BANCA D'ITALIA
EUROSISTEMA

PSD2 E OPEN BANKING: NUOVI MODELLI DI BUSINESS E RISCHI EMERGENTI

Novembre 2021

BANCA D'ITALIA
EUROSISTEMA

PSD2 E OPEN BANKING: NUOVI MODELLI DI BUSINESS E RISCHI EMERGENTI

Novembre 2021

Il presente lavoro illustra i risultati dell'analisi condotta nell'ambito del Gruppo di lavoro "Rischi connessi con l'Open Banking" costituito all'interno della Banca d'Italia per seguire l'evoluzione dell'Open Banking nel mercato italiano.

I componenti del gruppo di lavoro sono: Benedetto Andrea De Vendictis (Coordinatore), Francesco Abbinante, Costanza Alessi, Andrea Azzola, Paola Balestra, Alessandro Bracale, Daniela Bonito Oliva, Dorotea Clementi, Giovanni Di Balsamo, Simone Gemini, Simona Mascaro, Pietro Paolo Napolitano, Barbara Panunzi, Livia Picconi, Claudia Pavoni, Fabiana Roncaglia, Maria Grazia Topa, Maria Carmela Zaccagnino.

Indirizzo
Via Nazionale 91
00184 Roma - Italia

Sito internet
http://www.bancaditalia.it

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

INDICE

Elenco degli acronimi impiegati 4

1. Principali risultati 5

2. Introduzione 8

box: I servizi di pagamento PIS, AIS, CIS introdotti dalla PSD2 9

3. La diffusione nel mercato italiano dei nuovi servizi di pagamento introdotti dalla PSD2 10

4. Gli ostacoli 13

5. I modelli di business 16

I modelli di business prevalenti 16

6. I rischi 21

6.1 *I rischi tecnologici e di sicurezza* 21

6.2 *I rischi operativi e reputazionali - le garanzie per danni arrecati nell'esercizio dell'attività* 24

6.3 *La tutela dei clienti. Il presidio dei rischi approntato dalla PSD2: il regime di responsabilità dei PSP rispetto ad operazioni non autorizzate, la disciplina di trasparenza* 26

6.4 *Le interconnessioni tra normativa PSD2 e GDPR* 28

7. Conclusioni 30

Elenco degli acronimi impiegati

AIS: Account Information Service (Servizio di informazione sui conti)

AISP: Account Information Service Provider (Prestatore del servizio di informazione sui conti)

API: Application Programming Interface

ASPSP: Account Servicing Payment Service Provider (Prestatore del servizio di pagamento di radicamento del conto)

BFM: Business Financial Management

CIS: Card Initiated Service (Servizio di conferma fondi)

EBA: European Banking Authority

GDPR: General Data Protection Regulation

KYC: Know Your Customer

IMEL: Istituto di Moneta Elettronica

IP: Istituto di Pagamento

LPS: Libera Prestazione di Servizi

ML: Machine Learning

NPL: Non Performing Loans

PFM: Personal Financial Management

PIS: Payment Initiation Service (Servizio di disposizione di ordini di pagamento)

PISP: Payment Initiation Service Provider (Prestatore del servizio di disposizione di ordini di pagamento)

POS: Point of Sale

PSD2: Payment Service Directive 2

PSP: Payment Service Provider (Prestatore di servizio di pagamento)

SEPA: Single Euro Payments Area

TPP: Third Party Providers (Prestatori dei servizi AIS, PIS, CIS)

TUB: Testo Unico Bancario

1. PRINCIPALI RISULTATI

Con Open Banking si intende un ecosistema aperto e digitale che consente, anche senza la presenza di accordi prestabiliti, lo scambio di dati e informazioni, non solo finanziarie, tra gli operatori (bancari, finanziari e non) che ne fanno parte.

Questo lavoro illustra i primi risultati di un approfondimento condotto nella seconda metà del 2020 avente l'obiettivo di identificare le caratteristiche distintive e i rischi derivanti dalla diffusione di tale paradigma nel mercato italiano, anche al fine di definire adeguati assetti metodologici applicabili dalla Banca d'Italia nella conduzione della vigilanza sul nuovo comparto operativo.

L'analisi si è concentrata sui servizi di Open Banking regolati dalla direttiva PSD2 e dal Regolamento delegato 2018/389 della Commissione europea del 27 novembre 2017 entrato in vigore alla fine del 2019 e offerti alla clientela dalle cd. terze parti (*Third Party Providers* - TPP).

I TPP, nelle loro differenti tipologie, offrono: i) servizi di informazione sui conti di pagamento detenuti dal cliente presso uno o più prestatori di servizi di pagamento (Servizio di informazione sui conti/*Account Information Service* – AIS); ii) servizi attraverso i quali il TPP dispone, su richiesta del cliente, un ordine di pagamento a valere su un conto di pagamento che il cliente detiene presso un altro prestatore di servizi di pagamento (Servizio di disposizione di ordini di pagamento/*Payment Initiation Service* – PIS); iii) servizi di pagamento basati sulle carte, che richiedono una procedura di conferma fondi su un conto che il cliente detiene presso un altro prestatore di servizi di pagamento che non è preventivamente associato tramite un accordo contrattuale alla carta di pagamento (Servizio di conferma fondi/*Card Initiated Service* – CIS).

Il monitoraggio condotto evidenzia ancora un limitato ricorso ai servizi di Open Banking in termini di clienti coinvolti (dell'ordine di poche decine di migliaia) e transazioni eseguite (poco più di 350.000 operazioni dispositive in un semestre), sebbene il numero di TPP attivi non sia trascurabile (103 operatori nel secondo semestre del 2020 hanno eseguito almeno una chiamata su un'interfaccia di Open Banking); il servizio di informazione sui conti (AIS) risulta relativamente più diffuso rispetto al servizio di disposizione di un ordine di pagamento (PIS), il servizio di conferma fondi (CIS) appare pressoché trascurato dal mercato. L'elevato numero di transazioni non andate a buon fine sulle interfacce di accesso (ancora 10,5 per cento di transazioni andate in errore rispetto al totale delle transazioni eseguite nel secondo semestre 2020) rafforza l'impressione che il paradigma Open Banking si collochi ancora in una fase di sperimentazione[1)].

1) Mentre le chiamate alle interfacce in Italia sono state nel secondo semestre 2020 complessivamente ca. 47 mln, nel mercato del Regno Unito, ad oggi quello più evoluto nei servizi di Open Banking tra quelli europei, le chiamate alle interfacce nel solo mese di dicembre 2020 sono state ca. 700 mln.

In Italia, come peraltro in altre giurisdizioni dell'Unione Europea, sono ancora presenti ostacoli nelle procedure di acceso ai conti *on-line* tramite TPP, ostacoli che compromettono la *user experience* della clientela (ad esempio, introducendo un eccessivo numero di passaggi nelle procedure di autenticazione) ovvero che limitano l'operatività dei TPP (ad esempio, non fornendo sulle interfacce per i TPP dettagli informativi sui conti dei clienti presenti invece sulle interfacce dirette dei clienti). La rimozione delle criticità costituisce un fattore chiave per assicurare una rapida evoluzione del comparto. In questo contesto la Banca d'Italia sta svolgendo sin dall'avvio dei nuovi servizi introdotti dalla PSD2 azioni di verifica delle soluzioni adottate dagli intermediari e di contrasto agli ostacoli identificati.

I modelli di *business* proposti dagli operatori italiani e stranieri attivi nei nuovi servizi introdotti dalla PSD2 appaiono diversificati rispetto alle modalità *standard* originariamente previste dalla normativa. I servizi PIS, oltre che per i pagamenti ai *merchant* su *Internet*, vengono infatti offerti con l'obiettivo di fornire un servizio alla propria clientela *consumer* (ad esempio, per il pagamento di altri servizi offerti, anche commerciali o la ricarica di carte prepagate) o ai propri clienti *business* (ad esempio, per il pagamento delle fatture commerciali). Il servizio AIS viene utilizzato per offrire servizi per la predisposizione di scadenzari, la riconciliazione di fatture, il miglioramento della gestione della tesoreria aziendale, il miglioramento delle abitudini finanziarie dei clienti mediante la pianificazione delle spese e dei risparmi, a supporto di processi di *credit scoring*.

Piuttosto che dai servizi PIS e AIS in sé, che rivestono un ruolo ancillare, la redditività è generata dai servizi a valore aggiunto e da una più articolata offerta di *business* (ad esempio offrendo *in bundle* servizi finanziari, assicurativi, di investimento, commerciali), per i quali i servizi PIS e AIS fungono da vettore.

Le banche, dopo una fase iniziale in cui hanno assolto gli obblighi di *compliance* realizzando le interfacce di accesso e rendendo così raggiungibili ai TPP i dati relativi ai conti di pagamento *on-line* della propria clientela, nel corso del 2020 hanno avviato iniziative per sfruttare i nuovi servizi di pagamento e per porsi in competizione con i TPP non bancari. La strategia appare generalmente ancora circoscritta ai servizi AIS/PIS offerti in modalità *standard* e integrati all'interno dei siti *web* e delle *app* di *mobile banking*, con limitate funzionalità a valore aggiunto.

Quanto ai rischi, i principali emersi dall'analisi sono quelli tecnologici e di tutela della clientela; tra i primi rilevano i seguenti profili di attenzione:

- un rischio *cyber* intrinsecamente maggiore, perché legato all'aumento della superficie di attacco (*attack surface*) disponibile per i soggetti malevoli derivante dalla presenza di molteplici soggetti: banche e altri operatori che forniscono conti *on-line*, TPP, piattaforme di accesso, fornitori tecnici, "quarte parti" (*merchant* e/o operatori non finanziari che non rientrano nel perimetro di vigilanza) che partecipano al servizio di pagamento o che beneficiano, nella catena del valore, dell'utilizzo dei dati dei clienti dei servizi di pagamento;

- la presenza di una molteplicità di chiavi di autenticazione e di cifratura, il cui ciclo di vita deve essere gestito in maniera adeguata per garantire la corretta identificazione dei soggetti coinvolti e la protezione dei canali di comunicazione;
- la diffusa presenza di *Application Programming Interface (API)* e di interazioni tra *app* mobili riferibili a operatori distinti, che necessita di un opportuno utilizzo delle *best practice* di sviluppo sicuro del *software*;
- il rischio di un "depotenziamento" delle procedure anti-frode (*Transaction Risk Analysis*), derivante dall'interposizione del TPP tra il cliente e il prestatore di servizio di pagamento di radicamento del conto.

