PAYTECH e ML Risk: third party providers obbligati ai sensi del d.lgs. 231/2007

Eugenio Guardati

*Il legislatore della PSD2 ha riconosciuto e disciplinato modelli di servizio (*paytech*) basati sull'accesso di terze parti ai conti di pagamento della clientela. La segmentazione della* payment chain *e la pluralità di attori dalle inedite linee di* business *creano valore aggiunto nell'ecosistema dei servizi di pagamento ma rendono anche incredibilmente complessa l'attribuzione degli obblighi AML/CFT e pongono seri interrogativi circa l'opportunità di ricomprendere i TPP tra i soggetti obbligati.*
All'esito di consultazione pubblica, della quale si ripercorrono i principali argomenti assorbenti proposti dagli stakeholders*, il 1°marzo 2021 EBA ha pubblicato gli Orientamenti su CDD e fattori di rischio di riciclaggio per gli enti creditizi e istituti finanziari, dedicando l'orientamento18 ai PISP e AISP quali soggetti obbligati.*

1. *Account Information Service* e *Payment Initiation Service*

(AISP e PISP)

La PSD2 individua una nuova categoria di soggetti, cd. *Third Party Providers* (TPP), e due nuovi ulteriori servizi nell'ecosistema già delineato dalla PSD1: il servizio di disposizione di ordine di pagamento (*payment initiation service*: PIS) e il servizio di informazione sui conti (*account information service*: AIS)[1].

Con la prima locuzione si vuole identificare quel servizio che permette la disposizione dell'ordine di pagamento, su richiesta dell'utente di servizi di pagamento (PSU – *Payment Service User*), relativamente ad un conto detenuto presso un altro prestatore di servizi di pagamento (ASPSP – *Account Servicing Payments Service Providers*). La seconda locuzione si riferisce a quel servizio che fornisce informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente presso uno o più prestatori di servizi di pagamento. I nuovi *providers* di questi ser-

[1] Oltre ai relativi *Service Providers* cd. AISP punto 18 e PISP punto 19, art. 4 PSD2.

vizi potranno quindi operare su conti *online* accesi presso diversi prestatori di servizi di pagamento, ma a questi ultimi continuerà a competere l'amministrazione e gestione del conto (il cd. servizio di radicamento del conto).

La PSD2 articola i requisiti di sicurezza dei pagamenti elettronici su quattro pilastri, specificamente implementati da EBA all'interno del sistema SEPA:

1) l'autenticazione forte della clientela (cd. *strong customer authentication*-SCA) e la comunicazione sicura tra *provider* (cd. *common standard of communication-CSC*)[2]; 2) l'impiego di API[3]-TPP e l'armonizzazione dei processi autorizzativi tra IP; 3) requisiti per la gestione dei rischi di sicurezza IT dei PSP, valutati in fase di autorizzazione e costantemente aggiornamenti[4]; 4) il *reporting* obbligatorio in presenza di gravi incidenti IT[5] e in caso di frodi[6].

La resilienza dell'intero circuito dei pagamenti interbancari è condizionata all'affidabilità dei singoli operatori quali *endpoints* (punti di accesso). Come per una catena, la resistenza si misura dall'anello più debole. Ciò vale per la *cybersecurity,* ma analogo discorso vale per la permeabilità del sistema finanziario alla criminalità organizzata e alla costante ricerca di nuove forme di riciclaggio.

Il fenomeno delle terze parti nei servizi di pagamento deve essere opportunamente letto alla luce del crescente rigore delle regole poste a presidio dell'esercizio dell'attività bancaria e finanziaria. L'inasprimento dei requisiti di vigilanza patrimoniale e la conseguente contrazione del margine di redditività si sono incontrate con la disponibilità di nuove tecnologie e il concorso di queste circostanze avrebbe innescato una forza centrifuga dei servizi bancari, finanziari e di pagamento verso nuovi soggetti, creando nuove opportunità di mercato, nuove esigenze di tutela dei clienti e controllo dei nuovi fattori di rischio.

L'ampliamento della disponibilità soggettiva dei dati bancari e transazionali costituisce il fattore di rischio principale per la sicurezza IT dei servizi di pagamento,

[2] I *Regulatory Technical Standards* (RTS) EBA *on strong customer authentication (SCA) and common and secure open standars of communication (CSC)* (art.98 PSD2), pubblicati a marzo 2018 (applicazione 14 settembre 2019). Regolamento delegato 2018/389/UE integra la Direttiva 2015/2366/UE - RTS su SCA e CSC

[3] *Application programming interface.*

[4] *Guidelines on operational and security risk management* (art. 95 PSD2) pubblicate a dicembre 2017.

[5] *Guidelines on major incident reporting* (art. 96 PSD2) pubblicate a luglio 2017.

