VERSO LA REVISIONE DELLA PSD2

Il dialogo della Banca d'Italia con gli operatori del mercato dei pagamenti

Le valutazioni contenute nel documento sono state elaborate nell'ambito del Tavolo di lavoro del CPI dedicato alla revisione della seconda Direttiva sui servizi di pagamento (PSD2) prima della pubblicazione delle proposte normative della Commissione europea; esse intendono fornire un contributo, da parte dell'industria dei pagamenti nazionale, alle analisi connesse con lo svolgimento delle attività legislative in corso.

MAGGIO 2024
BANCA D'ITALIA

Indice

Premessa 3

1. Frodi e *Strong Customer Authentication* (SCA) 5

1.1. Introduzione 5

1.2. Regime di responsabilità in caso di transazioni non autorizzate 5

1.3. Blocco/recupero fondi 7

1.4. Ulteriori misure di rafforzamento della sicurezza 8

1.4.1. Sicurezza Antifrode 9

1.4.2. IBAN/*name check services* 9

1.4.3. *Data sharing* tra PSP 9

1.4.4. Educazione finanziaria degli utenti 10

1.5. Esclusioni/esenzioni per prevenire fenomeni di SCA *circumvention* 10

1.5.1. MIT - *Merchant Initiated Transaction* 10

1.5.2. MOTO - *Mail Orders or Telephone Order* 11

1.6. Nuove fattispecie di transazioni esentate dalla SCA 11

1.7. Nuovi sviluppi in tema di autenticazione forte 12

2. *Open Banking* 14

2.1. Introduzione 14

2.2. *Dedicated vs. adapted interfaces* 14

2.3. Standard unico API 14

2.4. Modello di remunerazione per servizi di *open banking* 15

2.5. Estensione dell'esenzione dalla SCA (transazioni effettuate tramite PISP) 16

2.6. Possibilità di revoca di un ordine effettuato tramite PISP 16

3. Accesso ai conti e ai sistemi di pagamento 18

3.1. Introduzione 18

3.2. Accesso ai conti di pagamento 18

3.3. Accesso ai sistemi di pagamento 19

4. *Scope* della nuova normativa sui servizi di pagamento al dettaglio 21

4.1. Introduzione 21

4.2. Possibili modifiche del *positive scope* 21
4.3. Possibili modifiche del *negative scope* 23
5. Coordinamento tra PSD2 e altre normative rilevanti per il settore pagamenti 26
5.1. Introduzione 26
5.2. PSD2 e EMD2 26
5.3. PSD2 e GDPR 28
5.4. PSD2 e DORA 29
5.5. PSD2, EMD2 e MiCAR 30
Annex I: Analisi d'impatto della Strong Customer Authentication (SCA) sulla sicurezza dei pagamenti con carte da remoto in Italia 33
Annex II: Il modello di remunerazione dell'Open Banking nel confronto internazionale 37
Bibliografia Annex II 38

Premessa

Nell'ambito del Comitato Pagamenti Italia (CPI) a marzo 2023 sono stati costituiti tre tavoli di lavoro in materia di: i) revisione della seconda Direttiva sui servizi di pagamento (PSD2); ii) *open banking*; iii) incassi e pagamenti pubblici.

Il presente documento sintetizza gli approfondimenti svolti dal Tavolo dedicato alla revisione della PSD2 le cui riflessioni svolte si inseriscono in un contesto di mercato caratterizzato da forti spinte innovative in chiave di digitalizzazione, spinte che arrivano dagli operatori ma anche dalla normativa che ha un ruolo importante anche in chiave di "trazione" del mercato.

In particolare, i lavori si sono concentrati sull'individuazione delle tematiche più rilevanti per il mercato italiano, avvalendosi della consolidata esperienza di cooperazione del CPI e favorendo il consolidamento di una visione il più possibile condivisa da parte di tutti gli attori dell'ecosistema nazionale dei pagamenti anche con l'obiettivo di identificare proposte e soluzioni in grado di raccogliere un più ampio consenso e di costituire un punto di riferimento nell'ambito delle attività di revisione della sopra cennata Direttiva.

Il tavolo ha affrontato le seguenti tematiche: (i) misure per il contenimento delle frodi e il conseguente regime di responsabilità di prestatori, fornitori di servizi tecnici e utenti dei servizi di pagamento; (ii) nuove modalità di autenticazione nell'ambito della *strong customer authentication* (SCA), esenzioni già operative e individuazione di nuove; (iii) modifiche da apportare ai servizi di *open banking*; (iv) ridefinizione del perimetro applicativo (positivo e negativo) della nuova normativa; (v) fusione con la Direttiva sulla moneta elettronica (EMD2) e coordinamento tra PSD2 e altre normative rilevanti per il settore pagamenti.

Il documento rappresenta una fotografia dei lavori sinora svolti dal Tavolo e riporta le riflessioni condotte alla luce dell'esperienza maturata nel contesto dell'applicazione della PSD2. Le valutazioni riportate nel presente documento sono state elaborate in un momento antecedente alla pubblicazione (avvenuta il 28 giugno 2023) delle proposte normative della Commissione europea per la revisione della PSD2 - che si compone di due distinti atti, una Direttiva e un Regolamento, nel solco dell'esperienza già seguita nell'ambito di altre normative finanziarie. Si precisa che il dibattito sulla revisione della richiamata disciplina è in corso di svolgimento nelle deputate sedi istituzionali europee e che i relativi contenuti non sono esaminati nel presente documento. Le valutazioni di seguito espresse non rappresentano posizioni vincolanti per gli attori istituzionali o per gli altri partecipanti al Tavolo.

Fermo restando quanto sopra, si fa presente che molte delle valutazioni emerse nell'ambito dei lavori del Tavolo risultano allineate alle soluzioni normative proposte nel testo della Commissione. Il presente documento tiene conto anche degli esiti del negoziato sul Regolamento sugli *instant payments*, di recente pubblicato come Regolamento (UE) 2024/886, limitatamente ai profili del Regolamento che potranno avere un impatto su alcuni dei temi dibattuti dal Tavolo.

Le attività del Tavolo proseguiranno, anche avendo a base le riflessioni contenute nel presente documento e la loro consistenza con la proposta della Commissione, con l'obiettivo di continuare a raccogliere le posizioni della comunità nazionale dei pagamenti e fornire potenziali spunti utili nel prosieguo dei lavori in sede europea.

1. Frodi e *Strong Customer Authentication* (SCA)

1.1. Introduzione

Nell'ambito della revisione[1] della Direttiva (UE) 2015/2366 (*Second Payment Services Directive* – PSD2)[2], il tema delle frodi a danno degli utenti e quello dei presidi posti a tutela della sicurezza dei pagamenti rivestono un'importanza cruciale.

Il dibattito in seno al tavolo tecnico del CPI si è concentrato su alcuni dei profili di maggiore interesse dal punto di vista del mercato, come illustrato nei paragrafi che seguono.

1.2. Regime di responsabilità in caso di transazioni non autorizzate

Con riguardo alle responsabilità delle parti in presenza di operazioni di pagamento non autorizzate dall'utente, sono in primo luogo emerse esigenze di chiarimento rispetto ad alcuni concetti che la PSD2 richiama nel dettare tale regime di responsabilità, senza tuttavia darne una compiuta definizione (ad esempio, "colpa grave" dell'utente, "frodi" e "truffe"[3]).

Questi concetti risultano inevitabilmente ancorati alle specificità dei diversi ordinamenti nazionali e, pertanto, potrebbe risultare difficile definirli a livello armonizzato. D'altra parte, come suggerito anche dall'*European Banking Authority* (EBA) nella *Opinion* sulla revisione della PSD2 del giugno 2022[4] potrebbe essere opportuno specificare meglio alcuni termini che la Direttiva non definisce (quali "*gross negligence*", "*fraudolent act*" o "*reasonable grounds to suspecting fraud*") per risolvere i dubbi interpretativi e le disomogeneità applicative che potrebbero derivarne nei vari Stati membri.

Inoltre, il Tavolo ha dibattuto l'adozione di misure volte a contenere le perdite derivanti da operazioni non autorizzate e spesso gravanti sui prestatori di servizio di pagamento (*Payment Service Provider* – PSP). Al riguardo, potrebbe essere rafforzato il ruolo di guida e indirizzamento previsto in capo a questi ultimi dalle *Guidelines* dell'EBA su *ICT and security risk management* (EBA/GL/2019/04). In particolare, potrebbero essere compiuti approfondimenti rispetto alla proposta dell'EBA (contenuta nella già menzionata EBA *Opinion*) di trasporre nella nuova normativa alcune delle suddette GL[5]. Ancora, potrebbe essere valutata la proposta di prevedere che i PSP

[1] In data 28 giugno 2023 la Commissione europea ha pubblicato una proposta di revisione della PSD2 che si compone di due atti: (i) una proposta di Direttiva (*Third Payment Services Directive* – PSD3) recante le disposizioni in tema di autorizzazioni e vigilanza e (ii) una proposta di Regolamento (*Payment Services Regulation* – PSR) con le disposizioni in materia di prestazione dei servizi di pagamento, tra cui la trasparenza delle condizioni e i requisiti informativi per i servizi di pagamento, nonché i diritti e gli obblighi in relazione alla prestazione di detti servizi.

[2] Consultabile al seguente link.

[3] Con riferimento al concetto di "truffa", si è osservato, nel corso dei lavori del Tavolo, che esso rinvia a fattispecie penalmente rilevanti diversamente dettagliate a livello nazionale e che fuoriescono dalle competenze di questo Tavolo.

[4] Cfr. *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2).*

[5] Per esempio, si potrebbe inserire nella futura normativa la GL che assegna ai PSP il compito di porre in essere *transaction monitoring mechanisms* (TMM) volti anche a rintracciare casi di *well-known fraud scenarios* sui quali

aggiornino i propri clienti sulle nuove minacce e vulnerabilità mediante l'invio di specifici *alert* che mettano in guardia gli utenti sulle più recenti o pericolose tecniche di frode riscontrate (es. *social engineering frauds*), così da diffondere la consapevolezza delle frodi e favorire comportamenti responsabili.

Sul tema si evidenzia che gli intermediari si stanno già attivando mediante attività di formazione dei propri dipendenti e informazione verso la clientela anche mediante campagne effettuate tramite le associazioni di categoria (ad. esempio l'Associazione Bancaria Italiana (ABI) ha richiamato le attività del CERT Finanziario Italiano-CERTFin e della Fondazione per l'Educazione Finanziaria e al Risparmio-FEduF. Anche la Banca d'Italia è fortemente coinvolta in iniziative della specie (cfr. par. 1.4.4).

In questo quadro, la valutazione della colpa grave dell'utente andrebbe comunque effettuata in concreto, tenendo in considerazione il grado di sofisticazione e la natura più o meno nota della frode subita dall'utente. Al riguardo, è emerso che un utile punto di riferimento, in tema di responsabilità, può essere rappresentato dalle pronunce dei collegi dell'Arbitro Bancario Finanziario (ABF), i quali sono già orientati nel senso di riconoscere di regola la colpa grave dell'utente in presenza di frodi che presentano indici di tale inattendibilità (quali ad esempio l'invio di messaggi c.d. civetta recanti errori grammaticali o sintattici) o anomalia (quale l'invito a inserire le proprie credenziali di autenticazione in un sito in nessun modo riferibile all'intermediario) tali da allertare l'utente avveduto. La negligenza dell'utente rileva anche nei casi in cui cada vittima di forme di frode (ad es. il c.d. *phishing*) che hanno raggiunto un grado di diffusione tale da potersi considerare ormai note da diversi anni.

Il comportamento dell'utente non può dirsi invece connotato da colpa grave nei casi in cui egli sia vittima di frodi sofisticate, caratterizzate da un effetto sorpresa capace di spiazzare l'utilizzatore, per esempio grazie alla perfetta inserzione nell'ambiente informatico originale e nella correlata simulazione di un messaggio che non potrebbe apparire che genuino.

Trattandosi di orientamenti consolidati e considerato che l'apprezzamento delle circostanze del caso concreto appare essenziale, anche per consentire la flessibilità interpretativa necessaria in scenari esposti a una rapida e continua evoluzione come quello in esame, eventuali modifiche del riparto di responsabilità attualmente previsto dalla PSD2[6] andrebbero valutate con attenzione.

Al riguardo è emersa anche la necessità di introdurre obblighi di cooperazione di operatori quali i fornitori di servizi di comunicazione elettronica (*Electronic Communication Service Providers*, e.g.

---

incrementare la consapevolezza degli utenti nonché fornire assistenza e *guidance* alla luce delle nuove minacce e vulnerabilità (cfr. *Guideline* 3.8 of the *Guidelines on ICT and security risk management* (EBA/GL/2019/04).

[6] Secondo la normativa vigente, il pagatore sopporta le perdite derivanti da operazioni non autorizzate e disconosciute solo nei casi in cui egli abbia agito in modo fraudolento oppure abbia violato gli obblighi su di esso gravanti con dolo o colpa grave. Di regola, dunque, la responsabilità di operazioni non autorizzate ricade sul PSP del pagatore, che ha anche l'onere di provare eventualmente che: i) l'operazione eventualmente disconosciuta è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti (art. 10, comma 1, d.lgs. n. 11/2010) ; ii) l'utente abbia agito in maniera fraudolenta, dolosa o gravemente colposa (art. 10, comma 2, d.lgs. n. 11/2010).

Telecommunications companies – Telco) e i fornitori di servizi tecnologici (*Technical Service Provider* – TSP) con i PSP così da consentire l'adozione di misure volte a prevenire/rilevare le frodi, salvaguardare la sicurezza e la riservatezza delle comunicazioni, agevolare il recupero delle somme e il rintracciamento dell'autore della frode (ad esempio tramite l'identificazione della linea chiamante e l'indirizzo di posta elettronica). Per alcune tipologie di TSP (es. *wallet provider*) che hanno un ruolo rilevante nella catena dei pagamenti, è stata evidenziata la necessità di prevedere una responsabilità finanziaria per danni derivanti dalla mancata prestazione dei servizi contrattualizzati (con i PSP) necessari all'applicazione della SCA[7].

1.3. Blocco/recupero fondi

Al tema della prevenzione delle frodi è legato quello del blocco dell'operatività degli strumenti di pagamento per ragioni antifrode.