Relativamente ai profili di tutela del cliente, occorre sottolineare che le modalità digitali con le quali i servizi sono offerti, soprattutto attraverso dispositivi mobili, potrebbero limitare l'efficacia dell'informativa di trasparenza, non consentendo di perseguire appieno gli obiettivi della disciplina di riferimento che mira ad assicurare un'informativa alla clientela più chiara e completa nelle diverse fasi che caratterizzano la prestazione del servizio di pagamento.

Inoltre, soluzioni operative che prevedano servizi AIS e PIS sviluppati da un TPP e integrati nell'offerta commerciale di un altro prestatore di servizi di pagamento potrebbero rendere non del tutto chiari alla clientela il mero ruolo di intermediazione svolto dal proprio intermediario finanziario di riferimento e la circostanza che l'accesso al nuovo servizio comporti l'avvio di un rapporto con un operatore terzo. Ciò può aumentare il rischio reputazionale per gli intermediari qualora questi ultimi non forniscano un'adeguata informativa alla clientela.

Le informazioni acquisite per lo svolgimento del servizio AIS vengono spesso utilizzate per finalità ulteriori rispetto ai servizi di pagamento e/o cedute a soggetti diversi dal titolare. In tali casi è centrale la corretta acquisizione dei consensi del cliente finale da parte degli intermediari, distinguendo tra quelli rilasciati ai sensi della PSD2, per consentire l'accesso ai dati dell'utente da parte degli intermediari che offrono i servizi PIS e AIS, e quelli necessari ai sensi della normativa *privacy* (GDPR) per consentire la cessione ad altri soggetti delle informazioni estratte o per elaborarli perseguendo finalità diverse da quelle del servizio di pagamento (ad esempio, *credit scoring*). Sotto questo profilo, assume rilevanza anche l'esigenza di una adeguata alfabetizzazione finanziaria e digitale della clientela quale presidio fondamentale per evitare l'assunzione inconsapevole di rischi derivanti dalle finalità ulteriori rispetto a quelle strettamente connesse alla fruizione dei nuovi servizi di pagamento.

Infine, il funzionamento dell'ecosistema di Open Banking è reso ulteriormente complesso dalla presenza di TPP in libera prestazione di servizi, localizzati in altre giurisdizioni dell'Unione Europea, e delle big-tech per ora principalmente nel ruolo di fornitori di servizi tecnici. La presenza di tali soggetti implica la possibilità che i dati dei clienti, prima residenti di prassi presso i data-center degli operatori italiani, possano essere ora memorizzati al di fuori del territorio nazionale ed eventualmente anche fuori della Unione Europea (con possibili impatti, in quest'ultimo caso, sui profili della protezione dei dati personali).

2. INTRODUZIONE

Con il termine Open Banking si fa riferimento a un ecosistema aperto e digitale che consente, anche senza la presenza di accordi prestabiliti, lo scambio di dati e informazioni, non solo finanziarie, tra gli operatori che ne fanno parte. Tale paradigma si associa usualmente all'utilizzo delle cosiddette *Open API*[2] che consentono a un'applicazione di avere accesso ai dati degli intermediari finanziari e che quindi permettono lo scambio di informazioni tra diversi operatori (intermediari finanziari, fornitori tecnici, altri soggetti non finanziari).

L'introduzione del modello di Open Banking, favorito dall'entrata in vigore della Direttiva Europea sui servizi di pagamento (PSD2), e la progressiva evoluzione tecnologica stanno spingendo gli intermediari ad adottare nuovi modelli di *business*; tali modelli ampliano le opportunità di ricavo ma accrescono al tempo stesso lo spettro dei rischi (ad esempio, frodi, minacce alla sicurezza e alla protezione dei dati personali, rischi operativi e strategici).

Il presente lavoro si propone di illustrare i nuovi modelli di *business*, i fattori che ne possano ostacolare l'adeguato sviluppo, i nuovi rischi emergenti.

L'analisi è focalizzata sulle iniziative di Open Banking promosse dagli intermediari direttamente collegate ai servizi di pagamento introdotti dalla PSD2, ovvero il *Payment Initiation Service* (PIS), l'*Account Information Service* (AIS), il *Card Initiated Service* (CIS) e i servizi forniti da soggetti autorizzati che, nel loro insieme, sono comunemente denominati *Third Party Providers – TPP* (cfr. il riquadro *I servizi di pagamento PIS, AIS, CIS introdotti dalla PSD2*).

L'analisi è stata condotta su una serie di *business case* presentati alla Banca d'Italia dagli intermediari finanziari, nell'ambito delle comunicazioni necessarie per l'avviamento o l'ampliamento dell'operatività o nell'ambito di incontri dedicati al tema dell'Open Banking[3]. Queste informazioni di base sono state integrate da un *framework* di monitoraggio delle attività di Open Banking, che ne fornisce un quadro evolutivo e da un *framework* di controllo dei rischi basato su specifici eventi e indicatori di rischio (ricorsi presentati all'Arbitro Bancario Finanziario, esposti presentati alla Banca d'Italia, incidenti di sicurezza, frodi, ecc.).

Il documento è organizzato come segue. Nella prima sezione, si fornisce un quadro dell'operatività associata ai nuovi servizi introdotti dalla PSD2, presentando i dati rivenienti da differenti fonti informative, inclusi il *framework* di monitoraggio dell'operatività presente sulle interfacce di accesso disponibili per i TPP. Nella sezione successiva, sono illustrati gli elementi presenti nel mercato europeo e italiano che possono rappresentare un ostacolo allo sviluppo del paradigma Open Banking. Nella terza parte, si espongono alcuni modelli di *business* introdotti dagli operatori tramite l'offerta dei servizi PIS e AIS. Nell'ultima sezione, si descrivono i rischi tecnologici e operativi identificati nel

2) Con Open API (*Application Programming Interface*) si intende un insieme di procedure *software* che consentono la comunicazione tra applicazioni e programmi. Il termine *Open* sta a specificare che le procedure sono disponibili tramite standard pubblici.

3) Sono stati tenuti nel 2020 incontri con 11 operatori italiani ed esteri attivi nel comparto.

corso dell'analisi e viene svolto un approfondimento sui profili di tutela della clientela. Nelle conclusioni, sono formulate alcune considerazioni sui principali punti di attenzione emersi e sui possibili futuri indirizzi di sviluppo delle analisi.

I SERVIZI DI PAGAMENTO PIS, AIS, CIS INTRODOTTI DALLA PSD2

La PSD2 (Direttiva 2015/2 366/UE sui servizi di pagamento nel mercato interno) ha ampliato la definizione dei servizi di pagamento introducendo i servizi PIS (*Payment Initiation Service*), AIS (*Account Information Service*) e CIS (*Card Initiated Service*).

PIS: è il servizio attraverso cui un prestatore di servizi di pagamento dispone, su richiesta di un utente, un ordine di pagamento a valere su un conto di pagamento che l'utente detiene presso un altro prestatore di servizi di pagamento (detto prestatore di servizio di radicamento del conto, *Account Servicing Payment Service Provider*, ASPSP). Ad esempio, si può acquistare un bene o un servizio *on line*, autorizzando il prestatore del servizio PIS (*Payment Initiation Service Provider - PISP*) ad utilizzare il proprio conto, emettendo un bonifico a favore del venditore.

AIS: è il servizio che fornisce informazioni sui conti di pagamento detenuti dall'utente presso uno o più prestatori di servizi di pagamento. Il cliente può avere una visione integrata dei propri conti in un'unica *dashboard,* monitorando il proprio *budget*, analizzando le spese e pianificando gli investimenti. Il prestatore di tale servizio di pagamento è comunemente denominato AISP (*Account Information Service Provider*).

CIS: è il servizio fornito da prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta. I pagamenti effettuati tramite la carta vengono addebitati su un conto di pagamento detenuto presso un altro prestatore di servizi di pagamento, in assenza di accordi contrattuali. Tali TPP fanno affidamento sul servizio di conferma di disponibilità di fondi sul conto tramite API. Questo servizio non è ricompreso tra quelli identificati dalla PSD2: non può costituire oggetto di esclusiva attività di un prestatore di servizi di pagamento, ma è svolto soltanto dai prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta.

3. LA DIFFUSIONE NEL MERCATO ITALIANO DEI NUOVI SERVIZI DI PAGAMENTO INTRODOTTI DALLA PSD2

L'entrata in vigore della PSD2 ed in particolare, nel settembre 2019, del Regolamento delegato 2018/389 della Commissione europea del 27 novembre 2017 rappresenta l'inizio dell'operatività per i servizi di pagamento PIS, AIS e CIS che, in quanto ancora non normati, erano pressoché assenti sul territorio nazionale[4].

A partire da quella data e fino alla fine del 2020 quattro istituti di moneta elettronica e tre istituti di pagamento sono stati autorizzati a svolgere servizi AIS e PIS in Italia, mentre due istituti di pagamento sono stati autorizzati a prestare in via esclusiva il servizio AIS.

Gli istituti bancari autorizzati in Italia, a differenza degli istituti di pagamento e di moneta elettronica, possono svolgere i servizi previsti dalla PSD2 senza una preventiva richiesta all'autorità di vigilanza. Pertanto, almeno potenzialmente, tutte le banche possono entrare nel mercato dei servizi regolati dalla PSD2. Alla fine del 2020 i nuovi servizi introdotti dalla PSD2 (PIS e AIS) risultavano effettivamente erogati ai propri clienti da 7 intermediari bancari (4 gruppi bancari e 3 banche individuali)[5].

Tavola 1

SERVIZI PIS E AIS IN ITALIA ALLA FINE DEL 2020

Istituti di pagamento autorizzati in Italia	9
Istituti di pagamento UE in LPS	96
Banche e gruppi bancari italiani operativi	7

Agli operatori italiani si affiancano quelli stranieri: a dicembre 2020 gli istituti di pagamento e di moneta elettronica comunitari che avevano notificato alla Banca d'Italia l'intenzione di fornire i servizi PIS e AIS in regime di Libera Prestazione di Servizi (LPS) erano 96, 60 dei quali avevano notificato la prestazione di entrambi i servizi, 33 esclusivamente la prestazione dei servizi informativi e 3 dei soli servizi dispositivi. Parimenti alle banche autorizzate in Italia, le banche autorizzate in altre giurisdizioni dell'Unione Europea che intendano operare sul territorio italiano, non sono tenute ad avanzare una preventiva istanza alla Banca d'Italia per svolgere i servizi di pagamento previsti dalla PSD2.