[6] *Guidelines on fraud data reporting* (art. 96 PSD2) pubblicate a luglio 2018. Al tema della sicurezza del settore finanziario si interessano anche il GDPR 2016/679 e la Direttiva NIS – *Network and Information Security* con obblighi di segnalazione di incidenti informatici, requisiti di sicurezza verosimilmente estesi anche a operatori bancari e finanziari in quanto gestori di dati personali ai sensi del GDPR o operatori di servizi essenziali ai sensi della Direttiva NIS.

comportando ad esempio l'aumento del rischio di utilizzo illecito delle credenziali di accesso ai servizi di *home banking*. L'interconnessione tra le piattaforme costituisce l'occasione ideale di perdita di controllo[7] sui dati ma anche fattore di incremento dell'esposizione al rischio di riciclaggio e finanziamento del terrorismo. Al contempo però, l'*open banking* rappresenta l'incredibile opportunità di ampliamento della base informativa ai fini AML/CFT.

Le Autorità di Vigilanza europee ritengono che l'operatività dei *third party providers* possa prestarsi a schemi criminali finalizzati all'occultamento e al lavaggio di capitali illeciti. Un'ipotesi avanzata di *moneylaundering* tramite i canali TPP potrebbe essere il frazionamento di un'unica operazione verso un unico beneficiario attraverso l'apertura di diversi rapporti con molteplici PISP. La pluralità di pagamenti a favore del medesimo beneficiario può costituire potenziale indicatore di anomalia una volta dimostrata l'unità logica ed economica delle diverse operazioni.

Nel perimetro del rischio penale a cui si espongono i TPP, quindi, devono annoverarsi le fattispecie penali *ex* d.lgs. 21 novembre 2007, n. 231 ma anche riciclaggio *ex* art. 648-*bis* c.p., reimpiego *ex* art. 648-*ter* c.p., autoriciclaggio *ex* art. 648-*ter*.1 c.p., senza considerare poi le misure in tema di sequestro e confisca *ex* 648-*quater* c.p. e le sanzioni pecuniarie e interdittive da responsabilità da reato degli enti *ex* d.lgs. 21 novembre 2007, n. 231.

2. AISP e PISP quali soggetti obbligati AML

La pubblicazione degli "Orientamenti EBA sulle informazioni che devono essere fornite per ottenere l'autorizzazione degli IP, IMEL e la registrazione degli AISP[8]" (da qui in avanti *Guidelines*) ha rappresentato l'occasione delle prime riflessioni sul ruolo dei *third party providers* nel flusso di pagamenti e quindi sull'opportunità o meno di considerarli soggetti obbligati AML. La *compliance* AML/CFT, specie nell'identificazione del cliente, è uno degli oneri più gravosi e il maggior ostacolo alla *customer conversion*, ovvero la monetizzazione del cliente; quindi, la risposta al quesito non è

[7] La protezione dei dati personali potrebbe essere compromessa da accessi e modifiche non autorizzate, intercettazioni, invii a controparti errate, confusione nella trasmissione.

[8] *Guidelines under Directive (EU) 2015/2366 (PSD2) on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers*, 11.07.2017.
Eba ha pubblicato quattro serie di orientamenti applicabili rispettivamente a istituti di pagamento e PIS (i servizi da 1 a 7 Allegato I PSD2, o 8 in combinazione con i precedenti) (4.1), prestatori di servizi di informazione (solo punto 8 Allegato I) (4.2), istituti di moneta elettronica (4.3) e autorità competenti (4.4).

priva di conseguenze sullo sviluppo di queste tecnologie.

L'elenco dei soggetti obbligati appartenenti alla categoria degli intermediari bancari e finanziari (art. 3, co. 2, d.lgs. 21 novembre 2007, n. 231), oltre alle banche, Poste Italiane S.p.a., IMEL[9] e agli altri intermediari, fa espresso riferimento agli Istituti di Pagamento (IP) così come definiti dall'art. 1 co. 2 lett. h-*sexies*) TUB, ovvero "le imprese, diverse dalle banche e dagli istituti di moneta elettronica, autorizzate a prestare i servizi di pagamento". La nozione di "servizi di pagamento" è invece alla lettera h-*septies*.1), intendendosi con ciò, oltre a tutte le operazioni richieste per la gestione di un conto di pagamento, anche i servizi di disposizione di ordini di pagamento (n. 7 Allegato I PSD2) e servizi di informazione sui conti (n. 8).

In ottica *de iure condito*, i PISP e gli AISP sembrano essere soggetti obbligati ai fini antiriciclaggio. La Banca d'Italia ha infatti preferito ricomprendere, secondo un approccio cautelare, i TPP all'interno della disciplina AML. Il *risk-based approach* impone l'applicazione della *customer due diligence* modulandone l'intensità e la frequenza degli obblighi non solo alla luce del *risk assessment* associato al cliente o al prodotto, ma anche alla dimensione e alle peculiarità dell'attività condotta dall'intermediario. Si potrebbe quindi proporzionare la frequenza e lo spettro di monitoraggio delle transazioni al livello di rischio a queste associato, oppure potrebbe avvenire sulla base di gruppi omogenei di clienti di cui è stato profilato il *transaction behaviour* e quindi agevolare il monitoraggio.

