BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

L'Open Banking nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza

di Roberto Pellitteri, Ravenio Parrini, Carlo Cafarotti
e Benedetto Andrea De Vendictis

Marzo 2023

Numero 31

BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento
(Markets, Infrastructures, Payment Systems)

Questioni istituzionali
(Institutional Issues)

L'Open Banking nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza

di Roberto Pellitteri, Ravenio Parrini, Carlo Cafarotti
e Benedetto Andrea De Vendictis

Numero 31 – Marzo 2023

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

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

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

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

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

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

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

L'Open Banking nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza

di Roberto Pellitteri*, Ravenio Parrini**, Carlo Cafarotti** e Benedetto Andrea De Vendictis***

JEL: G18, O31, O33.
Parole chiave: PSD2, open banking, sistema dei pagamenti, supervisione, vigilanza, soluzioni di sistema.

INDICE

* Banca d'Italia, Dipartimento Mercati e sistemi di pagamento.
** Banca d'Italia, Dipartimento Circolazione e pagamenti al dettaglio.
*** Banca d'Italia, Dipartimento Vigilanza bancaria e finanziaria.

Sintesi

Il termine *open banking* si riferisce alla possibilità che terze parti accedano a dati e informazioni relativi ai conti correnti tenuti presso le banche dai clienti, con l'assenso di questi ultimi, al fine di fornire loro nuovi servizi e applicazioni. Il lavoro illustra le caratteristiche dell'*open banking*, il suo impatto sul mercato italiano dei pagamenti e le conseguenti modifiche nelle procedure di vigilanza e sorveglianza che regolano le relazioni dell'autorità finanziaria con i nuovi attori della catena dei pagamenti e assicurano il mantenimento nel tempo dell'equilibrio complessivo del sistema. Nel mercato italiano, a seguito dell'applicazione della normativa comunitaria stabilita nella Direttiva PSD2, le interfacce predisposte dai prestatori di servizi di pagamento per consentire l'accesso di terze parti fanno prevalentemente leva su soluzioni di sistema, infrastrutture tecniche che realizzano un unico punto di accesso per una pluralità di intermediari. L'Autorità nazionale competente, nelle sue funzioni di vigilanza e supervisione, ha sviluppato inoltre un sistema dei controlli che tengono conto delle nuove caratteristiche del mercato, fortemente innovative. L'attività di sorveglianza prevede inoltre la raccolta di dati statistici per il monitoraggio dei profili di efficienza, affidabilità, sicurezza e conformità delle soluzioni di sistema, consentendo l'elaborazione di indicatori utili per valutare l'evoluzione del mercato nazionale.

Introduzione

Nell'ambito del sistema dei pagamenti l'*open banking*, avviatosi in Italia nel 2019 con l'entrata in vigore della direttiva (UE) PSD2 (2015/2366)[1], determina una discontinuità rispetto al tradizionale modello di sviluppo dei servizi di pagamento, che è basato sulla cooperazione, l'autoregolamentazione dei partecipanti, l'interoperabilità tecnica delle soluzioni sviluppate e l'adesione a schemi e infrastrutture multilaterali comuni. L'*open banking* sancisce, infatti, l'apertura del sistema dei pagamenti ad attori esterni che possono operare a valere sull'infrastruttura bancaria esistente anche a prescindere dall'esistenza di accordi, multilaterali o bilaterali, con le singole banche, nel quadro di diritti e obblighi definiti dal legislatore[2].

L'*open banking* supera il tradizionale modello di utilizzo del dato all'interno del perimetro del singolo intermediario bancario e amplia le dimensioni del sistema poiché incrementa sia il numero di punti di accesso sia la platea dei soggetti che possono accedere, utilizzare e, nei limiti imposti dalla normativa, rielaborare i dati dei conti di pagamento per offrire nuovi servizi. Di conseguenza diventa necessario fornire, già nella normativa primaria, indicazioni che permettano di attuare tale cambiamento mantenendo l'ecosistema stabile e resiliente e consentendo a tutti i soggetti coinvolti di operare con sicurezza ed efficienza.

L'*open banking* comporta la necessità, per l'Autorità di regolamentazione e controllo, di rimodulare le proprie prassi nel duplice obiettivo di favorire da un lato, anche in un'ottica europea, l'offerta dei nuovi servizi da parte del mercato e dall'altro di adattare le tradizionali metodologie di sorveglianza/vigilanza ai peculiari rischi connessi con il nuovo ambiente e alle specificità di nuovi sistemi e infrastrutture come le cosiddette piattaforme di sistema[3].

Il presente lavoro si propone di illustrare le caratteristiche peculiari dell'*open banking* e i cambiamenti che esso ha introdotto nel mondo dei pagamenti (da un punto di vista funzionale e di servizio e dal punto di vista delle tecnologie utilizzate per sviluppare i casi d'uso principali) così come nelle prassi di vigilanza e sorveglianza.

Il lavoro è articolato come segue. Nella prima parte viene analizzato il nuovo paradigma dell'*open banking* con riferimento ai suoi aspetti tecnologici e normativi più rilevanti. Nella sezione successiva si esaminano le caratteristiche dell'*open banking* all'interno del mondo dei pagamenti, prendendo in considerazione specificamente il mercato italiano. Nella terza parte vengono illustrate le funzioni svolte nell'ambito della vigilanza e sorveglianza sui soggetti rientranti nelle prescrizioni normative della PSD2. Segue un focus sull'evoluzione dell'*open banking* in Italia nei suoi primi anni di attività. Nelle conclusioni vengono infine proposti alcuni spunti sul ruolo attuale e futuro delle autorità pubbliche, nella prospettiva di un mercato dei pagamenti sempre più digitalizzato e aperto ad attori a forte connotazione tecnologica.

---

1 Direttiva 2015/2366 del Parlamento Europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno (https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015L2366&from=IT).

2 Cfr. Gammaldi e Iacomini (2019).

3 Si tratta di infrastrutture tecniche di supporto in grado di fornire servizi bancari mediante l'utilizzo di interfacce sviluppate con tecnologie specifiche (*Application Programming Interface* – API); ogni piattaforma consente di connettersi a una pluralità di intermediari attraverso un unico punto di accesso.

1. Il nuovo paradigma

Secondo la definizione della *Bank of International Settlements* (BIS)[4], con il termine "*open banking*" si intende una forma di "*condivisione e sfruttamento dei dati autorizzata dai clienti da parte delle banche con sviluppatori e aziende di terze parti per costruire nuovi servizi e applicazioni, come quelli che offrono pagamenti in tempo reale, maggiori possibilità di trasparenza finanziaria per i titolari di conti e opportunità di marketing e cross-selling*".

La condivisione dei dati dei clienti con soggetti terzi da parte delle banche[5] è un fenomeno presente nel settore finanziario da diversi anni e che ha subito un'accelerazione con il diffondersi delle tecnologie digitali, in particolare con l'avvento dell'*on-line banking* e del *mobile banking*. In questo nuovo schema la fornitura di servizi finanziari ai clienti, in passato integrata verticalmente nell'offerta della banca presso cui l'utente aveva aperto il proprio conto di pagamento, viene ora disaggregata e offerta anche da terze parti, come le società *fintech*, non necessariamente appartenenti al settore bancario. Allo stesso tempo queste terze parti, grazie al patrimonio informativo cui possono accedere, offrono nuovi servizi agli utenti, aggiungendo valore alla catena di distribuzione; ne sono un esempio i servizi di pagamento, le procedure di aggregazione per i titolari di conto[6] e processi di *cross-selling*[7]. Le stesse funzioni dispositive del conto del cliente possono diventare oggetto di condivisione, offrendo alle terze parti l'opportunità di disegnare

COS'È L'OPEN BANKING

Nel 2015, la Direttiva europea sui Servizi di Pagamento (PSD2) ha aperto la strada all'*open banking*, una forma di condivisione di dati grazie alla quale soggetti autorizzati possono interagire per creare valore aggiunto nell'ambito dei servizi di pagamento. Il cliente può concedere l'accesso al patrimonio informativo legato ai propri conti di pagamento a soggetti diversi dal proprio intermediario, al fine di utilizzare nuovi servizi, fatti salvi tutti i presidi di tutela previsti dalla normativa di settore.

---

4 Cfr. *BIS - Report on Open Banking and application programming interfaces* - November 2019. https://www.bis.org/bcbs/publ/d486.pdf: "*open banking – the sharing and leveraging of customer-permissioned data by banks with third party developers and firms to build applications and services, such as those that provide real time payments, greater financial transparency options for account holders, and marketing and cross-selling opportunities*".

5 Per facilità di esposizione, nel seguito ci si riferirà alle banche quali prestatori di Servizio di Pagamento di 'radicamento' del conto (ASPSP), cioè come i soggetti presso i quali la clientela ha aperto il conto oggetto dell'*open banking*. È importante rammentare che, oltre alle banche, possono essere prestatori di servizi di pagamento di radicamento del conto anche gli istituti di pagamento (IP) e gli istituti di moneta elettronica (IMEL).

6 Servizi di aggregazione dati consentono ad esempio di: i) predisporre quadri di riepilogo situazione finanziaria di utente con più conti, scadenzari e riconciliazione fatture, ii) fornire modalità di pianificazione spese e risparmi, iii) effettuare servizi di *credit scoring* a supporto di altri servizi di finanziamento.

7 Sulla base delle informazioni sui conti, ad esempio, è possibile individuare le abitudini finanziarie del cliente e offrire a quest'ultimo servizi/prodotti specificatamente disegnati (ad es. soluzioni per la gestione del risparmio o proposte di *lending* e di servizi di consulenza). In questo caso il servizio di base di aggregazione dei dati funge da punto di contatto con il cliente per offrire un ventaglio di servizi più ampio.

una offerta di servizi di pagamento articolata e innovativa (es: pagamenti con *e-banking* per acquisti tramite il web, gestione integrata fatture e pagamenti, soluzioni corporate).

Facendo leva sul principio di condivisione delle informazioni tra soggetti non necessariamente legati da accordi prestabiliti, l'*open banking* pone due aspetti da affrontare: uno di tipo tecnico-operativo, legato alle modalità di accesso all'informazione sull'utente detenuta dalla banca e l'altro di tipo normativo connesso con la regolamentazione dei processi di accesso e condivisione dei dati.

In relazione al primo aspetto, nei servizi di *open banking*, i clienti bancari concedono il permesso di accedere *on-line* alle proprie informazioni e/o servizi bancari a società terze. Prima che tali servizi fossero regolati, le terze parti utilizzavano, per accedere ai conti disponibili *on-line* dei clienti, tecniche che presentano molteplici fattori di rischio in termini di sicurezza e di conservazione dei dati. A livello globale le autorità, gli intermediari e gli altri operatori di settore hanno tentato di superare tali rischi e limiti ricorrendo a tecnologie alternative quali le *Application Programming Interface* (API) e l'autenticazione "tokenizzata"[8]. Con l'introduzione delle API i limiti di efficienza e di sicurezza posti dalle vecchie tecnologie risultano mitigati e si ottiene un maggior equilibrio tra ruoli e responsabilità delle parti coinvolte nei servizi di pagamento: da un lato le terze parti dispongono di una limitata visibilità sui dati del cliente, dall'altra beneficiano di risparmi nello sviluppo delle proprie applicazioni grazie ad una maggiore stabilità delle interfacce API rispetto alle vecchie procedure. L'adozione di modelli di autenticazione "tokenizzata" inoltre libera le terze parti dalle problematiche di gestione delle credenziali del cliente.

Per quanto riguarda gli aspetti normativi, l'accesso ai dati bancari dell'utente da parte di soggetti terzi, previo consenso, viene generalmente regolamentato o quantomeno controllato dalle autorità. Diverse istituzioni nazionali e internazionali hanno intrapreso azioni specifiche relative all'*open banking* adottando in alcuni casi schemi normativi (cd. "*open banking frameworks*") per facilitare, consentire o imporre alle banche di condividere dati con le terze parti, a valle del consenso dei clienti. Nelle diverse giurisdizioni tali quadri regolamentari[9] possono differire per estensione dei dati trattati e per tipologia di previsioni: ad esempio, la PSD2 riguarda unicamente l'acquisizione dei dati di pagamento e la disposizione di operazioni di pagamento; nel Regno Unito include anche informazioni accessorie[10]; in Australia è consentita solo la lettura dei dati per la loro aggregazione, eventualmente condivisi con altri settori commerciali (ad es. *utilities*). I quadri normativi possono inoltre includere elementi riguardanti diversi aspetti quali ad esempio: l'abilitazione

---

8 Per un approfondimento su tali aspetti e sulle innovazioni tecnologiche si veda le appendici A.1, A.2 e A.3.

9 Le regolamentazioni possono includere, oltre agli aspetti normativi, anche *standard* e *best practices* di settore, articolati e riferiti a contesti più o meno ampi, coinvolgendo talvolta più autorità di regolamentazione, specie nel caso in cui le terze parti cedano dati dei clienti a soggetti non regolamentati (cd. quarte parti).

10 Il regolamento e gli *standard* dell'iniziativa inglese sono disponibili al link: https://standards.openbanking.org.uk/customer-experience-guidelines.

dell'accesso di terzi ai dati del cliente, la richiesta di licenze o autorizzazioni per soggetti terzi, l'imposizione di restrizioni a pratiche tecnologiche che presentano rischi elevati in termini di sicurezza dei dati del cliente, l'attuazione di misure di protezione della *privacy* e requisiti per la divulgazione dei dati e la gestione del consenso. Gli assetti normativi possono talvolta contenere anche disposizioni relative alla possibilità da parte di soggetti terzi di condividere e/o rivendere i dati a "*quarte parti*"[11], utilizzare i dati per scopi oltre il consenso originale del cliente e disciplinare gli aspetti legati alla remunerazione del servizio di condivisione dei dati.

In tutte le giurisdizioni comunque sono state elaborate una serie di tutele a difesa del cliente dell'*open banking* con importanti implicazioni per le diverse autorità di settore, le quali possono: fissare requisiti e svolgere controlli su banche e prestatori di servizi di pagamento, stabilire standard e certificare le entità che li rispettano, vigilare e promuovere interventi per garantire la concorrenza nei mercati e proteggere i consumatori da atti o pratiche sleali o ingannevoli, definire obblighi per la tutela dei dati personali dei clienti e fornire piattaforme e processi per mediare le controversie tra consumatori e organizzazioni.

2. L'*OPEN BANKING* NELLA NORMATIVA EUROPEA E LE SUE APPLICAZIONI NEL MERCATO ITALIANO

L'*open banking* mette parzialmente in discussione alcune delle caratteristiche del sistema dei pagamenti "tradizionale", tra cui la cooperazione e gli accordi multilaterali, l'interoperabilità tecnica e le economie di rete.

Nell'impostazione tradizionale il corretto funzionamento di un sistema dei pagamenti richiede ai partecipanti una stretta collaborazione e accordi vincolanti. Come è tipico per le economie di rete, benefici comuni derivano dall'adozione di infrastrutture e *standard* condivisi, mentre possibili conflitti di interesse possono minare l'efficienza complessiva del sistema.

In Italia, fin dagli anni Ottanta dello scorso secolo, la cooperazione tra tutti gli attori interessati[12] ha reso possibile lo sviluppo di una solida architettura di reti e procedure per lo scambio di informazioni e il regolamento dei pagamenti al dettaglio. La realizzazione della rete interbancaria, così come lo sviluppo delle procedure applicative a supporto dei servizi di bonifico e di addebito diretto e del circuito nazionale delle carte di debito, sono il risultato del lavoro di sedi di coordinamento strutturate[13] e della stesura di complessi accordi multilaterali, che disciplinano le funzionalità dei servizi

---

11 Esempi di "quarte parti" possono essere i soggetti specializzati in servizi di valutazione dell'affidabilità creditizia della clientela, ad esempio per la concessione di prestiti: le quarte parti, attraverso accordi con le terze parti e dietro consenso del cliente, possono accedere al conto di pagamento del cliente per recuperarne lo stato e la storia finanziaria ed effettuarne poi la stima del profilo di rischio.