Queste consistenze legate al mero censimento dei soggetti autorizzati potrebbero tuttavia fornire un quadro distorto dell'effettivo stato di evoluzione del mercato, tenuto conto che: i) gli operatori bancari, sia italiani che europei, nonché gli istituti di pagamento in LPS costituenti la maggioranza dei PSP, pur autorizzati, non sono tutti effettivamente operativi nei nuovi servizi di pagamento introdotti dalla PSD2; ii) la diffusione dei nuovi servizi di pagamento è principalmente correlata all'effettivo interesse dei clienti e non dipende unicamente dalla presenza dell'offerta.

4) 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 cd. "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.

5) Fonte: Banca d'Italia, rilevazione di vigilanza sulle risultanze dell'analisi dei rischi operativi e di sicurezza relativi ai servizi di pagamento che tutti i PSP autorizzati in Italia sono tenuti a comunicare annualmente a partire dal 2020.

Il *framework* di segnalazione sulle interfacce di accesso messe a disposizione dei TPP dai prestatori di servizi di pagamento di radicamento del conto (ASPSP), definito nel 2020 dalla Banca d'Italia, permette di integrare le informazioni relative ai processi formali di *licencing* con dati quantitativi sull'effettiva operatività osservata nel 2020. Ricomprendendo le quattro piattaforme di mercato sorvegliate dalla Banca d'Italia ai sensi dell'art. 146 del TUB e i sei maggiori operatori italiani che hanno sviluppato proprie piattaforme, è possibile ottenere una fotografia pressoché completa della fruizione dei servizi di Open Banking da parte dei clienti finali nel mercato italiano.

I risultati delle prime due rilevazioni indicano un'operatività in significativa crescita, ma ancora limitata (Tavola 2). Sebbene il numero di operatori attivi sulle interfacce nel secondo semestre non sia trascurabile (103) e in netta crescita rispetto al semestre precedente, l'operatività dei clienti appare ancora poco significativa. I clienti che hanno utilizzato servizi di tipo PIS e AIS sono stati rispettivamente meno di 20.000 e meno di 100.000 unità[6]. In un mercato italiano con decine di milioni di clienti che dispongono di conti *on-line*, tali numeri, dell'ordine delle migliaia, indicano una penetrazione del paradigma Open Banking ancora marginale.

Tavola 2

OPERATIVITÀ INTERFACCE OPEN BANKING 2020

	I sem 2020	II sem 2020	variazione percentuale
Numero TPP che hanno acceduto all'interfaccia	35	103	194
Numero totale di chiamate alle API	18.870.462	47.389.332	151,1
Numero operazioni dispositive (andate a buon fine)	24.806	358.654	1345,8
Numero accessi informativi (andati a buon fine)	12.674.812	31.281.058	146,8
Numero controlli disponibilità fondi (andati a buon fine)	82.571	139.482	68,9
Tasso di errore (% chiamate non andate a buon fine)	17,16%	10,47%	-6,69

Per meglio inquadrare il numero totale di chiamate API[7], si consideri che, mentre in Italia se ne contano circa 66 milioni in un intero anno, nel Regno Unito, dove l'Open Banking si è maggiormente evoluto, sono state registrate 700 milioni di chiamate nel solo mese di dicembre 2020[8]. Il numero di chiamate per servizi informativi è risultato decisamente superiore a quello relativo ai servizi dispositivi, evidenziando che il servizio AIS al momento risulta maggiormente diffuso nel mercato rispetto al servizio PIS[9]. In base ai dati forniti dai 10 operatori oggetto della rilevazione, i servizi di tipo CIS risultano al momento pressoché trascurati dal mercato.

6) In sostanza assenti invece i "clienti" associati al servizio CIS.

7) Una chiamata API rappresenta il comando singolo utilizzato per richiamare una funzionalità e una risposta da parte dell'interfaccia dell'ASPSP. In generale una disposizione di pagamento e una richiesta di informazioni sui conti sono operazioni realizzate utilizzando più chiamate API.

8) Fonte: Open Banking Limited, dati relativi a 19 ASPSP operanti nel Regno Unito https://www.openbanking.org.uk/providers/account-providers/api-performance/.

9) Se è evidente una maggiore propensione dei TPP a proporre servizi informativi, rispetto a quelli dispositivi, è altresì da tenere presente che tale proporzione rispecchia sia la diversa natura dei due servizi (in generale, gli accessi informativi ai conti sono più numerosi di quelli dispositivi anche nell'operatività tradizionale di *on-line banking*) sia la possibilità offerta dalla normativa agli AISP di accedere ai conti di pagamento anche senza la richiesta esplicita dell'utente (allo scopo di aggiornare i dati di conto in maniera asincrona rispetto alle richieste dei clienti).

Anche il tasso di errore delle chiamate API sul complesso delle interfacce, dato dal rapporto tra le chiamate API non andate a buon fine a causa di errori di comunicazione e il totale di chiamate API, è coerente con lo stato di sviluppo ancora embrionale dell'Open Banking fin qui delineato: sebbene in diminuzione (dal 17 al 10,5 per cento nel corso dei due semestri) esso denota difficoltà tecniche significative e coerenti con uno stadio delle interfacce ancora sperimentale. Le informazioni sul tasso di errore, unitamente all'interlocuzione diretta con gli operatori, indicano inoltre che alcuni TPP utilizzano gli ambienti di produzione (in modalità cd. *family&friends*[10]) per svolgere *test* più efficaci rispetto a quelli svolti in ambienti di collaudo, non sempre perfettamente allineati agli ambienti di produzione (cfr. infra par. 4 "Gli ostacoli").

Nel secondo semestre del 2020, 103 TPP hanno avuto effettivo accesso alle interfacce; di questi, 29 sono intermediari autorizzati in Italia ed essenzialmente riconducibili ai principali gruppi bancari nazionali (cfr. Tavola 3). Rispetto ai 7 intermediari bancari che hanno dichiarato di offrire servizi AIS e PIS e ai 9 IP e Imel autorizzati nel 2020 (cfr. Tavola 1), il numero maggiore di soggetti italiani operanti sulle interfacce può essere spiegato precisando che: i) i dati della tabella fanno riferimento a banche individuali (un gruppo bancario potrebbe essere attivo con più entità individuali); ii) alcuni soggetti stanno operando sulle interfacce per svolgere *test* prima di offrire il servizio alla propria clientela (cfr. nota 10). Dei TPP esteri operanti in Italia in regime di libera prestazione, circa il 50 per cento è proveniente dall'Irlanda, la Finlandia, la Germania e il Regno Unito[11]. Il numero di operatori stranieri effettivamente attivi (74), che peraltro comprende anche banche straniere, era nel 2020 leggermente minore del numero di IP autorizzati ad operare in Italia nei servizi in questione.

Tavola 3

TPP ATTIVI NEL 2020 - DATI INTERFACCE

	Banche	IMEL	IP	Operatori non bancari passaportati	Totale
Italia	19	3	7	–	29
Finlandia	–	–	–	10	10
UK	–	–	–	10	10
Irlanda	–	–	–	7	7
Germania	2	–	–	5	7
Francia	–	–	–	5	5
Lituania	–	–	–	4	4
Lussemburgo	1	–	–	4	5
Spagna				4	4
Altri	7	–	–	15	22
Totale	**29**	**3**	**7**	**64**	**103**

10) In questi *test* il TPP apre un conto *on-line* presso l'ASPSP sul quale intende svolgere il collaudo ed esegue le operazioni nell'ambiente di esercizio dell'ASPSP come un qualunque altro utente standard del TPP e dell'ASPSP.

11) Si sottolinea ancora che i dati fanno riferimento al secondo semestre 2020, una fase precedente all'uscita del Regno Unito dall'Unione Europea, quando ancora gli operatori del Regno Unito potevano operare in Italia. Molti degli operatori autorizzati nel Regno Unito stanno comunque richiedendo la licenza in uno dei paesi della UE, per far fronte alla fuoriuscita del Regno Unito dall'Unione Europea.

4. GLI OSTACOLI

La possibilità di sperimentare una evoluzione più rapida dell'Open Banking e dei servizi di pagamento introdotti dalla PSD2 dipende, oltre che dall'offerta di prodotti che rappresentino delle adeguate proposte di valore per il mercato (cfr. per una descrizione dei modelli di *business* presenti nel mercato italiano il par. 5 "I modelli di business"), dalla rimozione di quei fattori che costituiscono un ostacolo al loro utilizzo.

La PSD2 prevede che i TPP facciano affidamento sulle interfacce di comunicazione e sulle procedure di autenticazione messe a disposizione dagli ASPSP. La normativa europea sui servizi di pagamento stabilisce inoltre che i servizi offerti tramite tali interfacce dedicate vengano assicurati nel continuo e senza ostacoli a carico del TPP e del cliente finale.

La quasi totalità degli ASPSP italiani ha scelto di realizzare un'interfaccia dedicata ai TPP e separata da quella utilizzata dai propri clienti allorché accedono direttamente al proprio conto. Sulla base delle evidenze emerse in questa prima fase di introduzione dei servizi regolati dalla PSD2, si osserva che sussistono ancora margini di miglioramento nelle interfacce dedicate messe a disposizione dei TPP e nelle correlate procedure di autenticazione dei clienti.

Tenuto conto che i problemi sono comuni alla gran parte delle giurisdizioni europee, sul punto, nel giugno 2020 l'EBA ha pubblicato un parere[12] che fornisce chiarimenti in merito ai possibili ostacoli presenti nelle interfacce dedicate e indicazioni circa la corretta applicazione della normativa di attuazione, in considerazione delle casistiche di ostacoli più comuni segnalati dai TPP europei.

Il parere identifica il concetto di "ostacolo" allo svolgimento di servizi dei TPP nelle procedure di autenticazione del cliente che compromettano la *user experience* del cliente ovvero quando nel *customer journey* si richiedano informazioni o passaggi aggiuntivi, superflui o non necessari rispetto a quelli richiesti nell'analogo processo di autenticazione per l'accesso ai medesimi servizi direttamente dal proprio conto *on-line,* detenuto presso l'ASPSP. L'EBA ribadisce inoltre il principio secondo cui l'interfaccia dedicata debba supportare tutte le modalità di autenticazione presenti sull'interfaccia di *on-line banking* del cliente.