Invece, in ottica *de iure condendo*, la domanda che ci dobbiamo porre è la seguente: premesso che la regolamentazione AML trova opportuna applicazione a fronte della collocazione e/o movimentazione di un flusso finanziario, l'intermediario potrebbe impedire l'interruzione della *digital trail* se fosse chiamato a collaborare attivamente con l'Autorità di Vigilanza? Se il PISP non fosse soggetto agli obblighi di CDD, conservazione e SOS, potrebbe agevolare la conversione, il trasferimento, l'acquisto, la detenzione, l'utilizzazione, l'occultamento o la dissimulazione dell'origine del denaro di provenienza illecita secondo la nozione di riciclaggio *ex* 231/2007[10]? Potrebbe apportare un contributo, attivo od omissivo, nel *placement, layering, integration* del flusso finanziario illecito?

La comprensione del rischio relativo all'operatività dei PISP è, ovviamente, presupposto preliminare di un corretto *risk based approach* all'AML. Il PISP altro non fa che avviare, comunicare, l'ordine di pagamento ma non lo esegue. La transazione è infatti eseguita esclusivamente dall'*account service provider* e il flusso finanzia-

[9] Art. 1., co. 2, ett. h-*bis*), TUB.

[10] In merito, si veda art. 2, co. 4.

rio non transita attraverso il PISP, il quale altrimenti sarebbe facilmente considerabile quale *gateway* e quindi opportunamente ricompreso tra i soggetti obbligati.

Il *considerando* 26 alle *Guidelines*[11] dispone: "*As for PISPs, the GLs already take into account that these providers do not enter into possession of funds and that, accordingly, all the information related to this is not required. The EBA therefore considers the level of information requested from these providers to be proportionate to their business model*".

A conferma del fatto che il PISP non entra in possesso dei fondi, la *Guideline* n. 3[12] di EBA esonera il richiedente che intenda prestare solo servizi di ordine di pagamento (PIS) dal presentare, all'interno del "Programma di Attività", il diagramma di flusso dei fondi e i meccanismi di regolamento[13].

Il riciclaggio di denaro richiede la conversione e l'occultamento di fondi illegittimamente acquisiti. Il denaro potenzialmente illecito invece transita solo dal conto del titolare, non del PISP.

Da queste premesse, sembra potersi dire che il ML/FT *risk* non incrementi quando nella filiera del servizio di pagamento si inserisce un PISP. Potrebbe quindi risultare non opportuna l'applicazione della normativa AML al prestatore di servizi di disposizione. D'altro canto, l'uso di PISP rappresenta un fattore di aumento del rischio di sottrazione dell'identità e del conseguente uso illegittimo del conto. Tuttavia, è bene precisare che, oltre a non essere un rischio specifico di *money laundering* ma un rischio generale dei conti *online*, il PISP è soggetto ai medesimi requisiti tecnici di accesso diretto all'*online banking*.

Altro elemento da tenere in considerazione è che il cliente (PSU) è stato già identificato dall'*account service payment provider* ASPSP nell'espletamento della *customer due diligence*. È quest'ultimo che detiene i fondi

[11] *Guidelines under Directive (EU) 2015/2366 (PSD2) on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers*, 11.07.2017.

[12] Serie 4.1 dedicata a IP e PISP.

[13] Inoltre, i PISP sono esonerati dal presentare le informazioni sui requisiti minimi di fondi propri in conformità al metodo *ex* art. 9 PSD2, previste per tutti gli altri all'interno delle stime previsione del bilancio dei primi tre esercizi finanziari (*Guideline* n. 4 – Piano Aziendale). Sono invece tenuti, insieme agli AISP, a fornire, all'interno del Programma di attività, l'importo monetario minimo dell'assicurazione della responsabilità civile professionale ai sensi dell'art. 5, par. 4 PSD2 (*Guideline* n. 3 – Programma di Attività), vedasi anche *Guideline* n.18. Inoltre, stando alla *Guideline* n. 7, AISP e PISP sono esonerati dall'adozione di misure di tutela dei fondi degli utenti dei servizi di pagamento 1-6 Allegato I PSD2 (gli AISP hanno una previsione specifica nella propria serie di *Guidelines* 4.2). *Guideline* n. 10 (Processo per l'archiviazione, monitoraggio, tracciabilità e limitazione dell'accesso ai dati sensibili relativi ai pagamenti) esonera il richiedente, che intenda fornire esclusivamente PIS, dalla descrizione delle modalità di archiviazione e dell'uso interno e/o esterno previsto dei dati acquisiti, anche da parte delle controparti.

ed esegue le transazioni, e da ciò consegue la titolarità di una posizione privilegiata non solo per l'esecuzione degli obblighi KYC ma anche per gli obblighi di monitoraggio dell'operatività del cliente.