12 Banche centrali, intermediari finanziari e gestori dei sistemi e infrastrutture tecniche di pagamento.

13 Tra queste rilevano i gruppi di lavoro della Convenzione Interbancaria per l'Automazione (CIPA), organismo di cooperazione tecnica costituito nel 1968 su iniziativa della Banca d'Italia, dell'ABI e delle principali banche nazionali.

di pagamento di base. Analogamente, negli anni 2000 sono state sviluppate le diverse componenti dell'area unica dei pagamenti in euro (*Single Euro Payments Area*, SEPA), che prevede, stavolta su scala europea, sedi di *governance* dedicate, accordi tra i partecipanti, reti di collegamento per lo scambio delle informazioni, per la compensazione e il regolamento dei pagamenti.

Su tale percorso, l'introduzione con la PSD2 dell'*open banking* rappresenta un momento di forte innovazione[14].

A differenza delle esperienze di altre giurisdizioni, il legislatore comunitario ha adottato un approccio prescrittivo[15] (cfr. sezione in appendice A.2), imponendo a tutti i prestatori di servizi di pagamento che gestiscono conti per la clientela di consentire l'accesso a terze parti per l'avvio di pagamenti o per l'elaborazione di informazioni aggregate. Come si può ricostruire dagli atti preparatori della direttiva, l'operazione nasce in primis dall'esigenza di promuovere maggiore concorrenza in un mercato dei pagamenti e degli altri servizi finanziari *on-line* fortemente concentrato su un limitato numero di prodotti e di operatori, come quelli del mondo delle carte; inoltre il legislatore ha inteso prendere atto dell'esistenza di servizi tecnologicamente evoluti, ormai diffusi anche in campi diversi da quello dei pagamenti, che dovevano essere opportunamente regolamentati per garantire una migliore protezione del consumatore, nonché valorizzati per un migliore sviluppo del settore.

Questo approccio consente di promuovere l'innovazione, la concorrenza e le tutele in un settore, quello dei pagamenti, per sua natura tendenzialmente oligopolistico. Esso tuttavia genera anche nuove complessità da gestire: sovrappone infatti all'architettura esistente un nuovo strato di offerta di servizi e forme di interazione obbligatorie tra terze parti e prestatori di servizi di pagamento di radicamento del conto, in assenza di procedure e regole operative concordate e di un quadro di standardizzazione consolidato. Le banche sono tenute ad accettare le richieste di accesso di tali soggetti terzi autorizzati, salvo che vi siano ragioni oggettive per non farlo (ad es. rischio di frode).

Il nuovo modello di *open banking* implica la modifica delle condizioni normative, tecniche ed economiche che governavano le relazioni tra i vari elementi della catena dei pagamenti e rende necessarie misure che assicurino il mantenimento nel tempo dell'equilibrio complessivo del sistema.

Queste misure devono essere volte a: i) definire un quadro normativo certo per tutti i soggetti coinvolti nella prestazione dei servizi di pagamento, ii) promuovere *standard* di mercato e sedi di confronto stabili tra le parti interessate, iii) adeguare le modalità di monitoraggio e supervisione in modo da tener conto dei nuovi rischi.

---

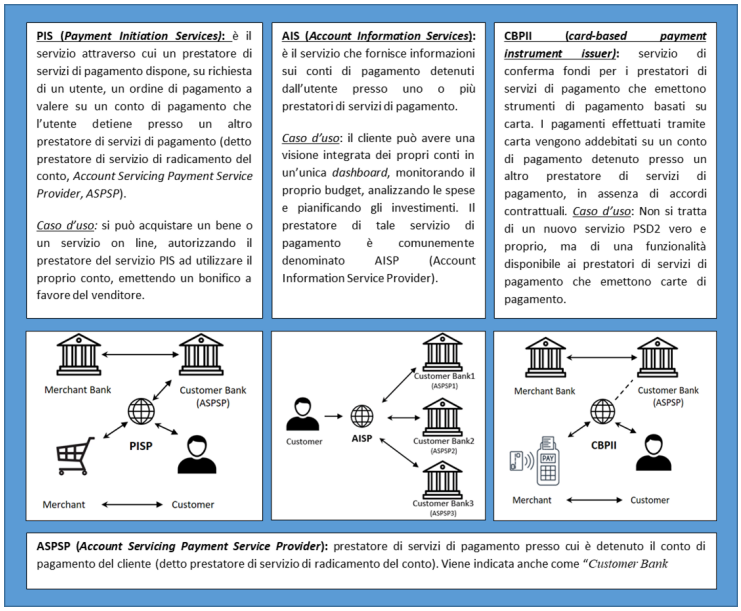
[14] Per una prima disamina delle molteplici novità introdotte dall'*open banking* nell'Unione europea, in una prospettiva interdisciplinare tra diritto, economia e finanza, si veda l'introduzione curata da Maimeri e Mancini (2019) a una raccolta di saggi di esperti della Banca d'Italia e dell'accademia.

[15] Approcci diversi sono quelle rinvenibili negli Stati Uniti, Singapore, Hong Kong e Nuova Zelanda.

2.1. La normativa europea

Nell'Unione europea la seconda direttiva sui servizi di pagamento (Direttiva UE 2015/2366), nota come PSD2, ha abilitato nuovi modelli di servizio di *open banking* (cfr. figura 1), grazie ai quali il cliente[16] di un prestatore di servizi di pagamento presso cui è aperto un conto *on-line* (*Account Servicing Payment System Provider* – ASPSP) può utilizzare una terza parte autorizzata (*Third Party Provider* – TPP) che può operare come fornitore di servizi di disposizione di ordini di pagamento (*Payment Initiation Services Provider* – PISP) per avviare pagamenti a valere sul proprio conto on-line oppure come fornitore di servizi di informazioni sui conti *on-line* (*Account Information Services Provider* – AISP) detenuti presso più prestatori di servizi di pagamento (ASPSP). Tali servizi, erogati esclusivamente *on-line* al cliente da una terza parte (TPP), presentano aspetti di complementarietà: il servizio fornito dal PISP ha carattere unicamente dispositivo (il cliente può fare un pagamento ma non visualizzare i dati del proprio conto durante l'operazione) mentre il servizio erogato dall'AISP ha carattere espressamente informativo (il cliente può visualizzare i dati del proprio conto ma non ha la possibilità di disporre un pagamento). Oltre ai servizi AIS e PIS, la PSD2 definisce una terza tipologia, il cd. "*Card-based payment instrument issuer*" o CBPII[17], che non è a rigore un nuovo servizio finanziario ma una nuova funzionalità, attraverso cui un intermediario che dispone della licenza PSD2 per gestire carte di pagamento (*card issuer*) è in grado di autorizzare pagamenti senza avere il controllo del conto del cliente o conoscere le sue disponibilità finanziarie. A titolo di esempio, questa funzionalità consente al CBPII, in fase di autorizzazione di un pagamento su un POS, di ricevere dall'ASPSP conferma o meno della disponibilità di fondi sul conto del cliente, senza conoscerne esattamente il saldo.

Figura 1 – Attori dell'open banking



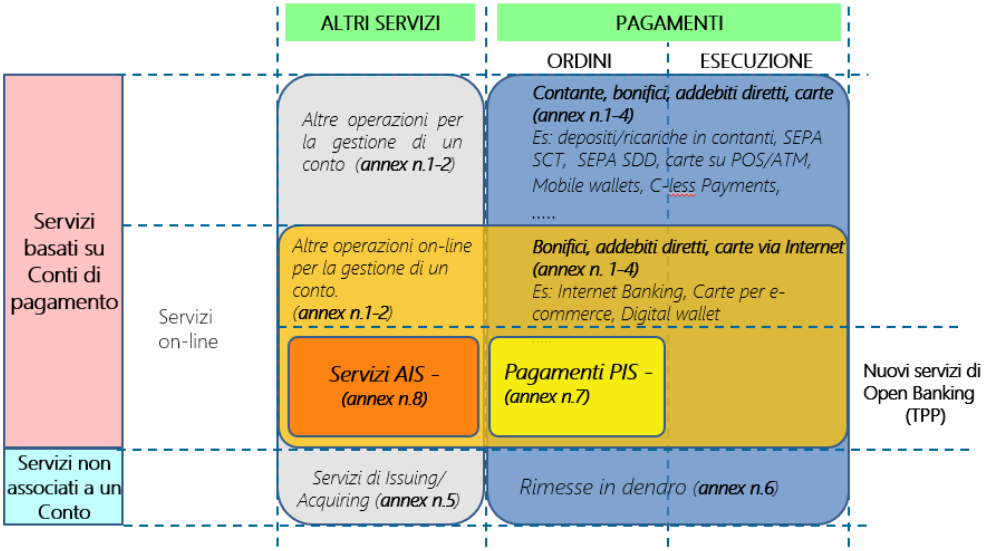
16 Spesso indicato come *Payment Service User* (PSU).

17 Il CBPII viene anche definito con altri acronimi, quali provider del servizio CIS (*Card Initiated Service*), CISP (*Card Issuers Service Provider*) o anche PIISP (*Payment Instrument Issuer Service Provider*).

La PSD2 riconduce nel perimetro normativo i soggetti TPP (che già in precedenza operavano ma senza essere "regolamentati"), che ora devono disporre di una licenza finanziaria ed essere sottoposti a Vigilanza.

Nella figura 2 i due nuovi servizi di pagamento vengono messi a confronto con quelli più tradizionali, secondo le due caratterizzazioni di *valenza dispositiva* e di associazione a un *conto di pagamento*; viene anche riportato il riferimento all'allegato alla direttiva dove sono descritti gli otto servizi di pagamento sottoposti a regolamentazione (cfr. PSD2, *Annex I*).

Figura 2 – I nuovi servizi di open banking nell'ambito dei servizi di pagamento previsti dalla PSD2



La PSD2 e la connessa normativa attuativa – i cd. *Regulatory Technical Standards* (RTS), predisposti dalla European Banking Authority (EBA) e adottati dalla Commissione Europea[18] – sono entrate in vigore il 14 settembre 2019. A partire da tale data i prestatori di servizi di pagamento (*Payment Service Providers* – PSPs) che mettevano a disposizione conti on-line per i propri clienti hanno dovuto consentire l'identificazione e la comunicazione sicura con i TPP mediante: i) adeguamento delle interfacce già utilizzate dai clienti oppure ii) predisposizione di un'interfaccia dedicata all'accesso dei TPP, secondo la tecnologia delle API. Nel contesto nazionale, come dettagliato nel paragrafo 2.2, la maggior parte degli intermediari ha realizzato l'interfaccia sotto forma di infrastrutture centralizzate (soluzioni "di sistema").

Nel caso di adozione di un'interfaccia dedicata, gli ASPSP devono anche predisporre un'interfaccia alternativa (cd. "soluzione di *fall-back*") da utilizzare in caso di indisponibilità dell'interfaccia principale, oppure richiedere alle autorità l'esenzione da tale obbligo (nota come *fall-back exemption* – cfr.

[18] Cfr. European Banking Authority (2018a) – Regolamento delegato della Commissione del 27 novembre 2017 n. 2018/389 riguardante le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli *standard* aperti di comunicazione comuni e sicuri previsti dall'articolo 98, paragrafo 4, della direttiva 2015/2366/UE (PSD2).

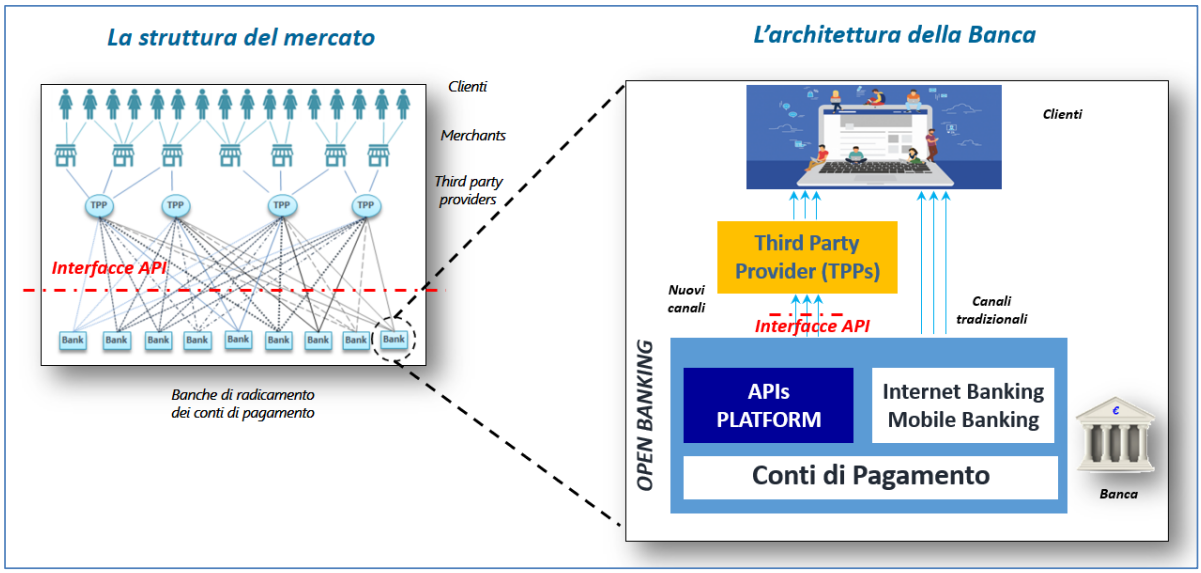
sezione in appendice A.4); in tale ultima evenienza, al fine di ottenere l'esonero occorre dimostrare che l'interfaccia dedicata rispetta i requisiti di *performance* e robustezza definiti nella normativa dell'EBA.

Le previsioni della PSD2 inducono una revisione profonda dell'infrastruttura tecnologica sottostante il sistema dei pagamenti elettronici, soprattutto nelle componenti di *internet banking*. I nuovi servizi, che consentono, tra l'altro, l'uso di pagamenti di *internet banking* nel settore dell'*e-commerce*, spingono il mercato verso una architettura operativa in cui la relazione cliente-esercente-banca viene in alcuni casi intermediata dai nuovi TPP. Questi soggetti, ovvero le loro applicazioni, consentono di effettuare il pagamento senza la necessità che vi sia alcuna relazione contrattuale tra la banca del cliente e i vari *merchant*. Allo stesso tempo le banche, con l'apertura delle interfacce API su Internet, devono rivedere i processi operativi interni consentendo l'accesso ai dati del cliente attraverso una sorta di doppio canale: da un lato, permettono al cliente di accedere direttamente al proprio conto di *internet banking*, dall'altro rendono disponibile l'accesso ai TPP, la cui identità è oggetto di specifici controlli. Nella figura 3 è illustrato un modello riassuntivo delle nuove architetture generate dalle previsioni normative in tema di *open banking*.

LA NORMATIVA DI SETTORE

L'*open banking* in Italia è disciplinato da una normativa articolata a più livelli fondata sulla direttiva adottata il 25 novembre 2015 (PSD2) e recepita dal Decreto legislativo del 15 dicembre 2017 che modifica il Testo Unico Bancario (TUB). Nello stesso periodo, la Commissione Europea ha dettagliato, nel Regolamento delegato del 27 novembre 2017, tutte le norme tecniche per l'autenticazione del cliente e gli standard di comunicazione.