L'applicazione della normativa vigente sul punto (art. 68 della PSD2 e disciplina nazionale di attuazione) ha fatto emergere la generale esigenza del mercato di ottenere un affinamento delle soluzioni previste a livello legislativo, così da consentire un più agevole recupero dei fondi e da ridurre i rischi legali per gli intermediari (es. appropriazione indebita). Il tema è menzionato anche dall'EBA nella sua *Opinion* sulla revisione della PSD2 e merita approfondimenti in merito alla potenziale modifica delle norme di riferimento, volta a favorire prassi applicative più omogenee nonché una maggiore efficacia nell'attività di prevenzione delle frodi, anche in riferimento a singole operazioni di pagamento.

A tale riguardo, i partecipanti al Tavolo hanno sottolineato l'opportunità di prevedere normativamente alcune misure volte a prevenire le frodi mediante il blocco dell'operazione o dello strumento di pagamento o a recuperare i fondi in caso in cui il sospetto di frode emerga dopo l'esecuzione del pagamento.

In particolare, sono state avanzate alcune ipotesi di modifica degli artt. 68 e 79 della PSD2. Per quanto riguarda l'art. 68, si è evidenziata l'opportunità di prevedere la facoltà (anche ove non previsto dal contratto quadro, come invece è richiesto dalla normativa vigente) per i PSP di effettuare il blocco dell'operazione (oltre al blocco della complessiva operatività dello strumento, già previsto dalla PSD2) in caso di sospetto di frode[8] per poter effettuare le necessarie verifiche (es. scambi informativi con il cliente e con il PSP del beneficiario per reperire i documenti e informazioni necessari attestanti la frode). A tale riguardo, risulterebbe necessario un allineamento tra la disciplina sui servizi di pagamento e il Regolamento (UE) 2016/679 (*General Data Protection Regulation* – GDPR) per contemperare l'interesse del pagatore ad ottenere le informazioni e la tutela del diritto di *privacy* del beneficiario[9]. Con riferimento all'art. 79, sarebbe opportuno valutare

[7] Le tematiche sono trattate più in dettaglio nel paragrafo 4.2.
[8] Tale esigenza è maggiormente sentita nel caso in cui non sia possibile effettuare una revoca del pagamento (es. bonifici *instant*).
[9] Il tema dell'allineamento tra le due normative è trattato più in dettaglio nel paragrafo 5.3. Il GDPR è consultabile al seguente link.

l'introduzione della facoltà per il PSP di rifiutare l'esecuzione di un ordine di pagamento quando sospetta una frode.

In via complementare con quanto sopra, potrebbe valutarsi la proposta di modificare l'art. 83 della PSD2, al fine di favorire il recupero dei fondi dopo l'esecuzione di un'operazione potenzialmente fraudolenta, per prevedere che in caso di sospetto di frode su una singola operazione eseguita dal PSP del pagatore, l'accredito sul conto corrente del beneficiario possa essere sospeso in attesa del compimento delle relative verifiche. Ove l'esito delle verifiche dovesse confermare la natura fraudolenta dell'operazione eseguita, ma non ancora accreditata, si potrebbe prevedere la possibilità per il PSP del beneficiario di restituire i relativi importi al PSP del pagatore (e quindi al pagatore), a prescindere dal consenso del beneficiario.

Sempre in relazione alle ipotesi di sospetta frode, sono emerse diverse valutazioni in merito alla potenziale modifica del termine previsto dall'art. 73 della PSD2 per il rimborso degli importi di operazioni non autorizzate (che nel vigente regime, come noto, deve avvenire immediatamente e in ogni caso al più tardi entro la fine della giornata operativa successiva a quella in cui il PSP prende atto dell'operazione o riceve una notifica in merito). Alcuni partecipanti riterrebbero opportuno modificare l'art. 73 per consentire ai PSP di sospendere il rimborso anche nei casi in cui sorga il sospetto che il cliente sia stato vittima di frode, in attesa degli esiti delle verifiche sulla genuinità dell'operazione. Altri partecipanti al Tavolo, da un lato concordano con l'esigenza di disciplinare in modo più chiaro ed esaustivo la procedura con la quale i PSP devono gestire le ipotesi di operazioni non autorizzate, definendo in particolare tempistiche certe entro le quali i PSP debbano svolgere le necessarie verifiche e procedere all'eventuale rimborso in via definitiva. Dall'altro, ritengono che le valutazioni in merito alla suddetta procedimentalizzazione dovrebbero riguardare più complessivamente tutte le ipotesi di operazioni non autorizzate e non limitarsi ai soli casi di sospetto di frode.

In merito al recupero dei fondi è stata evidenziata, infine, la necessità di individuare una soluzione che possa risolvere la discrasia delle tempistiche legate alla notifica delle operazioni non autorizzate o non correttamente eseguite, previste dalla normativa e dalle regole dei circuiti[10].

1.4. Ulteriori misure di rafforzamento della sicurezza

Attenzione particolare è stata rivolta al rafforzamento dei presidi di sicurezza attualmente previsti in normativa, mediante interventi indirizzati su più fronti, tra cui rilevano: i) sicurezza antifrode; (ii) IBAN/*name check services*; iii) condivisione di dati tra PSP e iv) educazione finanziaria dell'utente.

[10] Ad oggi, infatti, mentre il regime della PSD2 prevede un termine di 13 mesi per notificare operazioni non autorizzate o non correttamente eseguite, le regole dei circuiti internazionali fissano tale termine a 120 giorni. Tale discrasia temporale – riconducibile alle regole *ex* PSD2 che consentono al PSP di rendicontare all'utente le operazioni di pagamento anche solo annualmente – può in alcuni casi non consentire la gestione delle contestazioni nell'ambito dei circuiti (*chargeback*) richiedendo al PSP di ricorrere a modalità più onerose per il recupero delle somme.

1.4.1. Sicurezza Antifrode

In tema di sicurezza è stata valutata la possibilità di potenziare i processi antifrode dei prestatori del servizio di pagamento di radicamento del conto (*Account Servicing Payment Service Provider* – ASPSP) nel contesto dei servizi di *open banking*. Tali processi devono essere alimentati, tra l'altro, dai dati di contesto del cliente (es. strumento, indirizzo, *device*) al fine di calcolare degli indicatori di rischio. Tali informazioni sono tuttavia confinate, in certe fasi della sessione, al rapporto tra terze parti (*Third Party Providers* – TPP)[11] e cliente e non sono direttamente disponibili all'ASPSP. In questo ambito, per una piena efficacia dei sistemi antifrode, potrebbe essere utile ampliare il *set* informativo fornito dalle TPP agli ASPSP, rispetto a quanto previsto già ora dalla normativa.

Al riguardo si potrebbe prevedere l'obbligo per i prestatori di servizi di informazione sui conti (*Account Information Service Provider* – AISP) e i prestatori del servizio di disposizione di ordini di pagamento (*Payment Initiation Service Provider* – PISP) di effettuare gli stessi controlli all'accesso fatti dagli ASPSP e fornire tutte le informazioni utili per effettuare i necessari controlli (es. indirizzo IP dell'utente coperto dall'interfaccia TPP in modalità *embedded*), e/o uno *scoring* complessivo dell'operazione, bloccando le operazioni sospette *ab origine*.

1.4.2. IBAN/*name check services*

A fronte delle diverse proposte emerse dai partecipanti al Tavolo relativamente al servizio di verifica della corrispondenza tra identificativo unico (*International Bank Account Number* – IBAN) e nominativo del beneficiario del pagamento, si ha presente che il Regolamento in materia di bonifici istantanei, recentemente pubblicato, prevede che i PSP si dotino di un meccanismo di IBAN/*name check* da applicarsi a tutte le tipologie di bonifico (diversamente dalla proposta iniziale della Commissione che limitava l'obbligo di offerta di questo servizio in caso di pagamenti istantanei). L'estensione di tale meccanismo anche ai bonifici tradizionali concorrerà a rafforzare gli standard di sicurezza dei pagamenti all'interno dell'UE e la tutela degli utenti, benché possa comportare maggiori costi in capo agli intermediari.

1.4.3. *Data sharing* tra PSP

In tema di condivisione dei dati tra PSP, il Tavolo ha discusso le possibili iniziative per la creazione di un *database* centralizzato contenente i codici IBAN dei soggetti frodatori[12] che potrebbe rappresentare uno strumento utile a garantire un'azione tempestiva degli intermediari rispetto alle condotte di tali soggetti; potrebbe essere utilmente valutabile anche la creazione di un *repository* con le informazioni sulle tendenze riscontrate in tema di prassi fraudolente[13] nonché - avendo

[11] Nel presente documento con il termine terze parti (*Third Party Providers* – TPP) si fa riferimento ad entrambi i prestatori di servizi di *Open Banking*, ovvero PISP e AISP.

[12] Un *database* del genere conterrebbe solo riferimenti ai frodatori accertati poiché il mero sospetto nei confronti di un frodatore non potrebbe giustificare il blocco dei fondi o altre misure privative, che sarebbero in contrasto con il principio costituzionale della presunzione di innocenza.

[13] Le modalità di tenuta del registro potrebbero essere molteplici e andrebbero analizzate e coordinate a livello europeo, anche per tenere conto di iniziative già in essere, ad es. la piattaforma di *info sharing* sulle frodi promossa dal *Payment Scheme Fraud Prevention Working Group* (PSFPWG) nell'ambito dell'*European Payments Council* (EPC). Andrebbe anche valutata l'opportunità di un allineamento normativo tra PSD e GDPR al fine di garantire maggiore certezza sul perimetro delle informazioni che possono essere scambiate.

riguardo alla composizione e alla governance nonché alle modalità di coordinamento e integrazione con il CERTFin, al fine di evitare sovrapposizioni rispetto alle attività di prevenzione delle frodi e di *info sharing* già in essere – la possibile istituzione di un consesso – un eventuale comitato antifrode – volto a mettere a fattor comune le prassi efficaci adottabili dagli intermediari per il contrasto alle frodi. In ogni caso, lo scambio tra PSP di dati utili a prevenire potenziali frodi presuppone una chiara individuazione sia del perimetro informativo da condividere sia delle eventuali responsabilità in capo ai PSP che facciano ricorso alle informazioni acquisite.

1.4.4. Educazione finanziaria degli utenti

Si è valutata l'esigenza di potenziare le misure volte a prevenire e ridurre l'impatto delle frodi mediante l'incremento della consapevolezza degli utenti circa i rischi di sicurezza legati ai servizi di pagamento. A questo scopo, risulta cruciale "educare" la clientela, in particolare con riferimento ai servizi digitali, al loro corretto utilizzo, alle implicazioni in termini di responsabilità, ai comportamenti da tenere (anche volti alla collaborazione degli utenti con i PSP nel fornire le informazioni necessarie per l'identificazione e gestione dell'evento fraudolento), all'uso dei dati come mezzo per consentire la prestazione di servizi a valore aggiunto.

A tal proposito, potrebbe essere positivamente valutata la possibilità di fare esplicita menzione dell'educazione finanziaria degli utenti nella futura disciplina europea sui servizi di pagamento, come peraltro già avviene in altre Direttive in materia di trasparenza e correttezza dei rapporti tra intermediari e clienti[14].

Si sottolinea inoltre che la Banca d'Italia è direttamente coinvolta in varie iniziative volte a informare il pubblico sul tema delle frodi nei pagamenti e sui comportamenti da adottare per prevenirle[15].

1.5. Esclusioni/esenzioni per prevenire fenomeni di SCA *circumvention*

La PSD2 prevede l'obbligo di SCA nel caso in cui, fra gli altri, il pagatore disponga un'operazione di pagamento elettronico. Come tale, l'obbligo di SCA non si applica qualora l'operazione di pagamento sia disposta dal beneficiario, oppure sia disposta ed eseguita con modalità diverse rispetto all'uso di piattaforme o dispositivi elettronici. Tali forme di esclusione, nel loro essere definite in via generale dalla PSD2, pongono tuttavia il rischio di ingenerare fenomeni di SCA *circumvention*, a cui è opportuno far fronte in sede di revisione della PSD2.

1.5.1. MIT - *Merchant Initiated Transaction*

Le c.d. MIT – *Merchant Initiated Transactions*, in quanto rientranti tra le operazioni di pagamento disposte dal beneficiario, non sono soggette all'obbligo di SCA. La PSD2 non riporta tuttavia una definizione per quest'ultima tipologia di pagamenti, da cui dunque il rischio che operazioni che in

[14] Si vedano in proposito, ad es., i riferimenti contenuti nell'art. 20 della Direttiva (UE) 2014/92 (*Payment Account Directive* – PAD), nell'art. 6 della Direttiva (UE) 2014/17 (*Mortgage Credit Directive* - MCD) e nell'art. 34 della seconda Direttiva in materia di credito al consumo (Direttiva (UE) 2023/2225, *Second Consumer Credit Directive* – CCD2).

[15] Al tema in esame viene dedicata particolare attenzione sul sito di educazione finanziaria "L'economia per tutti" e ai moduli dedicati inclusi nelle iniziative formative destinate sia al largo pubblico sia a target specifici (donne, piccoli imprenditori, giovani in età scolare e adulti che frequentano le scuole serali). La protezione della clientela dalle frodi è inoltre al centro di varie campagne di sensibilizzazione promosse dalla Banca d'Italia.

realtà sono *Customer Initiated Transactions* (CIT) – a cui andrebbe pertanto applicato il requisito della SCA – vengano erroneamente trattate come MIT. Altra questione riguarda la differenza di trattamento in termini di tutela della clientela rispetto al *Sepa Direct Debit* (SDD) che, pur presentando delle similitudini con le MIT, consente al pagatore di richiedere, a certe condizioni, il rimborso dell'operazione già autorizzata entro otto settimane dall'addebito (artt. 76 e 77 della PSD2); in caso di disconoscimento di una MIT per il rimborso si applicano invece le previsioni generali di cui all'art. 71 della PSD2[16].

Per far fronte alle predette criticità, risulterebbe opportuno introdurre nella revisione della PSD2 una definizione di MIT (anche rispetto alla differenza con le MOTO, *infra*), che ne chiarisca il perimetro, valutando inoltre la possibilità di includere i contenuti di cui alle Q&A EBA[17]. Si tratterebbe, inoltre, di valutare l'opportunità di individuare soluzioni per superare la differenza di trattamento rispetto al SDD in termini di tutela della clientela.