Gli ostacoli enucleati dall'EBA possono essere classificati in due raggruppamenti:

- gli ostacoli che limitano la *user experience* dei clienti che utilizzano i servizi dei TPP. Tra questi rilevano: l'impossibilità di utilizzare i fattori biometrici per l'identificazione e l'autenticazione del cliente, utilizzati dall'ASPSP sulla propria *app mobile*, quando la soluzione di autenticazione adottata dall'ASPSP sia basata sul

12) *Opinion of the European Banking Authority on obstacles under Article 32(3) of the RTS on SCA and CSC*, Giugno 2020.

reindirizzamento (cd. autenticazione *app-to-app*[13]) o sulla modalità *decoupled*[14]*;* la presenza di richieste multiple di autenticazione forte del cliente addizionali rispetto a quelle previste nell'*on-line banking* tradizionale, sia nel caso di accesso informativo ai propri dati di conto (AIS), sia in quello finalizzato all'inizializzazione di un singolo pagamento (PIS); la richiesta al cliente di digitare manualmente l'IBAN per la selezione del conto su cui addebitare il pagamento[15]; la mancata attivazione dell'esenzione dalla SCA per 90 giorni prevista dalla normativa[16]; la richiesta di un esplicito consenso per l'accesso ai conti da parte dei TPP[17];

- gli ostacoli all'operatività del TPP. Tra questi rilevano: la presenza di una procedura di pre-registrazione dei TPP presso gli ASPSP, prima di iniziare ad operare sull'interfaccia dedicata; la presenza della sola modalità di autenticazione basata sul reindirizzamento nel caso di pagamenti al POS, che non renderebbe possibile l'utilizzo dei servizi di pagamento presso i POS da parte dei TPP.

Nell'ambito dell'interazione con gli operatori di mercato, la Banca d'Italia ha individuato ulteriori casistiche tipiche che possono rientrare nelle categorie di ostacolo:

- il disegno degli ambienti di *test* messi a disposizione dagli ASPSP ai TPP non risulta sempre perfettamente allineato con i corrispondenti ambienti di esercizio, obbligando i TPP a svolgere i *test* delle diverse funzionalità direttamente negli ambienti in produzione delle interfacce dedicate (utilizzando un approccio basato su utenze di tipo *family&friends*);

- i servizi di assistenza e supporto tecnico messi a disposizione dei TPP per la risoluzione di malfunzionamenti concernenti le interfacce presentano livelli di servizio non sempre equivalenti a quelli garantiti nell'ambito dell'*on-line banking* tradizionale;

- nell'ambito dei servizi AIS le informazioni relative ai conti fornite dagli ASPSP ai TPP non forniscono un sufficiente livello di dettaglio, come ad esempio, le informazioni relative alle causali delle transazioni.

---

13) Nel caso di autenticazione a due fattori basato sull'approccio del reindirizzamento tra *app* mobili o sulla possibilità di autenticarsi su un canale separato (cd. *decoupled*), la normativa stabilisce che il cliente che accede al proprio conto tramite *app* del TPP sia reindirizzato all'*app* dell'ASPSP, in tale dominio esegua l'autenticazione biometrica (se prevista dall'ASPSP e supportata dal dispositivo mobile in possesso del cliente) e poi sia nuovamente riportato sull'*app* del TPP. Tale soluzione evita che il cliente sia obbligato a digitare le proprie credenziali e ad avere una *user experience* peggiore di quella che avrebbe utilizzando l'*on-line banking* del proprio ASPSP.

14) Con il termine di autenticazione "decoupled" (letteralmente autenticazione "disaccoppiata") si intende una procedura di autenticazione in cui le credenziali del cliente sono trasmesse tramite un canale separato da quello che il cliente sta utilizzando per accedere al proprio *on-line banking* (ad esempio, un cliente potrebbe inserire le proprie credenziali su un'*app* mobile dell'ASPSP).

15) L'EBA indica come possibili alternative all'inserimento manuale dell'IBAN relativo al conto di addebito del cliente che ricorre a un TPP per un'operazione dispositiva, l'inserimento di *default* dell'IBAN (nel caso il cliente abbia un solo conto presso l'ASPSP) oppure, la possibilità per il cliente di selezionare da un menu a tendina il conto di addebito, in linea con quanto previsto nell'accesso all'*on-line banking* tradizionale (nel caso di presenza di più conti associati ad un unico cliente).

16) L'art. 10 del Regolamento Delegato (UE) 2018/389 della Commissione del 27 novembre 2017, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio relativamente alle norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli *standard* aperti di comunicazione comuni e sicuri, prevede che il cliente, nell'ambito dei servizi informativi, sia esentato dall'autenticazione forte nei 90 giorni successivi alla data dell'ultima autenticazione forte. Tale esenzione deve valere anche nel caso di utilizzo di un TPP.

17) La normativa prevede che il cliente fornisca il proprio consenso direttamente al TPP e che questo sia accertato implicitamente dall'ASPSP attraverso l'applicazione delle procedure di autenticazione forte del cliente, senza inserire ulteriori verifiche.

Un paradigma che non fa leva su prestabiliti accordi contrattuali tra i soggetti interessati, qual è quello dell'Open Banking, e che è altamente dipendente dalle soluzioni tecnologiche e dalle specifiche modalità di interazione tra i diversi operatori è per sua natura caratterizzato da un processo evolutivo che non può considerarsi concluso con la sola entrata in vigore della norma. Affinché tale processo continui ad evolvere in maniera soddisfacente è necessario uno sforzo da parte di tutti gli operatori interessati, consapevoli peraltro che in tale paradigma ciascun operatore può recitare di volta in volta un differente ruolo (essere cioè un TTP o un ASPSP) e che una posizione assunta in un ruolo potrebbe essere controproducente quando si assume un ruolo diverso.

In questo contesto la Banca d'Italia sta svolgendo sin dall'avvio dei nuovi servizi introdotti dalla PSD2 azioni di verifica delle soluzioni adottate dagli intermediari e di contrasto agli ostacoli identificati.

5. I MODELLI DI BUSINESS

Dai procedimenti autorizzativi e dalle comunicazioni preventive per l'estensione dell'operatività inoltrate dagli intermediari nel corso del 2020 unitamente agli incontri tenuti con operatori italiani e stranieri, emergono modelli di *business* eterogenei e a volte lontani dalle intenzioni originarie del legislatore europeo.

I modelli di business prevalenti [18)]

Relativamente al servizio PIS sono stati individuati 3 modelli di erogazione:

- servizio effettuato in modalità *standard*: consente all'utente di ricorrere all'utilizzo dello strumento del bonifico SEPA per effettuare pagamenti via *Internet*; il PISP inizializzerà un'operazione di pagamento mediante l'invio di un ordine alla banca di radicamento del conto su richiesta del proprio cliente. Attualmente, sono pochi gli operatori che intendono utilizzare il servizio PIS per offrire un servizio di pagamento alternativo nei canali *on-line*, convenzionando *web merchant*. Alcuni operatori, invece, studiano accordi di *partnership* con aziende operanti in Italia nei settori delle *utilities*, assicurazioni, telecomunicazioni e *media* per consentire di procedere al pagamento delle bollette, delle utenze e dei premi assicurativi mediante una nuova opzione di pagamento offerta direttamente sui canali digitali delle imprese (sito *web*, *mobile app*) o dopo aver ricevuto da queste una richiesta di pagamento tramite un apposito *link* inviato a mezzo *email*;

- servizio rivolto esclusivamente alla propria clientela: in tale configurazione il servizio PIS è reso disponibile alla clientela come modalità aggiuntiva di pagamento di servizi offerti dal PISP (o da una società del gruppo a cui fa capo), oppure come strumento alternativo di ricarica delle carte prepagate emesse dall'intermediario. Con questo modello, il PISP (o una società del gruppo a cui fa capo) diventa beneficiario finale della transazione. Molti operatori industriali sono intenti a configurare in tale modo il servizio di disposizione di ordini di pagamento allo scopo di rafforzare il legame con la propria clientela *captive,* acquisire nuova clientela rendendo i servizi *core* più "attraenti", nonché disintermediare i tradizionali canali bancari riducendo i relativi costi e tempi di esecuzione;

- servizio rivolto esclusivamente a una clientela *business*: diversi operatori stanno implementando tale modalità operativa a favore della clientela *business*, per lo più piccole e medie imprese, configurandola come uno strumento di pagamento alternativo per le fatture commerciali. In questo modo, l'impresa eviterebbe il superamento dei limiti previsti delle carte di credito e il PISP gestirebbe transazioni di importo medio più elevato rispetto alla clientela *retail*.

Il servizio AIS viene invece generalmente fornito attraverso i seguenti 3 modelli:

18) Si sottolinea come al momento non emergono iniziative relative al servizio CIS.

- servizio effettuato in modalità standard: consente all'utente di disporre immediatamente di un quadro generale della propria situazione finanziaria in un dato momento, attraverso l'aggregazione in un'unica interfaccia grafica delle informazioni contenute nei conti *on-line* detenuti presso altri prestatori di servizi di pagamento;
- servizio AIS alla base di ulteriori servizi a valore aggiunto: i dati di conto, eventualmente con un ulteriore consenso esplicito dell'utente (laddove necessario ai sensi della normativa *privacy*), possono essere rielaborati per la prestazione di servizi a valore aggiunto, che vanno oltre la semplice aggregazione delle transazioni. Le movimentazioni dei conti sono infatti utilizzate per fornire servizi differenti, sia a persone fisiche che a professionisti e aziende:
  - predisposizione di scadenzari, riconciliazione di fatture, miglioramento della gestione della tesoreria aziendale in un'ottica di semplificazione della gestione dei processi amministrativi della clientela *business*, spesso ripetitivi e manuali;
  - servizi focalizzati sul miglioramento delle abitudini finanziarie dei clienti e sulla comprensione dei bisogni futuri, in ottica di una migliore pianificazione delle spese e dei risparmi - *Personal Financial Management* (PFM) e *Business Financial Management* (BFM);
  - utilizzo dei dati per la prestazione di servizi di *credit scoring*: in questo caso le informazioni presenti sui conti di pagamento verrebbero rielaborate per ottenere una valutazione più accurata del merito creditizio del richiedente un finanziamento, a vantaggio dello stesso o dell'intermediario che eroga il finanziamento;
  - servizi strumentali alla verifica o reperimento delle coordinate bancarie di un utente, anche al fine di inizializzare il pagamento con il servizio PIS;
- AIS "*as a service*": questa modalità si distingue da quella precedente per la presenza di una "quarta parte", che può essere un soggetto che non svolge attività regolamentate e pertanto non sottoposto a vigilanza. L'AISP trasferisce i dati di conto del cliente, previo suo esplicito consenso (ai sensi della normativa *privacy*), alle "quarte parti" che li impiegano per fornire al cliente finale un servizio a valore aggiunto quale, ad esempio, il *credit scoring*. Le "quarte parti" sono spesso soggetti non vigilati, appartenenti ad esempio alla categoria *FinTech* o in generale al settore industriale, che vorrebbero fornire ai loro clienti servizi personalizzati basati sui dati di pagamento accessibili ai TPP, ma che non hanno caratteristiche dimensionali, organizzative e operative tali da rendere sostenibile l'intero onere organizzativo e finanziario necessario ad acquisire un'autorizzazione per operare in qualità di AISP.