Figura 3 – Modello di architettura dell'open banking secondo la PSD2



2.1.1. Il modello funzionale nella PSD2

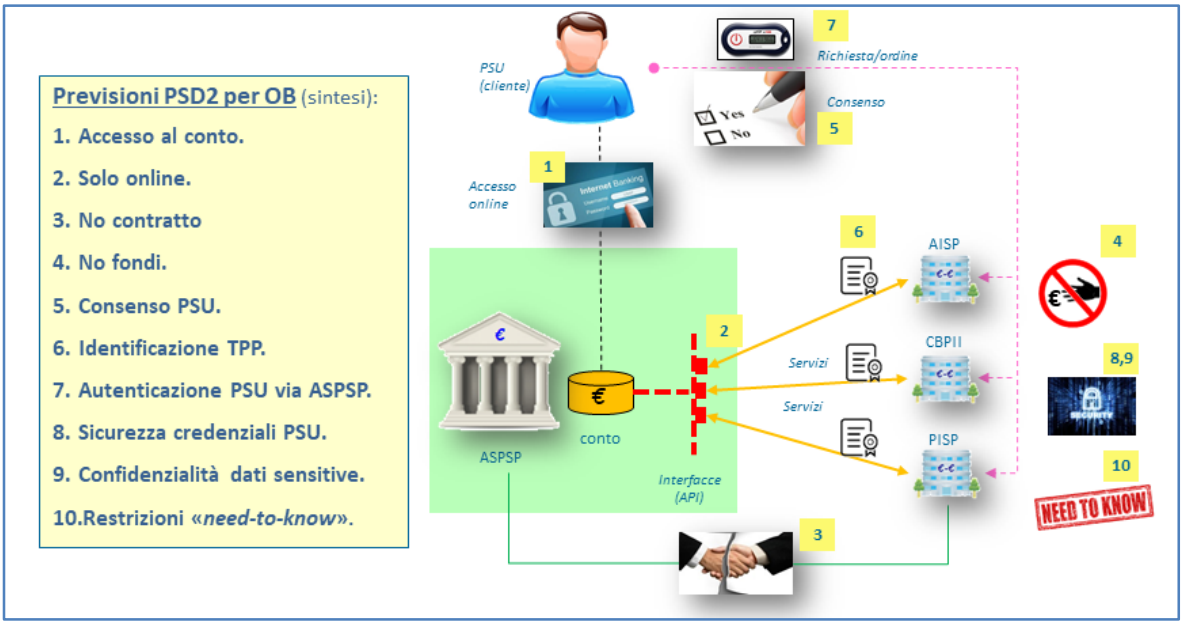
Il fulcro dell'innovazione sottostante la PSD2 è la condivisione del patrimonio informativo del cliente. In ciò il nuovo modello si discosta nettamente da quello classico basato su un puro rapporto bilaterale banca-cliente.

Con riferimento al tema dell'accesso ai conti bancari, le previsioni PSD2 sono in sintesi le seguenti:

1. ***Accesso al conto***: ASPSP consente l'accesso al conto a soggetti regolati/vigilati (art. 65-67);
2. ***Solo on-line***: l'accesso è consentito solo se il conto è «*accessibile on-line*» (art. 65-67);
3. ***No contratto***: non è richiesto un legame contrattuale tra i TPP e l'ASPSP (art. 66, 67);
4. ***No fondi***: i TPP non detengono fondi del *Payment Service User* (PSU; art. 66.3);
5. ***Consenso PSU***: accesso dei TPP subordinato all'esplicito consenso dell'utente (art. 65, 67);
6. ***Identificazione TPP***: autenticazione dei TPP verso l'ASPSP nell'accesso al conto (art. 65-67);
7. ***Autenticazione PSU via ASPSP***: l'ASPSP deve consentire ai TPP (AISP e PISP) di usare le proprie procedure di autenticazione utente (art. 97.5);
8. ***Sicurezza credenziali PSU***: i TPP non possono detenere le credenziali del cliente emesse da ASPSP; la trasmissione deve avvenire su canali sicuri (art. 66,67);
9. ***Confidenzialità dati sensitive***: i TPP non possono detenere "*sensitive payment data*" (art. 66,67);
10. ***Restrizioni «need-to-know»***: i TPP non possono accedere a dati diversi da quelli necessari alle operazioni consentite (art. 66,67).

La figura 4 presenta una raffigurazione stilizzata dei modelli e delle relazioni che si sviluppano tra i vari attori nell'*open banking*.

Figura 4 – Open banking e requisiti PSD2



Per consentire uno sviluppo dell'open banking competitivo ed esteso, non c'è necessità di accordi contrattuali tra le terze parti e le banche di radicamento del conto. A garanzia della sicurezza complessiva dei servizi e a tutela del cliente, la PSD2 richiede che le terze parti debbano ottenere un'apposita licenza finanziaria ed essere sottoposte a vigilanza finanziaria, per poter operare.

2.1.2. I riferimenti all'open banking nel quadro normativo europeo

L'affermarsi del modello di *open banking* solleva questioni normative complesse, che il regolatore europeo ha affrontato con una disciplina dei servizi di accesso ai conti articolata su più livelli: oltre alla PSD2 e alle fonti di recepimento nazionali, rilevano gli RTS e le altre regole attuative di secondo livello definite dall'EBA, a cui si aggiungono le interpretazioni fornite sia dalla Commissione sia dall'EBA nell'ambito del tool "*Questions and Answers*" pubblicato su Internet[19].

Il livello di dettaglio delle previsioni, inusuale nel campo dei pagamenti *retail*, riflette l'esigenza di contemperare gli interessi contrapposti delle banche, delle terze parti e dei rispettivi utenti, che non trovano composizione in una spontanea disciplina di mercato e in forme di autoregolamentazione strutturate.

Un **primo gruppo** di regole intende disciplinare, in assenza di un rapporto contrattuale diretto, i diritti e gli obblighi che connotano il rapporto tra la terza parte e la banca (es. artt. da 64 a 67 della PSD2); il servizio finale alla clientela può essere sviluppato e offerto nel rispetto dei vincoli stabiliti da queste norme ed è dunque ad esse che devono conformarsi i relativi contratti. Le regole che coinvolgono l'utente mirano essenzialmente a definire il regime delle responsabilità che, di norma, gravano sulla banca nel caso di operazioni svolte con l'intermediazione della terza parte: vi rientrano dunque le regole sulla corretta autenticazione ed esecuzione dei pagamenti, sulla gestione del consenso dell'utente, sul riparto di responsabilità in caso di operazioni non autorizzate.

Un **secondo gruppo** di previsioni normative attiene invece all'interazione operativa tra la banca e la terza parte. Si tratta in questo caso delle regole di secondo livello, definite dall'EBA in base all'art. 98 della PSD2, con cui sono fissati i requisiti tecnici per l'identificazione reciproca e la comunicazione sicura, le modalità di accesso tramite apposite interfacce e le misure per assicurare la continuità di servizio dei canali di colloquio.

Ci troviamo in questo caso in un ambito che nel mondo delle procedure di pagamento "tradizionali" sarebbe presidiato da accordi cooperativi e infrastrutture comuni e che invece, nel mondo dell'*open banking*, è disciplinato dai requisiti fissati dal regolatore. Il buon funzionamento dell'intero sistema dipende quindi soprattutto dalla corretta e uniforme applicazione di "*standard* normativi". Ciò implica l'esigenza di coprire anche aspetti di dettaglio e ridurre i margini di interpretazione, attraverso una costante attività di elaborazione normativa e di interazione con il mercato. L'EBA si è impegnata a fondo su questa linea, attivando le leve a sua disposizione: la pubblicazione di linee guida[20] e di opinioni[21] nonché l'estensione ai temi della PSD2 della pagina web di "*Questions and Answers*".

---

19 Cfr. https://www.eba.europa.eu/single-rule-book-qa

20 Cfr. European Banking Authority (2018c) – EBA Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC), December 2018.

21 Cfr. European Banking Authority (2018b) – opinion sui certificati eIDAS (dicembre 2018) o le due opinion più generali sui temi dell'autenticazione forte e della comunicazione sicura (giugno 2018 e giugno 2019).

2.1.3. Gli standard di mercato e il confronto tra gli operatori

Oltre alle regole, ulteriore condizione di successo per l'*open banking* è lo sviluppo di *standard* uniformi e largamente condivisi tra banche e terze parti: come insegna la storia dei sistemi di pagamento, l'adozione di un linguaggio e di funzionalità comuni, anche aggiuntivi rispetto ai requisiti minimi fissati dalla legge, è fondamentale per contenere i costi, assicurare economie di scala e promuovere la concorrenza e l'integrazione dei servizi a livello europeo.

La standardizzazione rileva soprattutto nell'offerta delle modalità tecniche di comunicazione: gli RTS richiedono che l'identificazione e la comunicazione delle banche con le terze parti avvenga tramite le interfacce già utilizzate dai clienti, opportunamente modificate, oppure mediante la messa a disposizione di interfacce dedicate, come quelle basate sulla tecnologia delle Open API.

Teoricamente ogni banca può definire proprie specifiche di interfaccia, in base a scelte di *business* o a esigenze tecniche, e in questo la normativa non impone requisiti di dettaglio, ma mantiene un approccio di sostanziale neutralità tecnica; questa scelta, se da un lato ha il vantaggio di non vincolare l'innovazione a specifiche soluzioni, di contro espone al rischio di un'elevata frammentazione delle modalità di accesso ai conti, che si traduce per le terze parti in un lavoro di sviluppo di interfacce plurime, ancorché basate tutte sulla tecnologia delle API. In assenza di puntuali indicazioni normative è quindi importante la convergenza dell'industria verso *standard* europei armonizzati, che assicurino uniformità di accesso per le terze parti, riuso delle soluzioni, competizione tra gli operatori e opportunità di ingresso sul mercato di nuovi soggetti, anche di piccole dimensioni. Un panorama troppo frammentato, in cui ogni terza parte debba sviluppare applicazioni diverse per ogni singola banca cui connettersi, rischia infatti di ostacolare lo sviluppo del comparto e di favorire i soggetti con maggiore disponibilità di risorse, aspetto non di poco conto in un mercato, quello dei servizi digitali, già da anni dominato da poche grandi aziende.

Tra le iniziative europee di standardizzazione promosse dal mercato rileva il "NextGenPSD2 Framework" *sviluppato dal* Berlin Group[22]*, associazione dei principali operatori europei dei pagamenti, con l'obiettivo di favorire la riduzione del numero di standard esistenti e promuovere servizi innovativi e modalità sicure di accesso ai conti in tutta Europa. Si tratta, in concreto, di un insieme di specifiche tecniche e di standard di messaggistica per il colloquio tra banche e terze parti, riviste periodicamente. Meritano inoltre menzione altre iniziative in ambito europeo con analoghe finalità, ma su scala nazionale, spesso convergenti con i lavori del* Berlin Group *quali, ad esempio: la polacca* "PSD2 Polish API"*, la francese* "STET PSD2 API" *e la portoghese* "SIBS Forward Payment Solutions"*. Infine, lo* Euro Retail Payments Board *(ERPB), organo di cooperazione pubblico-privato presieduto dalla BCE, ha costituito il* "Working Group on a SEPA API access scheme" *per la definizione di uno schema per l'offerta di* payment initiation services*. Tale schema dovrebbe costituire un vero e proprio accordo multilaterale che, similmente a quelli che regolano il funzionamento dei circuiti di carte e degli schemi di bonifico e addebito diretto della SEPA, definisca obblighi, responsabilità,*

---

[22] Cfr. The Berlin Group (2021).

regole di funzionamento e di governance del servizio di payment initiation. *Il gruppo ha definito gli obiettivi di alto livello a giugno 2021 e contestualmente, l'ERPB ha chiesto all'*European Payments Council *(EPC) di sviluppare lo schema, sulla base del modello degli schemi di pagamento SEPA. L'EPC ha avviato la fase preliminare di studio creando un gruppo con i principali soggetti coinvolti (SPAA-MSG) con l'obiettivo di pubblicare una prima versione delle specifiche.*

Nell'Unione europea lo sforzo messo in campo dalle autorità di settore – a cui si aggiunge la costante attenzione dedicata dalla Commissione europea – riflette l'esigenza di costruire un ecosistema in cui gli interessi dei vari attori dell'*open banking*, a volte contrapposti, possano trovare una sintesi adeguata in termini di qualità, efficienza e sicurezza dei servizi innovativi disponibili sul mercato, a beneficio degli utenti finali.

2.2. L'evoluzione del mercato Italiano: i *Gateway* PSD2

Gli obblighi e le altre previsioni normative sopra citati, funzionali ad assicurare la possibilità per i TPP di prestare i propri servizi, si sono posti all'attenzione degli operatori di mercato come un investimento ineludibile, con diverse possibili soluzioni attivabili per realizzare le interfacce dedicate. Gli operatori europei si sono adoperati per individuare spazi di cooperazione tali da favorire la riduzione dei costi di investimento e l'attivazione delle esternalità tipiche di un'economia di rete. In questa direzione è stato centrale in Italia il ruolo del Comitato Pagamenti Italia, come sede di confronto e sintesi per le scelte di sistema del mercato nazionale.

LE PIATTAFORME DI SISTEMA

Nel mercato italiano si sta affermando il ruolo delle Piattaforme di *Open Banking* (POB), infrastrutture tecniche per la predisposizione di interfacce API dedicate all'accesso delle terze parti. Ciascuna piattaforma si propone alle terze parti come punto unico di accesso, con funzione di *gateway*, per l'interazione con tutte le banche aderenti.

In Italia si è ricercata una convergenza su *standard* tecnici comuni per la realizzazione di interfacce dedicate ed è stato adottato lo *standard* (prima richiamato) *"NextGenPSD2 Framework"*, sviluppato dal *Berlin Group*.

Successivamente, il sistema bancario nazionale si è organizzato per definire soluzioni applicative "di sistema" per la realizzazione dell'interfaccia dedicata, in alternativa a soluzioni proprietarie per singolo ASPSP[23]. Nel nuovo ecosistema dei pagamenti hanno così assunto un ruolo centrale, a fianco di banche e terze parti, le cd. "piattaforme di sistema", infrastrutture tecniche a cui i prestatori di servizi di pagamento italiani si sono indirizzati in misura preminente per la predisposizione di interfacce dedicate all'accesso delle terze parti.

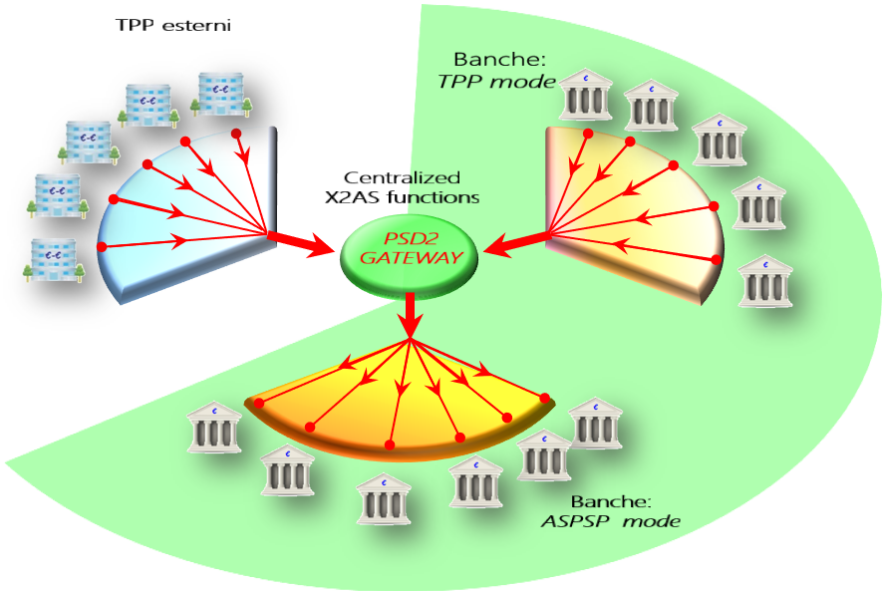
[23] Un approccio simile è stato seguito anche in Spagna.

Una piattaforma di sistema si propone alle terze parti come punto di accesso unico al cluster delle banche che vi aderiscono, offrendo:

- servizi comuni messi a disposizione delle terze parti, tra cui gestione delle specifiche tecniche delle interfacce, supporto allo sviluppo, *testing, change management, trouble-ticketing*[24];
- funzioni di base per la gestione delle transazioni: autenticazione dei TPP, controlli dei messaggi sulle API, supporto alle procedure di autenticazione forte del cliente, gestione dei consensi del cliente, monitoraggio delle performance, reportistica;
- funzioni di *rete*: punto unico di accesso per tutte le banche aderenti (ASPSP) e per i TPP;
- modalità duale per le banche: quelle aderenti possono operare come ASPSP (modalità passiva) o come TPP (modalità attiva) attraverso canali di accesso comuni.

La struttura delle piattaforme di sistema, dette anche *Piattaforme di Open Banking* (POB) o in alternativa *PSD2 Gateway*, può essere schematizzata come nella figura 5.

