Wise del febbraio 2022, che ha provocato ritardi diffusi nei trasferimenti *cross-border* e l'impossibilità, per una specifica categoria

[332] Ibid.

[333] G. Murri, F. Fintschj, "*KEY RESULTS - OSSERVATORIO DIGITAL BANKING L'ossimoro del Digital Banking: più vicino al cliente da lontano!"*, ABI Lab, luglio 2024

[334] Mentre con il termine di "*single point of failure*" (SPOF) intendiamo quel caso in cui il malfunzionamento di un singolo componente può causare il "guasto" dell'intero sistema, con quello di *lock-in* facciamo riferimento a quel caso in cui è difficile o costoso abbandonare una tecnologia o un fornitore. Pertanto, un sistema può essere affetto da un SPOF e non essere in lock-in, e viceversa. Per ulteriori approfondimenti in merito al tema del single point of failure si veda: IONOS, "*Single point of failure*", https://www.ionos.it/digitalguide/server/sicurezza/single-point-of-failure/, dicembre 2022

di utenti *mobile*, di avviarne di nuovi dal proprio dispositivo[335]. Pur non trattandosi di un disservizio esclusivo di N26, l'impatto si è comunque riflesso direttamente sulla sua clientela, che ha percepito il problema come responsabilità della banca. L'episodio dimostra dunque come il rischio di *single point of failure* non sia una nozione astratta, ma una vulnerabilità concreta, capace di erodere la fiducia dei clienti e di imporre a N26 nuovi investimenti in sistemi di monitoraggio dei partner, clausole contrattuali più stringenti e misure di *fallback* interne.

Alla luce di queste considerazioni, appare chiaro che l'approccio selettivo di N26, sebbene riduca la dipendenza strutturale da una molteplicità di TPP – e con essa le complessità e i costi di *switching* connessi a un eventuale sostituzione –, non elimina i rischi bensì li riconfigura. In assenza di alternative interne o di infrastrutture ridondanti, la gestione di eventuali shock esterni si traduce inevitabilmente in oneri aggiuntivi, che non si limitano al piano operativo ma si riflettono anche su quello regolatorio e di compliance. Infatti, ogni disservizio od inefficienza non intacca esclusivamente l'esperienza dell'utente, ma genera vulnerabilità anche sul fronte normativo, poiché la responsabilità ultima resta sempre in capo alla banca, indipendentemente dal ruolo dei TPP.

Proprio in quest'ottica, come già osservato per Revolut (§3.2.3), la disciplina europea in materia di Open Banking ha introdotto regole stringenti per l'accesso dei TPP ai conti dei clienti. In particolare, gli RTS emanati dall'EBA – in attuazione della PSD2 – stabiliscono esplicitamente che le banche, in qualità di *Account Servicing Payment Service Providers* (ASPSP), debbano verificare l'identità e l'autorizzazione dei *Third Party Providers,* la cui operatività è subordinata al possesso di certificati qualificati (*QWACs* e *QSealCs*) rilasciati da autorità fiduciarie accreditate ai sensi del Regolamento eIDAS[336]. In questo senso, N26 – pur esternalizzando in modo mirato servizi come i trasferimenti *cross-border*, il *top-up* dei conti o i servizi di investimento – non può mai trasferire sui TPP la piena responsabilità del presidio regolatorio. Al contrario, l'esternalizzazione amplifica gli obblighi in capo alla banca, la quale deve assicurarsi che ogni accesso sia conforme agli standard di sicurezza, che i fornitori siano effettivamente legittimanti ad operare e che i flussi di dati rispettino i requisiti di integrità e riservatezza previsti dalla normativa europea (cfr. §1.1.4)[337]. Ciò si traduce in un onere regolatorio significativo per N26, che – pur mantenendo *in house* le funzioni di *core banking* ed esternalizzando solo attività marginali – deve comunque farsi garante della piena conformità ai requisiti europei di sicurezza e trasparenza. Ne deriva una dinamica che, oltre a ridurre i benefici

[335] Wise, "*All transfers are currently delayed and Android customer cannot create transfers. Incident Report for Wise*", https://status.wise.com/incidents/5hm10021cgyn, febbraio 2022

[336] N26, "*PSD2 - Open Banking for Third Party Providers*", https://support.n26.com/en-es/security/open-banking-psd2/psd2-open-banking-for-third-party-providers

[337] N26, "*PSD2 - Secure Open Banking*", https://support.n26.com/en-eu/security/open-banking-psd2/psd2-and-secure-open-banking

immediati dell'esternalizzazione, finisce anche per comprimere sensibilmente i margini di autonomia della banca.

Accanto a questi vincoli regolatori emerge un'ulteriore criticità: la difficoltà per N26 di governare appieno i processi di innovazione. Se, da un lato, l'affidamento a un numero ristretto di TPP le ha permesso di consolidare il modello di banca digitale sotto la vigilanza della BaFin, dall'altro ha inevitabilmente limitato la capacità di crescita e di differenziazione rispetto a competitor più aggressivi. In particolare, l'integrazione diretta delle API di TPP specializzati ha permesso a N26 di contenere i costi e ampliare l'offerta, ma al contempo ha subordinato il ritmo di crescita e la capacità di differenziazione alle tempistiche e alle scelte dei partner. Se, ad esempio, Bitpanda rallentasse il rilascio di nuove funzionalità crypto o Upvest incontrasse difficoltà nello sviluppo di strumenti legati agli ETF, la *value proposition* di N26 ne risulterebbe inevitabilmente limitata, con il rischio di perdere competitività rispetto ad operatori più autonomi o dotati di soluzioni proprietarie.