In pratica, l'identificazione del cliente è stata già eseguita dall'ASPSP prima dell'instaurazione del rapporto, prima che il conto bancario sia reso disponibile al PSU; quindi, quale altra informazione potrebbe aggiungere il PISP? I PISP non aprono i conti di pagamento, non sono in possesso dei fondi del PSU e fanno affidamento sulle procedure di autenticazione effettuate dall'ASPSP durante il *payment flow*. L'ASPSP è il soggetto che ha il contatto diretto e la relazione più stretta con il PSU, basata sull'accordo e il servizio che fornisce. ASPSP apre e mantiene i conti dei PSU, ne detiene i fondi, e ben più rilevante, conduce la *strong customer authentication* durante i pagamenti e in fase di accesso. Tenendo conto che l'ASPSP già esegue i controlli AML sul PSU, se questi controlli fossero eseguiti anche dal PISP si giungerebbe ad una duplicazione degli adempimenti, incrementando la durata del *payment flow* e la frustrazione del PSU. Ciò causerebbe insoddisfazione e incrementerebbe l'abbandono del processo di pagamento. Una *due diligence* eccessivamente lunga durante il *payment flow* porterebbe all'abbandono, al *checkout* e allo spostamento su metodi di pagamento alternativi, ad esempio le carte o il *cash*, con relativo rischio di interruzione dell'*on boarding*. Si immagini di essere obbligati a caricare una foto del proprio passaporto ogni volta che si intende pagare un bene o un servizio. Questi obblighi incrementano radicalmente il costo del servizio di PI e del TPP in generale, risultando una barriera all'ingresso del mercato.

Quindi, da una duplicazione del tutto superflua si possono ottenere ben pochi benefici in termini di gestione del rischio, mentre comuni protocolli di collaborazione e comunicazione tra TPP, IP, IMEL possono svelare le molte potenzialità di guadagno in termini di prevenzione e rilevazioni efficaci. Tale duplicazione degli obblighi AML/CFT potrebbe, in effetti, risolversi in ostacoli decisamente gravosi sul *business profit* del PISP, mentre il proposito della PSD2 è facilitare l'accesso e la valorizzazione dei dati transazionali e quindi di incrementare la competizione tra i *player*. D'altra parte, però, se il cliente è stato già *onboarded*, l'aggiunta di un nuovo prodotto o canale di distribuzione è probabilmente un momento opportuno per riconsiderare il ML/FT *risk* associato al rapporto con lo stesso[14].

È bene chiarire che il rischio di ML non è sempre e solo connesso al *tainted funds management*

[14] In questo senso le RF CDD *Guidelines* in consultazione (p. 19) dispongono che gli AISP chiedano al cliente, ogni qual volta viene aggiunto un conto, se il conto è suo o è un conto condiviso, o se è di una persona giuridica della quale ha mandato di accedere ai conti (*corporate account*).

(gestione di fondi illeciti), ma anche alla semplice fornitura di servizi che indirettamente possano agevolare l'occultamento dell'origine e promuovere la fabbricazione della provenienza lecita fittizia. Se è vero che il PISP non detiene i fondi, è innegabile che il suo contributo possa ugualmente agevolare la dialisi del provento illecito, ad esempio attraverso la stratificazione (*layering*) di molteplici transazioni tra piattaforme di *e-commerce.*

A fornirci una risposta circa l'applicabilità ai PISP degli obblighi AML/CFT è la *Guideline* n.14 "Meccanismi di controllo interno al fine di conformarsi agli obblighi in materia di riciclaggio dei proventi di attività criminose e finanziamento del terrorismo"[15]. Con questa *guideline* EBA, nonostante tenga conto che il PISP non entra mai nel possesso dei fondi, decide di non esentarli dalla disciplina AML, come invece fa per gli AISP quando, tra le informazioni dovute per ottenere la registrazione, omette la *policy* AML.

Per quanto riguarda gli AISP, ai richiedenti la registrazione in merito alla prestazione del solo servizio del punto 8 Allegato I PSD2, come anticipato, è dedicata la seconda serie di *Guidelines* 4.2.

Prima facie, il servizio di informazioni aggregate su uno o più conti di pagamento non prevede il transito di alcun flusso finanziario attraverso il *provider*. Quindi, l'esenzione del servizio di informazione dagli obblighi AML non sembra compromettere le finalità della disciplina AML.