1.5.2. MOTO - *Mail Orders or Telephone Order*

Il legislatore UE (cfr. considerando 95, PSD2) non ha ravvisato la necessità di garantire lo stesso livello di protezione previsto per i servizi di pagamento elettronici – si pensi in particolare all'obbligo di SCA – alle operazioni di pagamento disposte ed eseguite con modalità diverse tra cui, ad esempio, gli ordini per corrispondenza e quelli telefonici (c.d. MOTO – *Mail Orders or Telephone Orders*). Purtuttavia, la PSD2 non riporta alcuna definizione per quest'ultima tipologia di pagamenti, cosa che può ingenerare confusione tra le MOTO e i pagamenti da remoto che richiedono invece la SCA, con il rischio di dar luogo a fenomeni di SCA *circumvention*.

A fronte di tale criticità, occorrerebbe fare chiarezza proponendo una definizione puntuale delle MOTO, anche rispetto alla differenza con le MIT, che ne definisca il perimetro e ne evidenzi le specifiche caratteristiche, al fine di distinguerle dalle operazioni di pagamento elettronico effettuate da remoto. In particolare, si ritiene utile esaminare le Q&A EBA sul tema[18], verificando la possibilità di includerne i contenuti nella revisione della PSD2. A complemento di tali proposte, si suggerisce altresì di individuare eventuali misure idonee a mitigare potenziali fenomeni fraudolenti dovuti a meccanismi di controllo meno stringenti (in particolare legati, come citato, all'esenzione dalla SCA).

1.6. Nuove fattispecie di transazioni esentate dalla SCA

La PSD2 e il relativo Regolamento delegato (UE) 2018/389 includono requisiti di sicurezza al fine di ridurre il rischio di frode nei pagamenti e garantire la sicurezza nelle transazioni. Con l'aumento del numero di acquisti effettuati online, si sono infatti rese necessarie ulteriori misure di protezione per garantire una maggiore tutela dei clienti. Se da un lato la sicurezza dei pagamenti, la protezione contro le frodi e il contrasto all'utilizzo improprio dei dati di pagamento sono obiettivi fondamentali, dall'altro lato risulta importante sostenere soluzioni di pagamento rapide, efficienti e facili da usare.

[16] Ai sensi dell'art. 71 della PSD2, l'utente dei servizi di pagamento ottiene una rettifica dal PSP se, venuto a conoscenza di un'operazione di pagamento non autorizzata o non correttamente eseguita, ne informa il PSP senza indugio ed entro 13 mesi dalla data di addebito.
[17] Cfr. Q&A EBA 2018/4031-4131, 2019/4664-4776-4866-4792-4794.
[18] Cfr. Q&A EBA 2018/4058, 2019/4788-4790, 4791, 2020/5215-5534, 2021/6315.

La continua ricerca del miglior *trade-off* tra sicurezza ed efficienza nei pagamenti *retail*, richiede di valutare, nel contesto della revisione della PSD2, se sia opportuno individuare nuove fattispecie di transazioni – a basso rischio frode – da ricondurre nell'ambito di esenzione dalla SCA. A tal proposito, la Banca d'Italia ha sottoposto alla valutazione dei partecipanti ai lavori del Tavolo l'eventualità di esentare dalla SCA alcuni tipi di transazioni, quali ad esempio i pagamenti verso le Onlus (Organizzazione non lucrativa di utilità sociale), i quali spesso non sono completati a causa di un processo di autorizzazione troppo complesso.

Perplessità sono state sollevate, nel corso dei lavori, in merito alla possibilità di prevedere esenzioni per una singola categoria di soggetti (in particolare, le Onlus), in considerazione degli oneri di implementazione – che potrebbero rappresentare un disincentivo per gli intermediari – e di alcune evidenze che mostrerebbero come le transazioni riferite a questi soggetti non siano sempre considerabili a basso rischio di frode. Si potrebbero, tuttavia, valutare eventuali applicazioni a specifiche categorie merceologiche (mediante l'uso del *merchant category code*), avendo comunque riguardo al fatto che l'esenzione dalla SCA relativamente a specifiche fattispecie di transazioni potrebbe essere utile, ma richiederebbe: i) una revisione periodica da parte dell'Autorità per verificare il tasso di frode su tali transazioni; ii) la definizione di maggiori requisiti di segnalazione e gestione delle frodi da parte degli *acquirer*.

Sempre nell'ambito delle esenzioni si potrebbe, inoltre, valutare sia la proposta di estendere alle stazioni di ricarica di veicoli elettrici e alle *charity donation stations* l'esenzione attualmente prevista per i terminali incustoditi, sia quella di innalzare i limiti per i pagamenti contactless (per operazione da 50 a 100 euro; cumulativo da 150 a 250 euro). Un eventuale maggior rischio connesso all'innalzamento dei limiti per i pagamenti contactless potrebbe essere mitigato accordando agli utenti la facoltà di selezionare delle soglie personalizzate entro i limiti consentiti[19].

1.7. Nuovi sviluppi in tema di autenticazione forte

L'autenticazione forte, introdotta dalla PSD2, ha apportato notevoli benefici per la sicurezza delle transazioni. Ciò nonostante, la tecnologia è in costante evoluzione e impone una riflessione sui miglioramenti che possono essere apportati in tale ambito.

A tale riguardo, alcuni partecipanti hanno prospettato i vantaggi dell'adozione di fattori di autenticazione basati su soluzioni innovative (ad esempio soluzioni basate sulla biometria comportamentale) che, pur mantenendo elevati requisiti di sicurezza, facilitino la *user experience* della clientela.

Un altro filone di innovazione potrebbe riguardare l'utilizzo dell'identità digitale quale possibile forma di autenticazione forte. Il quadro regolamentare vigente in tema di servizi di pagamento attualmente non prevede tale modalità di autenticazione forte. In questo ambito, si possono

[19] In tale contesto, sempre nell'ottica di assicurare un bilanciamento fra sicurezza e *user experience*, è stato inoltre proposto, da uno dei partecipanti ai lavori, di valutare l'innalzamento delle soglie di esenzione per l'analisi del rischio di transazione (*Transaction Risk Analysis* – TRA), in presenza di un attento e costante monitoraggio dei tassi di frode, così come già attualmente previsto dal Regolamento delegato (UE) 2018/389.

ipotizzare scenari (anche in connessione con la prevista emanazione del Regolamento eIDAS2[20] e della futura revisione della PSD2) che prevedano il ricorso a sistemi di identità digitale interoperabili in ambito comunitario. In questo contesto, potrebbe essere approfondito il possibile utilizzo dell'*European Digital Identity Wallet* (EUDIW) - strumento di identificazione digitale unico per tutti i cittadini europei - a fini di identificazione del pagatore per l'accesso al conto e l'autorizzazione del pagamento, tenendo in considerazione che un eventuale utilizzo di soluzioni di identità digitale per tali finalità dovrà tener conto della normativa di settore (i.e. PSD3/PSR). Restano aperti aspetti di approfondimento su alcune criticità emerse nell'ambito del confronto tra i partecipanti al Tavolo, ad esempio riguardo:

- le modalità di implementazione di tale soluzione, ferma restando la difficoltà di utilizzare l'identità digitale per l'effettuazione di operazioni di pagamento, per le quali è invece necessaria l'applicazione dell'autenticazione forte, comprensiva di *Dynamic Linking*;
- la necessità di individuare il regime di responsabilità nei rapporti tra *identity provider* e *service provider*
- il ruolo che le autorità potrebbero/dovrebbero svolgere per garantire che le identità digitali che soddisfano standard comuni di contenuto, sicurezza, affidabilità e interoperabilità siano riconosciute come entità legalmente valide sotto la loro giurisdizione.

[20] Consultabile al seguente link.

2. *Open Banking*

2.1. Introduzione

La PSD2 e la connessa normativa attuativa[21] hanno definito il quadro di riferimento per *l'open banking*. Attualmente l'ASPSP può consentire l'accesso alle TPP adattando l'interfaccia già utilizzata dall'utente per l'accesso diretto ai conti di pagamento oppure implementando un'interfaccia dedicata, basata sulla tecnologia delle *Open API* (*Application Programming Interfaces* – API). L'interfaccia dedicata può essere sviluppata su base proprietaria dal singolo ASPSP oppure tramite collegamento a infrastrutture centralizzate (c.d. soluzioni "di sistema") [22].

Teoricamente ogni ASPSP può definire proprie specifiche di interfaccia, in base a scelte di business o a esigenze tecniche; la normativa non impone infatti requisiti di dettaglio ma mantiene un approccio di sostanziale neutralità tecnica. Tale 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 TPP in un lavoro di puntuale sviluppo ed integrazione per ciascun ASPSP cui connettersi.

2.2. *Dedicated vs. adapted interfaces*

Nell'ambito dei lavori preparatori alla revisione della PSD2 è emersa la possibilità di imporre agli ASPSP l'obbligo di implementare un'interfaccia dedicata invece di mantenere la scelta, prevista dall'attuale normativa, tra un'interfaccia adattata o un'interfaccia dedicata.

I partecipanti al Tavolo non hanno ravvisato particolari criticità per gli ASPSP italiani, la maggioranza dei quali (circa 98%) ha implementato un'interfaccia dedicata; tale opzione sembra conveniente anche per le TPP, anche in ragione degli ingenti sforzi sostenuti nel corso degli ultimi anni per lo sviluppo di soluzioni tecniche specifiche per l'integrazione delle interfacce di ciascun ASPSP nei propri sistemi.

2.3. Standard unico API

Al fine di garantire una piena armonizzazione delle interfacce di accesso ai conti, è stata valutata anche la possibilità di adottare un unico standard tecnico di comunicazione tra TPP e ASPSP a livello europeo, ovvero di definire requisiti minimi più dettagliati per le interfacce. La proposta nasce soprattutto per superare le varie carenze tecnico-operative segnalate dalle TPP nei primi 3 anni di attività dei servizi di *open banking*.

---

[21] Regolamento delegato (UE) 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 PSD2, i c.d. *Regulatory Technical Standards* (RTS), predisposti dall'EBA e adottati dalla Commissione Europea, entrati in vigore il 14 settembre 2019.

[22] 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 l'esenzione da tale obbligo (cd. *fall-back exemption*). Al riguardo cfr. anche le 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)* (EBA/GL/2018/07).

La normativa ha indicato in maniera volutamente generica la necessità di utilizzare standard di comunicazione sviluppati nell'ambito di iniziative internazionali o europee (ad es. "NextGenPSD2 Framework" del Berlin Group), attribuendo al mercato il compito di autoregolarsi.

In Italia si è cercata una convergenza verso standard tecnici comuni per la realizzazione delle interfacce dedicate e sono state adottate le specifiche funzionali e tecniche elaborate dall'iniziativa "NextGenPSD2 Framework", sviluppate dal Berlin Group. Dalle recenti analisi svolte dal Tavolo tecnico del CPI sull'Open Banking è emerso che i problemi attualmente segnalati dalle TPP nascono da: i) incompletezza delle specifiche funzionali e tecniche su alcuni aspetti, ii) implementazioni degli ASPSP non ottimizzate. Considerati gli sviluppi e il lavoro svolto dalle iniziative di mercato dall'applicazione della PSD2 fino ad oggi, l'introduzione ora di un unico standard API a livello europeo dovrebbe essere attentamente valutata in quanto comporterebbe elevati costi di migrazione, limitazioni all'innovazione e la necessità di identificare un'autorità competente responsabile dell'emissione e dell'aggiornamento dello standard unico.

2.4. Modello di remunerazione per servizi di *open banking*

La PSD2 rappresenta l'avvio della strategia europea di *data sharing*, con l'obiettivo di fornire alla clientela vantaggi in termini di varietà e integrazione di servizi innovativi, favorendo la competizione[23]. La Direttiva non prevede la possibilità che si instauri un rapporto contrattuale tra le TPP e l'intermediario che detiene i dati del cliente e non prevede modelli di remunerazione per l'accesso a tali dati. L'ottica del legislatore europeo sta, tuttavia, in parte cambiando e ciò potrebbe portare a prevedere un modello di remunerazione per il prodotto offerto (il dato-merce), anche a compensazione dei significativi investimenti sostenuti dagli intermediari (cfr. *infra* proposta di Regolamento FiDA - *Financial Data Access Regulation*[24]).

Al riguardo, si è osservato che un'eventuale revisione della PSD2 sul punto potrebbe consentire lo sviluppo di servizi da parte di tutti i partecipanti al mercato con un'equa distribuzione del valore; parte dei partecipanti al Tavolo ritiene che dovrebbe essere lasciata al mercato la possibilità di individuare un modello di remunerazione per l'accesso ai dati da parte delle TPP al fine di contribuire a un rilancio dell'*open banking* superando le problematiche evidenziate anche dall'EBA in tema di ostacoli [25]. Gli ASPSP, a fronte dell'introduzione di una remunerazione che consenta loro di

[23] Con la Strategia europea in materia di dati del febbraio 2020, la Commissione si è impegnata a esplorare la necessità di un'azione legislativa specifica avente a oggetto la creazione di un autentico mercato unico di dati, aperto ai dati provenienti da tutto il mondo – nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore. In quest'ottica la Commissione ha previsto un pacchetto di norme che disciplinano il fenomeno più ampio sotto diversi aspetti, anche se in parte interconnessi: quello delle reti e dei servizi, col *Digital Services Act*, quello delle piattaforme e della concorrenza, col *Digital Market Act*, quello della condivisione dei dati personali, e non, fra settore pubblico e privato, col *Digital Governance Act*, ed infine col *Data Act*, l'accessibilità al valore rappresentato da quei dati. La Strategia è consultabile al seguente link.

[24] La proposta di Regolamento relativo a un quadro per l'accesso ai dati finanziari è disponibile al seguente link.

[25] *Opinion of the European Banking Authority on obstacles under Article 32(3) of the RTS on SCA and CSC*.

recuperare dei costi di infrastruttura, sarebbero infatti incentivati a migliorare la qualità delle API e dei processi di gestione e trasformazione dei dati a vantaggio anche delle TPP[26].

In proposito è stato, tuttavia, anche rilevato che occorrerebbe evitare che i maggiori costi sostenuti dalle TPP vengano ribaltati sulla clientela con la conseguenza di disincentivare l'utilizzo dei servizi basati sul *data sharing.* Ciò comporterebbe impatti negativi sia sulla diffusione dei servizi sia sulla sostenibilità dei modelli di business delle TPP.

Le eventuali spese addebitate alla clientela dovrebbero peraltro essere ragionevoli e proporzionate ai costi effettivi sostenuti dal prestatore dei servizi per ottenere l'accesso ai dati degli ASPSP, in linea con l'impianto generale della PSD2.