Pertanto, il rischio strategico connesso all' approccio selettivo di esternalizzazione adottato da N26 non riguarda soltanto la continuità operativa o la dipendenza tecnologica, ma si estende anche alla capacità stessa di innovare e di mantenere un vantaggio competitivo nel lungo periodo[338].

Ne deriva che, in un contesto in rapida evoluzione – nel quale player come Revolut o le Big Tech puntano ad integrare servizi sempre più diversificati – la dipendenza da un numero ristretto di TPP può tradursi in un vincolo strutturale, riducendo l'agilità di N26 e la sua possibilità di anticipare le esigenze della clientela[339]. A ciò si aggiunge che la natura *white-label* di alcune integrazioni con i TPP rende ancora più difficile costruire un posizionamento distintivo. In questi casi, infatti, la stessa soluzione può essere resa disponibile anche ad altri operatori fintech, a banche tradizionali o a piattaforme digitali, con il risultato che la *customer experience* non risulta più sufficiente a generare un reale vantaggio competitivo. A confermarlo è la collaborazione con Bitpanda, la quale, sebbene abbia permesso a N26 di introdurre rapidamente il trading di criptovalute senza dover sostenere i costi e i rischi legati allo sviluppo di un motore proprietario, ha reso l'offerta meno esclusiva garantendo l'integrazione della propria infrastruttura anche ad altri player del settore[340]. In tal modo, il valore aggiunto percepito dal cliente tende a diluirsi, poiché l'attenzione non si concentra più sulla piattaforma di N26 ma sul servizio specifico offerto dal TPP. Questo fenomeno non implica soltanto un rischio reputazionale in caso di disservizi, ma comporta anche una progressiva erosione della *brand identity* della banca: il cliente finisce per attribuire il valore dell'esperienza al partner tecnologico piuttosto che a N26 stessa. Ne deriva il pericolo che la banca venga percepita come un

[338] L. Sbriz, "*Considerazioni sui rischi strategici e sui rischi operativi",* https://www.esg360.it/risk-management/considerazioni-sui-rischi-strategici-e-sui-rischi-operativi/, ESG360 maggio 2022

[339] Contrary Research, "*N26*", cit.

[340] Bitpanda, "*Bitpanda si allea con HYPE grazie alla sua soluzione White Label*", https://blog.bitpanda.com/it/bitpanda-si-allea-con-hype-grazie-alla-sua-soluzione-white-label, novembre 2022

mero contenitore tecnologico, privo di una proposta distintiva autonoma. In questo senso, l'esternalizzazione, pur garantendo rapidità e contenimento dei costi, espone N26 non solo a vulnerabilità operative e regolatorie, ma anche al rischio strategico di indebolire la propria autonomia competitiva e la capacità di costruire un posizionamento riconoscibile sul mercato.

In definitiva, l'esperienza di N26 evidenzia come l'esternalizzazione ai TPP, se adottata in modo selettivo e prudente, possa rappresentare un valido strumento di supporto ma non una vera leva di scalabilità. Delegare a partner verticali funzioni accessorie – dai trasferimenti internazionali al trading di azioni ed ETF – si è presto rivelata un'arma a doppio taglio. Se inizialmente questa decisione ha garantito a N26 maggiore stabilità e coerenza regolatoria, permettendole di arricchire la propria offerta senza appesantire l'infrastruttura interna, successivamente essa ha comportato una crescita più lenta e una minore autonomia decisionale, con effetti diretti sul posizionamento strategico della società nel mercato. Dunque, il vero punto critico per N26 non risiede tanto nell'aver limitato l'esternalizzazione, quanto nella sfida di bilanciare stabilità e innovazione per rimanere la "*banca che il mondo ama usare*".

3.4 – Sintesi critica del confronto tra i due modelli di esternalizzazione

L'analisi dei casi Revolut e N26 offre una prospettiva privilegiata per riflettere sul ruolo dei TPP come fattore abilitante o, al contrario, come vincolo per le banche. Le traiettorie opposte seguite dalle due *challenger banks* – l'una orientata alla crescita rapida e alla diversificazione tramite un'estesa rete di partnership, l'altra focalizzata sul consolidamento regolatorio e su un'esternalizzazione mirata – dimostrano che non esiste un modello ideale di esternalizzazione ai TPP, ma piuttosto un equilibrio instabile tra efficienza, innovazione e controllo. In altri termini, l'esternalizzazione si rivela un potente acceleratore di innovazione – capace di ridurre significativamente costi operativi e *time-to-market* – e al tempo stesso una fonte di inefficienza operativa che, se non correttamente gestita, rischia di tradursi in vulnerabilità tecnologiche, maggiori oneri di compliance e perdita di autonomia strategica.

In questa prospettiva, il caso Revolut evidenzia con chiarezza che se, da un lato, l'ampio ricorso all'esternalizzazione ha costituito una leva decisiva per sostenere la propria espansione e per posizionarsi come piattaforma finanziaria integrata – consentendole di ridurre i tempi di *rollout*, entrare in nuovi mercati e sperimentare servizi sempre più complessi –, dall'altro si è progressivamente tradotta in una dipendenza strutturale da terze parti. Tale dipendenza l'ha esposta a vulnerabilità operative e reputazionali difficilmente controllabili, costringendola in seguito a una parziale internalizzazione delle funzioni core (ad. AMAL/KYC) per bilanciare innovazione e

resilienza. Ne deriva che la rapidità e la scalabilità conquistate da Revolut, pur evidenziando il lato "abilitante" dell'esternalizzazione, finiscono per evidenziarne la fragilità intrinseca.