Tavola 4

MODELLI DI BUSINESS E "USE CASE"

Servizio di pagamento	Modelli		Use case
PIS	Standard	Servizio che consente l'utilizzo dello strumento del bonifico SEPA per effettuare pagamenti via Internet. Il PISP inizializzerà un'operazione di pagamento mediante l'invio di un ordine alla banca di radicamento del conto (ASPSP) su richiesta del proprio cliente. Rappresenta una alternativa al pagamento via carta nel mondo e-commerce.	Pagamenti e-commerce tramite bonifico (eventualmente istantaneo) con la soluzione PIS.
	Servizio rivolto esclusivamente alla propria clientela	Servizio reso disponibile alla clientela come modalità aggiuntiva di pagamento di servizi offerti dal PISP (o da una società del gruppo a cui fa capo), oppure come strumento alternativo di ricarica delle carte prepagate emesse dall'intermediario. Il PISP diventa beneficiario finale della transazione.	Intermediario (es. IP) facente parte di un gruppo industriale che fornisce servizi commerciali (es. utilities) consente al cliente di pagare tali servizi, tramite mobile app, attraverso la soluzione PIS.
	Servizio rivolto esclusivamente a una clientela business	Strumento di pagamento alternativo per le fatture commerciali.	Il PISP fornisce al cliente un'interfaccia di visualizzazione delle fatture commerciali che possono essere pagate utilizzando la soluzione PIS, integrata nell'interfaccia stessa.
AIS	Standard	Servizio che consente al cliente di disporre immediatamente di un quadro generale della propria situazione finanziaria attraverso l'aggregazione in un'unica interfaccia grafica delle informazioni contenute nei conti on-line.	Cliente retail che aggrega i conti per monitorare le proprie spese e i flussi di cassa.
	Servizi a valore aggiunto	In tale modello i dati di conto, eventualmente con un ulteriore consenso esplicito dell'utente (laddove necessario ai sensi della normativa sulla privacy), vengono rielaborati per la prestazione di servizi a valore aggiunto.	L'AISP utilizza i dati andamentali accessibili dai conti on-line per integrare la base informativa dei propri modelli di credit scoring. Applicazioni di PFM e BFM.
	As a service	In tale modello, l'AISP trasferisce i dati di conto del cliente, previo suo esplicito consenso, a "quarte parti" che li impiegano per fornire al cliente finale un servizio a valore aggiunto. Le "quarte parti" sono spesso soggetti non vigilati, appartenenti ad esempio alla categoria FinTech o in generale al settore industriale.	Società che si occupa di gestionali di fatturazione integra nei propri sistemi i dati di conto dei propri clienti trasmessi dall'AISP, per efficientare i processi di riconciliazione bancaria.

La redditività

La redditività dei modelli di *business* esaminati deriva principalmente dai servizi a valore aggiunto o da una maggiore articolazione dell'offerta di *business,* ad esempio offrendo i servizi di pagamento in combinazione ("*in bundle")* con servizi finanziari, assicurativi, di investimento e commerciali. I servizi PIS e AIS, meno remunerativi, fungono da porta d'ingresso per l'erogazione dei servizi a valore aggiunto.

Quando la prestazione dei servizi di PIS e AIS si rivolge a una clientela *retail*, i nuovi servizi di pagamento vengono prestati generalmente in modo gratuito. La redditività delle iniziative viene garantita:

- dal futuro aumento dei clienti dei servizi *core* già offerti (ad esempio i servizi non finanziari offerti dalla controllante di derivazione industriale ai propri clienti) grazie a un miglioramento della *user experience* o a nuove funzionalità collegate al servizio di accesso ai conti e di disposizione di ordini di pagamento;

- dalla clientela *corporate* convenzionata, alla quale è richiesto un canone periodico per poter integrare i servizi tra le proprie modalità di pagamento o nella propria offerta commerciale.

La prestazione dei servizi nei confronti della clientela *corporate* prevede generalmente la richiesta di un canone annuo fisso per il servizio di informazione sui conti e per il servizio di disposizione di ordini di pagamento; talvolta sono richieste anche commissioni fisse o variabili per singola disposizione. In alcuni casi i servizi di pagamento vengono prestati gratuitamente alle aziende e la redditività viene garantita dalla prestazione di servizi basati sull'elaborazione dei dati di conto.

Mediamente le iniziative dei nuovi intermediari (IP e IMEL) esaminate in fase di autorizzazione prevedono il raggiungimento del *break-even* tra il secondo e il terzo anno dall'avvio dell'iniziativa.

Tra le principali voci di costo dei modelli di *business* riferibili ai nuovi operatori (molti dei quali non hanno ancora, ad oggi, avviato alcuna operatività) figurano le spese di *marketing* e di comunicazione, i costi di *set-up* e di sviluppo dell'infrastruttura IT, queste ultime in media pari a € 331 mila nel primo anno di avvio dei servizi. I costi del personale hanno una minore incidenza, considerato che i nuovi operatori si avvalgono di strutture snelle, con un numero di addetti in genere inferiore alle 10 unità e con un ampio ricorso all'esternalizzazione di funzioni amministrative e di controllo. Mediamente l'indicatore *cost/income* per tali operatori risulta essere intorno al 60 per cento nel primo anno di avvio dei servizi, scendendo al 45 per cento al termine del primo triennio di attività.

Per quanto riguarda le estensioni dell'operatività, gli intermediari già presenti sul mercato dei servizi di pagamento stimano che l'introduzione dei servizi PIS e AIS avrà un impatto limitato sulla redditività complessiva del *business*, mediamente inferiore al 5 per cento. Per quanto poco remunerativo, l'ampliamento dello spettro

dei servizi a disposizione della clientela, attraverso l'erogazione dei servizi PIS e AIS è ritenuto comunque indispensabile per salvaguardare le proprie quote di mercato attraverso un maggiore *engagement* del cliente ed in prospettiva accrescerle. Tale considerazione è particolarmente valida per il servizio AIS, spesso utilizzato come veicolo da parte degli intermediari per la promozione o la commercializzazione di altre attività o servizi.

Questa impostazione sarebbe valida soprattutto per le banche: dopo gli investimenti tecnologici necessari per la predisposizione delle interfacce attraverso cui "aprire" i propri conti di pagamento, alcune banche, nel corso del 2020, hanno avviato iniziative per sfruttare commercialmente i nuovi servizi di pagamento. La strategia appare al momento ancora circoscritta all'offerta dei servizi AIS e PIS in modalità *standard* (cfr. *supra*) integrati all'interno dei siti *web* e delle *app* di *mobile banking*, già disponibili ai clienti della banca e spesso privi di funzionalità a valore aggiunto. I nuovi servizi consentono la visualizzazione dei dati associati a conti diversi oppure di effettuare pagamenti a valere su altri conti diversi da quelli della banca. In alcuni casi, i servizi informativi di base sono arricchiti da funzionalità che visualizzano l'andamento delle spese, da previsioni basate sui mandati di pagamento attivi sui conti correnti e da funzionalità del tipo PFM e BFM. Solo in un caso tali servizi sono stati lanciati con lo scopo di attrarre nuova clientela.

Per gli intermediari bancari il raggiungimento del *break-even point* non sembra essere il tema principale delle iniziative in questa prima fase: alcune banche prevedono di raggiungere il *break-even* non prima di cinque anni; altri operatori non hanno previsto una data di *break-even*; per altri ancora la redditività è valutata in termini di potenziale perdita di clientela nel caso di mancata realizzazione dei servizi di Open Banking.

In uno scenario in cui è ancora arduo identificare quelli che saranno i servizi di successo, gli intermediari *incumbents* "occupano le posizioni" al fine di non trovarsi impreparati allorquando si affermerà la soluzione tecnologica dei servizi Open Banking vincente nel medio-lungo termine (la cd. "killer application"). Gli intermediari pertanto investono nel paradigma Open Banking, estendendo le funzionalità già realizzate o sviluppando nuovi servizi, spesso stringendo collaborazioni con soggetti esterni, al fine di arricchire la propria offerta commerciale con più servizi e diverse esperienze di acquisto, non limitate a prodotti finanziari. In questo contesto, una possibile strategia adottata già da alcuni intermediari è improntata al concetto di ecosistema e *platformization*, quest'ultimo reso possibile dall'utilizzo diffuso delle API, che consente a un intermediario di arricchire e diversificare il portafoglio prodotti con i servizi di altri operatori.

Infine, anche dal confronto con i principali operatori esteri operanti in Italia, nel ruolo di fornitori tecnici specializzati nell'ambito dell'Open Banking o di PSP in regime di LPS, emerge che un obiettivo primario sia il raggiungimento di una quota di mercato significativa e, solo in una fase successiva, non ancora definita, il conseguimento di un risultato economico.

6. I RISCHI

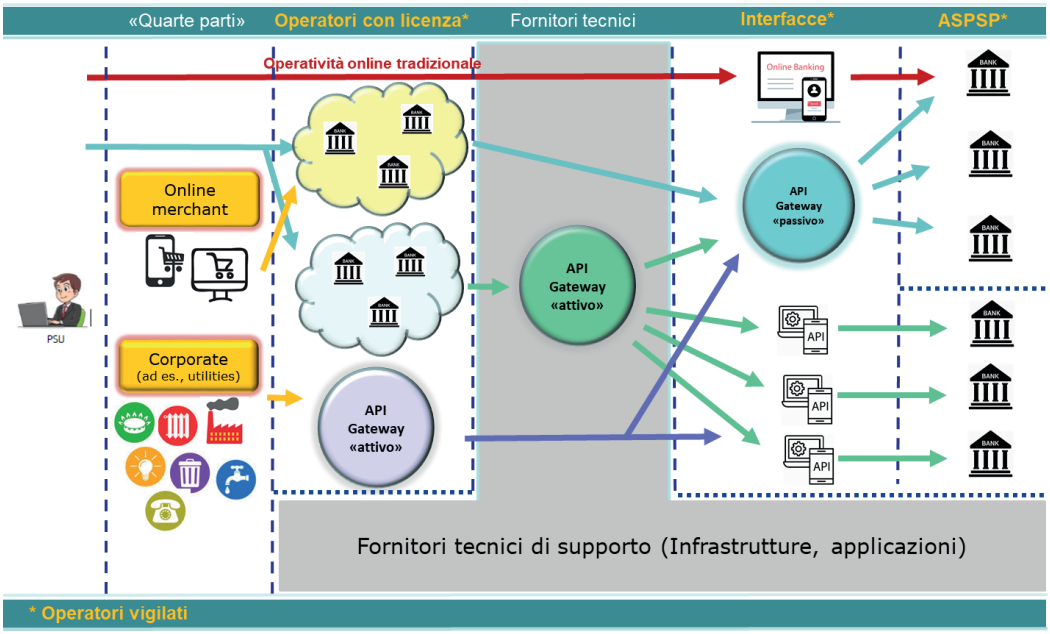
6.1 *I rischi tecnologici e di sicurezza*

Per valutare i rischi tecnologici e quelli di sicurezza associati al paradigma di Open Banking è utile preliminarmente rappresentare l'ecosistema che lo caratterizza.