Alla luce di quanto precede, si potrebbe valutare una graduale transizione verso un modello di remunerazione che tenga conto anche delle riflessioni che emergeranno nell'ambito dei lavori sulla proposta di Regolamento FiDA (cfr. par. 4.2) per i servizi di accesso ad altre tipologie di dati finanziari. Spunti interessanti potranno anche derivare dall'entrata a regime del modello dello schema SPAA (S*EPA Payment Account Access*) dell'*European Payment Council* (EPC)[27].

2.5. Estensione dell'esenzione dalla SCA (transazioni effettuate tramite PISP)

È stata discussa la possibilità di consentire anche al PISP di proporre l'esenzione dalla SCA già previste dal Regolamento delegato (UE) 2018/389 per i pagamenti online. In tal caso troverebbe applicazione il principio generale che riconosce al prestatore del servizio di pagamento la facoltà di proporre l'esenzione, con conseguente responsabilità in capo al PISP per i pagamenti disconosciuti. Resterebbe comunque all'ASPSP la facoltà di accettare o meno la proposta di applicazione dell'esenzione del PISP, secondo quanto già previsto per l'esenzione proposta dall'*acquirer* all'i*ssuer* per le transazioni con carte di pagamento. In tale ambito, andrebbe valutato anche l'ampliamento dell'oggetto della polizza assicurativa per coprire la responsabilità in capo ai PISP derivante dal disconoscimento delle operazioni per le quali ha proposto l'esenzione SCA.

2.6. Possibilità di revoca di un ordine effettuato tramite PISP

Tenuto conto che il servizio di disposizione di ordini di pagamento trova applicazione anche nel settore del commercio elettronico, si è osservato che l'eventuale revoca di un bonifico ordinario effettuato tramite PISP[28] e richiesta dal cliente all'ASPSP avviene di norma all'insaputa del PISP stesso e del *merchant.* Potrebbe per esempio verificarsi il caso concreto di una compravendita online in cui il *merchant*, non essendo al corrente dell'avvenuta revoca dell'operazione, spedisca comunque la merce acquistata. Al riguardo, si evidenzia che la PSD2 stabilisce che, di regola, l'utente non può più revocare l'operazione disposta tramite prestatore di servizi di disposizione di ordine di pagamento dopo aver prestato il proprio consenso a disporre l'operazione stessa (art. 80, paragrafo

[26] Il consenso per la cessione dei dati da parte della clientela andrebbe sorretto da un'informativa adeguata volta a favorire la consapevolezza sia dell'oggetto che delle finalità di tale consenso.
[27] Si tratta di un insieme di regole, pratiche e standard (funzionalità di messaggistica) che faciliterà lo scambio di dati relativi a conti di pagamento tra ASPSP e TPP per la prestazione di servizi a valore aggiunto (c.d. *premium*), allo scopo di consentire un'equa distribuzione del valore e del rischio tra i partecipanti allo schema.
[28] Ci si riferisce qui ai pagamenti in data odierna escludendo quelli a data futura e ricorrenti.

2, PSD2). Dopo questo termine generale, le suddette operazioni possono essere revocate «*solo se è stato concordato tra l'utente di servizi di pagamento e i prestatori di servizi di pagamento interessati»* (art. 80, paragrafo 5, PSD2).

La disposizione pone alcuni dubbi interpretativi in relazione all'individuazione dei PSP "interessati" il cui consenso è necessario ai fini della revoca. In proposito, i partecipanti al Tavolo convengono che tra questi dovrebbe essere incluso il PISP tramite il quale l'operazione sia stata eventualmente disposta. Tuttavia, dalla prassi attuativa riferita da alcune TPP[29] è emerso come - a fronte di una potenziale incertezza della norma – i PISP non siano talvolta informati della revoca richiesta dall'utente all'ASPSP. Per tale motivo, i partecipanti riterrebbero auspicabile che, nella revisione della PSD2, tale disposizione venisse rivista per chiarire, nel senso sopra indicato, il regime normativamente previsto per la revoca dell'ordine di pagamento disposto tramite PISP e per ovviare al problema della circolarità informativa tra tutti i PSP coinvolti.

[29] Su tale tematica alcuni PISP hanno segnalato fenomeni di frodi commerciali cd. "esterne" perpetrate, sfruttando la poca chiarezza della norma, a danno di *merchant* che hanno inviato i beni venduti confidando nella irrevocabilità del bonifico effettuato tramite PISP.

3. Accesso ai conti e ai sistemi di pagamento

3.1. Introduzione

Nell'ambito della revisione della PSD2, si potrebbe valutare l'opportunità di apportare delle modifiche all'art. 36 in materia di accesso ai conti di pagamento e all'art. 35 relativo all'accesso ai sistemi di pagamento. Quest'ultimo potrebbe richiedere modifiche alla Direttiva (CE) 98/26 (*Settlement Finality Directive* – SFD)[30].

Di seguito, viene riportata per ciascun tema una descrizione della problematica con riferimento al contesto normativo attuale e della possibile proposta di modifica della PSD2, così come analizzate nelle riunioni del Tavolo.

3.2. Accesso ai conti di pagamento

Per consentire ai prestatori di servizi di pagamento non bancari (istituti di pagamento e di moneta elettronica, IP e IMEL) di prestare servizi di pagamento è necessario che questi abbiano la possibilità di aprire e detenere conti di pagamento presso gli enti creditizi. A tal fine, l'art. 36 della PSD2 prevede che sia garantito l'accesso a tali conti in modo non discriminatorio e proporzionato al legittimo scopo che si intende perseguire[31]. In caso di rifiuto la norma richiede che gli enti creditizi notifichino alla propria Autorità competente il rifiuto dell'accesso a un conto di pagamento a un IP/IMEL richiedente; tuttavia, l'art. 36 della PSD2 non prevede alcuna notifica e/o spiegazione nei casi in cui la banca chiuda il rapporto di conto con l'IP/IMEL e non contempla il diritto di ricorso.

A livello nazionale, l'art. 36 della PSD2 è stato recepito dall'articolo 114-octiesdecies del D.Lgs. 385/1993 (Testo Unico Bancario – TUB), secondo il quale le banche – previa motivata notifica all'Autorità competente – possono rifiutarsi di aprire o decidere di chiudere conti di pagamento per motivi di ordine pubblico o di sicurezza pubblica, ovvero se sussistono altri giustificati motivi fondati su disposizioni in materia di antiriciclaggio e di contrasto al finanziamento del terrorismo (AML/CFT). Inoltre, per garantire una corretta applicazione della disposizione, la Banca d'Italia ha adottato il provvedimento attuativo del 23 luglio 2019[32] (c.d. provvedimento sul *de-risking*).

---

[30] Consultabile al seguente link.

[31] L'art. 36 della PSD2 richiama nel testo solo gli IP; per meglio comprendere l'ambito di applicazione della norma occorre leggerla alla luce di quanto riportato nel considerando 39 ove si specifica che: «*È opportuno che i prestatori di servizi di pagamento, quando prestano uno o più dei servizi di pagamento contemplati dalla presente direttiva, detengano sempre conti di pagamento utilizzati esclusivamente per le operazioni di pagamento. Per consentire ai prestatori di servizi di pagamento di prestare servizi di pagamento, è indispensabile che questi abbiano la possibilità di aprire e detenere conti presso gli enti creditizi. Gli Stati membri dovrebbero garantire che l'accesso a tali conti sia fornito in modo non discriminatorio e proporzionato al legittimo scopo che si intende perseguire. Può trattarsi di un accesso di base, che dovrebbe però essere sufficientemente ampio da consentire all'istituto di pagamento di prestare i propri servizi in modo agevole ed efficiente».*

[32] L'art. 114-octiesdecies TUB reca infatti una disciplina più dettagliata rispetto alla PDS2 riguardo le motivazioni che consentono il rifiuto, prevedendo anche il caso di chiusura successiva del rapporto di conto. Inoltre, in base al citato provvedimento attuativo, le banche devono notificare alla Banca d'Italia, entro cinque giorni lavorativi dall'assunzione della decisione, il rifiuto dell'apertura di un conto o la revoca fornendo evidenze debitamente motivate e allegando

In quest'ambito, nel corso della sessione dedicata del Tavolo, è stata valutata, anche alla luce dell'esperienza italiana sopra richiamata, l'opportunità di rivedere l'art. 36 della PSD2 sull'accesso ai conti bancari, prevedendo un allineamento della normativa comunitaria a quella nazionale al fine di creare un *level playing field* fra tutti gli intermediari. A seguito di tale modifica verrebbe esteso a tutte le banche comunitarie l'obbligo di giustificare per iscritto all'Autorità competente sia il rifiuto che la revoca, sempre nel rispetto della libertà di impresa degli intermediari. Dalla discussione è emerso infatti che la norma della PSD2 sembra prevedere attualmente solo la necessità di giustificare il diniego di apertura di un conto e non anche il caso di interruzione di rapporti commerciali con gli IP/IMEL che espongono la banca stessa a rischi non adeguatamente presidiati da tali operatori. Tale obbligo è invece disciplinato per entrambe le fattispecie a livello nazionale nelle disposizioni di recepimento del TUB e nel provvedimento della Banca d'Italia sul *de-risking*.

A tal riguardo, occorre considerare che il diritto all'apertura (e/o al mantenimento) di un conto di pagamento per IMEL e IP trova un limite negli obblighi AML cui sono soggetti gli intermediari. Infatti, qualora questi, in virtù del principio dell'approccio basato sul rischio, ritengano che un soggetto sia qualificabile ad alto rischio di ML, possono legittimamente rifiutare o revocare l'apertura di un conto. Anche le *GLs on policies and controls for the effective management of money laundering and terrorist financing (ML/TF) risks when providing on access to financial services* dell'EBA[33], di recente approvazione, vanno nella direzione di richiedere agli intermediari di valutare caso per caso l'effettivo rischio di riciclaggio di un soggetto, senza compromettere la loro libertà contrattuale.

3.3. Accesso ai sistemi di pagamento

Un altro tema di rilievo, affrontato nel corso dei lavori del Tavolo sulla revisione della PSD2, riguarda l'accesso ai sistemi di pagamento da parte di IP e IMEL. Questi soggetti, infatti, spesso affrontano alcuni ostacoli per ottenere l'accesso ai sistemi di pagamento designati, in quanto, in ragione delle interconnessioni applicative della PSD e della SFD[34], possono accedervi solo indirettamente per il tramite di enti creditizi. L'obiettivo sarebbe quello di garantire condizioni di parità concorrenziale per tutti i PSP, a prescindere dalla loro natura.

Mentre procedevano i lavori del Tavolo, il tema è stato affrontato nell'ambito del Regolamento sugli *Instant payments*; il regolamento ha previsto la modifica della SFD, consentendo l'accesso ai sistemi di pagamento anche per IP e IMEL; per accompagnare tale estensione, vengono introdotti requisiti rafforzati in tema di tutela dei fondi degli utenti, governance, presidio dei rischi e continuità operativa (analogamente a quanto si sta discutendo nell'ambito della revisione della PSD2), lasciando ai singoli Stati Membri la definizione delle procedure per valutare la conformità dei PSP ai

tutte le informazioni necessarie per ricostruire l'iter decisionale e le relative motivazioni. Il TUB è consultabile al seguente link mentre il provvedimento sul *de-risking* è disponibile qui.

[33] EBA/GL/2023/04 del 31 marzo 2023, link.

[34] Le due direttive hanno oggetti diversi, ma un tema comune è rappresentato dall'accesso ai sistemi di pagamento. Ai sensi della SFD, le regole di un sistema devono definire il momento di immissione di un ordine di trasferimento, ai fini della sua opponibilità a terzi anche in caso di apertura di una procedura di insolvenza nei confronti di un partecipante al sistema. La revisione della PSD2 potrebbe offrire alla Commissione il veicolo normativo per eventuali modifiche al *framework* attuale.

requisiti richiesti (in particolare, si prevede sia la possibilità di un *self-assessment* da parte del PSP sia il rilascio di una apposita autorizzazione da parte dell'Autorità competente).

Stante la delicatezza e l'interesse del tema e le novità introdotte, esso potrà formare oggetto di successivi confronti in seno al Tavolo.

4. *Scope* della nuova normativa sui servizi di pagamento al dettaglio

4.1. Introduzione

Da quando è stata adottata la PSD2 il mercato dei servizi di pagamento ha conosciuto una notevole evoluzione, stimolata in particolare dall'innovazione tecnologica, con la diffusione di nuovi servizi e soluzioni di pagamento basate sull'interazione e l'interdipendenza di tecnologie e soluzioni diverse (*Distributed Ledger Technologies* (DLT)/*blockchain*, API, *cloud*) che hanno reso sempre più preponderante il ruolo di alcuni attori nel mercato (fornitori di servizi tecnologici, gestori di infrastrutture tecnologiche e di piattaforme digitali), richiamando l'attenzione di varie Autorità di regolamentazione europee nel campo della vigilanza/sorveglianza.

A fronte di questi cambiamenti, i lavori del Tavolo sulla revisione della PSD2 si sono focalizzati sulla valutazione dell'adeguatezza dell'originario ambito di applicazione della Direttiva. Ciò con riferimento sia al *positive scope*, per valutare un possibile ampliamento dell'ambito di applicazione della PSD2 per ricomprendervi i nuovi servizi sviluppatisi sul mercato ovvero i soggetti che li offrono, sia al *negative scope*, per valutare il mantenimento, la modifica e l'armonizzazione di alcune delle fattispecie di esenzione attualmente previste.

4.2. Possibili modifiche del *positive scope*

L'art. 3, paragrafo 1, lett. j) della PSD2 attualmente esclude dallo *scope* i servizi prestati dai TSP, quali i fornitori di reti o servizi di comunicazione elettronica (es. *Telco service providers*), i fornitori di servizi tecnici a supporto dei servizi di pagamento (es. *processors*) e i fornitori di portafogli digitali (*digital wallet providers*). Al riguardo alcuni partecipanti al Tavolo hanno rappresentato l'opportunità di predisporre in via preliminare una mappatura dei servizi offerti dai TSP per individuare quelli rilevanti nella catena dei pagamenti; per i prestatori di tali servizi la nuova normativa potrebbe prevedere l'applicazione di specifici obblighi e relative responsabilità (es. in materia di sicurezza e di scambio informativo volto a prevenire le frodi).