All'estremo opposto, N26 ha scelto di limitare l'esternalizzazione alle sole funzioni ancillari, costruendo sulle API proprietarie il cuore del proprio modello operativo. Una strategia che le ha permesso, in parte, di preservare resilienza operativa e credibilità regolatoria, ma che ha imposto un ritmo di innovazione più lento e condizionato dalle *roadmap* dei partner, oltre che un forte limite alla velocità di espansione internazionale. A dimostrarlo sono i dati: mentre Revolut ha superato i 52 milioni di utenti nel 2024, registrando una crescita del 38%[341] rispetto all'anno precedente, N26 si è fermata a circa 8 milioni. Inoltre, anche il ritiro dai mercati del Regno Unito e degli Stati Uniti rappresenta un chiaro segnale dei limiti di questa strategia prudenti, che ha privilegiato il consolidamento interno rispetto a una rapida espansione internazionale.

A rafforzare ulteriormente queste differenze si inserisce il contesto regolatorio, che ha giocato un ruolo decisivo nel plasmare le strategie di entrambe le *challenger banks*. Se, infatti, le scelte di crescita e di esternalizzazione riflettono precise filosofie aziendali, esse non possono essere comprese appieno senza considerare l'ambiente normativo in cui i due modelli si sono sviluppati.

Mentre Revolut, operando inizialmente sotto la vigilanza più flessibile della FCA, ha potuto beneficiare di un ambiente favorevole all'innovazione fintech, oltre che di sandbox regolatorie, N26, è stata sottoposta fin dall'inizio alla severa vigilanza della BaFin e, successivamente, anche della Banca d'Italia. In particolare, i provvedimenti sanzionatori per carenze AML/KYC hanno dimostrato come il modello centrato sul *core banking*, benché ideato per rafforzare la *compliance* interna rispetto ad approcci maggiormente TPP-centrici, si sia tradotto in un freno alla crescita e in un danno reputazionale potenzialmente più incisivo di quanto sarebbe potuto derivare da una parziale esternalizzazione di tali presidi[342]. Ne deriva uno dei principali paradossi del modello di business di N26, che espone la banca all'incapacità di governare appieno i processi di innovazione.

In definitiva, da queste divergenze emerge con chiarezza che l'esternalizzazione non rappresenta né un'opportunità da cogliere incondizionatamente né un rischio da evitare a priori, ma piuttosto un processo che funziona solo se accompagnato da una governance solida e da meccanismi di controllo proporzionati. Non esiste un modello "universale", bensì il successo dipende dal contesto regolatorio e dagli obiettivi strategici. In un ambiente più predisposto all'Open Banking come quello britannico,

---

[341] La Repubblica, "Revolut utile netto più che raddoppiato a 1 miliardo di euro", https://finanza.repubblica.it/News/2025/04/24/revolut_utile_netto_piu_che_raddoppiato_a_1_miliardo_euro-33/, aprile 2025

[342] R. Dillet, "*Germany's financial regulator ends anti-money laundering cap on N26 signups after $10M fine*", https://techcrunch.com/2024/05/29/german-financial-regulator-lifts-restrictions-on-n26-signups/, TechCrunch, maggio 2024

l’approccio aggressivo di Revolut ha trovato terreno fertile; invece, in un contesto severo come quello tedesco il modello prudente di N26 ha rappresentato la scelta più sostenibile.

Alla luce di tali considerazioni è possibile affermare che il *trade-off* tra rapidità e stabilità non può essere eliminato, ma solo gestito. Invero, le esperienze di Revolut N26 dimostrano che il punto non è scegliere *se* esternalizzare, quanto piuttosto definire in maniera chiara *cosa* affidare all’esterno, *quando* internalizzare e *come* garantire che i benefici non si trasformino in rischi sistemici.

CONCLUSIONI

Il percorso sin qui delineato ha messo in luce come l'Open Banking non possa essere ridotto a una semplice innovazione tecnologica, bensì rappresenti una trasformazione sistemica al centro della quale si colloca l'esternalizzazione ai TPP, una variabile capace di ridefinire ruoli, responsabilità e modelli di business nel settore finanziario. per poter comprendere appieno la portata di questo fenomeno è stato necessario partire dal profilo giuridico, poiché la disciplina introdotta con la PSD2 ha segnato un vero e proprio punto di svolta, imponendo alle banche l'obbligo di consentire ai TPP l'accesso ai conti e ai dati dei clienti. Un'apertura che, nonostante sia stata presentata dal legislatore europeo come strumento per promuovere la concorrenza e stimolare l'innovazione, ha avuto conseguenze profonde sul piano della *governance*. Nel corso della trattazione è emerso, infatti, che l'esternalizzazione obbligata di funzioni centrali ha determinato una ridistribuzione delle responsabilità e un indebolimento generale della posizione delle banche come custodi privilegiati delle informazioni finanziarie. Ne consegue che, almeno per quanto attiene il piano giuridico, l'esternalizzazione non può essere intesa solo come "*outsourcing*" tradizionale, poiché non si tratta di delegare attività accessorie, bensì di aprire il "*cuore*" dell'attività bancaria – l'accesso ai dati e ai conti – a soggetti terzi, spesso privi degli stessi vincoli prudenziali cui sono soggette le banche. Da qui deriva non solo l'evidente necessita di chiarire le responsabilità in caso di violazioni o malfunzionamento nei servizi offerti dai TPP, ma anche la crescente rilevanza della *compliance* come strumento di presidio dei rischi, soprattutto in un contesto in cui i dati vengono condivisi con soggetti eterogenei e non sempre sottoposti agli stessi requisiti prudenziali delle banche.