Figura 5 – Struttura di una piattaforma di open banking di sistema



In questo assetto la piattaforma può offrire vantaggi ai vari *stakeholders*. In particolare:

i. le banche possono affrontare gli adempimenti di conformità rivolgendosi a un operatore specializzato, senza dover sviluppare in proprio strutture e competenze dedicate;

[24] Col termine *change management* si intende l'attività che governa l'insieme dei cambiamenti effettuati, a fini correttivi o evolutivi, di componenti applicativi o infrastrutturali di sistemi che offrono servizi su piattaforme tecnologiche. Col termine di *trouble ticketing* si indica il processo che gestisce le richieste di assistenza, supporto o manutenzione, rivolte ad un fornitore ed effettuate dai suoi clienti, per la risoluzione di problemi relativi a servizi erogati.

ii. le terze parti possono accedere con le medesime modalità ai conti detenuti da una pluralità di intermediari e quindi possono disporre di un solo punto di contatto verso tutti gli ASPSP aderenti, con una razionalizzazione delle documentazioni tecniche, del relativo supporto e degli ambienti di test;

iii. per le autorità è più agevole verificare la corretta realizzazione di quanto richiesto dalla normativa. Un esempio in questo senso sono le valutazioni necessarie alla "*fall-back exemption*" (cfr. sezione in appendice A.4): l'esame degli elementi comuni presenti sulla piattaforma semplifica notevolmente ciò che sarebbe necessario verificare sui singoli ASPSP aderenti alla piattaforma stessa.

Sul mercato italiano sono state sviluppate quattro soluzioni di sistema (cd. piattaforme di sistema), aperte anche a soggetti non italiani: CBI GLOBE, offerta da CBI S.c.p.a.; Cedacri Open Banking API Portal, di Cedacri S.p.a.; Fabrick Platform, offerta da Fabrick S.p.a. (società del Gruppo Sella); SIA Open Banking Platform di NEXI.

---

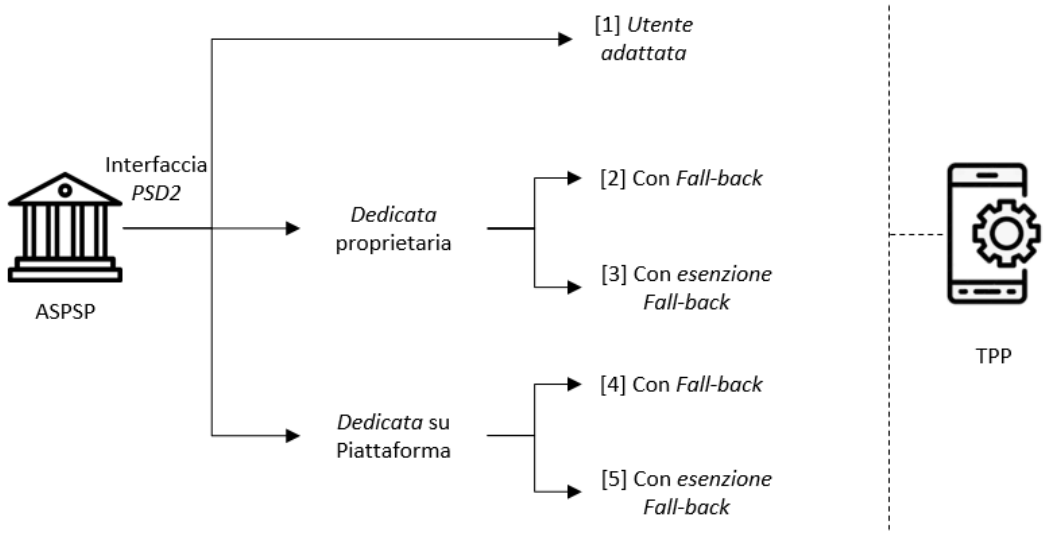
*Il mercato italiano dell'*open banking *si compone, al terzo trimestre del 2022, di 377 ASPSP e di 85 operatori attivi in qualità di terza parte, di cui 39 italiani, in larga parte rappresentati da intermediari che hanno integrato funzionalità* open banking *per erogare, principalmente, servizi di tipo* Personal Finance Management *(PFM): il cliente bancario ha così la possibilità di visualizzare, in maniera aggregata, tutti i conti detenuti presso diversi intermediari, oltre che di analizzare i propri movimenti, classificati per tipologia di spesa. Il vantaggio per l'intermediario è quello di profilare il proprio cliente in un perimetro più esteso, potendo accedere anche ai movimenti nei rapporti che il cliente detiene presso i competitor, e poter dunque declinare l'offerta proponendo personalizzazioni e servizi che il proprio cliente acquisisce da altri intermediari. Meno di una decina sono invece gli operatori italiani, non intermediari, che erogano servizi con licenza di terza parte, di cui alcuni autorizzati al più come Istituti di Pagamento: questi adottano modelli di business che hanno visto, in larga parte, i primi ricavi apprezzabili nel corso dell'anno 2022. Interessante la verticale* corporate *che vede l'erogazione di servizi per le aziende legati ad attività gestionali e di tesoreria, ottenuti integrando sistemi* Enterprise Resource Planning *(ERP) con le funzionalità AIS e PIS, che permettono di realizzare funzionalità di* Business Finance Management *(BFM), inclusa la generazione automatica delle scritture contabili come rivenienti dalla movimentazione bancaria, funzionalità utile in ambito domestico per specifici tipi di clientela (es. commercialisti e PMI).*

Gli ASPSP consentono l'accesso al conto di pagamento dell'utente ai TPP o adattando l'interfaccia utente già disponibile o fornendo un'interfaccia API dedicata. Quest'ultima può essere o sviluppata su base proprietaria dal singolo ASPSP o costituita dal collegamento a una piattaforma di sistema. In entrambi i casi, l'ASPSP deve implementare una seconda interfaccia da utilizzare in caso di indisponibilità della prima (cd. *fall-back*), oppure chiedere all'Autorità nazionale competente[25] l'esenzione da tale obbligo (cd. *fall-back exemption*). Ne segue che tecnicamente sono possibili 5 distinte tipologie di interfaccia, come riportato nella figura 6.

---

25 In Italia tale autorità è la Banca d'Italia.

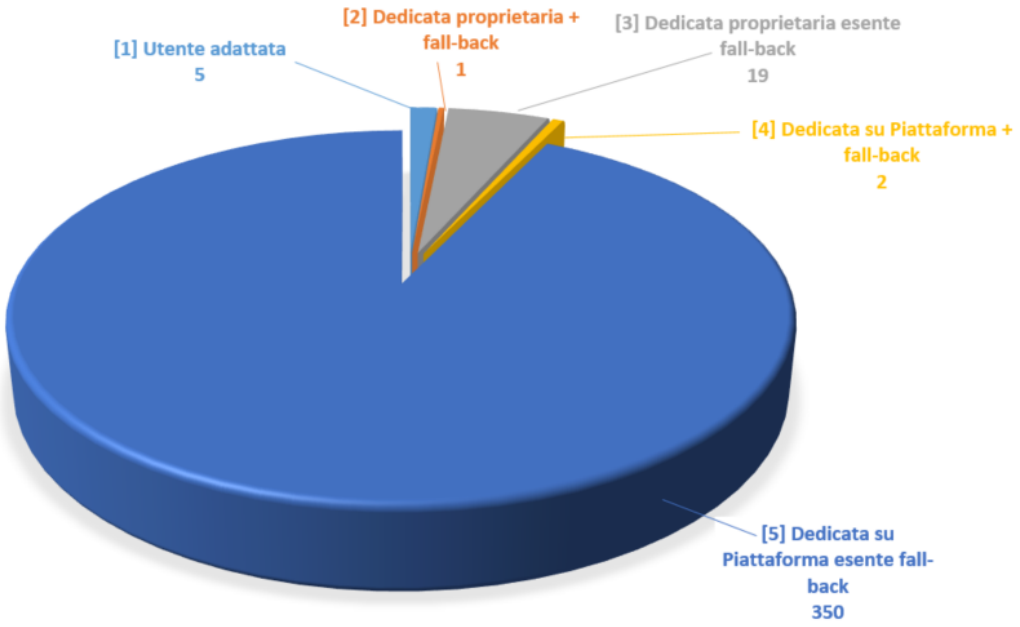
Figura 6 - Possibili tipologie di interfaccia



La maggioranza degli ASPSP ha aderito alle piattaforme di sistema e richiesto l'esenzione da *fall-back*. Gli altri operatori hanno per lo più adottato soluzioni basate su un'interfaccia utente adattata, sviluppata in autonomia.

Alla data di avvio del 14 settembre 2019, 382 ASPSP avevano aderito alle iniziative basate su piattaforma di sistema, mentre 25 ASPSP avevano scelto di realizzare in autonomia un'interfaccia dedicata. I numeri aggiornati a dicembre 2022 sono riportati nella figura 7.

Figura 7 – Numero di interfacce nel mercato italiano a dicembre 2022

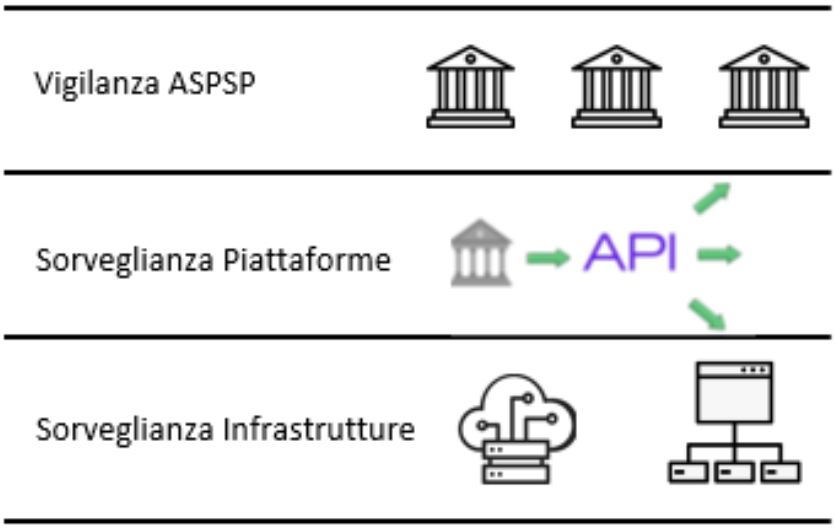


Ai benefici offerti dalle soluzioni di sistema si accompagnano alcuni aspetti di attenzione per le Autorità legati, tra l'altro, ai rischi di esternalizzazione[26], che devono essere adeguatamente governati dagli intermediari in linea con i requisiti di vigilanza, e alla concentrazione del rischio operativo in capo a un numero limitato di gestori di piattaforme di sistema (rischio di *single point of failure*[27]).

3. La funzione di controllo dell'Autorità nazionale

L'evoluzione del mercato italiano dei pagamenti, prodotta anche dall'adeguamento degli operatori ai requisiti della PSD2 in tema di *open banking*, ha portato l'Autorità nazionale competente (la Banca d'Italia) ad articolare il sistema dei controlli previsti dalla normativa secondo una struttura articolata su tre livelli distinti, ognuno specializzato su particolari funzioni, focalizzato su specifici attori dei servizi di *open banking* e svolto da una specifica funzione della Banca d'Italia (cfr. figura 8).

Figura 8 – Articolazione del sistema dei controlli



Gli elementi su cui si basa l'attuale assetto dei controlli sono i seguenti:

- l'adeguamento ai requisiti PSD2, in termini di apertura dei conti di pagamento dei clienti all'accesso delle terze parti, è un obbligo che

[26] I rischi di esternalizzazione sono i rischi derivanti dalla pratica di affidare a terze parti la gestione di funzioni specialistiche (talvolta anche di core business): in tal caso una cattiva gestione delle funzioni esternalizzate alla terza parte potrebbe provocare danni operativi, economici, di immagine etc. al soggetto che ha fatto ricorso a tale pratica.

[27] Con rischio di *single point of failure* si intende il rischio che una parte o una componente di un sistema, nella quale sono concentrate attività o funzioni critiche, in caso di errore o indisponibilità porti al blocco dell'operatività e dei servizi forniti dall'intero sistema. La gestione del rischio del *single point of failure* prevede l'analisi di tale condizione e l'adozione di contromisure che evitino la realizzazione di tale scenario.

ricade sugli ASPSP i quali sono conseguentemente sottoposti ai controlli di Vigilanza;

- le piattaforme di sistema di *open banking*, prevalentemente utilizzate dagli intermediari italiani, ricadono nel perimetro dei poteri di sorveglianza sul sistema dei pagamenti assegnati alla Banca d'Italia ai sensi dell'art. 146 del Testo Unico Bancario (TUB);
- in alcuni casi le piattaforme sono gestite da soggetti che svolgono funzioni "*infrastrutturali*" rilevanti nel sistema dei pagamenti, funzioni sottoposte alla funzione di sorveglianza nell'ambito applicativo dell'articolo 146 del TUB con riferimento alle infrastrutture tecnologiche e di rete[28].

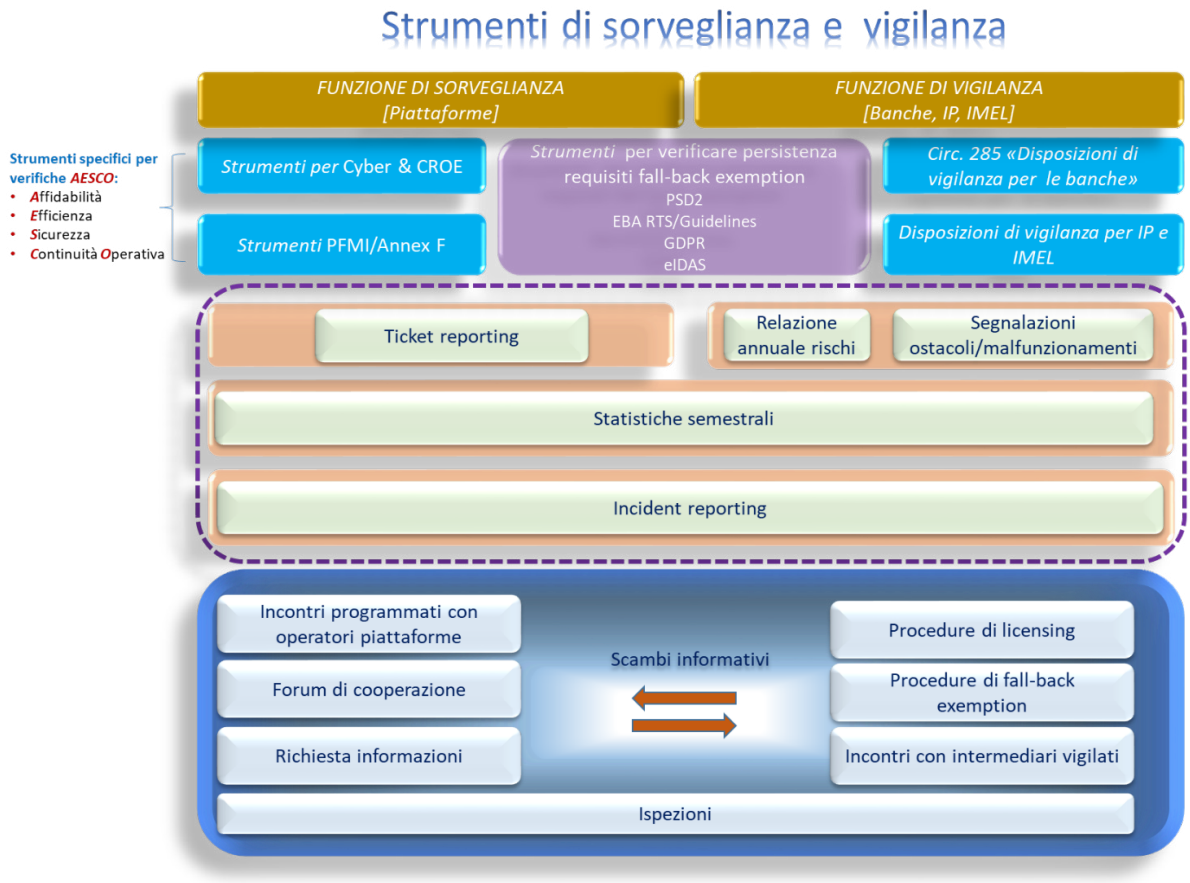
La struttura dei controlli è stata quindi predisposta secondo una organizzazione a più livelli, nella quale ogni livello sfrutta le informazioni ricevute dagli altri, evitando duplicazioni delle attività con importanti recuperi di efficienza. In particolare le valutazioni di vigilanza sugli intermediari riutilizzano le analisi di sorveglianza sulle piattaforme di *open banking*, le quali a loro volta tengono conto dei controlli svolti sulle infrastrutture utilizzate a supporto delle piattaforme per il contenimento dei rischi operativi, di sicurezza informatica e per la continuità di servizio, come argomentato al paragrafo 3.2. La figura 9 mostra l'insieme degli strumenti utilizzati dall'Autorità per un'articolata e ordinata attività di sorveglianza e vigilanza sull'ecosistema dell'*open banking*. Alcuni vengono utilizzati sia per l'attività di sorveglianza delle piattaforme che per la vigilanza degli ASPSP mentre altri vengono applicati specificatamente in via esclusiva, come descritto in seguito.