Al contempo, nel valutare l'estensione dello *scope* occorrerebbe prestare attenzione alle possibili sovrapposizioni con altri ambiti e discipline, tra cui il PISA *framework*[35], la Direttiva (UE) 2016/1148 (*Network and Information Security* – NIS)[36], il Regolamento (UE) 2022/2554 (*Digital Operational Resilience Act* – DORA)[37] e le competenze di altre Autorità (es. Autorità per le Garanzie nelle Comunicazioni, AGCOM). Altro aspetto di potenziale rilievo emerso attiene alla possibilità di attribuire ai *merchant*, anziché ai PSP, la responsabilità delle operazioni non autorizzate e/o fraudolente qualora eventuali carenze nelle misure di sicurezza (in particolare, SCA) siano da imputare ai *merchant* stessi. Al riguardo sono state evidenziate le difficoltà connesse all'attuazione

[35] L'*Eurosystem oversight framework for electronic payment instruments, schemes and arrangements*, elaborato dalla BCE ed entrato in vigore a novembre 2022, è consultabile al seguente link.
[36] Il testo della Direttiva è disponibile qui.
[37] Il testo del Regolamento è disponibile qui.

di tale proposta in particolare nel chiarire gli obblighi applicabili ai *merchant*, nel valutare la *compliance* e nell'assicurare l'*enforcement*[38].

Altro ambito di rilevanza analizzato concerne i servizi volti a consentire l'effettuazione di pagamenti a partire da disponibilità in cripto-attività (previa conversione delle stesse in fondi) o l'impiego diretto di cripto-attività con funzione di pagamento. Mentre con riferimento ai primi le relative operazioni di pagamento, in quanto effettuate in fondi, risulterebbero già coperte dalla disciplina PSD, per quanto invece concerne i "pagamenti" direttamente effettuati utilizzando cripto-attività, essi non sono oggetto di una disciplina specifica nel Regolamento europeo sui mercati delle cripto-attività (Regolamento (UE) 2023/1114, *Market in Crypto Assets Regulation* – MiCAR)[39]. Si pone pertanto l'opportunità di valutare un'eventuale inclusione degli stessi nell'ambito di applicazione della revisione della PSD2, così da evitare situazioni di vuoto normativo (sul punto si rimanda al par. 5.5).

Con riferimento al servizio di *Buy Now Pay Later* (BNPL), tipicamente erogato da piattaforme online che permettono ai consumatori di frazionare il pagamento di un acquisto in rate da ripagare nel breve-medio termine, si è convenuto che la componente di credito prevalga su quella di pagamento e che, pertanto, lo stesso trovi più adeguata collocazione nella disciplina afferente al settore del credito[40]. Ciò premesso, si evidenziano i due seguenti aspetti che sono stati discussi dal Tavolo sui quali potrebbero essere utili dei chiarimenti nella futura normativa sui pagamenti: *i*) applicazione della disciplina PSD all'eventuale prestazione di un servizio di pagamento collegato al BNPL – in base allo specifico modello di business; *ii*) riconduzione del BNPL nelle attività di concessione di crediti accessori alla prestazione di servizi di pagamento che attualmente l'art. 18, paragrafo 4 della PSD2 consente di effettuare agli istituti di pagamento[41].

---

[38] Ad analoghe considerazioni è giunta anche l'EBA (cfr. *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*, paragrafo 84).

[39] Il Regolamento – pubblicato nella Gazzetta ufficiale dell'Unione europea del 9 giugno 2023 – è entrato in vigore il 29 giugno e si applicherà dal 30 dicembre 2024, eccezion fatta per i Titoli III (*asset-referenced token* - ART) e IV (*e-money token* - EMT) la cui applicazione è anticipata al 30 giugno 2024. Il testo è consultabile al seguente link.

[40] In sede di revisione della *Consumer Credit Directive* - CCD, il BNPL è stato ricompreso nell'ambito di applicazione della Direttiva. Il testo della Direttiva è consultabile al seguente link. Nello specifico, il BNPL consiste in una dilazione di pagamento collegata all'acquisto di un bene o di un servizio. Di conseguenza, esso può (ma non necessariamente deve) essere associato a un'operazione di pagamento. In questi casi il BNPL, come qualsiasi altra forma di credito, può costituire credito "accessorio" a un'operazione di pagamento e, come tale, essere offerto da IP e IMEL nel rispetto dell'art. 18 della PSD2. La versione revisionata della CCD esonera da specifici requisiti autorizzativi gli IP e gli IMEL in relazione all'esecuzione di operazioni di pagamento quando i fondi rientrano in una linea di credito accordata ad un utente di servizi di pagamento.

[41] L'art. 18, paragrafo 4, PSD2, consente agli istituti di pagamento di concedere crediti relativi a servizi di pagamento di cui al punto 4 o 5 dell'allegato I della Direttiva (esecuzione di operazioni di pagamento quando i fondi rientrano in una linea di credito accordata ad un utente di servizi di pagamento; emissione di strumenti di pagamento e/o convenzionamento di operazioni di pagamento) ove siano rispettate determinate condizioni, tra cui il carattere accessorio del credito in relazione all'esecuzione dell'operazione di pagamento. Rispetto all'opportunità di fornire i chiarimenti summenzionati, cfr. *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*, paragrafo 96: «[…] *the EBA proposes to*

Rispetto a un'eventuale revisione dell'elenco dei servizi di pagamento di cui alla PSD2, si è valutata la possibilità di espungere dalla lista il servizio di informazione sui conti (*Account Information Service* – AIS) per attrarlo all'ambito di applicazione della legislazione sull'*open finance* in corso di discussione. Al riguardo, si ritiene opportuno che per il momento la disciplina dell'AIS continui a essere ricompresa nella normativa sui servizi di pagamento, in attesa di una completa stabilizzazione del quadro che evolverà con l'attuazione della proposta FiDAR. Potrebbe essere inoltre utile implementare forme di collaborazione strutturate con il Garante Privacy europeo (*European Data Protection Board* – EDPB) per approfondire l'interrelazione con il GDPR dei servizi che in generale consentono l'accesso ai dati di pagamento/finanziari (cfr. par. 5.3 su allineamento GDPR-PSD2).

Sempre con riferimento alla lista dei servizi di pagamento, tra le proposte su cui c'è stata convergenza tra i partecipanti vi è quella relativa a una possibile scissione del servizio di cui al numero 5 dell'Allegato I della PSD2 – che a oggi ricomprende sia l'emissione di strumenti di pagamento che il convenzionamento di esercenti per l'accettazione di operazioni di pagamento – in due distinti servizi di pagamento relativi, rispettivamente, all'*issuing* e all'*acquiring*, così da conferire maggiore granularità alle definizioni e alla relativa disciplina. A sua volta, il servizio di *acquiring* potrebbe essere definito in modo più puntuale anche in relazione ai nuovi modelli operativi, tra cui ad esempio il prelievo al POS/*cash in shop*[42], per il quale andrebbe comunque tenuta presente la necessità di specificare che il servizio è offerto dall'esercente *retailer* per conto di un PSP, principale destinatario dei relativi obblighi normativi.

4.3. Possibili modifiche del *negative scope*

Con riferimento al *negative scope*, si è posta anzitutto l'opportunità di un chiarimento sul perimetro dell'esclusione dell'agente commerciale. L'art. 3, paragrafo 1, lett. b), PSD2, esclude dall'ambito di applicazione della Direttiva le operazioni di pagamento dal pagatore al beneficiario effettuate tramite un agente commerciale autorizzato, in base ad un accordo a negoziare o a concludere la vendita o l'acquisto di beni o servizi per conto del solo pagatore o del solo beneficiario. Il chiarimento appare opportuno in particolare nel caso di piattaforme di *e-commerce* che agiscano per conto sia dei pagatori che dei beneficiari: ciò considerando che a oggi, in assenza di criteri nella PSD2, l'EBA (Q&A 2020/5355) ha chiarito che l'autorità nazionale competente deve valutare caso per caso se il modello di business ricada o meno nell'esenzione. È stato convenuto che bisognerebbe anzitutto: specificare i parametri di riferimento per stabilire che l'operatore stia agendo solo per conto di una delle parti oppure per entrambe (in questo secondo caso non può entrare in possesso

clarify in PSD2 the nature of the ancillary credit to the provision of payment services and whether it covers BNPL services and how the interplay between BNPL services and the provision of payment services should be treated».

[42] Uno spunto per elaborare una nozione di servizi di *cash in shop*, potrebbe trarsi dal *Report of the ERPB Working Group on Access and Acceptance of Cash* dello *Euro Retail Payments Board* (ERPB) del novembre 2021, che al riguardo ha formulato due proposte di definizione, una estesa («*A cash withdrawal, or a cash deposit, which is offered by a retailer on behalf of a payment service provider without being linked to a purchase of goods or services, which is settled through the customer's account and which is considered a payment service pursuant to the Payment Services Directive.*»), l'altra semplificata «*A cash withdrawal or deposit at the retailer's checkout which is settled through the customer's account and is not being linked to a purchase of goods or services*» (p. 41).

o controllare i fondi dei clienti [43]), cogliendo altresì l'occasione per chiarire le seguenti questioni interpretative: *i*) individuare i casi d'uso da ricomprendere nell'esclusione, posto che gli agenti commerciali sono solitamente definiti nel diritto civile nazionale); *ii*) definire cosa si intende per "negoziare o concludere" la vendita o l'acquisto di beni o servizi; *iii*) indicare se un soggetto che consegna beni e accetta un pagamento a nome di un venditore possa considerarsi escluso dallo *scope*[44]; *iv*) precisare l'applicabilità o meno dell'esclusione ai servizi di *escrow*; *v*) individuare la delimitazione tra le attività che rientrano nella definizione di "agente" ai sensi dell'art. 4, paragrafo 1, n. 38, PSD2, e le attività ricomprese nell'esclusione dell'agente commerciale; *vi*) risolvere l'interazione con la Direttiva (CEE) 86/653, relativa al coordinamento dei diritti degli Stati membri concernenti gli agenti commerciali indipendenti.

In tema di ATM c.d. indipendenti, l'art. 3, paragrafo 1, lett. o), PSD2, disapplica la Direttiva ai servizi di prelievo di contante offerti tramite ATM da operatori, per conto di uno o più emittenti della carta, che non siano parti del contratto quadro con il cliente, a condizione che detti operatori non forniscano altri servizi di pagamento. La norma non risulta tuttavia del tutto chiara, specialmente rispetto all'eventualità che questa esenzione si applichi solo qualora l'operatore abbia stipulato un accordo specifico con uno o più emittenti, oppure se la condizione ivi prevista possa essere soddisfatta in via indiretta anche mediante accordo con un circuito di pagamento nazionale o internazionale a cui aderiscono una pluralità di emittenti[45]. Più in generale, si tratterebbe di: *i*) auspicare una maggiore chiarezza sull'applicazione di questa fattispecie di esenzione, anche alla luce delle difficoltà riscontrate nel valutare i singoli casi concreti; *ii*) valutare di ricondurre tale fattispecie allo *scope* della nuova disciplina, tenendo conto delle incertezze applicative, ove vi fossero evidenze su un'eventuale crescita nella diffusione degli ATM indipendenti.

Infine, rispetto all'ampia diffusione degli strumenti di pagamento a spendibilità limitata – c.d. strumenti privativi – riscontrata in determinati settori (es. *fuel*, Grande Distribuzione Organizzata – GDO, servizi per la mobilità), si è convenuto circa l'opportunità di circoscrivere meglio l'ambito dell'esenzione attualmente prevista dall'art. 3, paragrafo 1, lett. k), PSD2 che, nonostante le indicazioni e i chiarimenti forniti con le Linee Guida dell'EBA 2022/02, resta ancora disomogeneo a livello di singoli Paesi UE. Al riguardo, si è ritenuta condivisibile la proposta di EBA[46] di incorporare le indicazioni a oggi fornite nelle suddette Linee Guida (o parte di esse) nella nuova normativa, o meglio di introdurre un mandato sotto forma di *Regulatory Technical Standards* (RTS), così da

[43] A tal proposito il considerando n. 11, PSD2, riporta: «[…] *l'esclusione dovrebbe applicarsi ove gli agenti agiscano soltanto per conto del pagatore o soltanto per conto del beneficiario, indipendentemente dal fatto che siano o meno in possesso dei fondi dei clienti. Ove agiscano per conto sia del pagatore sia del beneficiario (ad esempio mediante una piattaforma di commercio elettronico) gli agenti dovrebbero essere esclusi solo qualora non entrino mai in possesso dei fondi dei clienti o non li controllino.*».

[44] In senso affermativo sembrerebbe deporre il richiamato considerando n. 11, secondo il quale l'esclusione dovrebbe applicarsi ove gli agenti agiscano soltanto per conto del pagatore o soltanto per conto del beneficiario, indipendentemente dal fatto che siano o meno in possesso dei fondi dei clienti);

[45] Si evidenzia che su tale tematica la Banca d'Italia ha sottoposto un quesito all' EBA cui non è stata ad oggi fornito riscontro.

[46] *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*, paragrafo 66.

garantire una piena armonizzazione, ma, soprattutto si è concordato sull' opportunità, in sede di revisione della PSD2, di affrontare le questioni interpretative, che non è stato possibile definire nelle Linee Guida, riguardanti in particolare: *i*) la differenza tra "emittente professionale" ed "emittente", ambedue menzionati dall'art. 3, paragrafo 1, lett. k), PSD2; *ii*) il limite geografico di ogni specifica esclusione; *iii*) l'interpretazione del termine «locali», di cui alla Linea guida n. 3, la quale prevede che gli strumenti di pagamento che consentono al titolare di acquistare beni o servizi solo nei locali (*premises*) dell'emittente possono essere utilizzati solo nei locali fisici e non nei negozi online*; v)* i criteri per la valutazione della limitatezza della rete di accettazione degli strumenti.

5. Coordinamento tra PSD2 e altre normative rilevanti per il settore pagamenti

5.1. Introduzione

La PSD2 – pur costituendo il principale *framework* normativo su cui è strutturato, attualmente, il mercato europeo dei servizi di pagamento – appare caratterizzata da un'eterogenesi dei fini che ne determina tratti marcati di interdisciplinarietà con altri plessi normativi che interessano il medesimo settore. Questo complesso ecosistema giuridico necessita di interventi mirati di integrazione, coordinamento, allineamento e affinamento volti a superare problematiche spesso emerse dall'applicazione delle prescrizioni in materia di pagamenti e la cui soluzione richiede una visione coordinata tra la PSD2 e altre normative rilevanti per il settore pagamenti (ad es. EMD2, GDPR, DORA e MiCAR). Le questioni più rilevanti sono state discusse in apposite riunioni del Tavolo che hanno visto emergere alcune possibili soluzioni sotto forma di proposta di modifica della PSD2 che si riportano di seguito.