È proprio nel tentativo di porre rimedio a queste incertezze interpretative, che la PSD2 ha lasciato irrisolte, che la Commissione europea ha proposto recentemente una revisione della normativa, confluita nel *Payment Services Package* (PSP) e nell'iniziativa sul regolamento FIDA.

Tuttavia, se da un lato il PSP mira a chiarire i profili di responsabilità tra banche e TPP e a rafforzare la tutela dei clienti – confermando così la centralità dell'accesso ai dati come leva competitiva –, dall'altro il FIDA estende la logica di apertura a dati finanziari ancora più ampi, avvicinando l'Europa all'Open Finance e ampliando ulteriormente i nodi giuridici legati alla *governance* dell'esternalizzazione. Ciò significa che la questione dell'esternalizzazione non solo non si attenua, ma si estende a nuovi ambiti, ampliando tanto le opportunità quanto le fragilità del sistema.

Come sottolineato nel corso dell'analisi, le incertezze normative non rimangono sul piano teorico, ma incidono direttamente sui costi, sui modelli di business dei TPP e sulla capacità delle banche di mantenere un controllo strategico. In particolare, la disciplina dell'accesso ai dati non si limita a definire i confini giuridici della responsabilità, ma plasma anche gli equilibri competitivi e le prospettive di sostenibilità economica dell'intero sistema. Talvolta, l'esternalizzazione si trasforma

in un pericolo per le banche di perdere il controllo operativo sul rapporto con il cliente e una rilevante difficoltà di monetizzare i servizi per i TPP – data la dipendenza dai volumi e la pressione regolatoria –, rivelandosi una fonte di fragilità strutturale se non accompagnata da strategie di lungo periodo e da un quadro regolatorio adeguato.

L'analisi empirica, condotta attraverso i casi di Revolut e N26, ha permesso di mettere alla prova tali riflessioni. I due modelli, pur differenti, confermano l'ambivalenza dell'esternalizzazione. Revolut ha fatto leva su un'esternalizzazione estesa per accelerare la crescita e ampliare i servizi offerti, con un'espansione geografica che abbraccia oltre 35 paesi e un'offerta che spazia dai pagamenti alle criptovalute, dal trading azionario alle assicurazioni. Tuttavia, ciò ha comportato una maggiore dipendenza da partner esterni e una complessità gestionale crescente. Al contrario, N26 ha scelto una strategia più selettiva, riducendo il ricorso a partner esterni per mantenere un maggiore controllo interno, ma incontrando limiti di scalabilità e difficoltà di espansione internazionale. Entrambi i casi, quindi, dimostrano che l'esternalizzazione può essere al tempo stesso un vantaggio competitivo e un fattore di fragilità strutturale, se non viene gestita con equilibrio.

In questo senso, la risposta alla domanda di ricerca non è dicotomica. L'esternalizzazione rappresenta un vantaggio quando viene inserita in una strategia consapevole di governance e di gestione del rischio, ma diventa un ostacolo se utilizzata come scorciatoia per crescere rapidamente senza considerare le vulnerabilità di lungo periodo.

Queste dinamiche son rese ancora più evidenti dall'evoluzione verso l'Open Finance, con l'estensione della condivisione dei dati oltre i pagamenti – verso investimenti, assicurazioni, credito. Tale espansione renderà ancora più rilevante il ruolo dei TPP e moltiplicherà i nodi giuridici legati a responsabilità e protezione dei dati. Solo affrontando insieme le dimensioni giuridiche ed economiche sarà possibile costruire un ecosistema di Open Banking e di Open Finance che sia al tempo stesso competitivo, resiliente e orientato al cliente.

BIBLIOGRAFIA

A. G. (2017, settembre). *Un bundle anche per l'offerta digitale*. *Aziendabanca*. https://www.aziendabanca.it/notizie/bundle-open-banking-fintech-digitale

Accenture. (2025). *Reinvent banking operations with data and AI*. https://www.accenture.com/us-en/industries/banking/banking-operations

American Fintech Council (AFC). (2024, ottobre). *Statement on the Consumer Financial Protection Bureau's personal financial data rights final rule*. https://www.fintechcouncil.org/press-releases/statement-from-american-fintech-council-afc-senior-vice-president-head-of-policy-and-regulatory-affairs-ian-p-moloney-on-the-consumer-financial-protection-bureaus-personal-financial-data-rights-final-rule

Andreasyan, T. (2018, novembre). *Revolut to bring processing in-house*. *FinTech Futures*. https://www.fintechfutures.com/digital-banking/revolut-to-bring-processing-in-house

Asif, C., Olanrewaju, T., Sayama, H., & Vijayasrinivasan, A. (2021, luglio). *Financial services unchained: The ongoing rise of open financial data* (p. 12). McKinsey & Company.

Azzelini, G. (2024, maggio). *Parere dell'EBA sulle nuove tipologie di frode*. AntiriciclaggioeCompliance. https://www.antiriciclaggiocompliance.it/parere-delleba-sulle-nuove-tipologie-di-frode/

Baily, M. N., & Klein, A. D. (2014, ottobre). *The impact of the Dodd-Frank Act on financial stability and economic growth*. Bipartisan Policy Center & Brookings.

Banca centrale europea (BCE). (2021, 29 aprile). *Il rapporto della BCE mostra che le frodi sulle carte sono diminuite nel 2019*.