Il *considerando* 25 dispone: "*The EBA arrived at the conclusion that no further changes should be made because such exemptions are already provided in PSD2 itself, through Article 33 of PSD2 for AISPs (for example the requirements related to AML and statutory auditors)*"[16]. L'art. 33 co. 1 PSD2 esenta gli AISP dall'essere AML/CFT *compliant* e in particolare dal presentare una descrizione dei meccanismi di controllo interno *ex* art. 5, co. 1, lett. k) PSD2[17].

[15] In occasione del *feedback table* e con specifico riferimento alla *Guideline* n. 14, è stato osservato da un partecipante che 1) il PISP non entra nel possesso dei fondi e quindi non dovrebbe essere soggetto obbligato AML; 2) la necessità di dotare l'AISP di un AML *prevention programme* basato su specifici indicatori di monitoraggio adattati alle peculiarità dell'attività condotta 3) di assicurare proporzionalità degli obblighi AML su AISP e PISP. EBA risponde: "*PSD2 does not provide for any exemption for PISPs in relation to AML. It might be the case that they are obliged entities under national law: there are other entities that do not enter into possession of funds and are subject to AML regulation*".

[16] Art. 33 esenta tali soggetti dall'applicazione della procedura e delle condizioni di cui alle sezioni 1 (disposizioni generali) e 2 (tempi di esecuzione e data valuta), ad eccezione dell'articolo 5, paragrafo 1, lettere a), b), da e) a h), j), l), n), p) e q), dell'art. 5, par. 3, nonché degli articoli 14 e 15. La sezione 3 (autorità competenti e vigilanza) si applica ad eccezione dell'art. 23, par. 3.

[17] Che prevede per gli IP una descrizione dei meccanismi di controllo interno predisposti dal richiedente al fine di conformarsi agli obblighi AML.

Da quanto emerge dalle *Guidelines* 4.2 dedicate all'AISP, questa categoria di TPP non sarebbe tenuta a presentare la policy AML. La conseguenza potrebbe essere di ritenere che gli AISP non siano soggetti obbligati AML. È di tutta evidenza l'incongruità nel ritenere soggetti obbligati i PISP e non anche gli AISP. Questi ultimi non entrerebbero mai in possesso dei fondi dei propri clienti, proprio come i PISP[18].

Alla luce del fatto che gli AISP non conducono i controlli AML sui PSU, è ancora più forte la domanda perché invece i PISP dovrebbero essere soggetti obbligati se oltre a non partecipare al *payment flow* hanno una base informativa meno ampia degli AISP e degli ASPSP.

Sembra legittimo porsi dei dubbi di tutela della *fair competition*. Assoggettare solo banche, IMEL, IP e i PISP agli obblighi AML e non anche gli AISP potrebbe essere fattore distorsivo della *fair competition*? Anche se è evidente che le linee di *business* non sono perfettamente coincidenti, la PSD2 vuole creare un unico campo da gioco nei servizi di pagamento. Sembra difficile rispettare questo obiettivo considerando solo alcuni intermediari obbligati ai fini AML/CFT ed esentando gli altri.

È fondamentale comprendere che tipo di servizio viene eseguito dal PISP e quale il suo ruolo nel *payment flow*. Il PISP fornisce *payment initiation services* ricevendo istruzioni dal PSU attraverso la piattaforma del commerciante e genera così un ordine di pagamento senza mai entrare in possesso dei fondi. L'ordine di pagamento è, quindi, inviato all'APSP, dove sono depositati i fondi e, ovviamente, autorizzato dal PSU usando le credenziali di autenticazione fornite dall'ASPS, in *compliance* con SCA e requisiti di collegamento dinamico. PISP è responsabile della generazione di ordini di pagamento basati sulla richiesta del PSU e non influenza in alcun modo l'esecuzione del pagamento.

Tra PISP e *card processor* corrono diverse similitudini (quest'ultimo però non esegue gli obblighi AML/CFT sul PSU, ma esclusivamente sul commerciante), a partire dal ruolo nel *payment flows*:

- entrambi fanno affidamento sulle credenziali emesse dall'ASPSP al PSU, il PISP sulle credenziali di autenticazione e il *card processor* sui *card details* (come *PAN, CVV/expiration date, pin, 3d secure credentials*);
- entrambi i tipi di credenziali ricadono sotto la SCA e i *dynamic linking requirements* della PSD2; in entrambi i casi il PSU autorizza l'esecuzione della transazione di pagamento.

[18] Per "possesso dei fondi" si intende anche la "*temporary possession*" così da ricomprendere anche l'IP che possiede i fondi solo temporaneamente, cioè limitatamente all'esecuzione del servizio di pagamento. L'IP inoltre non può accettare depositi.

PISP e c*ard processor* hanno ruoli simili, ma quest'ultimo può essere in possesso dei fondi, il più delle volte ha accesso ai dati di autenticazione (*card details*, inclusi il PAN/CVV/PIC). Ora la domanda è, se il *card processor*, un operatore con un ruolo simile al PISP, non conduce i controlli AML sul PSU, perché dovrebbe farlo il PISP?