5.2. PSD2 e EMD2

La prima proposta valutata dal Tavolo ha riguardato la fusione tra la PSD2 e la Direttiva (CE) 2009/110 (*Second Electronic Money Directive* – EMD2)[47] che comporterebbe una maggiore armonizzazione, semplificazione e un'applicazione coerente dei requisiti giuridici per IP e IMEL, evitando arbitraggi normativi, garantendo parità di condizioni e un unico quadro giuridico di riferimento, in ragione del principio *same risks, same rules*. Le regole in materia di trasparenza e di diritti e obblighi delle parti disciplinate dalla PSD2 si applicano infatti anche agli istituti di moneta elettronica; risulterebbe quindi opportuno prevedere per IP e IMEL anche lo stesso regime prudenziale, in particolare in relazione all'*iter* autorizzativo e ai requisiti di salvaguardia, capitale iniziale e fondi propri, in quanto non vi sono sostanziali differenze tra le due tipologie di intermediari in termini di attività esercitabili e di rischi che derivano da tali attività. La nuova normativa potrebbe inoltre includere l'emissione di moneta elettronica tra i servizi di pagamento per la natura molto simile delle attività e dei rischi che entrambe comportano.

È stata evidenziata anche l'opportunità di chiarire o superare del tutto la differenza tra conto di pagamento e conto di moneta elettronica; per quest'ultimo, potrebbe essere valutata la possibilità di inserire una definizione normativa che attualmente non esiste. La mancanza di una espressa definizione ha infatti causato problemi di interpretazione e applicazione delle norme legati principalmente alla difficoltà di stabilire se il conto abbinato a una carta prepagata con iban possa essere definito un conto di moneta elettronica o un conto di pagamento. Questa incertezza normativa riguarda anche le modalità di tutela dei fondi e il regime distributivo, dal momento che non risulta chiaro se debba essere applicato quello previsto per la moneta elettronica o quello previsto per i servizi di pagamento che, soprattutto nell'ordinamento italiano, differiscono notevolmente (cfr. *infra*).

[47] Il testo della Direttiva è consultabile al seguente link.

La fusione consentirebbe anche di superare il disallineamento in materia di copertura dal *de-risking*, in quanto l'art. 36 della PSD2 tutela solo gli IP (il citato articolo, che garantisce agli IP "*l'accesso ai conti intrattenuti presso un istituto di credito*", si applica agli IMEL solo quando prestano servizi di pagamento e non quando emettono esclusivamente la moneta elettronica) (cfr. par. 3.2).

In assenza di una specifica definizione nell'EMD2, la nuova normativa sui servizi di pagamento dovrebbe chiarire, inoltre, la natura e lo *status* dei distributori di moneta elettronica. Sarebbe altresì opportuna l'applicazione di un quadro normativo coerente ad agenti e distributori, tenuto conto che, in relazione all'evoluzione dei modelli di business, si rileva una convergenza delle attività svolte da tali operatori.

L'allineamento delle definizioni di agenti nei servizi di pagamento e distributori di moneta elettronica dovrebbe anche essere finalizzato a facilitare l'inquadramento delle attività svolte da IP e IMEL su base transfrontaliera, tenuto conto che l'utilizzo di agenti e/o distributori in un altro stato membro da parte di un IP o IMEL non comporta automaticamente uno stabilimento nel paese ospitante; è infatti rimessa all'Autorità *home* la valutazione della natura del passaporto. A tal fine, l'EBA ha emanato un'apposita *Opinion* del 24 aprile 2019[48] stabilendo i criteri per distinguere l'esercizio del diritto di stabilimento dalla libera prestazione di servizi quando le attività sono svolte da IP e IMEL nello stato ospitante tramite agenti o distributori. L'*Opinion*, tuttavia, non ha garantito approcci omogenei tra le autorità nazionali competenti ed è quindi auspicabile che la fusione delle direttive PSD2 ed EMD2 faciliti le valutazioni delle Autorità *home* riguardo alla natura dei passaporti, in quanto l'esistenza di uno stabilimento in uno stato membro ospitante comporta alcuni obblighi giuridici aggiuntivi per gli IP e gli IMEL rispetto alla libera prestazione di servizi e ha conseguenze per la ripartizione delle competenze di supervisione tra Autorità *home* e Autorità *host* (art. 29, paragrafi 2 e 4, PSD2)[49]. La norma, peraltro, non si applica agli IMEL che si avvalgano esclusivamente di distributori[50]. È pertanto auspicabile che con la revisione della Direttiva venga superato tale attuale disallineamento[51].

---

[48] Cfr. *Opinion of the European Banking Authority on the nature of passport notifications regarding agents and distributors under Directive (EU) 2015/2366 (PSD2), Directive 2009/110/EC (EMD2) and Directive (EU) 2015/849 (AMLD)*.

[49] In particolare, ad oggi, l'Autorità *host* può richiedere: (i) sia agli IP che agli IMEL che utilizzano agenti e distributori, una relazione periodica sulle attività svolte per monitorare il rispetto delle disposizioni della normativa nazionale di recepimento della disciplina di trasparenza e in materia di diritti e obblighi delle parti (art. 29, paragrafo 2, PSD2); (ii) l'istituzione di un punto di contatto per il presidio delle materie della PSD2 applicabili in base al principio di territorialità (trasparenza e diritti e obblighi delle parti) agli IP e agli IMEL che si avvalgono di agenti per la prestazione dei servizi di pagamento (art. 29, paragrafo 4, PSD2).

[50] Cfr. art. 3, paragrafo 4, EMD2, come modificato dall'art. 111, paragrafo 1, PSD2.

[51] Ancora in relazione al riparto di competenze tra Autorità *home* e *host*, è stato evidenziato che l'attuale quadro regolamentare PSD2, applicabile a IP e IMEL, assegna alle prime la verifica dell'osservanza delle disposizioni in materia di "trasparenza" e di "diritti e obblighi" (titoli III e IV della Direttiva) da parte degli operatori in regime di libera prestazione di servizi, sebbene la disciplina nazionale applicabile a tali operatori in relazione all'operatività transfrontaliera sia quella del paese *host* (art. 100, paragrafo 4, PSD2); per le seconde, sono previste determinati poteri di *enforcement* solo con riferimento all'operatività transfrontaliera in regime di libero stabilimento. Al contempo, è previsto uno scambio informativo tra le Autorità *home* e *host* in relazione, tra le altre circostanze, al verificarsi di violazioni nell'esercizio della libera prestazione di servizi (art. 29, paragrafo 3, PSD2); inoltre, è previsto che al verificarsi

Con l'occasione andrebbero dunque valutati anche possibili interventi sulla disciplina del regime di *enforcement* delle Autorità *host* anche nei comparti della trasparenza e della disciplina dei diritti e obblighi, per definire con maggiore efficacia i poteri delle Autorità *host* sugli operatori in libera prestazione nonché per assicurare ulteriormente adeguata tutela agli utenti di servizi di pagamento prestati da IP e IMEL per via transfrontaliera.

5.3. PSD2 e GDPR

Un'ulteriore sessione dei lavori del Tavolo si è concentrata sull'allineamento tra PSD2 e GDPR. La PSD2 ha fatto emergere l'esigenza di chiarimenti per quanto riguarda la possibilità, per i soggetti interessati, di mantenere il pieno controllo dei loro dati personali. La PSD2 e il GDPR presentano, infatti, alcuni aspetti che evidenziano profili di complessità applicativa, frutto di una mancanza di coordinamento tra le rispettive norme, relativi in particolare alla nozione di "dato sensibile"[52] e all'eventuale ulteriore trattamento e/o utilizzo dei dati personali trattati e raccolti per le specifiche finalità della prestazione di servizi di "informazione sui conti" mediante trasmissione a terzi (c.d. "quarte parti") per lo svolgimento di servizi a valore aggiunto (quali, ad esempio, il *credit scoring*).

Il tema è da tempo all'attenzione della comunità nazionale e internazionale. Sul punto sono infatti intervenute le Linee Guida dell'EDPB chiarendo, con riferimento al primo aspetto, che nel contesto della PSD2 il trattamento di "particolari categorie di dati" è legittimo se l'interessato ha prestato il proprio consenso esplicito al trattamento per una o più finalità specifiche e/o se il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (articolo 9, paragrafo 2, lettere a) e g), GDPR). Anche con riferimento alla seconda questione, le Linee Guida sopra citate chiariscono che gli artt. 66, paragrafo 3, lett. g) e 67, paragrafo 2, lett. f) PSD2, limitano notevolmente le possibilità di trattamento per altre finalità, consentendolo solo nel caso in cui l'interessato abbia dato uno specifico consenso ai sensi dell'articolo 6, paragrafo 1, lett. a), del GDPR o il trattamento sia basato su un atto legislativo dell'Unione o degli Stati membri. La questione della legittimità del trasferimento dei dati a soggetti terzi è stata inoltre oggetto di una Q&A dell'EBA 2018/4098[53] che ha esplicitamente consentito il trasferimento delle informazioni di conto anche a soggetti diversi dall'utente finale del servizio purché ciò avvenga nel rispetto delle previsioni del GDPR.

I partecipanti al Tavolo hanno convenuto che tali interventi, sebbene abbiano avuto il pregio di fare chiarezza su alcune questioni, ne lasciano ancora aperte altre; potrebbe essere dunque utile la

---

di una "grave minaccia agli interessi collettivi degli utenti di servizi di pagamento" del paese *host*, le autorità competenti di quest'ultimo possano adottare misure cautelari in via temporanea (art. 30, paragrafo 28, PSD2). Pertanto, alla luce dell'attuale riparto delle competenze tra l'Autorità *home* e *host*, emergono dubbi riguardo all'effettiva possibilità per le Autorità *host* di accertare eventuali violazioni degli operatori in libera prestazione di cui informare le Autorità *home* o per le quali disporre misure cautelari.

[52] È possibile cogliere una distanza definitoria tra la PSD2 e il GDPR con riguardo al concetto di "dato sensibile". La PSD2 fornisce esclusivamente una definizione di "dati sensibili relativi ai pagamenti", mentre il GDPR rinuncia tout court a tracciarne una, preferendo invece elencare alcune "categorie particolari" di dati personali , alle quali applicare una disciplina maggiormente stringente prevedendo che il trattamento di queste categorie particolari di dati personali è vietato a meno che non ricorrano alcune condizioni quali, a titolo esemplificativo, il consenso esplicito dell'interessato o motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (art. 9 GDPR).

[53] Consultabile al seguente link.

predisposizione di Linee Guida congiunte dell'EBA e dell'EDPB, che: (i) ricomprendano una mappatura dei dati che possono rientrare nel concetto di "dati sensibili relativi ai pagamenti"; (ii) chiariscano, in relazione al trattamento di "particolari categorie di dati", in quali circostanze può ravvisarsi un «*interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri*»; (iii) esplicitino, con riferimento ai dati trasmessi e gestiti alle cd. "quarte parti", quanto già chiarito nella sopra citata Q&A dell'EBA. Queste Linee Guida avrebbero il pregio di compendiare gli interessi relativi ad entrambi gli ambiti normativi, costituendo un punto di riferimento per gli operatori del mercato dei pagamenti (pagamenti e protezione dei dati).

5.4. PSD2 e DORA

Il Tavolo ha affrontato anche la tematica dell'allineamento delle previsioni della PSD2 e del nuovo Regolamento in materia di resilienza operativa digitale (DORA), la cui applicazione è prevista nel 2025, che mira, tra l'altro, ad armonizzare la disciplina applicabile all'*incident reporting* – disapplicando le previsioni *ex* PSD2, comprese quelle sugli incidenti operativi e di sicurezza sui pagamenti – all'intero settore finanziario. Risulta quindi importante un coordinamento tra le due normative per evitare sovrapposizioni e assicurare, al contempo, continuità di applicazione di talune previsioni normative al fine di non creare distorsioni sul mercato.

Il Regolamento DORA affronta, inoltre, il rischio di terza parte, prevedendo: (i) il profilo relativo all'*outsourcing* da parte delle entità finanziarie al fine di armonizzarne e estenderne la disciplina all'intero settore finanziario; (ii) un nuovo *framework* di sorveglianza sulle terze parti critiche (*critical ICT third-party service provider* – CTPP). Rispetto a quest'ultimo profilo, è stato rilevato, nell'ambito dei lavori del Tavolo, che le terze parti critiche ai sensi di DORA, che in futuro verranno identificate congiuntamente dalle tre Autorità di Vigilanza Europee sulla base di quattro criteri di criticità[54], sono diverse da quelle definite dalla PSD2 (es. AISP e PISP)[55] e non dovrebbe presentarsi un tema di coordinamento tra le relative discipline. Inoltre, ad oggi, nelle more della valutazione lasciata alla Commissione europea sulla loro inclusione, i sistemi di pagamento e i relativi fornitori[56] sono esclusi dall'ambito applicativo del DORA, anche tenuto conto del *framework* di sorveglianza europeo (art. 127 TFUE). È stato evidenziato infine che, anche qualora la futura normativa dovesse includere in *scope* alcuni fornitori tecnologici, non è detto che il perimetro coincida con quello di DORA (ciò dipenderebbe dai rispettivi criteri di identificazione). Tali profili potranno in prospettiva essere meglio apprezzati una volta definiti gli RTS di DORA per l'individuazione dei CTPP.

[54] Ai sensi dell'art. 31, paragrafo 2, e specificamente: i) l'impatto sistemico su servizi finanziari in caso di incidente; ii) l'importanza dei soggetti serviti (tenendo conto sia delle entità finanziarie di importanza sistemica che le loro interconnessioni); iii) l'affidamento delle entità finanziarie sui servizi erogati dalle CTPP per lo svolgimento di funzioni critiche; iv) il grado di sostituibilità (tenendo conto sia di potenziali sostituiti sia delle difficoltà riscontrabili nel processo di migrazione).

[55] Le terze parti introdotte dalla PSD2 sono PSP che forniscono servizi agli utenti finali, mentre quelle a cui fa riferimento la DORA sono fornitori di servizi tecnologici alle entità finanziarie.