Banca centrale europea (BCE). (2024). *2024 outsourcing register – Horizontal analysis* (pp. 4–5). Directorate General Horizontal Line Supervision. https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.outsourcing_horizontal_analysis_202402~2b85022be5.en.pdf

Banca d'Italia. (2021, novembre). *PSD2 e open banking: Nuovi modelli di business e rischi emergenti*.

Banca d'Italia. (2021). *Che cosa è l'autenticazione forte del cliente (SCA)*. https://www.bancaditalia.it/focus/sca/sca-funzione/index.html

Bank Policy Institute (BPI). (2024, ottobre). *Banks Challenge CFPB Rule Jeopardizing Security and Privacy of Consumer Financial Data* https://bpi.com/banks-challenge-cfpb-rule-jeopardizing-security-and-privacy-of-consumer-financial-data/

Bank Policy Institute. (2024, novembre). *Screen scraping: What is it and how does it work?* https://bpi.com/screen-scraping-what-is-it-and-how-does-it-work/

Basel Committee on Banking Supervision. (2019, November). *Report on open banking and application programming interfaces* (p. 8). Bank for International Settlements.

BBVA. (2016, aprile). *The open banking standard*. *Digital Economy Outlook*.

Bellens, J. (2021, marzo). *Five questions about banking in today's digital age, answered*. EY Global. https://www.ey.com/en_pt/insights/banking-capital-markets/five-questions-about-banking-in-todays-digital-age-answered

Bianco, M., & Vangelisti, M. (2024). Open banking e inclusione finanziaria. In V. Falce & U. Morera (a cura di), *Dall'open banking all'open finance: Profili di diritto dell'economia* (pp. 33–34). Torino: G. Giappichelli.

Booth, H. (2010, marzo). *AFR on the passage of historic financial reform legislation*. Americans for Financial Reform. https://web.archive.org/web/20100523065059/http://ourfinancialsecurity.org/2010/05/afr-on-the-passage-of-historic-financial-reform-legislation/#

Borgogno, O., & Colangelo, G. (2020). Data, innovation and competition in finance: The case of access to account rule. *European Business Law Review, 31*(4), 585–586.

Brackert, T., et al. (2021, gennaio). *Global retail banking 2021: The front-to-back digital retail bank*. Boston Consulting Group. https://www.bcg.com/publications/2021/global-retail-banking-report

Camporeale, R. (2024). Le asimmetrie della PSD2 e il nuovo payments package. In V. Falce & U. Morera (a cura di), *Dall'open banking all'open finance: Profili di diritto dell'economia* (p. 71). Torino: G. Giappichelli.

Centre for European Policy Studies (CEPS), & Directorate-General for Financial Stability, Financial Services and Capital Markets Union. (2023). *A study on the application and impact of Directive (UE) 2015/2366 on payment services (PSD2)* (p. 11). Luxembourg: Publications Office of the European Union.

Cerrato, E., Detto, E., Natalizi, D., Semorile, F., & Zuffranieri, F. (2024, marzo). *Mercati, infrastrutture e sistemi di pagamento. I fornitori di tecnologia nel sistema dei pagamenti: Evoluzione di mercato e quadro normativo* (Quaderni Banca d'Italia, No. 47, p. 9). Banca d'Italia.

Coeurderoy, R., & Guilhon, M. (2022). "Dancing in the dark": Regulatory reforms and incumbent banks' evolution towards new value creation models in the process of open banking (*ESCP Impact Paper No. 2022-24-EN*).

Coeurderoy, R., & Guilhon, M. (2023, aprile). *Why banks are moving towards the banking-as-a-platform model*. LSE Business Review. https://blogs.lse.ac.uk/businessreview/2023/04/28/why-banks-are-moving-towards-the-banking-as-a-platform-model/

Colangelo, G. (2024). Open banking goes to Washington: Lessons from the EU on regulatory-driven data sharing regimes. *Computer Law & Security Review, 56*, 106018. https://doi.org/10.1016/j.clsr.2024.106018

Commissione europea. (2023, 28 giugno). *Commission staff working document: Impact assessment report accompanying the proposal for a regulation on a framework of financial data access…* (SWD(2023) 224 final, pp. 12–14). Brussels.

Competition and Markets Authority (CMA). (2016, agosto). *Making banks work harder for you*.https://assets.publishing.service.gov.uk/media/5a800298ed915d74e33f7ea3/overview-of-the-banking-retail-market.pdf

Competition and Markets Authority (CMA). (2017). *The Retail Banking Market Investigation Order 2017* (Part 2, Art. 10.1).

Consumer Financial Protection Bureau (CFPB). (2011, luglio). *Building the CFPB* (pp. 5–6).

Consumer Financial Protection Bureau (CFPB). (2023, ottobre). *CFPB proposes rule to Jumpstart Competition and Accelerate Shift to Open Banking.* https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-jumpstart-competition-and-accelerate-shift-to-open-banking/

Consumer Financial Protection Bureau (CFPB). (2023). *Notice of final rulemaking: Required rulemaking on personal financial data rights* (CFPB-2023-0052, p. 13).

Contrary Research. (2023, febbraio). *N26*. https://research.contrary.com/company/n26

Crif. (2024). *La nuova frontiera dell'open finance: AI ed evoluzione normativa* (p. 4).