Richiedere ai PISP di condurre i controlli AML sul PSU presenta due ordini di incoerenze con le condizioni legali e di mercato: anzitutto contraddice l'art. 5, co.1, lett. c) del GDPR sulla minimizzazione dei dati, poi ai sensi dell'art. 66, co. 3 lett. f) PSD2, il PISP non dovrebbe chiedere al PSU nessun dato oltre a quelli strettamente necessari al *payment initiation service*; stando alla lett. f) dello stesso articolo, il PISP non dovrebbe usare, avere accesso o memorizzare nessuno dato per fini diversi dalla fornitura del PIS come esplicitamente richiesto dal pagatore.

Obbligare i PISP a condurre gli obblighi AML sul PSU significa creare ostacoli alla fornitura di PIS, si finirebbe per assoggettare i PISP a obblighi più stringenti rispetto a quelli dei *card processors,* mettendo a repentaglio il principio della *fair competition* tra i PSP, postulato dalla PSD2; non permetterebbe lo sviluppo di sistemi di pagamento *user friendly*, accessibili e innovativi, come invece richiesto dalla PSD2; non assicurerebbe la neutralità tecnologica, come invece richiesto dalla PSD2.

I nuovi *market players* come I PISP e gli AISP sono già chiamati ad affrontare ostacoli come la pessima qualità delle API, documentazioni incomplete, limitati *testing facilities*, mancanza di *fallback channels*, richieste di diversi consensi del PSU, l'applicazione della SCA senza un periodo di transizione, certificati eIDAS, e molte altre. Per altro verso, è sostenibile la *risk tollerance*? Può sostenersi che una limitata quota di flussi illeciti sia un rischio tollerabile, un costo accettabile e sostenibile a fronte della necessità di non intralciare l'*open banking*[19] nelle sue delicate fasi iniziali?

Molte risposte durante le consultazioni EBA hanno considerato il livello di informazioni richiesto un fattore fortemente negativo per l'offerta di PIS e AIS. Hanno sottolineato che il livello di informazioni richieste è sproporzionato all'obiettivo di sicurezza e alla *customer protection*, rappresentando un pesante onere specialmente per i piccoli soggetti che

[19] "*Open banking is the practice of sharing financial information electronically, securely, and only under conditions that customers approve of. Application programming interfaces (APIs) allow third-parties to access financial information efficiently, thus promoting the development of new apps and services. Ideally, open banking should result in a better experience for consumers*". *Quora*, "*What is open banking?*". "*Banks have to share certain customer data and to utilize modern technology in a secured, integrated, customer-centric ecosystem, where the data can be shared by relevant parties and players with the permission of the data owner*".

potrebbero essere scoraggiati dall'entrare nel mercato anche se offrono servizi utili al cliente.

Un lato positivo di ritenere assoggettati alla disciplina aml tutti i TPP anche quando sono di piccola dimensione, è che, specialmente per i nuovi servizi come i PIS, l'elemento della fiducia del cliente ha bisogno di essere consolidato, e su questa fiducia è necessario costruire un unico campo da gioco dove gli *small services* potranno crescere progressivamente.

3. PISP e AISP sono realmente *gatekeepers*?

Argomento decisivo non sembra poter essere il possesso dei fondi. È chiaro che se alcuni soggetti obbligati AML sono nella effettiva detenzione di fondi (banche, IP, avvocati, trust, ecc.) (e il *wallet* decentralizzato?) ne esistono di altri che invece non detengono fondi ma hanno una posizione di prossimità agli *asset* tale da giustificare l'applicazione degli obblighi AML (vedasi revisori contabili).

È innegabile che i TPP si trovino in una posizione decisamente privilegiata per l'individuazione dei rischi, possono infatti costituire canali capaci di alimentare i flussi informativi indispensabili per la prevenzione del *financial crime*, in modo non dissimile ai *main actors*[20] dell'ecosistema criptovalutario, che non necessariamente detengono i beni ma ricadono nell'ambito di applicazione del d.lgs. 21 novembre 2007, 231. Tuttavia, mentre *exchanger* e *wallet provider* sono gli unici titolari di informazioni che permettono di limitare l'opacità del *beneficial owner* dell'*asset* criptovalutario e quindi hanno la concreta possibilità di atteggiarsi quali *gatekeeper*, lo stesso non può dirsi per i TPP.

Ci chiediamo, quindi, se è vero che l'unico dato transazionale di cui vengono a conoscenza è una risposta affermativa o negativa circa la disponibilità dei fondi sul conto da parte dell'ASPSP[21], i PISP hanno i dati necessari per comportarsi da *gatekeeper*? È indispensabile, infatti, capire quali sono i dati che i PISP raccolgono nel rispetto del principio di minimizzazione e se questi dati permettano un effettivo monitoraggio delle transazioni.