A differenza di quanto accade nell'operatività bancaria tradizionale *on-line* in cui il cliente accede direttamente ai servizi esposti su *Internet* dall'intermediario, l'ecosistema Open Banking è caratterizzato dalla presenza di molteplici soggetti che si interpongono tra il cliente consumatore del servizio e l'intermediario presso cui è radicato il conto (Figura 1 – il collegamento tra cliente e ASPSP in alto nella figura rappresenta la modalità di accesso tradizionale all'*online banking*).

Figura 1

ARCHITETTURA DELL'ECOSISTEMA OPEN BANKING



La maggior parte degli ASPSP nel mercato italiano, al fine di soddisfare i requisiti previsti dalla PSD2, espone *on-line* i servizi bancari dei propri clienti adottando interfacce sviluppate da piattaforme sorvegliate ai sensi dell'articolo 146 del TUB (i cosiddetti *gateway* Open Banking "passivi"[19]); un numero limitato di ASPSP ha invece adottato proprie interfacce.

19) Tali piattaforme possono essere realizzate dallo stesso fornitore di servizi IT dell'ASPSP oppure da un soggetto diverso dal fornitore dei sistemi IT. In vece del termine di *gateway* "passivo" può trovarsi anche il termine "interfaccia inbound". I termini "passivo" o "inbound" stanno ad indicare che tali piattaforme hanno il ruolo di ricevere le chiamate che arrivano dai TPP e instradarle verso i sistemi degli ASPSP.

I TPP accedono alle interfacce degli ASPSP tramite propri protocolli di accesso oppure tramite i cosiddetti *gateway* "attivi"[20]. I *gateway* attivi rendono trasparente la comunicazione con le diverse interfacce di accesso agli ASPSP e instradano le istanze dei TPP verso le interfacce ovvero verso i *gateway* passivi. Gli operatori che offrono servizi di *gateway* "attivo" possono operare come meri fornitori di servizi tecnici, ma anche dotarsi di licenza AIS e/o PIS e relazionarsi con soggetti giuridici non vigilati (cd. "quarta parte"), offrendo servizi AIS/PIS ai clienti finali.

Il funzionamento di questo ecosistema è reso ulteriormente più complesso dalla presenza di TPP in libera prestazione di servizi, localizzati in altre giurisdizioni dell'Unione Europea, e delle *big-tech* per ora principalmente nel ruolo di fornitori di servizi tecnici[21]. La presenza di tali soggetti implica la possibilità che i dati dei clienti, prima residenti unicamente presso i *data-center* degli ASPSP italiani, possano essere memorizzati al di fuori del territorio nazionale ed eventualmente anche fuori della UE.

L'elevato grado di interconnessione tra soggetti numerosi ed eterogenei, eventualmente non vigilati, localizzati in paesi differenti e non necessariamente legati da accordi, estende la cosiddetta "superficie d'attacco disponibile" (*attack surface*), implicando un intrinseco aumento della vulnerabilità al rischio *cyber* del sistema nel suo insieme:

- il dato sensibile (o più precisamente una sua copia) associato al cliente, nel sistema bancario tradizionale localizzato presso i sistemi di un singolo ente, può essere ora memorizzato potenzialmente su una molteplicità di sistemi dell'architettura Open Banking;
- il servizio di disposizione di ordini di pagamento e le informazioni sui conti dei clienti transitano attraverso una molteplicità di sistemi.

È quindi sufficiente che uno solo dei nodi interessati sia vulnerabile perché:

- l'informazione sia acquisita da soggetti non autorizzati (rischio di perdita di riservatezza e/o integrità delle informazioni);
- un attaccante trovi un punto di accesso per realizzare la frode ("*single point of failure*");
- il servizio sia reso inutilizzabile (rischio di perdita di disponibilità, ad esempio, a causa di un attacco di tipo *Distributed Denial of Service*-DDOS[22]).

---

20) In vece del termine *gateway* "attivo" può trovarsi anche la denominazione "interfaccia outbound". I termini "attivo" o "outbound" stanno ad indicare che tali piattaforme hanno il ruolo di abilitare i TPP a instaurare la comunicazione con le diverse interfacce messe a disposizione dagli ASPSP.

21) La diffusione delle Big-Tech costituisce peraltro un elemento connotativo dell'attuale evoluzione dei servizi bancari.

22) Il termine *DOS - Denial of Service* (in italiano letteralmente negazione del servizio abbreviato in *DoS*) nel campo della sicurezza informatica indica un malfunzionamento dovuto ad un attacco informatico in cui si fanno esaurire deliberatamente le risorse di un sistema informatico che fornisce un servizio ai *client*, ad esempio un sito *web* su un *web server*, fino a renderlo non più in grado di erogare il servizio ai clienti richiedenti. In un attacco denial-of-service distribuito (attacco *DDoS - Distributed Denial of Service*), il traffico in entrata che inonda la vittima proviene da molte fonti diverse. Ciò rende effettivamente impossibile fermare l'attacco semplicemente bloccando una singola fonte.

Mentre la superficie di attacco disponibile a soggetti criminali si estende, è pure vero che, come sottolineato dalla BIS[23], i rischi tecnologici dell'Open Banking sono gli stessi tipici rischi di qualunque sistema ICT: il rischio di violazione dei dati, il rischio di uso improprio delle procedure e dei sistemi, il rischio di falsificazione, i rischi di disponibilità con attacchi *Denial of Service* (DOS) e DDOS, malfunzionamenti dei sistemi, problemi di *performance* delle procedure, attacchi *man-in-the-middle*[24], attacchi basati sulla compromissione delle credenziali e *IP address spoofing*[25]. Tali rischi, come sopra illustrato, sono amplificati dalla presenza di una pluralità di soggetti che concorrono alla erogazione dei servizi di pagamento, ma sono pure attenuati dai seguenti fattori:

- in principio, la Direttiva PSD2 ha creato un quadro regolamentare a presidio dell'interazione tra i vari soggetti e della sicurezza tecnica concernente attività che in precedenza potevano essere condotte da soggetti non autorizzati e sui quali non si applicavano pertanto i requisiti e i controlli di vigilanza;

- la presenza di enti vigilati (gli ASPSP e i TPP), tenuti entrambi a seguire le previsioni contenute nelle Disposizioni di vigilanza per le banche e nelle Disposizioni di vigilanza per IP e gli IMEL e nell'Unione Europea gli "Orientamenti sulla gestione dei rischi relativi all'ICT e di sicurezza", può rappresentare un duplice controllo sui servizi offerti al cliente, mitigando il rischio di frode (ad esempio, la disposizione di pagamento è monitorata sia dal TPP che dall'ASPSP);

- anche in presenza di "quarte parti" non vigilate (peraltro tenute alla salvaguardia dei dati sensibili dei clienti nell'ambito di esistenti regolamentazioni) è possibile per i TPP cooperanti con le "quarte parti" prevedere una serie di requisiti contrattuali che obblighino queste ultime a implementare livelli minimi di sicurezza in linea con quelli applicati dal soggetto vigilato (e quindi con la normativa di vigilanza vigente).

Unitamente ai rischi validi per ogni sistema ICT, si individuano i seguenti ulteriori punti di attenzione specifici dell'ecosistema Open Banking:

- in presenza di interazioni remote tra soggetti in generale privi di accordi prestabiliti, la corretta gestione del ciclo di vita dei certificati e delle chiavi (ad. esempio le *API Key*), utilizzate per l'identificazione dei soggetti coinvolti e la protezione delle comunicazioni, è un elemento fondamentale al fine di mitigare il rischio di frodi e attacchi *cyber*;

- la diffusa presenza delle API e di interazioni tra diverse APP mobili gestite da operatori distinti è un elemento che caratterizza il paradigma Open Banking. Il progetto di API e di modalità di interazione tra le diverse APP mobili secondo le *best practice* dello sviluppo del *software* sicuro rappresenta pure un elemento di base per garantire la sicurezza dell'ecosistema;

---

23) *Bank for international settlements*, "*Report on Open Banking and Application Programming Interfaces* (APIs)", novembre 2019.

24) Un tipo di attacco *cyber* in cui qualcuno segretamente ritrasmette o altera la comunicazione tra due parti che credono di comunicare direttamente tra di loro.

25) Un tipo di attacco *cyber* in cui viene falsificato l'indirizzo IP del mittente.

- il rischio di un "depotenziamento" delle procedure anti-frode (*Transaction Risk Analysis*), peraltro già noto in fase di definizione della normativa relativa all'Open Banking, derivante dall'interposizione del TPP tra il cliente e l'ASPSP. Tale interposizione potrebbe ridurre la capacità predittiva dei sistemi anti-frode degli ASPSP (i sistemi anti-frode si basano su informazioni associate al cliente, quali la localizzazione, l'utilizzo di uno specifico dispositivo, il *merchant*, ecc. che, nel caso di ordini di pagamento disposti tramite TPP, potrebbero non essere disponibili all'ASPSP per la specifica transazione) e rendere più facile il successo del tentativo di frode. D'altra parte, anche il TPP, che la normativa obbliga a realizzare un sistema di monitoraggio delle transazioni, potrebbe avere un insieme di informazioni solo parziale a supporto delle proprie procedure anti-frode rispetto all'ASPSP[26], in particolare quando è intermediato da una "quarta parte".

6.2 *I rischi operativi e reputazionali – le garanzie per danni arrecati nell'esercizio dell'attività*

Gli istituti di pagamento e di moneta elettronica che intendono prestare il servizio di disposizione di ordini di pagamento ovvero di informazione sui conti devono presentare la documentazione comprovante il possesso di una polizza di assicurazione della responsabilità civile o un'analoga forma di garanzia per i danni arrecati nell'esercizio dell'attività, unitamente alla comprova che le modalità con cui è stato calcolato il relativo importo minimo sono conformi a quanto stabilito dagli Orientamenti dell'EBA[27].