D'Orsi, R. (2023, maggio). *La BCE aumenta i tassi.* Chi ne paga le conseguenze? Fondazione Feltrinelli. https://fondazionefeltrinelli.it/scopri/la-bce-aumenta-i-tassi-chi-ne-paga-le-conseguenze/

Dahiwelkar, S. (2023, ottobre). *PSD3: An evolution of the EU payments framework and enabling Open Finance.* Delta Capita. https://www.deltacapita.com/insights/psd3-an-evolution-of-the-eu-payments-framework-and-enabling-open-finance

Desando, C. (2020, settembre). *Challenger banks: che cosa sono, come funzionano, le europee e le italiane.* EconomyUp. https://www.economyup.it/fintech/challenger-banks-che-cosa-sono-come-funzionano-le-europee-e-le-italiane/

Desario, M. S., & Croce, R. (2024, settembre). *La nozione di banca nell'evoluzione storica dell'ordinamento del credito*. DB – Non solo Diritto Bancario.

Di Giorgio, A., & Mascagni, B. (2020, luglio). *PSD2: Gli ostacoli all'operatività dei TPP alla luce dei chiarimenti dell'EBA.* Annunziata & Conso. https://annunziataconso.eu/articolo/psd2-gli-ostacoli-alloperativita-dei-tpp-alla-luce-dei-chiarimenti-delleba/

Donadio, G. (2019, settembre). *Open banking facile con True Layer, la fintech di italiani che piace all'Europa.* StartupItalia. https://startupitalia.eu/economy/economia-digitale/open-banking-facile-con-true-layer-la-fintech-di-italiani-che-piace-alleuropa/

ECB Banking Supervision. (2015, settembre). *Reintegrating the banking sector into society: earning and re-establishing trust.* https://www.bankingsupervision.europa.eu/press/speeches/date/2015/html/se150928.it.html

Economy Magazine. (2024, settembre). *Aziende e fondi d'investimento accelerano verso il modello "asset light" per una crescita agile.* https://www.economymagazine.it/aziende-modello-asset-light-crescita-agile/

Enfuce. (2020, settembre). *How banks can overcome PSD2 compliance challenges*. https://enfuce.com/blog/how-banks-can-overcome-psd2-compliance-challenges/

European Banking Authority (EBA). (2018, giugno). *Opinion on preparations for the withdrawal of the United Kingdom from the European Union* (EBA/Op/2018/05, p. 2).

European Central Bank (ECB). (2023, gennaio). *Brexit and the EU banking sector: from the fundamental freedoms of the Internal Market to third country status.* https://www.bankingsupervision.europa.eu/press/interviews/date/2023/html/ssm.in230130~cd7de9ce0c.en.html

European Commission. (2018, January 12). *Payment Services Directive: Frequently asked questions (Fact Sheet)*. Brussels.

European Data Protection Board (EDPB). (2020, dicembre). *Linee guida 06/2020 sull'interazione tra la seconda direttiva sui servizi di pagamento e il GDPR* (p. 8).

EY Global. (2021, marzo). *How both banks and customers can seize the upside of disruption*. https://www.ey.com/en_nl/insights/banking-capital-markets/how-both-banks-and-customers-can-seize-the-upside-of-disruption

EY. (2022, marzo). *Banking & capital markets*. https://www.ey.com/en_lt/industries/banking-capital-markets

Fathi, A. (2023, ottobre). *FCA indaga su Revolut per aver facilitato transazioni in violazione delle sanzioni.* FinanceFeeds. https://financefeeds.com/it/FCA-indaga-su-Revolut-per-aver-facilitato-le-sanzioni-in-caso-di-violazione-delle-transazioni/

Financial Conduct Authority (FCA). (2024, dicembre). *Approach to final Regulatory Technical Standards and EBA guidelines under the revised Payment Services Directive (PSD2)* (PS18/24, pp. 10–11).

Financial Data and Technology Association (FDATA). (2020, giugno). *Competition issues in data-driven consumer and small business financial services* (pp. 3–5).

Financial Data and Technology Association (FDATA). *Opportunities in open banking* (p. 9). FDATA North America.

Financial Data Exchange (FDX). (2022, dicembre). *Financial Data Exchange response to Small Business Advisory Review Panel for required rulemaking on personal financial data rights* (CFPB).

Financial IT. (2016, ottobre). *Onfido boosts Identity Verification Solution to Make KYC for Financial Services Even Easier.* https://financialit.net/news/security/onfido-boosts-identity-verification-solution-make-kyc-financial-services-even-easier

Frattini Passi, L., & Raganelli, B. (2024). Open finance e innovazione finanziaria: Opportunità, questioni e sfide. In V. Falce & U. Morera (a cura di), *Dall'open banking all'open finance: Profili di diritto dell'economia* (p. 140). Torino: G. Giappichelli.

Genovese, A., & Falce, V. (2021, aprile). *La portabilità dei dati in ambito finanziario* (*Quaderni FinTech*, No. 8, p. 189). Consob.

Gozman, D., Liebenau, J., & Mangan, D. (2021). The innovation mechanisms of fintech start-ups: Insights from open banking. *Journal of Management Information Systems*.

Grassi, L. (2025, 9 giugno). *Challenger Bank, cosa sono e diffusione in Italia e UE.* Osservatorio Fintech & Insurtech. https://www.osservatori.net/blog/fintech-insurtech/challenger-bank-cosa-sono-diffusione-in-italia-ue/

Grassi, L., & Garitta, C. (n.d.). *Embedded Finance, Insurance ed erogazione dei servizi in modalità as-a-Service.* Osservatorio Fintech & Insurtech. https://www.osservatori.net/insight/fintech-insurtech/embedded-finance-insurance-erogazione-servizi-modalita-as-a-service-insight/

Guardati, E. (2022, marzo). *PAYTECH e ML Risk: third party providers obbligati ai sensi del d.lgs. 231/2007*. (p. 15). Osservatorio Normativo.