Gli unici dati che il PISP è legittimato a trattare sono esclusivamente quelli che permettono di svolgere la sua funzione ma è chiaro che se tra le funzioni del soggetto rientra quella anti-

[20] *Exchanger e wallet provider*, specie quando decentralizzati (cd. DAO).

[21] *Funds checking*, ovvero la modalità di controllo della disponibilità dei fondi *ex* art. 65 psd2. Si tratta della conferma della disponibilità di fondi da parte dell'ASPSP verso il PISP, a fronte di un'operazione di pagamento richiesta dal pagatore. Il dato comunicato dall'ASPSP è una semplice conferma o diniego, non potendo includere alcuna informazione di natura quantitativa o qualitativa.

riciclaggio, perché considerato soggetto obbligato, allora le informazioni che sarà legittimato a raccogliere saranno anche tutte quelle utili ai fini AML. Per concludere, nessun TPP che agisca esclusivamente quale PISP avrebbe un patrimonio informativo più vasto dell'ASPSP.

Lo stesso si può dire per gli AISP? L'aggregazione di dati transazionali e personali potrebbe favorire l'individuazione di operazioni sospette con indicatori di anomalie opportunamente adattati alla propria operatività? Potrebbero individuare *red flags* e fattori di rischio invisibili agli occhi dell'ASPSP?

Anzitutto non può la semplice detenzione di dati essere determinante nella decisione di inglobare tali prestatori nei soggetti obbligati, altrimenti tutte le società *big data analytics*, per il sol fatto di trattare grandi quantità di dati, dovrebbero essere considerati alla stessa stregua.

Tuttavia, non assoggettare i TPP ad alcun obbligo di collaborazione con le Autorità di Vigilanza e di prevenzione del *financial crime* potrebbe essere una reale perdita di opportunità, a patto che la *compliance* che si immagina per questi nuovi soggetti sia effettivamente ispirata al *risk based approach*.

Così come per le *data companies* che forniscono servizi ai soggetti vigilati (la *outsourced customer due diligence*), le esternalizzanti garantiscono l'effettivo espletamento degli obblighi. Allo stesso modo, gli ASPSP dovrebbero vigilare sulla reale capacità dei TPP ai quali hanno aperto i conti, di prevenire il crimine finanziario e quindi di garantire la stabilità del settore finanziario. D'altronde se si tratta di una transazione finalizzata a stratificare fondi illeciti, allora illecita sarà l'acquisizione, l'iniziazione e l'esecuzione. Quindi, ha senso parcellizzare l'applicazione degli obblighi AML magari omettendo tra i soggetti obbligati proprio quei nuovi operatori economici a diretto contatto con il potenziale riciclatore?

Partendo dal presupposto che il trasferimento dei fondi è elemento centrale della *payments value chain,* il ruolo di un TPP è troppo importante, destinato ad evolversi e a cambiare nel tempo. Ometterli dalla regolamentazione sarebbe una scelta irresponsabile sia per la stabilità della *payments industry* che per la tutela del PSU (*payment system user*).

In Olanda, in Belgio e in Germania, il recepimento della PSD2 e il relativo aggiornamento della disciplina AML hanno imposto di considerare gli AIS e PIS quali servizi di pagamento e i soggetti che prestano tali servizi come istituti di pagamento IP e, in quanto tali, soggetti obbligati AML. In Francia, l'AISP non è soggetto ai fini AML. Invece i PISP sono soggetti obbligati, ma il loro servizio è qualificato come *low risk service*. Interessante vedere come la Banca Centrale olandese consideri l'obbligo di monitoraggio delle transazioni AML sul PISP

utile anche ai fini della protezione dal rischio di frodi[22].

La Banca Centrale australiana ha, invece, sottolineato come la mancanza di *expertise* nella prevenzione e controllo del *financial crime* per questi nuovi *non-bank players* potrebbe rappresentare un *vulnus* di tutela della stabilità dell'intero sistema finanziario. Questi soggetti, pur essendo *tech-ready* per affrontare le sfide del *crimetech* con sofisticati sistemi automatici di monitoraggio, potrebbero deficitare dell'esperienza umana e fare eccessivo affidamento sul monitoraggio automatico. Dietro l'automazione del monitoraggio, specie quando non accompagnata da una certa quota di manualità, può nascondersi il *financial crime* e rimanere indisturbato per diverso tempo. Senza considerare che l'*open banking* rappresenta il terreno tecnologico ideale per il proliferare di *data breach* e *cyber threats,* specie del tipo *DDoS* e *man in the middle attack*.

Resta di fondamentale importanza garantire l'uniformità del campo da gioco in tutto il territorio comunitario per evitare forme distorsive della concorrenza e pericolosi fenomeni di arbitraggio normativo.