La polizza costituisce un presidio a fronte del rischio operativo cui sono soggetti i TPP: considerato che non entrano mai in possesso dei fondi della clientela, si è ritenuto eccessivo assoggettarli a requisiti prudenziali (che, tra l'altro, si basano sulla fattorizzazione di volumi di pagamento).

L'adeguatezza della polizza di assicurazione viene valutata sia in fase di accesso al mercato, sia a regime sulla base delle seguenti considerazioni:

1) l'oggetto deve espressamente indicare i rischi citati dall'Orientamento 1.2, lettere (a), (b) e (c), ovvero:

   a) nel caso di imprese che chiedono l'autorizzazione a offrire il servizio PIS, le responsabilità nei confronti del pagatore per le operazioni di pagamento non autorizzate e per la mancata esecuzione o l'esecuzione inesatta o tardiva delle operazioni di pagamento, nonché nei confronti dell'ASPSP per la mancata esecuzione o l'esecuzione inesatta o tardiva dell'operazione di pagamento, il diritto di regresso[28];

   b) nel caso di imprese che chiedono la registrazione per offrire il servizio AIS, le responsabilità nei confronti degli ASPSP o degli utenti dei servizi di pagamento

26) Si pensi al caso di un PISP, che non svolge anche servizi AIS e che pertanto non conosce lo storico delle transazioni del cliente e quindi lo storico delle sue transazioni sul quale costruire un sistema di rilevazione delle frodi.

27) EBA/GL/2017/08, "*Orientamenti sui criteri per stabilire l'importo monetario minimo dell'assicurazione per la responsabilità civile professionale o analoga garanzia a norma dell'articolo 5, paragrafo 4, della direttiva (UE) 2015/2366*", EBA, settembre 2017.

28) Responsabilità specificate negli articoli 73, 89, 90 e 92 della PSD2.

derivanti dall'accesso non autorizzato o fraudolento alle informazioni del conto di pagamento o dall'uso non autorizzato o fraudolento delle stesse;

c) nel caso di imprese che chiedono l'autorizzazione a offrire PIS e AIS, le responsabilità indicate sia al punto a) che al punto b);

2) scoperti, franchigie o massimali non devono esser tali da pregiudicare la capacità della società di far fronte ai rimborsi derivanti dalle richieste degli utenti o dei prestatori di servizi di pagamento di radicamento del conto[29)];

3) la polizza deve fornire copertura costante a fronte dei rischi assicurati, anche in caso di sostituzione della compagnia di assicurazione tra due periodi assicurativi, con particolare attenzione alla presenza di clausole di *claims made*, *loss occurance*[30)] o "regolazione premio"[31)] nella polizza.

Anche a fronte della stipula della polizza, residuano dei rischi in capo ai TPP. Nell'ambito della vigilanza sugli operatori, la Banca d'Italia pone particolare attenzione nel valutare la presenza di franchigie molto elevate nella polizza e la numerosità ed entità delle richieste di rimborso, da cui potrebbero derivare difficoltà finanziarie per il TPP.

Si segnala inoltre che, in base alla normativa vigente, il cliente deve rivolgersi all'ASPSP in caso di transazioni non autorizzate disposte dal PISP; l'ASPSP procede al rimborso e acquisisce il diritto di regresso nei confronti del TPP. In questo caso, l'incapienza della polizza potrebbe costituire un impedimento al rimborso dell'ASPSP, che quindi sopporterebbe una perdita economica. Nel caso di richieste di risarcimento per l'accesso non autorizzato o fraudolento alle informazioni del conto di pagamento o l'uso non autorizzato o fraudolento delle stesse, non esiste una disciplina normativa che stabilisca l'onere della prova o il diritto di regresso (come accade per il servizio PIS). Bisognerebbe quindi in via preliminare stabilire se un determinato danno lamentato dal cliente sia riferibile al TPP o all'ASPSP; l'onere del rimborso ricade sul TPP ovvero sull'ASPSP sulla base del riparto di responsabilità, con il conseguente impatto economico sulla polizza ovvero sulla dotazione patrimoniale del TPP e/o dell'ASPSP.

---

29) A tal fine, si richiede che l'istituto fornisca un'autovalutazione attestante la congruità delle clausole economiche previste nella polizza tenendo in considerazione i rischi che si prevede di assumere con la futura operatività e che scoperti, franchigie o massimali non siano tali da pregiudicare la capacità della società di far fronte ai rimborsi derivanti dalle richieste degli utenti o dei prestatori di servizi di pagamento di radicamento del conto. In aggiunta, si può richiedere alla società di valutare l'opportunità di introdurre meccanismi di monitoraggio nel corso del tempo dell'adeguatezza della polizza e del relativo massimale.

30) La clausola "claims made" implica che la richiesta di risarcimento dovrà esser presentata alla compagnia assicuratrice che risulta controparte contrattuale all'atto della richiesta medesima, ciò indipendentemente dal fatto che l'evento sia precedente alla data della stipula della polizza. In caso di clausola di "loss occurance" è la data di avvenimento dell'evento a determinare chi sarà l'assicuratore che dovrà risarcire il danno. Nel momento in cui la società decidesse di non rinnovare una polizza con clausola di "claims made" e attivarne una diversa, per non creare vuoti nel periodo assicurato la nuova polizza dovrà garantire copertura anche per gli eventi passati e non contenere la clausola "loss occurrance" altrimenti – in caso di ricevimento di una richiesta risarcitoria relativa ad un evento verificatosi prima del periodo di copertura della nuova polizza – la prima assicurazione potrebbe negare la copertura assicurativa per la tardività della richiesta rispetto al periodo assicurato e la seconda compagnia potrebbe declinare la propria responsabilità non essendosi verificato il sinistro nel periodo di copertura assicurativa.

31) Questa clausola comporta che la società assicurata comunichi periodicamente all'assicurazione gli elementi variabili stabiliti nel contratto (come ad esempio il fatturato) che saranno utilizzati per il ricalcolo del premio. In caso di mancata comunicazione l'assicurazione non avrebbe gli elementi informativi necessari per procedere al conteggio del premio che, qualora non pagato dall'assicurato, potrebbe comportare l'applicazione dell'art. 1901 del c.c. con conseguente sospensione dell'assicurazione. La società potrà essere invitata a chiedere alla compagnia assicurativa di escludere espressamente la sospensione prevista dall'art. 1901 del codice civile in caso di ritardo nella comunicazione periodica dei dati richiesti. In mancanza di tale modifica l'istituto dovrà quindi assicurare tempestivamente la comunicazione all'assicurazione dei dati variabili necessari per il conguaglio del premio al fine di evitare la sospensione della copertura assicurativa.

6.3 *La tutela dei clienti. Il presidio dei rischi approntato dalla PSD2: il regime di responsabilità dei PSP rispetto ad operazioni non autorizzate, la disciplina di trasparenza*

La PSD2 ha introdotto regole volte a tutelare l'utente dei servizi di pagamento rispetto all'utilizzo non autorizzato di informazioni o all'esecuzione di transazioni non autorizzate (per esempio, per i casi di accesso da parte di frodatori ai conti del cliente): viene inoltre definito il regime di responsabilità qualora nella prestazione del servizio di pagamento intervengano soggetti terzi (TPP) oltre al prestatore di servizi di pagamento di radicamento del conto (ASPSP).

Nel caso di operazioni che risultano disposte tramite il PISP, ma non autorizzate dal cliente[32] è previsto uno specifico riparto di responsabilità tra il PISP e l'ASPSP. In queste ipotesi, l'ASPSP è tenuto a rimborsare il pagatore e, per il recupero delle somme rimborsate all'utente finale, può agire in via di regresso nei confronti del PISP; quest'ultimo è tenuto a risarcire l'ASPSP a meno che non dimostri di non essere responsabile per l'operazione fraudolenta.

Relativamente ai servizi AIS, in caso di accesso non autorizzato ai conti dei clienti o di cessione non autorizzata di dati a terzi, rimangono ferme le responsabilità dell'AISP o dell'ASPSP nei confronti della clientela in relazione all'attività concretamente svolta. Su un piano generale, l'AISP è responsabile in caso di accesso ai conti in assenza di esplicito mandato conferito dal cliente, di accesso secondo modalità diverse rispetto alle pattuizioni contrattuali, nonché in caso di cessione a terzi di tali dati in mancanza di un preventivo esplicito consenso. L'ASPSP è invece responsabile nei confronti del cliente del mancato rispetto dell'obbligo di verifica della corretta identificazione e autenticazione dell'AISP al momento dell'accesso ai conti. Inoltre, l'ASPSP è chiamato a rispondere nei confronti del cliente anche nel caso in cui abbia consentito l'accesso all'AISP oltre quattro volte nell'arco di 24 ore (a meno che non risulti una diversa pattuizione contrattuale) o a seguito di revoca del consenso dell'utente.

Allo stato attuale, anche tenendo conto della limitata operatività del comparto, non sono emerse sostanziali criticità connesse a frodi o ad altri eventi avversi legati all'intervento di PISP e AISP nella prestazione di servizi di pagamento. Va comunque evidenziato che la presenza di più soggetti che intervengono nella prestazione del servizio di pagamento estende la c.d. "superficie di attacco" (cfr. *supra*) ed espone gli utenti finali a maggiori rischi potenziali (furto di dati o credenziali, frodi, ecc.).

Come già evidenziato, forme di tutela sono comunque previste per gli utenti finali in caso di operazioni fraudolente o di accesso non autorizzato ai propri dati e il quadro normativo prevede anche specifici obblighi in materia di trasparenza a carico degli intermediari che offrono i servizi AIS e PIS.

---

32) Uno specifico riparto di responsabilità è pure previsto per la mancata esecuzione o per l'esecuzione inesatta o tardiva delle operazioni di pagamento.

In termini generali, quando il servizio è prestato nell'ambito di un contratto quadro, per consentire alla clientela di conoscere preventivamente le condizioni applicate, l'intermediario deve mettere a disposizione del cliente un foglio informativo e consegnargli, prima della stipula del contratto, la copia del testo contrattuale. Gli operatori che offrono unicamente il servizio di informazione sui conti (AIS) sono tenuti al rispetto dei soli obblighi di informativa precontrattuale che, in questo caso, possono essere soddisfatti con modalità semplificate. Forme di informativa semplificata sono peraltro previste anche in caso di operazioni non rientranti in un contratto quadro.