Hamilton, S. (2024, dicembre). *CFPB's Section 1033: Will US open banking reach its potential*?. Finextra. https://www.finextra.com/the-long-read/1198/cfpbs-section-1033-will-us-open-banking-reach-its-potential

HM Treasury. (2017, luglio). *Implementation of the revised EU Payment Services Directive II: Response to the consultation* (p. 5).

House of Lords. (2022, giugno). *The UK-EU relationship in financial services* (pp. 47–49). Authority of the House of Lords.

Joint statement – *Financial data sharing: Finding a sound approach for an effective Open Finance Framework.* (2024, December 9). WSBI & ESBG. https://www.wsbi-esbg.org/wp-content/uploads/2024/12/Final_Joint-Statement-FiDA_03.12.24_v3_clean.pdf

Junghanns, H., & Niebudek, M. (2019, marzo). *Platform banking & digital ecosystems* (p. 22). PwC's Study.

KPMG. (2021). *Evoluzione dei modelli distributivi bancari: L'impatto del COVID-19 sui modelli di servizio delle banche italiane*.

L'Hostis, A. (2016, agosto). *Banche e fintech: Meglio insieme*. Forrester. https://www.forrester.com/blogs/16-08-22-banks_and_fintechs_better_together/

La Repubblica. (2025, aprile). *Revolut utile netto più che raddoppiato a 1 miliardo di euro.* https://finanza.repubblica.it/News/2025/04/24/revolut_utile_netto_piu_che_raddoppiato_a_1_miliardo_euro-33/

Leonards, A. (2024, settembre). *Final UK banks complete open banking roadmap*. FStech. https://www.fstech.co.uk/fst/Final_UK_Banks_Complete_Open_Banking_Roadmap.php

Lucantoni, P., & Villani, C. (2025, gennaio). *La gestione e supervisione dei rischi ICT e di sicurezza nelle attività finanziarie esternalizzate tra DORA e CRD VI*. DirittoBancario. https://www.dirittobancario.it/art/la-gestione-e-supervisione-dei-rischi-ict-e-di-sicurezza-nelle-attivita-finanziarie-esternalizzate-tra-dora-e-crd-iv/

Maimeri, F., & Mancini, M. (2019). *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale* (*Quaderni di ricerca giuridica della consulenza legale*, p. 49). Banca d'Italia.

Makortoff, K. (2025, gennaio). *NatWest apologises to millions of customers locked out of app.* The Guardian. https://www.theguardian.com/business/2025/jun/06/natwest-apologises-to-millions-of-customers-locked-out-of-app

Marasà, F. (2020). Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR. *Orizzonti del diritto commerciale*, (2I2020), 634.

Milanesi, D. (2017). *A new banking paradigm: The state of open banking in Europe, the United Kingdom, and the United States* (TTLF Working Paper No. 29, pp. 97–98).

Moden, N. (2021, marzo). *Five questions about banking in today's digital age, answered.* EY Global. https://www.ey.com/en_nl/insights/banking-capital-markets/five-questions-about-banking-in-todays-digital-age-answered

Mordor Intelligence. (n.d.). *Banking as a service market size & share analysis Analysis - Growth Trends & Forecasts (2025 - 2030).* https://www.mordorintelligence.com/industry-reports/global-banking-as-a-service-market

Murri, G., & Fintschj, F. (2024, luglio). *Key results – Osservatorio Digital Banking: L'ossimoro del digital banking: più vicino al cliente da lontano!* ABI Lab.

Ninfole, F. (2024, febbraio). *La Vigilanza BCE mette in guardia le banche sui rischi legati a cloud e outsourcing di attività critiche.* Milano Finanza. https://www.milanofinanza.it/news/la-vigilanza-bce-mette-in-guardia-le-banche-sui-rischi-legati-all-outsourcing-di-attivita-critiche-202402211841269565?refresh_cens

OBIE. (2025). *Delivering the roadmap: Open banking – A UK success story*. https://www.openbanking.org.uk/delivering-the-roadmap/

OECD. (2023). *Open finance policy consideration* (pp. 8–9). OECD Publishing.

OECD. (2023). *Shifting from open banking to open finance* (pp. 37–38). OECD Publishing.

One Hundred Eleventh Congress of the United States of America. (2010). *Dodd-Frank Wall Street Reform and Consumer Protection Act* (Title I, Sub. B, Sec. 153; 12 U.S.C. § 5343).

Open Banking Implementation Entity (OBIE). (2020). *Annual report 2020* (pp. 15–16).

Open Banking Implementation Entity (OBIE). (2024, marzo). *The open banking impact report*. https://openbanking.foleon.com/live-publications/the-open-banking-impact-report-2024-march/adoption-analysis

Open Banking Ltd. (2024, marzo). *The open banking impact report*. https://openbanking.foleon.com/live-publications/the-open-banking-impact-report-2024-march/

Open Banking Working Group (OBWG). (n.d.). *The open banking standards: Unlocking the potential of open banking to improve competition, efficiency and stimulate innovation* (Chap. 7a, pp. 24–25).

Open Data Institute, & Fingleton Associates. (2014, settembre). *Data sharing and open data for banks: A report for HM Treasury and Cabinet Office* (pp. 4–5).

Open Data Institute, & Fingleton Associates. (2019, giugno). *Open banking: Preparing for lift-off* (pp. 5–6).