IL SISTEMA DEI CONTROLLI

L'organizzazione dei controlli coinvolge diverse strutture della Banca d'Italia: le valutazioni circa il rispetto dei requisiti PSD2 da parte degli intermediari sono svolte dalla funzione di Vigilanza, mentre le funzioni di Sorveglianza svolgono controlli sulle infrastrutture tecnologiche con riguardo al contenimento dei rischi operativi, di sicurezza informatica e per la continuità di servizio, nonché al regolare funzionamento delle piattaforme, ai sensi dell'art. 146 del Testo Unico Bancario.

[28] Il potere di sorveglianza "diretta" sui fornitori di servizi infrastrutturali del sistema dei pagamenti, attribuito alla Banca d'Italia dal legislatore, rappresenta quasi un unicum a livello internazionale. Esso si distingue dal modello di sorveglianza dei fornitori "indiretto" effettuato per il tramite dei gestori dei sistemi sorvegliati (o soggetti serviti), prevalente in altre giurisdizioni. Tra le poche eccezioni urano alcune normative di sorveglianza europee, tra le quali quelle belga e olandese. Esse conferiscono alle banche centrali poteri di vigilanza sui soggetti che forniscono servizi di processing di carte di pagamento e gestiscono infrastrutture e servizi tecnici. Si tratta tuttavia di ambiti applicativi specifici e più limitati rispetto a quanto previsto dal Testo Unico Bancario.

Figura 9 – Open banking in Italia: quadro integrato di sorveglianza e vigilanza



3.1. La Vigilanza sugli intermediari finanziari

La vigilanza sugli intermediari in relazione ai nuovi servizi di open banking fa leva sulle previsioni e le prassi già adottate per tutti gli operatori vigilati, integrate dai requisiti indicati dalla PSD2 e dalle corrispondenti norme attuative (i *Regulatory Technical Standards* – RTS) recepiti nella normativa nazionale di primo e secondo livello[29].

Banche, gruppi bancari, istituti di pagamento e istituti di moneta elettronica sono tenuti al rispetto delle disposizioni di vigilanza della Banca d'Italia anche per quanto riguarda i nuovi servizi di pagamento introdotti dalla PSD2, sia quando svolgono il ruolo di ASPSP che quando operano in veste di TPP.

Facendo riferimento, a titolo esemplificativo, ai profili di rischio operativo e di sicurezza, le previsioni contenute nella normativa hanno l'obiettivo di garantire che gli intermediari realizzino tutti i presidi necessari per tenere sotto controllo questi rischi nello svolgimento della loro attività, inclusa l'esecuzione dei servizi di pagamento offerti ai clienti.

[29] In base alla normativa comunitaria, la vigilanza sugli aspetti concernenti la PSD2 è responsabilità dell'Autorità nazionale, non del Meccanismo di Vigilanza Unico europeo.

In particolare, per quanto riguarda il contenimento dei rischi operativi e informatici degli intermediari bancari, la normativa fornisce requisiti di dettaglio[30] sui seguenti aspetti:

- il governo e l'organizzazione del sistema informativo;
- la gestione del rischio e della sicurezza informatici;
- il *change management* e gli incidenti di sicurezza informatica;
- il sistema di gestione dei dati;
- l'esternalizzazione del sistema informativo;
- la continuità operativa;
- la sicurezza dei servizi di pagamento.

Sia le disposizioni di vigilanza per gli intermediari bancari sia quelle indirizzate agli istituti di pagamento e di moneta elettronica recepiscono gli orientamenti sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento[31] emanati dall'EBA il 12 gennaio 2018[32]. Oltre a fornire requisiti sui punti già indicati nell'elenco precedente, gli orientamenti EBA richiamano previsioni specifiche in relazione a test di sicurezza, formazione del personale e gestione della relazione con gli utenti dei servizi di pagamento.

Come per gli altri rischi, l'azione di presidio dei rischi operativi e di sicurezza da parte della Banca d'Italia si esplica sia in occasione di eventi specifici (ad esempio, i procedimenti di *licensing* e le iniziative di esternalizzazione che riguardano i sistemi informativi) sia con un'azione di controllo nel continuo svolta "a distanza" ovvero "on-site", con visite ispettive. L'azione a distanza fa leva sulla documentazione prodotta periodicamente dagli intermediari (piani strategici, indagini periodiche, esercizi di autovalutazione, segnalazioni di gravi incidenti informatici); in questo contesto è da segnalare la previsione, introdotta nel 2020, di fornire annualmente all'Autorità di Vigilanza la relazione sull'analisi dei rischi operativi e di sicurezza relativi ai servizi di pagamento[33].

Il controllo di natura prudenziale dei rischi è svolto dalle funzioni di vigilanza competenti sui singoli operatori. A testimonianza del carattere innovativo e specialistico della materia, i controlli sugli aspetti di natura spiccatamente tecnica connessi con la PSD2[34] sono svolti da una funzione di vigilanza sulla materia e trasversale alle altre strutture.

---

30 Circolare 285 del 17 dicembre 2013 "Disposizioni di vigilanza per le banche", Parte Prima, Tit. IV, Cap. 4 e 5.

31 Ai sensi dell'articolo 95, paragrafo 3, della direttiva 2015/2366/UE (PSD2).

32 Sia per gli intermediari bancari che per IP e IMEL sono stati recepiti gli Orientamenti EBA sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (*Information and Communication Technology – ICT) e di sicurezza*.

33 Cfr. https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/direttiva-psd2/Relazione-analisi-rischi-operativi-e-di-sicurezza-servizi-di-pagamento-ver-2.pdf

34 Ad es. la valutazione dell'adeguatezza delle interfacce dedicate nelle richieste di esenzione dalla fall-back solution, o la valutazione degli ostacoli all'attività dei TPP e delle procedure di 'autenticazione forte' dei clienti predisposte dagli intermediari.

Inoltre, data la rilevanza del tema, con l'entrata in vigore della PSD2 la Banca d'Italia ha inserito l'*open banking* tra le priorità di Vigilanza per il 2020 e ha costituito un gruppo di lavoro con l'obiettivo di seguire l'avvio e l'evoluzione del comparto, monitorando l'operatività dei servizi delle terze parti, analizzandone i modelli di business con riguardo ai rischi nel continuo, verificando la presenza di possibili ostacoli alla corretta evoluzione del comparto e valutando l'adeguatezza delle procedure di sicurezza adottate dagli intermediari[35].

Seguendo quanto previsto dalle linee guida dell'EBA[36], l'Autorità di Vigilanza ha introdotto anche uno specifico strumento per il monitoraggio dell'adeguatezza delle interfacce di accesso per i TPP, basato sulla segnalazione diretta da parte di TPP e ASPSP di eventuali problemi nelle interfacce dedicate utilizzate. Sulla base di queste segnalazioni la Banca d'Italia avvia un'analisi che può includere anche un'interlocuzione diretta con l'ASPSP interessato, per definire, laddove necessario, azioni di rimedio.

3.2. La sorveglianza sulle piattaforme e infrastrutture di *open banking* (POB)

L'attività di sorveglianza POB, attribuita dalla normativa alla Banca d'Italia, ha l'obiettivo di presidiare i profili di affidabilità ed efficienza nonché la tutela degli utenti dei servizi di pagamento. Le POB possono essere assimilate ai soggetti che offrono servizi di rete e tecnologie per i servizi di pagamento. Pertanto, per l'Autorità di Sorveglianza sono doppiamente rilevanti:

- come piattaforme tecnologiche, perché forniscono un servizio in *outsourcing* ai prestatori di servizi pagamento a supporto dei servizi erogati, garantendone conformità normativa e funzionalità operativa;
- come infrastrutture di pagamento, perché concentrano la gestione dei flussi informativi e di pagamento introdotti dalla PSD2, la cui continuità di servizio e sicurezza sono fondamentali per il funzionamento del sistema finanziario.

La sorveglianza sulle POB è stata avviata nel 2019, immediatamente prima dell'avvio dei nuovi servizi, adottando un processo strutturato e in raccordo con le attività svolte dalla Vigilanza sugli intermediari in materia di *open banking*[37].

---

35 I primi risultati dell'analisi sono confluiti nella pubblicazione "*PSD2 e Open Banking: nuovi modelli di business* e rischi emergenti" (https://www.bancaditalia.it/compiti/vigilanza/analisi-sistema/approfondimenti-banche-int/2021-PSD2-Open-Banking.pdf).

36 Cfr. art. 33, comma 3, degli RTS.

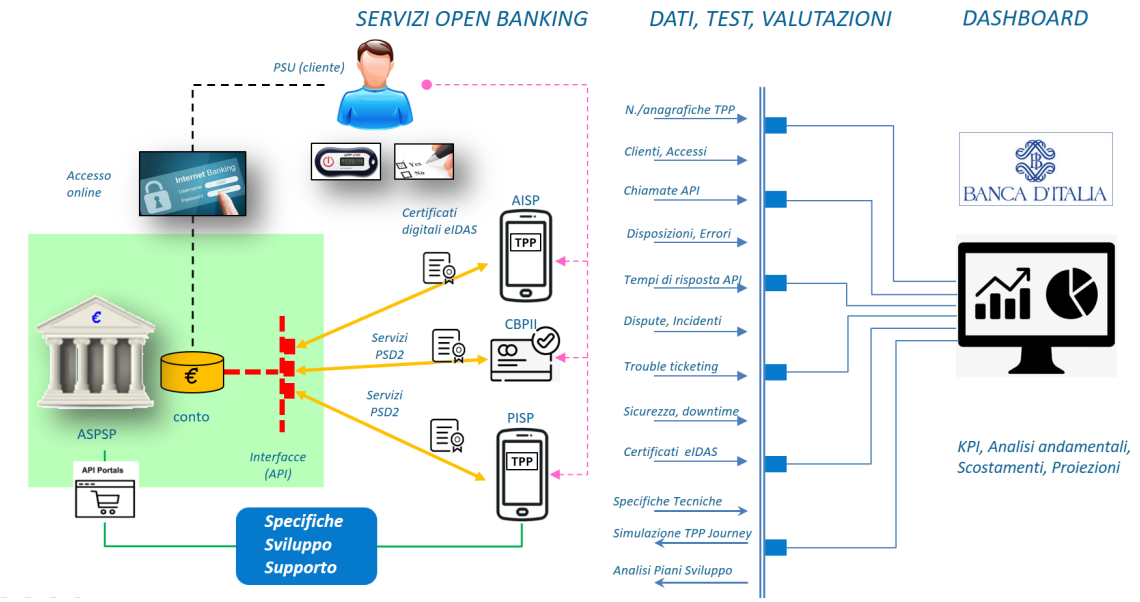
37 In questa prima fase l'attività si è focalizzata sul supporto al procedimento amministrativo di esenzione degli ASPSP aderenti alle piattaforme dall'obbligo di realizzare, ai sensi dell'art. 33(1) degli RTS, la misura di *contingency* (cd. *fall-back solution*) da attivare in caso di malfunzionamenti e indisponibilità dell'interfaccia dedicata (cfr. 3.3). Le risultanze dell'analisi finalizzata all'esenzione dalla *fall-back solution* hanno costituito il punto di partenza di un organico piano di sorveglianza volto al periodico monitoraggio della rispondenza dei servizi offerti ai requisiti normativi, alla valutazione dei profili di efficienza e affidabilità delle POB e alla verifica dei diversi profili di rischio, incluso quello cibernetico.

Il piano di sorveglianza sulle POB comprende diverse tipologie di strumenti:

4. il dialogo e lo scambio di informazioni con i gestori in modo: i) programmato, come gli incontri semestrali; ii) programmabile, come le eventuali visite ispettive; iii) nel continuo, come la richiesta e gli scambi di informazioni e flussi statistici con la funzione di vigilanza;
5. un insieme di rilevazioni statistiche, avviate nel gennaio 2020 per monitorare i profili di efficienza, affidabilità e sicurezza delle soluzioni di sistema e costituite da:
   - una rilevazione *semestrale* dei volumi di attività, della performance dei sistemi e delle dispute/reclami, per ciascuno ASPSP e TTP collegato alle piattaforme;
   - un rapporto *mensile* sulle richieste di supporto rivolte alle POB e aperte su richiesta di ASPSP e TPP, con indicazione della competenza del ticket e dei tempi di gestione;
   - la segnalazione *a evento* di incidenti classificati come "gravi" in base ai criteri previsti per il *major incident reporting* sui sistemi di pagamento.

La raccolta sistematica di queste informazioni permette alla Banca d'Italia di monitorare le prestazioni e i livelli di conformità normativa delle piattaforme. I dati raccolti consentono poi l'elaborazione di *Key Performance Indicators* (KPIs) e altri indicatori utili per valutare l'evoluzione delle POB (e quindi della quota del mercato nazionale da esse servito) e per rilevare anomalie e scostamenti. A tal fine è stato sviluppato dalla Banca d'Italia un ambiente statistico di raccolta e sfruttamento dei dati in grado di elaborare indicatori specifici, sviluppare analisi per l'individuazione degli andamenti sottostanti ed effettuare proiezioni (figura 10). Tenendo presenti i risultati di queste elaborazioni e gli sviluppi normativi, la sorveglianza della Banca d'Italia svolge interventi sulle piattaforme in raccordo con la vigilanza bancaria e finanziaria.

Figura 10 – Piattaforme di open banking in Italia: ambiente statistico di raccolta e sfruttamento dati



Relativamente alla valenza delle POB come infrastrutture rilevanti (tecnologiche e di rete), l'attività di sorveglianza è basata su valutazioni ispirate a *standard* internazionali ed europei ed è condotta secondo un principio di proporzionalità. Per la sorveglianza dei soggetti che gestiscono queste infrastrutture il riferimento immediato sono i requisiti per i fornitori di servizi critici di infrastrutture del mercato finanziario, contenuti nell'allegato F (*Annex F – oversight expectations applicable to critical service providers)* dei *Principles for Financial Market Infrastructures*[38] (*PFMI*), che costituiscono gli standard internazionali per la supervisione dei sistemi di pagamento di rilevanza sistemica, dei depositari centrali e sistemi di regolamento titoli, delle controparti centrali e *trade repositories*.

Le previsioni indicate nell'*Annex* F riguardano aspetti connessi con i profili di rischio operativo e stabiliscono requisiti nelle aree relative a: i) identificazione e gestione dei rischi; ii) implementazione di un *security framework* per la gestione dei rischi di sicurezza informatica; iii) affidabilità e resilienza dei servizi offerti; iv) pianificazione tecnologica; v) comunicazione con gli utenti.