[56] L'art. 31, paragrafo 8, DORA, prevede l'esclusione delle terze parti già assoggettate ad un *framework* di sorveglianza volto al perseguimento degli obiettivi di cui all'art. 127 del TFUE.

5.5. PSD2, EMD2 e MiCAR

Sono state analizzate nell'ambito dei lavori del Tavolo, in una prospettiva di coordinamento tra discipline, i principali punti di contatto e le potenziali frizioni tra la normativa sui servizi di pagamento e il Regolamento relativo ai mercati delle cripto-attività (MiCAR).

Quale possibile schema di analisi, si è operata una macro-distinzione tra le due seguenti fattispecie, posto che in ambedue il termine "pagamenti" è utilizzato in senso a-tecnico, in quanto i servizi di pagamento propriamente detti possono avere ad oggetto esclusivamente fondi (mentre, nel contesto di MiCAR, i soli *e-money token* (EMT)[57] sono qualificabili come fondi ai sensi della PSD2):

- "pagamenti'' direttamente eseguiti in cripto-attività;
- pagamenti "avviati" a partire da una disponibilità del cliente in cripto-attività, ad es. in un *wallet*, e poi eseguiti in fondi (previa conversione delle cripto-attività, c.d. *exchange*).

Con riferimento alla prima fattispecie, una precisazione si è resa anzitutto necessaria rispetto alla distinzione tra EMT, da un lato, e le altre cripto-attività disciplinate da MiCAR (*asset-referenced token*[58] – ART e c.d. *crypto other than*[59]), dall'altro. Gli EMT rappresentano infatti l'equivalente "tokenizzato" della moneta elettronica, trattandosi dell'unica categoria di cripto attività prevista da MiCAR che mantiene un valore stabile e prevede un diritto di rimborso in rapporto di parità 1:1 con una valuta *fiat*. Dunque i pagamenti effettuati con EMT, stante la qualificazione degli stessi come strumenti di pagamento, potrebbero ragionevolmente essere ricompresi nella futura revisione della PSD2, nell'ambito di un raccordo con MiCAR e con la nozione di "servizi di trasferimento" ivi impiegata. In quest'ottica, ai pagamenti effettuati con EMT si dovrebbero applicare disposizioni in tema di trasparenza e diritti e obblighi delle parti *in toto* o in parte mutuate, con opportuni adattamenti, dalle attuali previsioni contenute nei titoli III e IV della PSD2.

Più problematico risulta definire le finalità di utilizzo degli ART, in quanto gli stessi possono essere impiegati sia con funzione di investimento, sia come mezzo di scambio o, comunque, come riserva di valore. In particolare, l'utilizzabilità degli ART come mezzo di scambio è riconosciuta da MiCAR, seppur con una forma di monitoraggio e restrizioni quantitative[60] per prevenirne un'ampia diffusione e dunque evitare effetti di sostituzione monetaria. La circostanza per cui MiCAR riconosce e, al tempo stesso, limita l'utilizzabilità degli ART come mezzo di scambio solleva un importante punto di attenzione nel contesto della revisione della PSD2: da un lato, il possibile impiego come mezzo di scambio deporrebbe a favore di una copertura degli ART nella revisione della PSD2, così

[57] Gli EMT – token di moneta elettronica – mirano a mantenere un valore stabile facendo riferimento a una valuta ufficiale.

[58] Gli ART – token collegati ad attività – mirano a mantenere un valore stabile facendo riferimento a una singola attività – purché diversa da una valuta ufficiale – oppure a un paniere di attività diverse (ad es. valute ufficiali, *commodity* o altre cripto-attività).

[59] Cripto-attività che non sono ART o EMT e che, lungi dal costituire una mera casistica residuale, rappresentano la maggior parte delle cripto-attività attualmente esistenti.

[60] Il numero medio e il valore aggregato medio trimestrali stimati delle operazioni giornaliere associate a usi come mezzo di scambio in una determinata area monetaria non devono essere superiori, rispettivamente, a un milione di operazioni e a 200.000.000 euro (al superamento di queste soglie si attivano delle restrizioni, tra cui il divieto di emettere ulteriori ART).

da prevenire situazioni di vuoto normativo; dall'altro lato, occorre evitare di far percepire l'inclusione all'interno della revisione della PSD2 dei servizi di "pagamento" basati sugli ART come una piena legittimazione del loro utilizzo come mezzi di scambio (utilizzo che MiCAR cerca di limitare). Un ulteriore aspetto che i lavori del Tavolo hanno considerato è rappresentato dalla necessità di valutare se l'eventuale inclusione nella revisione della PSD2 delle transazioni con ART utilizzati come mezzo di scambio richieda un'estensione del concetto di "fondi". Dal momento che, per definizione, il valore degli ART si riferisce al valore di uno o più *asset* diversi da una singola valuta ufficiale, potrebbe non essere appropriato classificare gli stessi come fondi, rappresentando piuttosto "un valore". Altro elemento da valutare concerne l'opportunità – già espressa con riferimento agli EMT – di prevedere presidi a tutela della clientela, qualora si optasse per portare *in scope* della nuova PSD le transazioni in cui gli ART sono usati come mezzo di scambio. In particolare, occorrerà, da un lato, individuare le disposizioni in materia di trasparenza e diritti e obblighi delle parti nella prestazione dei servizi di pagamento attualmente incluse nella PSD2 che si prestano – su un piano sia tecnico-operativo sia giuridico – a essere applicate alle transazioni in ART e, dall'altro, definire gli adattamenti che si renderanno necessari alla luce delle peculiarità degli ART (anzitutto, in considerazione del fatto che il loro valore, espresso in euro o in un'altra valuta ufficiale dell'UE, potrebbe essere oggetto di oscillazioni, anche notevoli). Una possibile soluzione discussa con i partecipanti potrebbe consistere nel ricondurre i servizi di trasferimento in ART utilizzati come mezzo di scambio all'ambito di applicazione della nuova normativa, valutando al contempo la possibilità di considerare gli ART quale categoria giuridica aggiuntiva, distinta da quella di fondi, ad es. trasponendo in ambito PSD il più ampio concetto di valore di cui al PISA *framework*[61].

Un discorso diverso e più complesso vale invece per le *crypto other than*. Queste cripto-attività, in quanto prive di valore intrinseco, non riferite ad attività dell'economia reale o finanziaria e non assistite da un diritto di rimborso in capo all'utilizzatore, non sono, come tali, idonee a svolgere una funzione di pagamento[62]. Alla luce delle caratteristiche di volatilità e rischiosità, per le *crypto other than* varrebbe a maggior ragione la riflessione svolta relativamente agli ART: un'ipotetica attrazione all'ambito di applicazione della PSD2 delle *crypto other than* dovrebbe essere attentamente vagliata a motivo della particolare rischiosità di questi strumenti ed essere comunque tenuta nettamente distinta dal concetto di fondi, nonché venire possibilmente corredata da una serie di salvaguardie per far fronte ai rischi per l'utenza, stante la menzionata inidoneità a un utilizzo con finalità di pagamento.

In merito alla seconda fattispecie richiamata in precedenza, ossia i pagamenti "avviati" a partire da una disponibilità del cliente in cripto-attività e poi eseguiti in fondi, previa conversione delle cripto-attività, è stato evidenziato come negli ultimi anni si sia assistito alla comparsa sul mercato, anche europeo, di diverse iniziative finalizzate al collocamento presso la clientela, da parte di piattaforme

[61] Il PISA *framework* supera la nozione di "trasferimento di fondi" – tipica della funzione degli strumenti di pagamento tradizionali – in favore di quella di "trasferimento di valore", più ampia e idonea a intercettare ogni forma di sistema digitale organizzato per gestire (anche) finalità di pagamento o finanziarie.

[62] Tale inidoneità di utilizzo nell'ambito dei pagamenti trova evidenza anche nella "Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività" del 15 giugno 2022 presente al seguente link.

crypto, di carte di pagamento che consentono l'utilizzo di cripto-attività – previa loro conversione in fondi – per effettuare acquisti in valuta *fiat* di beni e servizi presso esercenti fisici o siti di commercio elettronico. L'emissione delle carte *crypto-linked* avviene tipicamente tramite accordi con IMEL (*issuer*), la conversione delle cripto-attività in fondi avviene generalmente al momento del pagamento, a opera della piattaforma che offre le carte[63]. In una prospettiva di revisione della PSD2 è stato ritenuto opportuno, dai partecipanti al Tavolo, definire la qualificazione giuridica dei "pagamenti avviati in cripto-attività e successivamente eseguiti in fondi", anche rispetto ai profili di interazione con la disciplina dei servizi per le cripto-attività stabilita da MiCAR[64]. In tali casi si assiste alla prestazione di due servizi in sequenza temporale: i) l'*exchange* (conversione) di cripto-attività in fondi, disciplinato da MiCAR; ii) un servizio di pagamento (PSD2) grazie a cui l'utente utilizza i fondi rinvenienti dalla conversione per acquistare beni e servizi. Si evidenziano pertanto i seguenti elementi di rilevanza già condivisi con i partecipanti:

(i) oggetto di conversione potrebbero essere, oltre agli EMT, anche ART e *crypto other than*. Rispetto a queste ultime, occorrerebbe prestare particolare attenzione agli elevati profili di rischio dovuti principalmente alla volatilità di questi strumenti che li rende sostanzialmente poco idonei a essere utilizzati come strumenti di pagamento;

(ii) i due servizi menzionati potrebbero essere prestati direttamente dal medesimo soggetto (se in possesso delle autorizzazioni richieste sia dalla PSD2 che dal MiCAR) o da due soggetti distinti. In questo secondo caso andrebbe compreso come potrebbe configurarsi, da un punto di vista contrattuale e organizzativo, la relazione tra i due prestatori di servizio, anche rispetto al rapporto con il cliente e, di conseguenza, potrebbe valutarsi l'eventuale necessità di inserire specifiche disposizioni nella revisione della PSD2 con riferimento a questa fattispecie (in MiCAR alcune indicazioni al riguardo sono riportate nel summenzionato art. 70, paragrafo 4).

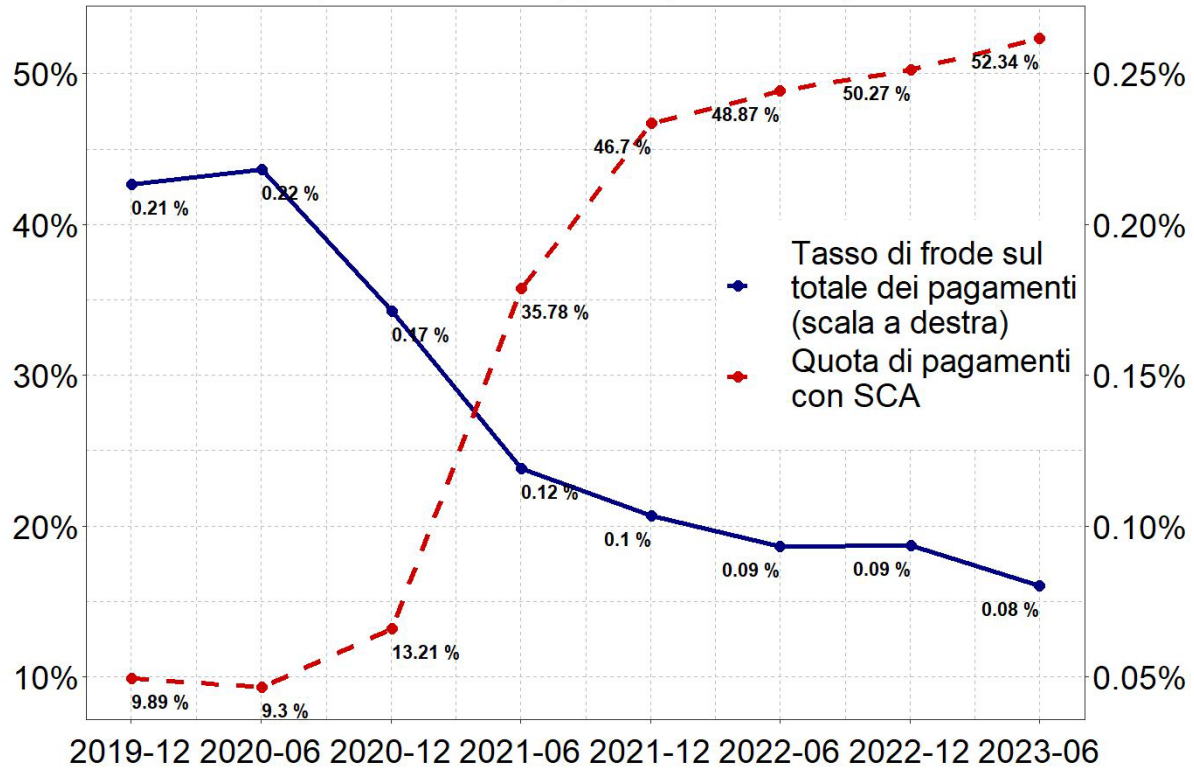
[63] In alcuni casi, l'utilizzo delle carte per effettuare acquisti consente di ottenere ricompense (*reward program*) nella forma di cripto-attività, secondo un'impostazione che dapprima vede l'utente convertire le proprie cripto-attività in fondi per realizzare acquisti e, una volta effettuata la transazione, ottenere sotto forma di premio altre cripto-attività (in alcuni casi, token nativi della piattaforma a cui è collegata la carta).

[64] Sul punto, l'art. 70, paragrafo 4, MiCAR precisa che «*I prestatori di servizi per le cripto-attività* [CASP] *possono prestare essi stessi, o tramite terzi, servizi di pagamento connessi al servizio per le cripto-attività che offrono, a condizione che il prestatore di servizi per le cripto-attività stesso, o il soggetto terzo, sia autorizzato a prestare tali servizi a norma della direttiva (UE) 2015/2366. Qualora siano prestati servizi di pagamento, i prestatori di servizi per le cripto-attività informano i rispettivi clienti di tutti gli elementi seguenti: a) la natura nonché i termini e le condizioni di tali servizi, fornendo riferimenti al diritto nazionale applicabile e ai diritti dei clienti; e b) se tali servizi sono offerti direttamente da essi o da terzi*».