Per il servizio PIS è inoltre previsto che prima della conferma di un ordine di pagamento, al cliente siano fornite informazioni sulle eventuali commissioni da riconoscere al prestatore del servizio di disposizione dell'ordine di pagamento (PISP); dopo l'esecuzione dell'operazione, il PISP deve fornire un'informativa circa il buon esito dell'operazione di disposizione, il riferimento univoco dell'operazione di pagamento e il relativo importo, nonché il riepilogo di tutte le eventuali commissioni pagate dall'utente a favore del PISP.

L'impianto previsto dalla normativa mira quindi ad assicurare un'informativa alla clientela più chiara e completa nelle diverse fasi che caratterizzano la prestazione del servizio. Limiti alla sua efficacia potrebbero derivare tuttavia dalle modalità prevalentemente digitali con cui i servizi sono offerti e che potrebbero rendere non particolarmente agevole la fruizione per la clientela – soprattutto su dispositivi mobili – delle informazioni precontrattuali, con possibili impatti anche in termini di comprensione e consapevolezza delle caratteristiche e degli obblighi derivanti dall'apertura del rapporto contrattuale.

I casi d'uso analizzati hanno inoltre evidenziato come l'offerta dei nuovi servizi AIS e PIS possa avvenire in maniera integrata nell'offerta commerciale di un altro prestatore di servizi di pagamento. In un contesto digitale, la descritta operatività – che si sostanzia nell'offerta di un prodotto di terzi sull'interfaccia digitale (*web*, *app*) della banca o altro PSP con il quale il cliente ha già un rapporto contrattuale – potrebbe rendere non particolarmente chiaro alla clientela il mero ruolo di intermediazione svolto dalla propria banca e che l'accesso al nuovo servizio comporta l'avvio di un rapporto con un operatore terzo. Ciò può aumentare il rischio reputazionale per gli intermediari, qualora questi ultimi non forniscano un'adeguata informativa alla clientela.

A tale dinamica potrebbe contribuire anche il fatto che spesso i servizi AIS e PIS sono offerti alla clientela gratuitamente in quanto gli intermediari e gli operatori *FinTech* mirano a generare redditività, piuttosto che dall'applicazione di commissioni/canoni, dallo sfruttamento dei dati ceduti dalla clientela. Quest'ultima, attratta dalla possibilità di disporre gratuitamente di nuovi servizi, potrebbe a sua volta non ponderare adeguatamente il valore delle informazioni che ha accettato di cedere o gli effetti che potrebbero derivare dalla suddetta cessione.

I dati ceduti potrebbero essere utilizzati dagli intermediari per l'offerta di prodotti personalizzati e maggiormente rispondenti alle esigenze finanziarie della clientela

ma anche per la proposta di servizi accessori di natura non finanziaria, ovvero per la costruzione di nuovi servizi da destinare a soggetti terzi. Delle possibili conseguenze sarebbe pertanto opportuno rendere adeguata informativa alla clientela. Sotto questo profilo, assume rilevanza anche l'esigenza di una adeguata alfabetizzazione finanziaria e digitale della clientela quale presidio fondamentale per evitare l'assunzione inconsapevole di rischi.

In aggiunta a una ripartizione della responsabilità e a specifici obblighi di trasparenza previsti per i servizi AIS e PIS, altra importante componente dell'attività di tutela è rappresentata dagli strumenti di *private enforcement* resi disponibili dalla Banca d'Italia per la tutela dei clienti degli intermediari bancari e finanziari, che trovano naturalmente applicazione anche con riferimento all'Open Banking. Anche per queste fattispecie il cliente finale potrà sia rivolgersi all'Arbitro Bancario Finanziario per la risoluzione delle controversie che potranno insorgere con gli intermediari, sia segnalare con un esposto alla Banca d'Italia comportamenti che ritengono irregolari o scorretti.

Sotto questo profilo l'attivazione degli strumenti di tutela potrebbe essere resa più difficoltosa per il cliente dalla non agevole individuazione dell'intermediario contro cui agire dovuta alla pluralità degli operatori coinvolti nella prestazione di tali servizi.

6.4 *Le interconnessioni tra normativa PSD2 e GDPR*

Il tema dell'utilizzo/sfruttamento dei dati personali va analizzato anche in relazione alle interconnessioni tra la normativa sui servizi di pagamento (PSD2) e la regolamentazione *privacy* (GDPR).

La PSD2 prevede che i dati acquisiti nello svolgimento dei servizi PIS e AIS non possano essere utilizzati dalle terze parti per finalità diverse da quelle funzionali allo svolgimento dei servizi di pagamento[33]. L'analisi dei modelli di *business* ha però evidenziato che, soprattutto nel caso di informazioni acquisite per lo svolgimento del servizio AIS, le informazioni in parola vengono utilizzate per finalità ulteriori e/o fornite a soggetti diversi dal titolare (sul punto si rinvia al paragrafo 5 "I modelli di *business*").

In tali casi è centrale la corretta acquisizione dei consensi del cliente finale da parte degli intermediari, distinguendo tra quelli rilasciati ai sensi della PSD2, per consentire l'accesso ai dati dell'utente da parte degli intermediari che offrono i servizi PIS e AIS, e quelli necessari ai sensi della normativa privacy (GDPR) per consentire la cessione alle "quarte parti" delle informazioni estratte o per elaborarli per finalità diverse da quelle del servizio di pagamento (ad esempio, *credit scoring*).

33) L'accesso ai conti di pagamento e l'uso delle informazioni sui conti di pagamento sono parzialmente regolamentati dagli art. 66 e 67 della PSD2, che contengono alcune garanzie in merito alla protezione dei dati personali. In particolare l'art. 66 lettera f) stabilisce che il PISP non deve richiedere dati diversi da quelli necessari per fornire il servizio all'utente e alla lettera g) prevede che i PISP non utilizzino, accedano o memorizzino dati per scopi diversi da quelli di esecuzione del servizio di disposizione esplicitamente richiesto dall'utente del servizio di pagamento. Tali previsioni sono previste specularmente per gli AISP all'articolo 67, dove la lettera d) prevede l'accesso esclusivo alle informazioni sui conti di pagamento designati e sulle operazioni di pagamento a questi associati, e la lettera f) impone l'obbligo di non utilizzo, accesso o conservazione dei dati per scopi diversi dall'esecuzione del servizio informativo esplicitamente richiesto dall'utente, in conformità alle norme sulla protezione dei dati.

Il tema è da tempo all'attenzione della comunità nazionale e internazionale. In particolare, la legittimità del trasferimento dei dati a soggetti terzi è stata oggetto di un parere dell'EBA[34] che ha esplicitamente consentito al trasferimento delle informazioni di conto anche a soggetti diversi dall'utente finale del servizio purché ciò avvenga nel rispetto delle previsioni del GDPR.

Rilevano inoltre le linee guida EDPB che forniscono orientamenti in merito all'applicazione del GDPR a questi nuovi servizi di pagamento, affrontando anche alcuni aspetti di intersezione con la disciplina di settore relativa al trattamento di speciali categorie di dati e ai consensi richiesti all'utente finale[35].

34) EBA Q&A id: 2018_4098 nella quale viene chiarito che: "Articles 4(16) and 67(1),(2) *PSD2 do not require that the account information service provider (AISP) provides the consolidated information to the payment service user (PSU) in order for the service to constitute an 'account information service' according to PSD2. The AISP may therefore transmit the consolidated information to a third party with the PSU's explicit agreement. Regarding the use made by any third party of the consolidated information transmitted, other provisions of EU law may apply, for instance the General Data Protection Regulation* (EU) 2016/679 (GDPR)."

35) "*Guidelines on the interplay on the second payment service directive on the GDPR*", pubblicate dall'European Data Protection Board (EDPB) a dicembre 2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-062020-interplay-second-payment-services_en.

7. CONCLUSIONI

L'Open Banking rappresenta un paradigma solo di recente introdotto nel mercato italiano che, anche per il suo carattere innovativo, pone diversi punti di attenzione per la vigilanza bancaria e finanziaria. Di seguito si desidera mettere in evidenza alcuni degli elementi di maggior interesse dal punto di vista della vigilanza emersi in questa prima fase di analisi ed evidenziati nei paragrafi precedenti.

L'affermazione dei nuovi modelli di *business* associati all'Open Banking rappresenta un elemento chiave per il successo del comparto nel suo insieme e degli intermediari che hanno investito in esso. È interesse di tutti gli *stakeholder* comprendere i modelli che si stanno proponendo e quelli che effettivamente troveranno l'apprezzamento del mercato.

È pure fondamentale per l'autorità di vigilanza seguirne la sua rapida evoluzione per meglio comprendere e mitigare i rischi che esso comporta.

I rischi tecnologici non presentano specificità non presidiate dalla corrente regolamentazione. Tuttavia, va considerato il presumibile futuro andamento esponenziale che caratterizzerà questi servizi e le già complesse nuove interconnessioni stabilite tra gli intermediari finanziari e tra questi ed altri operatori non vigilati.

Il conseguente ampliamento della superficie esposta a minacce tecnologiche potrebbe essere più che proporzionale, rivelando una componente sistemica, legata alle crescenti interazioni tra gli operatori coinvolti. Complice la ridotta scala dell'operatività, non sono emerse finora particolari criticità, che potrebbero tuttavia manifestarsi con una certa virulenza non appena l'Open Banking raggiunga una soglia critica.

Analoghe considerazioni possono essere avanzate anche per la tutela della clientela, dove il basso livello di rischio finora osservato con riguardo ai servizi AIS e PIS riflette essenzialmente lo stadio embrionale del comparto. Emerge come i profili riguardanti la tutela della clientela saranno influenzati non solo dalle modalità innovative con cui verranno offerti i servizi di pagamento e finanziari, ma anche dall'affermarsi di politiche commerciali sempre più orientate al *cross-selling*, anche intersettoriale (finanziario e commerciale), e di modelli di *business* basati sulla compresenza di molteplici operatori che collaborano per la definizione e l'offerta di nuovi servizi.

Il presente documento si è principalmente concentrato sui servizi di pagamento introdotti dalla PSD2. Considerati gli ampi e diversificati rami evolutivi dell'Open Banking, ulteriore spazio di indagine potrà essere indirizzato in futuro a quei servizi che, sebbene non direttamente regolati dalla PDS2, faranno leva sulle opportunità tecnologiche e informative che caratterizzano l'Open Banking e che vanno anche al di là dei servizi di pagamento (ad esempio, la cd. *open finance*, oggetto di rilevante interesse sia da parte degli enti regolatori che del mercato).