L'utilizzo dell'*Annex* F permette di cogliere sinergie sia con la supervisione sui soggetti serviti (con una conseguente riduzione degli oneri per supervisionati e supervisori) sia con i requisiti a valenza generale e applicabili nella sorveglianza su diverse tipologie di servizi. Tuttavia, pur rientrando in un'ottica di controlli di vigilanza sulle funzioni esternalizzate da una *Financial Market Infrastructures* (FMI), l'*Annex* F non comprende profili che devono essere considerati nel caso dei gestori di infrastrutture tecniche che sono rilevanti per una molteplicità di operatori e indispensabili per il buon funzionamento dell'industria dei pagamenti nel suo complesso. Quindi l'azione di sorveglianza su questi gestori considera oltre ai requisiti dell'*Annex* F anche quelli connessi con i profili di governo societario, di rischio di impresa e di esternalizzazione ed il cyber risk[39].

3.3. La rimozione degli ostacoli all'accesso delle Terze Parti

Monitorare l'evoluzione dell'*open banking* comporta un'attività di supervisione e vigilanza anche sulle fasi di sviluppo e di rilascio di nuovi servizi all'utenza. In quest'ottica e in base anche alle segnalazioni effettuate dalle terze parti, l'EBA ha individuato soluzioni e comportamenti da parte degli ASPSP che sono riconoscibili come una barriera allo sviluppo e che possono minare l'efficienza dei nuovi servizi.

---

38 https://www.bis.org/cpmi/info_pfmi.htm

39 Riguardo al rischio cyber, di crescente rilevanza, esso viene valutato tenendo conto della *Guidance on cyber resilience for financial market infrastructures*, https://www.bis.org/cpmi/publ/d146.pdf, anch'essa sviluppata in sede CPMI-IOSCO, nonché dei toolkit elaborati nell'ambito della *Eurosystem Cyber Resilience Strategy for FMIs*, https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html, tra cui la *Cyber Survey* e le *Cyber Resilience Oversight Expectations* (CROE), https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_ma%20rket_infrastructures.pdf

L'Opinion EBA del 4 giugno 2020[40] ha elencato sette ambiti di funzionalità che presentano criticità di implementazione ovvero ostacoli[41] e ha fornito indicazioni utili al loro superamento e un'interpretazione dei requisiti fissati dalla normativa. Nel contesto italiano, un ostacolo può generarsi sia nello 'strato' della piattaforma che in quello dell'ASPSP. Dall'approfondimento delle sette aree di ostacolo collegate a specifiche funzionalità evidenziate dall'EBA, sono emerse varie problematiche riferibili ai seguenti macro-aspetti:

– *biometria e mobile APP*: difficoltà per le TPP a integrare le soluzioni di autenticazione dell'ASPSP basate su biometria[42] e mobile APP; l'integrazione è in certi casi tecnicamente difficoltosa, oppure la procedura risulta macchinosa o non ottimale sui vari dispositivi del cliente, caratterizzati, ad esempio, da diversi sistemi operativi[43];

– *esperienza dell'utente*: navigazione del cliente tra le varie schermate dei menu di autenticazione e dispositivi (sia web che APP) spesso complessa, con controlli ridondanti (ad es. procedure di autenticazione, consensi e selezioni non necessari) e informative spesso non significative; l'esperienza complessiva risulta a volte peggiorativa rispetto alle pari funzionalità dell'*internet banking*;

– *sviluppi delle TPP*: le interfacce PSD2 possono presentare caratteristiche che limitano gli sviluppi dei servizi proposti dalle TPP (ad es. sull'aggiornamento dei dati presentati al cliente e sulle applicazioni al POS), o possano rallentare l'integrazione dell'applicazione della TPP con l'interfaccia (ad es. complessità delle procedure di registrazione).

L'EBA ha invitato le Autorità nazionali a intensificare le attività di controllo sugli intermediari e sulle piattaforme, al fine di rimuovere quanto di ostacolo allo sviluppo dei nuovi servizi e tale rendere più fluida l'esperienza d'uso degli utenti delle TPP.

---

40 Cfr. European Banking Authority (2020) – https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2020/884569/EBA%20Opinion%20on%20obstacles%20under%20Art.%2032%283%29%20RTS%20on%20SCA%26CSC.pdf

41 Le categorie e ambiti a cui fanno riferimento gli ostacoli individuati sono: (a) modalità di autenticazione e ricorso alla biometria, (b) re-indirizzamento del sito ASPSP per pagamenti al POS, (c) richiesta doppia SCA per i servizi PIS e AIS, (d) attivazione esenzione SCA per 90 giorni, (e) selezione del conto da addebitare (IBAN), (f) richiesta di esplicito consenso per l'accesso conti ai TPP, (g) richiesta di preregistrazioni TPP presso le banche ASPSP prima di cominciare ad operare.

42 Una soluzione di autenticazione basata su dati biometrici permette il riconoscimento di un individuo mediante la misurazione di una o più caratteristiche biologiche e/o comportamentali, acquisite tramite sensori e confrontate con dati precedentemente memorizzati. Gli esempi più comuni sono l'impronta digitale, l'iride, il riconoscimento vocale e quello facciale.

43 La verifica biometrica, al pari delle altre modalità di autenticazione via APP, si effettua tramite una specifica APP dell'ASPSP. Questo pone in genere un tema di dialogo tra l'APP della TPP, che avvia il pagamento, e quella dell'ASPSP che gestisce l'autenticazione biometrica dell'utente. Tale dialogo, che devi svolgersi in maniera fluida e veloce nell'ambito dello stesso dispositivo, richiede una particolare con urazione dell'APP di autenticazione dell'ASPSP.

4. Le segnalazioni e i trend nazonali

La Banca d'Italia ha avviato nel gennaio 2020 un modello di segnalazione semestrale relativo all'operatività delle interfacce di accesso ai TPP, che coinvolge le quattro piattaforme di sistema nonché i principali operatori che hanno realizzato autonome interfacce dedicate[44]. La segnalazione fornisce all'Autorità una visione dell'operatività del comparto nel mercato italiano e la possibilità di valutare dinamicamente i profili di efficienza e affidabilità delle piattaforme e degli intermediari, attraverso la raccolta strutturata di informazioni statistiche relative a: i) adesione; ii) accessi all'interfaccia; iii) volumi di operatività; iv) tempi di risposta; v) disponibilità del servizio; vi) dispute; vii) supporto alle terze parti[45].

Il quadro che emerge dalle segnalazioni, disponibili fino al primo semestre 2022, evidenzia un aumento del numero di TPP, oltre ottanta, a fronte di un coinvolgimento dei clienti finali ancora limitato rispetto al potenziale, a dimostrazione che il mercato si trova ancora in una fase di avvio; una quota significativa dell'operatività, soprattutto nel 2020, è stata legata ad attività di *testing* svolta dalle terze parti direttamente sui sistemi degli ASPSP o delle piattaforme.

LE TENDENZE NAZIONALI

In Italia si osserva una crescita dell'*open banking* particolarmente evidente nel primo semestre del 2022. Sebbene le analisi mostrino valori ancora contenuti rispetto al potenziale, gli importi transati sono cresciuti del 161% rispetto al semestre precedente, mentre nello stesso periodo l'incremento del numero di utenti è stato pari al 15%. Dal punto di vista tecnico, le chiamate API per i servizi PIS e AIS sono cresciute rispettivamente del 9% e dell'82%.

La ripartizione delle interazioni API tra profili mono-servizio (che svolgono solo AIS, o PIS, o PIIS) e multi-servizio (AIS, PIS e PIIS) fornisce una indicazione di come le terze parti si stiano inserendo nel mercato. I dati disponibili, relativi agli anni 2020, 2021 e primo semestre 2022 (figura 11), indicano che vi è una netta preponderanza delle interazioni di terze parti con molteplice ruolo, dunque multi-licenza, che possono offrire servizi sia informativi (come AIS) che dispositivi (come PIS). L'ulteriore aumento dell'incidenza dei ruoli multi-servizio sino al 2022 riflette anche l'ingresso nel mercato di nuovi TPP multi-licenza e l'aumento delle attività, con ruolo di terza parte, di molti ASPSP.

La scomposizione delle interazioni API per tipologia di servizio (AIS, PIS e PIIS) segnala che alla fine del primo semestre 2022 quelle di tipo informativo costituivano circa il 91% del totale (figura 12)[46].

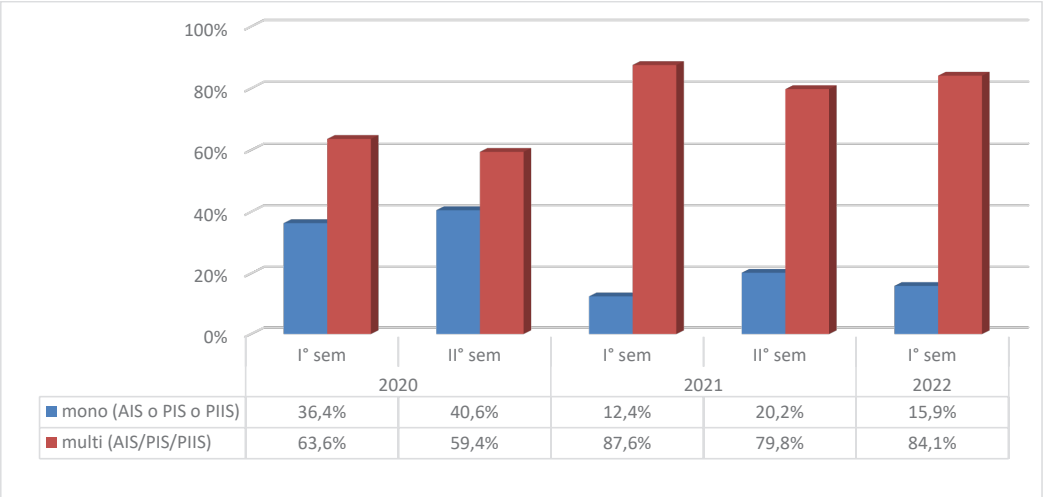
---

44 Le segnalazioni delle piattaforme sono state avviate nel gennaio 2020, con riferimento all'attività del secondo semestre 2019; quelle degli intermediari autonomi sono iniziate nel secondo semestre 2020, con riferimento all'attività del primo semestre dello stesso anno.

45 Le segnalazioni sui ticket di supporto, sono disponibili solo per le piattaforme.

46 I dati relativi al servizio di conferma della disponibilità dei fondi CBPII (o PIIS) sono omessi nel grafico perché trascurabili.

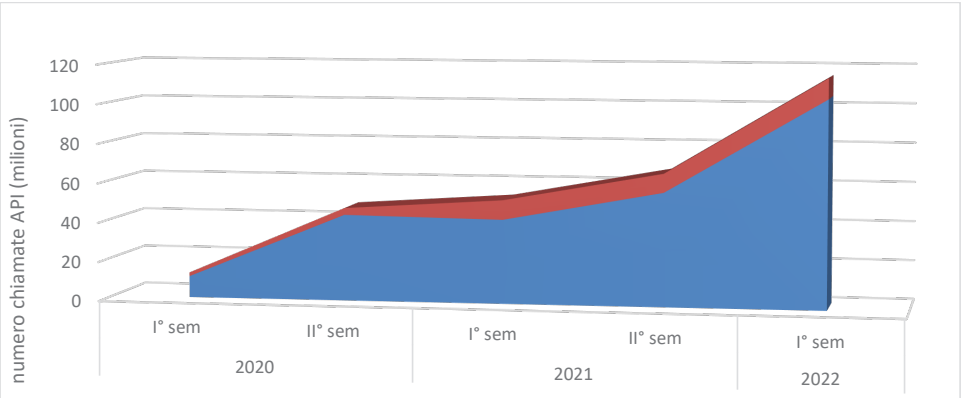
Figura 11 – Accesso di terze parti alle API: ripartizione percentuale per ruolo di accesso (mono o multi)



	I° sem 2020	II° sem 2020	I° sem 2021	II° sem 2021	I° sem 2022
mono (AIS o PIS o PIIS)	36,4%	40,6%	12,4%	20,2%	15,9%
multi (AIS/PIS/PIIS)	63,6%	59,4%	87,6%	79,8%	84,1%

Al forte peso dei servizi AIS contribuiscono anche due fattori tecnici: il primo è l'attività di testing, particolarmente intensa dal secondo semestre del 2020; il secondo è che, nell'attuale contesto normativo, le terze parti sono autorizzate ad accedere alle informazioni anche in assenza del cliente (accesso cd. "*unattended*") fino a 4 volte nel corso delle 24 ore al fine di effettuare il cd. "*mirroring*" dei dati (cioè, l'allineamento delle informazioni delle basi dati proprietarie con i dati degli ASPSP). È possibile che, già dal 2021, l'incidenza dell'attività di testing da parte dei TPP abbia cominciato a ridursi gradualmente e che stia prendendo quota l'operatività della clientela, riscontrabile anche nella crescita della quota di servizi di pagamento dispositivi (PIS). Ciò nonostante, rimane l'assoluta prevalenza dei servizi AIS che, nell'ultima rilevazione del primo semestre 2022, hanno generato circa 104,8 milioni di chiamate API, contro i 10,4 milioni di chiamate API relative ai servizi PIS.

Figura 12 – Numero delle chiamate API per tipo di servizio (PIS/AIS)



	2020		2021		2022
	I° sem	II° sem	I° sem	II° sem	I° sem
API per servizi PIS	1.924.977	3.442.987	9.849.575	9.513.747	10.397.137
API per servizi AIS	10.826.496	43.806.851	42.650.329	57.478.378	104.768.637

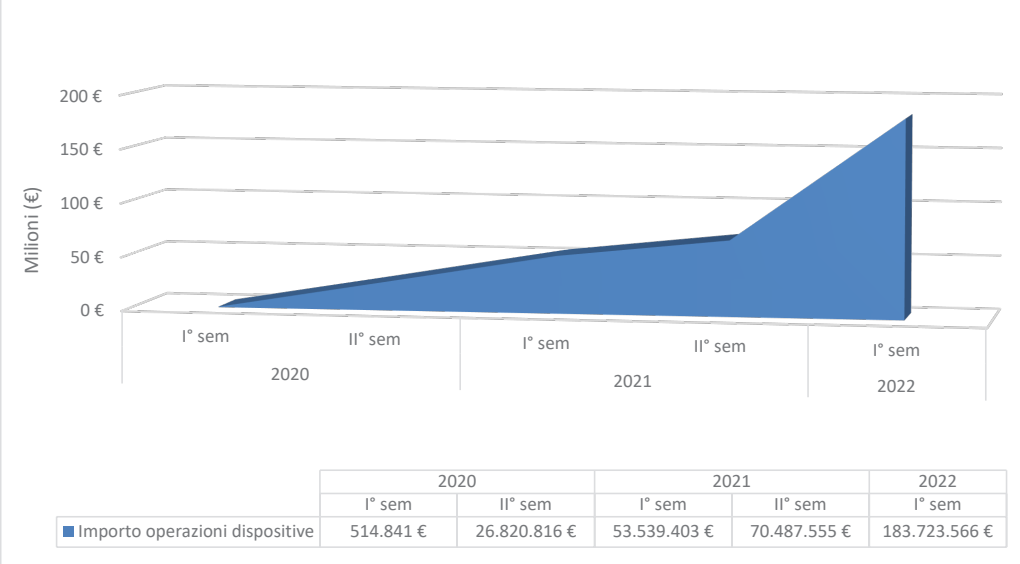
Il totale dei clienti che utilizzano i nuovi servizi, come riportato nella Tavola 1, è ancora limitato ma presenta margini di crescita elevati nei prossimi anni, non appena sarà terminata la fase iniziale di sviluppo del mercato.

Tavola 1 – Servizi di open banking in Italia: numero clienti (PSU)

Voce	II° 2020	I° 2021	II° 2021	I° 2022
Clienti che hanno utilizzato l'interfaccia per servizi di tipo PIS	15.109	31.337	48.108	65.498
Clienti che hanno utilizzato l'interfaccia per servizi di tipo AIS	98.016	131.998	305.810	341.821
Clienti che hanno utilizzato l'interfaccia per servizi di tipo CBPII o PIIS (conferma di disponibilità di fondi)	3	2	2	0
Totale clienti di servizi di open banking in Italia	**113.128**	**163.337**	**353.920**	**407.319**

Riguardo ai servizi di pagamento (PIS), la figura 13 mostra che l'importo complessivo transitato nel sistema dal primo semestre del 2020 ha seguito una tendenza lineare, sino alla fine del 2021, per poi accelerare in maniera importante durante il primo semestre 2022. L'importo semestrale transato da ciascun cliente dapprima ha oscillato tra valori compresi tra i €1.465 e i €1.775 mentre, a metà del 2022, è incrementato notevolmente attestandosi a €2.805 (figura 14).