Annex I: Analisi d'impatto della Strong Customer Authentication (SCA) sulla sicurezza dei pagamenti con carte da remoto in Italia

In Italia la quota di transazioni con carte (debito e credito) da remoto che richiedono la SCA è progressivamente aumentata dopo la sua introduzione, stabilizzandosi negli ultimi due anni al di sopra del 50% (54.3% nel I semestre del 2023). Congiuntamente, si è osservata un'importante riduzione del tasso di frode calcolato sul valore complessivo delle transazioni da remoto (Figura 1). Questi andamenti, nel loro complesso, suggeriscono un impatto positivo dell'utilizzo della SCA sulla sicurezza delle transazioni con carte da remoto.

Figura 1
Sicurezza nei pagamenti con carte da remoto
(dati semestrali; punti percentuali)



Elaborazione sui dati dell' EBA Fraud Reporting e della Matrice dei Conti.
SCA: Autenticazione Forte del cliente.

Relativamente alle transazioni che sono escluse dall'adozione della SCA (Figura 2a), nel I semestre 2023, la quota prevalente è l'esenzione dall'utilizzo (42.2%), mentre le operazioni Merchant Initiated Transactions (MIT) e le transazioni che non richiedono la SCA per altro motivo sono rispettivamente pari a 24.4% e 33.4%.

Relativamente alle esenzioni (Figura 2b) in base ai *Regulatory Technical Standards on strong customer authentication and secure communication under PSD2* (RTS), nel I semestre 2023, l'esenzione maggiormente utilizzata è l'analisi dei rischi (71.5%). Il rimanente 28.5% è ripartito

equamente tra operazioni ricorrenti (9.3%), beneficiari di fiducia (9.1%) e transazioni di valore modesto (9.5%). Un'esenzione residuale è invece quella costituita dai processi/protocolli sicuri per le imprese (0.6%).

Figura 2
Transazioni che non richiedono l'autenticazione forte del cliente

Figura 2a: esclusioni alla SCA

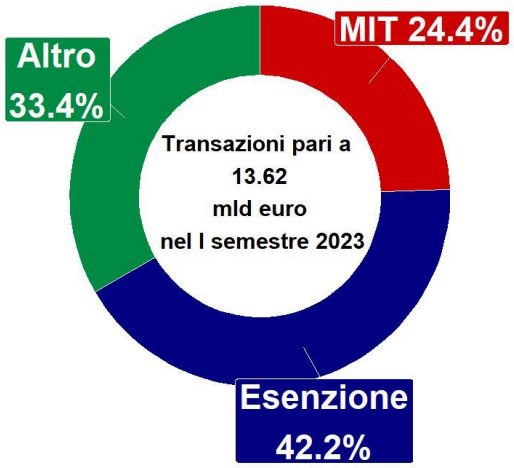
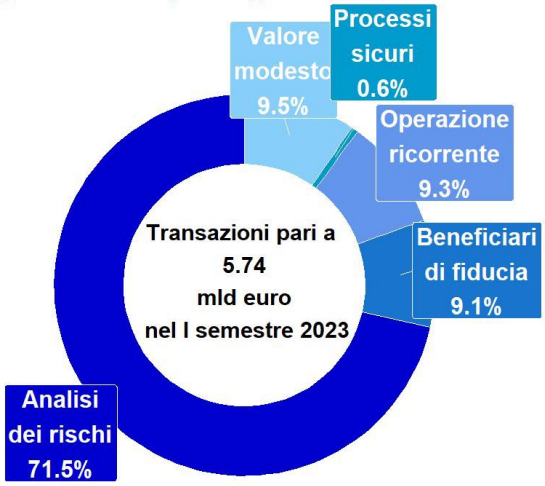


Figura 2b: tipologia di esenzione



Note: *Per "Esenzione" s'intende la quota di transazioni non soggette a SCA dovute a: i) analisi dei rischi (transazioni di importo contenuto, per prestatori di servizio con tasso di frode pari o inferiore a un determinato tasso indicato nell'RTS, per le quali il prestatore di servizi di pagamento non ha individuato elementi critici indicati nell'RTS); ii) valore modesto (importo inferiore a 30 euro o importo cumulato relativo alle ultime transazioni inferiore a 100 euro o numero di transazioni dall'ultima applicazione della SCA inferiore a cinque); iii) operazioni ricorrenti (serie di operazioni dello stesso importo e a favore dello stesso beneficiario); iv) beneficiari di fiducia (se il beneficiario del pagamento è incluso in un elenco di beneficiari di fiducia precedentemente determinato), processi/protocolli sicuri per le imprese (pagamenti da persone giuridiche tramite canali dedicati riconosciuti come sicuri dall'Autorità alla stregua della SCA).*

Per "Altro" s'intende la quota di altre transazioni non soggette a SCA quali le transazioni effettuate per ordine telefonico o via mail ("Mail Order Telephone Order", M.O.T.O), quelle per le quali l'acquirer o l'issuer ha sede al di fuori del SEE (cd "One-leg transactions"), quelle per le quali l'autenticazione viene realizzata in precedenza per il tramite di un terzo soggetto ecc.

Per "MIT" s'intende la quota di transazioni avviate dal commerciante senza bisogno di ulteriore autenticazione da parte del cliente, che ha precedentemente già autorizzata una serie di pagamenti (cd. "Merchant Initiated Transaction").

In termini di sicurezza (Tabella 1, Figura 1), nel I semestre 2023, le transazioni eseguite da remoto non soggette a SCA hanno riportato un tasso di frode sul valore dei pagamenti pari a 0.088%,

risultando dunque nel complesso più rischiose delle transazioni da remoto eseguite con la SCA (tasso di frode pari a 0.073%). Tuttavia, emergono differenze importanti per quanto riguarda le diverse tipologie di transazioni non soggette a SCA (Tabella 1 e Figura 3). Le transazioni in esenzione risultano maggiormente sicure, con un tasso di frode inferiore a quello delle transazioni con SCA (0.066%). Risultano invece notevolmente più rischiose le transazioni "MIT" e "Altro" (rispettivamente 0.115% e 0.097%).

Tra le varie tipologie di esenzione, quella più affidabile è connessa ai processi/protocolli sicuri per le imprese (0.016%), mentre quella più rischiosa riguarda le transazioni di valore modesto (0.09%). Le transazioni con analisi dei rischi, che costituiscono l'esenzione maggiormente frequente, hanno un tasso di frode pari a 0.065%, pressoché analogo a quello che caratterizza le transazioni SCA. Risultano maggiormente sicure delle transazioni soggette a SCA anche le transazioni verso beneficiari di fiducia (tasso di frode pari a 0.048%).

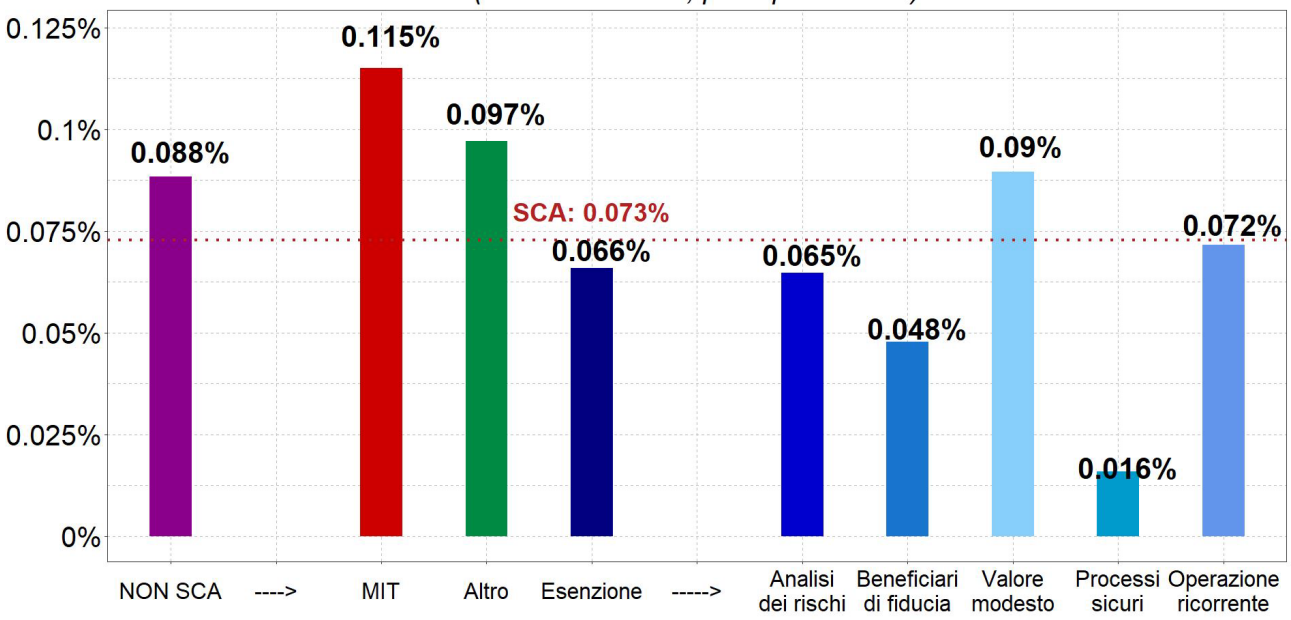
Tabella 1 - Tassi di frode per tipologia di transazione

I semestre 2023

Transazione	Frodi (€mln)	Pagamento (€mln)	Tasso di frode (pp)
SCA	10.9	14,952	0.073
Non SCA	12	13.616	0.088
MIT	3.8	3,327	0.115
Altro	4.4	4,545	0.097
Esenzione	3.8	5,743	0.066
Analisi dei rischi	2.6	4,104	0.065
Beneficiari di fiducia	0.25	520	0.048
Valore modesto	0.49	548	0.09
Processi sicuri	0.005	34	0.016
Operazioni ricorrenti	0.38	537	0.072

Figura 3
Tassi di frode nelle transazioni con carte da remoto senza SCA: complessivo, per esclusione, per esenzione

(I semestre 2023; punti percentuali)



Annex II: Il modello di remunerazione dell'Open Banking nel confronto internazionale

L'Open Banking ha portato un notevole mutamento nell'industria dei servizi finanziari in molti Paesi ed è uno dei principali trend della trasformazione digitale del mercato dei pagamenti (He, Huang, e Zhou, 2023). Alla fine del 2021, in base a quanto riportato in Babina, Buchak e Gornall (2022), erano circa 80 i Paesi che avevano iniziato a introdurre una regolamentazione in materia di Open Banking con l'obiettivo di incentivarne l'uso e generando in poco tempo significativi aumenti di investimenti di *venture capital* nel settore del fintech. Grazie all'Open Banking, le società fintech e gli altri innovatori nel mercato possono accedere alle informazioni sui clienti con il loro consenso potendo usufruire delle basi dati delle banche tradizionali, e utilizzare questi dati per sviluppare nuovi prodotti e servizi che siano più adatti alle esigenze dei consumatori.

Nei servizi di Open Banking, un elemento determinante per garantire un adeguato funzionamento nel tempo del nuovo modello di business è quello della distribuzione dei costi sostenuti per predisporre l'infrastruttura di condivisione dei dati e mantenerla nel tempo.

Nella letteratura economica (Plaitakis e Staschen, 2020), sono stati identificati tre modelli di remunerazione, definiti in base alla condivisione dei costi tra entità incaricate di condividere i dati (cd. *incumbent*), utilizzatori dei dati (cd. Third Party Providers, TPP) e consumatori.

In Australia, Unione Europea e Regno Unito, l'autorità di regolamentazione ha posto la maggior parte dell'onere dei costi sulle entità incaricate di condividere i dati. In Australia e nel Regno Unito, l'onere faceva parte delle "sanzioni" imposte agli *incumbent* per precedenti pratiche di mercato anticoncorrenziali. In tutte e tre le giurisdizioni, l'attribuzione dei costi agli *incumbent* riduce gli ostacoli alla condivisione dei dati per i TPP e per i consumatori.

D'altra parte, Brasile, Hong Kong, Messico e Singapore autorizzano esplicitamente gli enti incaricati di condividere i dati ad addebitare tariffe ai TPP per ogni singola richiesta di dati, mentre i TPP in Bahrain sono autorizzati ad addebitare il costo ai consumatori. In Bahrain e Hong Kong le tariffe devono essere concordate bilateralmente, mentre in Messico devono essere approvate dall'autorità di regolamentazione. In Brasile, oltre un certo numero di chiamate API dati gratuite, le tariffe devono essere concordate dalla convenzione dei partecipanti al sistema di Open Banking, che è supervisionata dal regolatore.

Altri Paesi come gli Stati Uniti e la Cina hanno optato per un approccio non regolamentato ma stanno valutando l'adozione di norme specifiche in tema di Open Banking (He et al. op.cit.; e Babina et al. op. cit.).

Il fatto che un'autorità di regolamentazione imponga dei costi a una determinata parte o consenta alle parti di negoziare bilateralmente sembra dipendere da una varietà di fattori, tra cui la motivazione legata alla promozione dell'Open Banking nel mercato finanziario e la forza relativa dell'autorità di regolamentazione rispetto agli operatori storici del settore. Va notato che nelle giurisdizioni in cui l'autorità di regolamentazione ha imposto l'onere dei costi agli operatori *incumbent*, questi hanno espresso aspre critiche sul fatto che ciò possa rendere il modello di Open

Banking insostenibile a lungo termine, a meno che gli operatori *incumbent* possano porre in essere meccanismi di recupero dei costi, anche attraverso tariffazione incrociata in altri segmenti delle loro attività.

Bibliografia Annex II

Pellitteri, Parrini, Cafarotti, De Vendictis (2023). "L'Open Banking nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza", Banca d'Italia, Mercati, Infrastrutture e Sistemi di Pagamento, n.31.

Babina, Tania, Greg Buchak e Will Gornall (2022). "Customer Data Access and Fintech Entry: Early Evidence from Open Banking". Stanford University Graduate School of Business Research Paper.

Cologgi, Massimiliano (2023a). "The security of retail payment instruments: evidence from supervisory data", Banca d'Italia, Mercati, Infrastrutture e Sistemi di Pagamento, n.30.

Cologgi, Massimiliano (2023b). "The impact of regulation on retail payments security: Evidence from Italian supervisory data". Finance Research Letters, 54, 103799.

He, Zhiguo, Jing Huang e Jidong Zhou (2023). "Open banking: Credit market competition when borrowers own the data", Journal of Financial Economics, Volume 147, Issue 2.

Plaitakis, Ariadne, e Stefan Staschen (2020). "Open Banking: How to Design for Financial Inclusion." Working Paper. Washington, D.C.: CGAP.