Open Data Institute. (2016, gennaio). *Introducing the open banking standard: Helping customers, banks and regulators take banking into a truly 21st-century, connected digital economy* (pp. 5–6). https://theodi.org/documents/239/298568600-Introducing-the-Open-Banking-Standard.pdf

Open Data Institute. (2019). *Introducing the open banking standards* (p. 9).

Organisation for Economic Co-operation and Development (OECD). (2023). *Data portability in open banking: Privacy and other cross-cutting issues* (*OECD Digital Economy Papers*, No. 348, pp. 11–12). Paris: OECD Publishing.

Patenge, R., Anand, A., & Goel, R. (2024, ottobre). *Managing bank IT spending: Five questions for tech leaders.* McKinsey. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/managing-bank-it-spending-five-questions-for-tech-leaders

Pelletteri, R., Parrini, R., Cafartti, C., & De Vendictis, B. A. (2023, marzo). *Questioni istituzionali… L'open banking nel sistema dei pagamenti…* (No. 31, p. 11).

Porta, R. (2018, aprile). *Banche e PSD2*. LinkedIn. https://it.linkedin.com/pulse/banche-e-psd2-riccardo-porta

Prallini, E. (2021, giugno). *Perché Visa ha acquistato la fintech svedese Tink per 1,8 miliardi di euro. Forbes Italia*. https://forbes.it/2021/06/24/tink-la-fintech-svedese-acquistata-da-visa-per-sbarcare-nell-open-banking

PwC. (2024, luglio). *What does banking-as-a-service (BaaS) mean for a business?* https://www.pwc.com/gx/en/issues/technology/baas-banking-as-a-service.html

PwC's Digital Service. (2019, marzo). *Platform banking & digital ecosystems* (pp. 22–25).

Reuters. (2025, aprile). *Lithuania fines Revolut 3.5 million euros for money-laundering prevention failures.* https://www.reuters.com/technology/lithuania-fines-revolut-35-million-euros-money-laundering-prevention-failures-2025-04-08/

Revolut Ltd. (2018-2024). *Annual report and financial statements for the year ended 31 December.*

Rulli, E. (2025, maggio). *Profili critici della banca come servizio (bank-as-a-service).* DirittoBancario. https://www.dirittobancario.it/art/profili-critici-della-banca-come-servizio-bank-as-a-service/

Rybacki, P. (2022, luglio). *Revolut's revolution: The rise of a digital bank* (p. 10). University of Chicago.

Sbriz, L. (2022, maggio). *Considerazioni sui rischi strategici e sui rischi operativi.* ESG360. https://www.esg360.it/risk-management/considerazioni-sui-rischi-strategici-e-sui-rischi-operativi/

Stanzione, P. (2024). Open banking, open finance e protezione dei dati personali. In V. Falce & U. Morera (a cura di), *Dall'open banking all'open finance: Profili di diritto dell'economia* (p. 67). Torino: G. Giappichelli.

Tink AB. (2020). *Open banking survey 2020. The use cases driving open banking investments in UK.*

U.S. Department of the Treasury. (2022, novembre). *Report to the White House Competition Council: Assessing the impact of new entrant non-bank firms on competition in consumer finance markets* (pp. 86–90).

Valentini, M. (2023, maggio). *Banche e innovazione, raddoppiata la spesa in tecnologia: ecco le sfide future*. EconomyUp. https://www.economyup.it/fintech/banche-e-innovazione-raddoppiata-la-spesa-in-tecnologia-ecco-le-sfide-future/

Virtusa. *Banking-as-a-platform.* https://www.virtusa.com/digital-themes/banking-as-a-platform

Visa Open Banking. (2023). *The U.S. open banking movement: How consumers are driving U.S. open banking innovation* (Chap. I, p. 5).

Wade, M., Gauchat, M., & Srinivas, V. (2024, ottobre). *2025 banking and capital markets outlook.* Deloitte Center for Financial Services. https://www.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-outlooks/banking-industry-outlook.html

White, B. (2023, gennaio). *Plaid's support for a strong consumer financial data right.* Plaid.

SITOGRAFIA

https://axaxl.com

https://blenheimchalcot.com/blog

https://blog.bitpanda.com

https://blog.workday.com

https://businesscasestudies.co.uk

https://d3security.com

https://fintechmagazine.com

https://frogcapital.com

https://gearinc.com

https://ico.org.uk

https://it.strikingly.com

https://media.chase.com

https://mia-fintech.io/it/blog

https://n26.com/blog

https://plaid.com/en-eu/

https://status.wise.com

https://stripe.com

https://techcrunch.com

https://tink.com/blog

https://truelayer.com

https://tuum.com/blog

https://tyk.io/blog

https://vitolavecchia.altervista.org

https://wise.com

https://writeupcafe.com

https://www.zerounoweb.it

https://www.10xbanking.com

https://www.abnamro.com

https://www.agendadigitale.eu

https://www.aziendabanca.it

https://www.bbvaspark.com

https://www.berlin-group.org

https://www.businessofapps.com
https://www.capgemini.com
https://www.currencycloud.com
https://www.exabeam.com
https://www.fabrick.com
https://www.ibm.com
https://www.ionos.it
https://www.konsentus.com
https://www.kontomatik.com
https://www.macroglobal.co.uk
https://www.numberanalytics.com
https://www.opyn.eu
https://www.revolut.com/blog
https://www.solarisgroup.com
https://www.starlingbank.com
https://www.startupgeeks.it
https://www.virtusa.com
https://www.workinvoice.it/blog