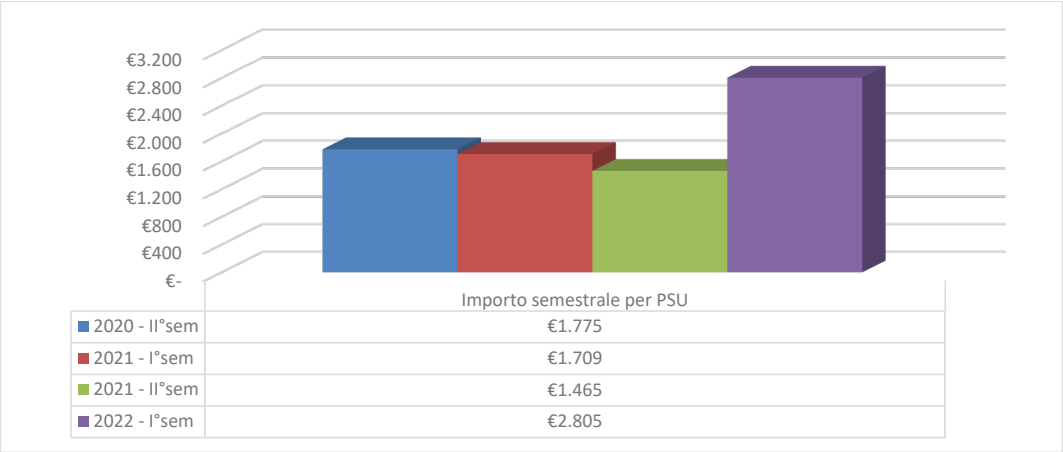
Figura 13 – Importo semestrale delle operazioni dispositive (PISP)



	2020		2021		2022
	I° sem	II° sem	I° sem	II° sem	I° sem
Importo operazioni dispositive	514.841 €	26.820.816 €	53.539.403 €	70.487.555 €	183.723.566 €

L'affidabilità e le performance delle interfacce dedicate sono tendenzialmente migliorate nel tempo: la percentuale media di errore nell'esecuzione delle API, calcolata sull'intero periodo, è stata pari al 10,9%, sebbene nell'ultimo semestre abbia mostrato un incremento non trascurabile, con un valore pari a 13,5%; la velocità di risposta delle interfacce è migliorata considerevolmente, con tempi di esecuzione per le richieste API scesi dai 1056 millisecondi del

Figura 14 – Importo transato semestrale per utente



	Importo semestrale per PSU
2020 - II°sem	€1.775
2021 - I°sem	€1.709
2021 - II°sem	€1.465
2022 - I°sem	€2.805

secondo semestre 2020 agli attuali 578 millisecondi; quest'ultima tendenza è in atto dall'avvio del mercato, a riprova della qualità delle attività di sviluppo e di testing così come degli investimenti in capacità di calcolo effettuati dagli operatori.

5. Conclusioni

La diffusione dell'*open banking* sta determinando una profonda discontinuità nelle modalità di possesso e di utilizzo dei dati degli utenti dei servizi finanziari. Nel settore dei pagamenti esso porta a un parziale ridimensionamento del ruolo – finora esclusivo – degli intermediari presso cui i conti dei clienti sono radicati, consentendo a "terze parti", ovvero alle loro applicazioni basate sulla tecnologia delle API, di effettuare il pagamento per conto del consumatore, senza la necessità che esse abbiano una relazione contrattuale con la banca. Si creano le basi, di mercato e infrastrutturali, per un'inedita competizione tra gli operatori tradizionali (i cosiddetti *Account Servicing Payment Service Providers – ASPSP*) e nuovi soggetti (i *Third-Party Providers – TPP*) caratterizzati da una forte connotazione digitale.

L'*open banking* genera una maggiore complessità tecnologica e aumenta le interconnessioni all'interno dell'industria dei pagamenti. Ciò richiede che le autorità pubbliche definiscano assetti regolamentari e di vigilanza in grado di fare evolvere l'intero sistema finanziario verso una maggiore efficienza e inclusività, mantenendolo nel contempo sicuro e affidabile.

Il regime dell'*open banking* in Italia è incardinato nella normativa comunitaria (fissata nella PSD2) e allineato a *standard* di mercato paneuropei. A differenza delle esperienze di altre giurisdizioni, il legislatore comunitario ha adottato un approccio prescrittivo, imponendo a tutti i gestori di conti *on-line* per la clientela di consentire l'accesso a terze parti, favorendo così l'innovazione e la concorrenza. Gli *standard* normativi comunitari adottati sono molto dettagliati, per l'esigenza di contemperare gli interessi contrapposti delle banche, delle terze parti e dei rispettivi utenti, che altrimenti rischiano di non trovare composizione nella spontanea interazione tra le forze di mercato.

In questi primi anni di *open banking*, il percorso di applicazione della normativa di riferimento ha portato le autorità pubbliche italiane a strutturare percorsi di sorveglianza e supervisione, declinati secondo la struttura dei controlli previsti dalla normativa e operati in sinergia dalle competenti strutture, tali da rispondere alle nuove caratteristiche del mercato, fortemente innovative, e rivolti all'intera platea di soggetti coinvolti.

Il sistema bancario italiano si è adeguato ai requisiti PSD2 per l'*open banking* adottando non solo *standard* comuni ma spesso anche sistemi tecnologici di interfaccia condivisi e centralizzati, le cosiddette piattaforme di sistema, che gestiscono l'accesso delle terze parti ai dati e ai conti istituiti presso più prestatori di servizi di pagamento; in Italia, attualmente, di tali piattaforme ve ne sono quattro mentre negli stati membri soluzioni di questo tipo compaiono a macchia di leopardo, con alcune esperienze nazionali simili al nostro mercato domestico come in Spagna.

L'evoluzione che ne è scaturita ha consentito, da un lato, di valorizzare l'infrastruttura interbancaria nazionale e contenere i costi di realizzazione e gestione, dall'altro di stimolare le stesse banche a sviluppare nuovi servizi digitali, proponendosi loro stesse come terze parti.

Dal suo avvio nel 2019, il nuovo mercato sta mostrando miglioramenti su vari fronti: dalla *performance*, con tempi di esecuzione delle chiamate API che sono praticamente dimezzati, sino all'ampiezza dell'offerta (in termini di numero di terze parti) e alla diffusione tra i clienti finali con un generale miglioramento dell'affidabilità. Ciò attesta sia la qualità delle attività di sviluppo e di *testing* svolte dagli operatori sia l'entità dei loro investimenti in capacità di calcolo. Nell'ambito dei servizi utilizzati continuano a predominare le attività ai fini informativi mentre il totale semestrale dei pagamenti effettuati da ciascun cliente, nel primo semestre del 2022, è in media di poco superiore ai €2.800.

Ulteriori miglioramenti sono attesi dalle nuove iniziative in atto, sia per la completa rimozione degli ostacoli per le terze parti (come da linee guida EBA), ma ancor di più per i comportamenti maggiormente proattivi da parte degli operatori di mercato.

La spinta tecnologica in corso funge da stimolo anche alla ricerca di nuovi servizi e strumenti di pagamento e, con essi, allo sviluppo di quei sistemi e infrastrutture ad alta operatività e resilienza che sono necessari per rendere disponibili e accessibili le forme di pagamento innovative. Diversi fattori spingono per una maggiore integrazione della fase di puro pagamento nella più ampia catena dei servizi finanziari offerti al cliente. Quelli di *open banking* previsti dalla PSD2 hanno definito un nuovo paradigma di interazione per i pagamenti al dettaglio, basato essenzialmente su tecnologia API, soggetti vigilati e accesso al conto del cliente.

Questo approccio in futuro potrà essere esteso in varie direzioni, a servizi finanziari di diversa natura e a soggetti non necessariamente regolamentati dalla PSD2. La disponibilità *on-line* dei dati del cliente apre infatti la strada a servizi che vanno oltre quelli disciplinati dalla direttiva. Il mondo dell'*open banking* potrebbe evolvere verso paradigmi più ampi, come ad esempio l'*open finance*: ciò è reso possibile dalle tecnologie che oggi abilitano

l'utilizzo di strumenti quali l'intelligenza artificiale, i *big data* e i registri distribuiti. Alle autorità pubbliche spetta il compito di creare le condizioni affinché tale ricchezza di strumenti non porti le forze di mercato a divergere in una costellazione di soluzioni frammentate, quanto piuttosto a convergere verso ecosistemi coerenti e interdipendenti, nell'ottica di un pieno governo delle tendenze evolutive.

Lo sviluppo di soluzioni avanzate dovrebbe consentire di contemperare le esigenze degli operatori con le ambizioni del legislatore europeo, così come definite nella "Strategia dei pagamenti *retail*"[47] e nella connessa "Strategia sulla finanza digitale"[48]. A questo fine, gli sviluppi di mercato dovranno essere accompagnati e indirizzati da una evoluzione dell'impianto normativo che, nel rispetto degli interessi delle varie parti coinvolte e secondo un criterio di proporzionalità, continui a favorire la diffusione di nuovi servizi nell'ambito di un sistema finanziario solido, inclusivo e aperto all'innovazione.

47 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0592

48 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591

Appendice

A.1 Evoluzione delle tecniche di accesso ai dati

Le terze parti, prima che i servizi di *open banking* venissero regolati, utilizzavano diverse tecniche per accedere ai conti disponibili *on-line* dei clienti che avevano concesso il permesso di accedere alle proprie informazioni bancarie, tra cui:

1. ***Screen Scraping***. Una forma di intercettazione dei dati dai siti web, che nacque inizialmente come copia/incolla manuale, evolvendo poi in processi *software* automatizzati in grado di emulare le modalità di accesso del cliente. Per accedere ai conti *on-line* i metodi di *screen scraping* richiedono che il cliente inserisca le credenziali di accesso al sito di *internet banking* della propria banca (ad es. nome utente e password) nella pagina web, o nell'APP, che la terza parte utilizza per i servizi di pagamento; la terza parte effettua così l'accesso al sito di *on-line banking* simulando, tramite appositi software, la navigazione del cliente ed eseguendo operazioni dispositive e/o informative al posto del cliente stesso.
2. ***Reverse Engineering***. Queste pratiche sono volte a ricostruire il codice delle applicazioni di *mobile banking* per capire quali informazioni sono scambiate tra l'applicazione del cliente e i server delle banche, realizzando successivamente una versione "*reverse engineered*"[49] dell'applicazione in grado di instaurare direttamente la comunicazione da/verso i server delle banche, senza possibilità di rilevamento e consapevolezza da parte di queste ultime.

Entrambe le tecniche presentano diversi fattori di rischio in termini di sicurezza e di conservazione dei dati. La terza parte, memorizzando le credenziali del cliente e avendo pieno accesso al suo conto ha, ad esempio, la possibilità di accedere a ulteriori informazioni rispetto a quelle per le quali ha ottenuto l'autorizzazione; oppure potrebbe eseguire transazioni finanziarie non autorizzate e modificare, in maniera autonoma e senza consenso, le stesse credenziali di accesso ai dati e ad altre operazioni bancarie del cliente[50]. In tale approccio, inoltre, la terza parte non si identifica esplicitamente nel corso dell'interazione con la banca, con possibili impatti negativi sull'adeguato tracciamento delle attività e sulla ricostruzione delle responsabilità delle transazioni da parte della banca.

Più specificamente, queste tecniche sono state riconosciute dai vari *stakeholder* come poco adatte allo sviluppo di servizi finanziari digitali sicuri ed avanzati, a causa dei rischi sottostanti seguenti:

- sottrazione delle credenziali: le terze parti utilizzano i metodi descritti per raccogliere le credenziali del cliente, che però potrebbero essere sottratte o utilizzate in modo improprio, anche a fini fraudolenti;

---

[49] Con il processo di *reverse engineering* applicato ad una APP di *mobile banking*, è possibile sviluppare una nuova applicazione, una sorta di clone, in grado di replicare gli stessi comandi dell'APP originale. Con questa tecnica le terze parti, disponendo del consenso e delle credenziali del cliente, possono accedere al suo conto dall'applicazione che hanno realizzato.

[50] Vi è inoltre il rischio che una compromissione dei presidi di sicurezza informatica dell'ambiente della terza parte permetta ad un hacker di sottrarre le credenziali degli utenti, precedentemente memorizzate, ed utilizzarle per attività illecite e fraudolente.

- frode: *screen scraping* e *reverse engineering* possono minare la capacità di una banca di identificare transazioni fraudolente, poiché le banche non possono sempre distinguere tra cliente, aggregatore di dati, esecutore di disposizioni di pagamento autorizzato o una terza parte non autorizzata che effettua l'accesso ed estrae informazioni;
- forzatura della capacità di traffico: le terze parti, ad esempio gli aggregatori di dati, possono accedere all'interfaccia cliente della banca ed estrarre grandi volumi di dati a intervalli ravvicinati, il che può mettere a dura prova i sistemi informatici della banca.

Al fine di superare questi limiti si fa ricorso a due tecnologie alternative allo *screen scraping* e al *reverse engineering*:

a. *Application Programming Interface* (API) – le API, come meglio illustrato nel seguito, consentono ai programmi software di comunicare tra loro e di condividere informazioni. In particolare, forniscono un maggiore controllo sul tipo e sull'estensione dei dati condivisi[51] e garantiscono un livello di sicurezza più elevato nell'interazione tra intermediari e terze parti. In questo modo le banche possono sia delimitare l'insieme dei dati dell'utente e dei servizi resi disponibili alle terze parti, sulla base di normative e/o accordi contrattuali, sia sviluppare velocemente interfacce dedicate con cui consentire l'accesso diretto a dati e servizi bancari da parte di tali soggetti;

b. *autenticazione tokenizzata* – i moderni protocolli di autenticazione consentono di disaccoppiare il soggetto che verifica l'identità del cliente e che ne conosce le credenziali (*identity provider – IP*) dal soggetto che gestisce i dati e fornisce servizi al cliente (*resource provider – RP*). Secondo questi modelli: i) il cliente si identifica con le sue credenziali presso l'IP; ii) quest'ultimo emette un codice identificativo temporaneo, cd. '*token*', verso il RP; iii) la presentazione di tale *token* consente l'accesso ai dati e servizi autorizzati[52]. In questi modelli il RP, che coincide con la terza parte, pur accedendo ai dati non viene mai in possesso delle credenziali dell'utente.

Le soluzioni tecnologiche che si stanno affermando nel settore dell'*open banking* sono spesso basate su queste due tecnologie, che, se da un lato accrescono il livello di sicurezza ed efficienza dei processi di condivisione dei dati bancari, dall'altro possono introdurre maggiori vincoli e limitazioni ai soggetti terzi, con riferimento ad esempio alla visibilità sui dati che è ricondotta ad un esplicito e puntuale consenso del cliente. Con riferimento a quest'ultimo aspetto va tuttavia considerato che, rispetto ad esempio allo screen *scraping*, i modelli di autenticazione *tokenizzati* tramite API pubbliche garantiscono benefici anche alle terze parti, poiché non richiedono loro di adeguare i propri processi automatizzati ogni volta che una singola banca ridisegna la propria interfaccia informatica, spesso composta da complesse pagine multimediali.

---

51 Con la tecnica dello *screen scraping*, di fatto la terza parte ha visibilità su tutti i dati del conto, anche se il cliente è interessato a recuperare solo una parte di essi. In aggiunta potendo la terza parte disporre delle credenziali dell'utente, potrebbe collegarsi anche senza la sua presenza attiva nella sessione di accesso. Al contrario le API consentono di profilare i dati visibili alle terze parti a quelli strettamente necessari all'esecuzione del servizio richiesto.

52 Un esempio molto diffuso di questo modello è l'accesso di un utente a un servizio on-line effettuato inserendo le proprie credenziali di Google, Facebook, etc.

A.2 Implicazioni normative dell'accesso ai dati

Diverse sono le istituzioni nazionali e internazionali che hanno intrapreso azioni specifiche relative all'open banking; alcune hanno adottato nelle proprie giurisdizioni schemi normativi (cd. "*open banking frameworks*") per facilitare, consentire o imporre alle banche di condividere dati con le terze parti, a valle del consenso dei clienti. Tali approcci possono essere classificati secondo tre categorie, riportate di seguito.

1. *Prescrittivo* – Le autorità *impongono* alle banche di condividere i dati dei clienti e richiedono alle terze parti di registrarsi presso le autorità di regolamentazione o di vigilanza competenti (ad es. la PSD2 obbliga le banche a condividere i dati, previo consenso del cliente, con soggetti opportunamente autorizzati dalle autorità nazionali).
2. *Wait & See* – Le autorità adottano un approccio orientato al mercato, non prevedendo regole o linee guida esplicite che richiedano o vietino la condivisione dei dati autorizzati dai clienti da parte delle banche con terze parti.
3. *Facilitatore* – Le autorità adottano una strategia intermedia rispetto alle due precedenti, emettendo linee guida e raccomandazioni, promuovendo la adozione di standard API aperti[53] e specifiche tecniche: l'iniziativa è avviata con provvedimento della autorità, ma la realizzazione della infrastruttura è demandata al mercato. Va in questa direzione, ad es., l'iniziativa *open banking* nel Regno Unito dove l'autorità competente, tramite specifica ordinanza[54], ha richiesto alle maggiori banche del paese di creare un consorzio di sviluppo con compiti di standardizzazione, *governance* e supervisione del sistema[55].

Nelle diverse giurisdizioni sono stati previsti meccanismi a tutela dei clienti che utilizzano i servizi dell'*open banking*, coinvolgendo varie autorità di settore, che possono essere classificate come segue:

- *Bank Supervisors and Overseers* (Autorità di Vigilanza bancaria e di Sorveglianza sul sistema dei pagamenti): fissano i requisiti e svolgono i controlli sulle banche, sulle infrastrutture e sugli altri prestatori di servizi di pagamento regolamentati;
- *Technical Standards Setting Bodies* (organismi per la definizione degli standard tecnici): stabiliscono gli standard e certificano le entità che li rispettano;
- *Competition Authorities* (autorità garanti della concorrenza): vigilano, promuovono e se necessario intervengono per garantire la concorrenza nei mercati;

---

53 Uno *standard* si definisce aperto (*open*) se è disponibile pubblicamente e le cui specifiche possono essere utilizzate senza diritti di licenza. Uno standard chiuso (*closed*) è al contrario proprietario.

54 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/600842/retail-banking-market-investigation-order-2017.pdf

55 Nel 2017 la CMA – *Competition and Markets Authority* – ha emesso una ordinanza con la quale ha chiesto alle principali 9 banche inglesi di creare e finanziare la Open Banking *Implementation Entity (OBIE)* con l'obiettivo di implementare i servizi di Open Banking in UK.

- *Consumer Protection Authorities* (autorità per la protezione dei consumatori): garantiscono che i consumatori non siano svantaggiati da atti o pratiche sleali, ingannevoli o abusivi da parte di tutti i soggetti coinvolti nella prestazione del servizio.
- *Data Privacy Authorities* (autorità garanti per la protezione dei dati personali): stabiliscono gli obblighi a tutela della protezione dei dati personali dei clienti.
- *Alternative Dispute Mechanisms* (meccanismi per la risoluzione delle controversie alternativi alle sedi giudiziarie): forniscono una sede tecnologica (piattaforma) o un processo per mediare le controversie tra consumatori e organizzazioni.

Con l'obiettivo di promuovere l'innovazione e facilitare la concorrenza nel settore bancario, in alcuni casi la responsabilità della regolamentazione e del monitoraggio delle nuove soluzioni di open banking viene affidata all'autorità garante della concorrenza (ad es. in Australia), mentre in altri casi (UE, India, Singapore) questo ruolo è assunto dalla banca centrale o dall'Autorità di Vigilanza bancaria.

A.3 Ruolo delle API

L'offerta dei servizi di open banking non può prescindere dall'utilizzo di una tecnologia che garantisca l'accesso sicuro a parti del patrimonio informativo dei correntisti detenuto dal mondo bancario da parte di attori esterni, quali, ad esempio, le società *fintech* o altri operatori attivi in campo finanziario. Questa tecnologia deve inoltre: i) permettere la segregazione dei dati a cui si ha accesso, ii) consentire modalità di interazione sicure e iii) limitare la complessità tecnica necessaria all'integrazione tra il tradizionale mondo dei pagamenti e i nuovi soggetti. Dal punto di vista operativo questa apertura e condivisione di informazioni avviene prevalentemente attraverso la tecnologia delle API che realizza l'interfaccia di comunicazione tra i vari soggetti coinvolti nell'erogazione dei servizi di pagamento o di consultazione delle informazioni sulle transazioni realizzate.

Le API – Application Programming Interface

Dal punto di vista tecnico un'API è una modalità utilizzata da due sistemi *software* (applicazioni), presenti o meno sullo stesso *computer*, per scambiare dati. Una API consente di collegare i sistemi in modo tale che, prescindendo dalla conoscenza del loro funzionamento interno o della struttura dei dati sottostanti e con uno sforzo ridotto nello studio della documentazione[56], sia possibile sviluppare rapidamente *software* per accedere alle informazioni condivise. Il concetto di API è generale e si può utilizzare anche in procedure

[56] L'interfaccia API rende visibile solo alcuni aspetti di una procedura o di un sistema. La documentazione tecnica necessaria a soggetti esterni per accedere al sistema, tramite l'interfaccia, può limitarsi alla sola descrizione degli elementi esposti su questa, trascurando la struttura interna e l'insieme delle funzioni implementate. Ad esempio la documentazione tecnica di un'interfaccia API che permette di effettuare operazioni dispositive su un conto descrive, e rende disponibili, solo le informazioni e le funzioni di esecuzione di un bonifico on-line e non tutte le funzionalità di *internet banking* implementate e rese disponibili per quel conto (es. lettura lista movimenti, trading, finanziamenti, fatture, etc.).

che dialogano da remoto tramite una rete di comunicazione. In generale quando le API consentono la comunicazione tra applicazioni attestate su sistemi diversi, queste sono anche definite come "*network-based API*".

Con la diffusione di Internet, le cd. "*network-based API*" sono diventate sempre più diffuse, in virtù della loro idoneità allo sviluppo di applicazioni distribuite (costituito da più elementi *software* eseguiti su diversi nodi della rete) che cooperano per realizzare funzioni complesse, accedendo a dati ospitati in diversi punti della rete. Nei casi in cui le specifiche dell'interfaccia (modalità di accesso e uso) siano pubbliche e basate su protocolli/*standard* pubblici ("*standard* aperti") si parla di "*Open API*". Un esempio è quello di una pubblica amministrazione che mette a disposizione i propri dati fornendo un'interfaccia di cui rende note le specifiche tecniche (catalogo dati e modalità di accesso), definite a loro volta usando standard aperti (es: formato *XML* per i dati e protocollo di trasmissione *FTP* o *HTTP*). Questo approccio favorisce la cooperazione tra applicazioni, procedure e organizzazioni distinte, ognuna delle quali da un lato espone dati e funzioni proprie in rete e dall'altro è in grado di richiamare dati e funzioni esposte dalle altre.

Con la diffusione del web, le modalità di implementazione delle API via rete sfruttano protocolli e modelli dati tipici di questo ambiente; si parla in questo caso delle cd. *web-API*. Il modello di scambio dati utilizzato è quello di un'entità ("*client*") che interagisce tramite protocollo *HTTP*[57] con un soggetto che ospita dati e servizi ("server"); da un punto di vista operativo, le web API consentono il dialogo tra due applicazioni via rete, con le stesse modalità attraverso cui il browser sul PC dell'utente recupera i dati dai siti web a cui si collega. Con queste nuove interfacce il web evolve da ambiente di navigazione degli umani a luogo di interazione tra entità *software*, sviluppate a partire da interfacce pubbliche e documentate; va segnalato che le API di natura commerciale e industriale incorporano generalmente anche altri *standard* di natura accessoria, con riferimento, ad esempio, alla sicurezza[58].

A.4 La fall-back exemption in Italia

Gli ASPSP che realizzano interfacce dedicate hanno anche l'obbligo di implementare e rendere operativa un'interfaccia alternativa (cd. interfaccia di *fall-back)*, da utilizzarsi nel caso di indisponibilità dell'interfaccia principale. Gli ASPSP possono richiedere alle autorità competenti di essere esentati dalla realizzazione di detta interfaccia (cd. *fall-back exemption*) dimostrando che l'interfaccia dedicata rispetti i requisiti di performance e robustezza definiti nella normativa. Il legislatore ha previsto tale opportunità al fine di contenere gli oneri derivanti dall'applicazione della PSD2, a carico degli ASPSP, prevedendo al contempo passaggi di verifica nel processo dell'esenzione che garantiscono in ogni caso l'affidabilità dei servizi esposti

---

57 HTTP acronimo di *Hypertext Transfer Protocol*, protocollo standard di trasferimento per ipertesti che governa il trasferimento delle pagine ipertestuali e dei contenuti multimediali nel web tra elaboratori anche dotati di diversa architettura hardware e diverso sistema operativo.

58 Alcuni tra gli *standard* più frequentemente richiamati nelle Open API sono: standard SSL (la connessione tra client e server può essere cifrata attraverso un protocollo SSL/TLS facendo uso di certificati digitali e tecniche di crittografia simmetrica e asimmetrica.); *HTTP con strumento di firma JSON Web Signature* (*JWS*) (a garanzia della integrità e origine dei vari messaggi sulla interfaccia API), e *protocollo OAUTH 2.0* che consente di gestire le autorizzazioni all'accesso a una data risorsa senza condividere password con il gestore della risorsa stessa- Cfr. Hardt (2012).

dalle interfacce. Al fine di armonizzare tale processo, la vigilanza ha predisposto, sin dal 2019, un modello framework di segnalazione tramite cui l'ASPSP fornisce le evidenze richieste dalla normativa EBA per la valutazione dell'adeguatezza delle interfacce dedicate[59]. In particolare, gli ASPSP devono fornire informazioni riguardanti i livelli di servizio, le modalità di pubblicazione delle statistiche di performance dell'interfaccia, le modalità di autenticazione, la descrizione delle funzionalità dell'interfaccia, il processo di risoluzione dei problemi, le evidenze quantitative circa il risultato degli stress test e dei test di funzionalità previsti dagli RTS e confermare infine l'avvio in esercizio dell'interfaccia dedicata.

Come sopra accennato, il mercato italiano ha fatto ampio ricorso alle piattaforme di sistema per lo sviluppo delle interfacce dedicate; ciò ha determinato una stretta interazione tra la funzione di sorveglianza e quella di vigilanza nella valutazione delle domande di esenzione. Infatti, nell'ambito delle soluzioni basate su piattaforme di sistema coesistono, da un lato, elementi specifici che riguardano i singoli prestatori, dall'altro, un sostrato di elementi propri della piattaforma che sono comuni per tutti gli intermediari aderenti. La verifica della coerenza con la normativa di riferimento di tali elementi comuni è stata effettuata per ogni piattaforma una sola volta, dalla funzione di sorveglianza in coordinamento con le strutture di vigilanza. Ciò ha consentito una maggiore celerità dal lato delle autorità e una riduzione degli oneri per gli intermediari.

Nel valutare la conformità delle interfacce dedicate rispetto ai requisiti sanciti dalla PSD2 e dalla sua normativa attuativa (RTS)[60] si tiene conto, in particolare, dell'assenza di aspetti ostativi per l'accesso dei TPP ai conti dei clienti[61]. Altri elementi ritenuti significativi per la valutazione riguardano l'architettura dei sistemi, i servizi offerti, i livelli di servizio garantiti, i piani di *business continuity* e di *disaster recovery*, le misure di sicurezza e di *cyber resilience* adottate per far fronte alle minacce informatiche e il rispetto delle norme per il trattamento dei dati personali.

Infine, dato che le piattaforme di sistema offrono ai singoli prestatori di servizi di pagamento un servizio in outsourcing, è stata verificata la loro aderenza ai requisiti per gli intermediari bancari e finanziari in materia di esternalizzazione.

---

59 EBA GLs EBA/GL/2018/07 "Orientamenti sulle condizioni per beneficiare dell'esenzione dal meccanismo di emergenza a norma dell'articolo 33, paragrafo 6, del regolamento (UE) 2018/389 – norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri".

60 *Regulatory Technical Standards* sulla *Strong Customer Authentication* (cd. SCA) e sulla *Common and Secure Communication (*cd. CSC), Orientamenti, Opinioni e Q&A dell'EBA, ma anche Regolamento UE n. 2016/679 sulla Protezione dei Dati (*General Data Protection Regulation* – GDPR) e Regolamento UE n. 910/2014 sull'identità digitale (*electronic IDentification Authentication and Signature* – eIDAS).

61 In una sintesi non esaustiva, tra gli elementi oggetto di valutazione rientrano: i) livelli di prestazione e disponibilità delle interfacce dedicate equivalenti a quelle già disponibili agli utenti; ii) adeguata pubblicità alla documentazione relativa alle specifiche funzionali e tecniche realizzate per la costruzione delle API; iii) rispetto delle scadenze fissate dagli RTS dell'EBA; iv) ampio utilizzo da parte dei *Third Party Providers*; v) risoluzione tempestiva di eventuali problemi.

Riferimenti bibliografici

Banca d'Italia (2021), PSD2 e *Open Banking: nuovi modelli di business e rischi emergenti*, novembre 2021.

Basel Committee on Banking Supervision (2019), *Report on open banking and application programming interfaces*, BIS, novembre 2019.

Committee on Payment and Settlement Systems (2012), *Principles for financial market infrastructures*, BIS, aprile 2012.

European Banking Authority (2018a), *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*, EBA, giugno 2018.

European Banking Authority (2018b), *Opinion of the European Banking Authority on the use of eIDAS certificates under the RTS on SCA and CSC*, EBA, dicembre 2018.

European Banking Authority (2018c), *Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation* (EU) 2018/389 (RTS on SCA & CSC), EBA, dicembre 2018.

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

European Union (2015), *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC*, EUR-Lex, dicembre 2015.

Gammaldi, D. e C. Iacomini (2019), Mutamenti del mercato dopo la PSD2, in F. Maimeri, M. Mancini (a cura di) "Le *nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*", Banca d'Italia, Quaderni di ricerca giuridica, n. 87, settembre 2019.

Hardt, D. (ed.) (2012), The OAuth 2.0 *Authorization Framework*, IETF, ottobre 2012.

Maimeri, F. e M. Mancini (2019), Introduzione, in F. Maimeri, M. Mancini (a cura di) "Le *nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*", Banca d'Italia, Quaderni di ricerca giuridica, n. 87, settembre 2019.

The Berlin Group (2021), NextGenPSD2 XS2A *Framework Implementation Guidelines*, settembre 2021.

Altre iniziative di Open Banking

Hong Kong - https://www.hkma.gov.hk/eng/key-information/press-releases/2018/20180718-5.shtml

France - https://www.stet.eu/en/psd2

Australia - https://treasury.gov.au/consultation/c2018-t247313

New Zeland - https://www.apicentre.paymentsnz.co.nz/

UK-OBIE - https://www.openbanking.org.uk/about-us

Glossario

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)

BCE: Banca Centrale Europea

CBPII: Card-based payment instrument issuer

EBA: European Banking Authority

EPC: European Payments Council

ERPB: Euro Retail Payments Board

IMEL: Istituto di Moneta Elettronica

IP: Istituto di Pagamento

NCA: National Competent Authority (Autorità Nazionale Competente)

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)

PSU: Payment Service User (Utente di servizio di pagamento)

RTS: Regulatory Technical Standards

SEPA: Single Euro Payments Area

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

TUB: Testo Unico Bancario

Pubblicazioni della collana Mercati, infrastrutture, sistemi di pagamento

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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