Oltre ai problemi di *legacy*, la comunità finanziaria ha ancora diverse difficoltà nel ripensare la *compliance* nell'era digitale. Pensiamo ancora in termini di scambio di documenti che verranno controllati solo in un secondo momento. La tecnologia digitale permette già la definizione di "binari protetti" tra *business partners* identificati digitalmente, lo scambio protetto di *links* (URLs)[23] di documenti commerciali per giustificare le transazioni finanziarie (fatture, bolle di consegna, certificati di origine, tutti i documenti digitali certificati). Tuttavia, in mancanza di un unico set di standard di trasmissione dati, ogni banca sviluppa la propria API, e ad eccezione di rari sforzi congiunti, si rischia che i protocolli di comunicazione si moltiplichino per tanti quanti sono i gruppi bancari. Secondo EQUENS, esistono più di 100 varianti dei messaggi SEPA ISO20022. Un numero molto più alto rispetto al numero dei *market* in UE che svela non differenti pratiche di mercato per quanti sono gli operatori, ma più modelli

[22] "*There is also a risk of fraud. Under PSD2, banks may block third parties (such as PISPs) from accessing bank accounts if they have evidence that a transaction is fraudulent or unauthorised. Banks must monitor transactions proactively and implement adequate systems that enable them to do so as part of their operational management. Although banks are subject to this obligation, PISPs must also meet the transaction monitoring requirements. For PISPs, transaction monitoring serves as a second defence mechanism in addition to Strong Customer Authentication (SCA) to prevent fraud. This means that transaction monitoring should offer protection against money laundering, terrorist financing and fraud*", DeNederlandsche Bank – Eurosysteem, 14 maggio 2018.

[23] L'url è una delle opzioni in ISO20022 standard, ma non è stata presa in considerazione per psd2.

di implementazione per ogni operatore. Tutto ciò potrebbe evitarsi partendo dall'assunto di considerare un'effettiva standardizzazione come un fattore di sviluppo importante[24]. *Internet* è un buon esempio di benefici dell'adozione di standards globali. È un fattore chiave dell'innovazione e permette agli *stakeholders* di un unico ecosistema la condivisione di tutti i tipi di risorse e la possibilità di focalizzarsi sul *core business*.

4. La *Customer Due Diligence* e l'obbligo di segnalazione operazione sospetta

Le attività di disposizione di ordini di pagamento e di informazione sui conti non prevedono atti configurabili come realizzatori o attivatori di trasferimenti, prelievi, ritiri di fondi o altre operazioni attinenti a pagamenti, così come non prevedono l'intermediazione di alcun valore monetario. In considerazione di ciò, l'indisponibilità del mezzo di pagamento ma più in generale l'assenza di intermediazione di strumenti finanziari potrebbe ridurre qualitativamente gli obblighi AML/CFT all'adeguata verifica della clientela, al monitoraggio delle operazioni di disposizione degli ordini di pagamento, alla restituzione delle informazioni aggregate, oltre ovviamente alla conservazione dei dati, delle informazioni e dei documenti derivanti dalla prestazione di tali attività[25].

Dal *Quaderno di ricerca Giuridica* della Banca d'Italia n. 87 di settembre 2019 emerge una sostanziale identità degli obblighi di identificazione del cliente[26], di acquisizione e di valutazione delle informazioni relative allo scopo e alla natura dell'operazione, quando a condurre la *customer due diligence* sia un TPP o un qualunque altro intermediario in riferimento a qualunque altra attività finanziaria continuativa. Data la possibilità di avviare transazioni da remoto, l'autorizzazione del cliente e il consenso sono gli argomenti di maggiore sensibilità in relazione all'AML/CFT. A fronte di transazioni ad alto rischio o di cd. *unusual transaction behaviour*, può essere richiesto un consenso rafforzato e coinvolgere ad esempio canali aggiuntivi di conferma quali SMS, biometrica, *soft tokens*

[24] *Global Risk Report 2020* di *World Economic Forum* sottolinea l'importanza di una "*global tech and cyber governance*", individua nella "*disruption of the multilateral system*" e la relativa proliferazione di *standard* una delle ostilità principali allo sviluppo di un unico *framework* tecnologico. Protocolli tecnologicamente divergenti e la *cyberspace fragmentation* riducono la capacità di *incident response* oltre a mettere in discussione le fondamenta dell'*open banking*, aumentare i costi transazionali e ridurre la produttività.

[25] Presidiati da sanzioni di carattere penale quanto alla violazione degli obblighi di *customer due diligence*, mentre l'omessa segnalazione operazione sospetta è incredibilmente punita con la sola sanzione amministrativa.

[26] Del *beneficial owner* e degli eventuali soggetti deputati ad operare in nome e per conto del cliente.

(ad es. *password* temporanee). Nel contesto dell'*open banking* e dell'*e-finance*, la verifica dell'identità digitale diviene elemento fondamentale per l'approvazione della transazione ma al contempo *target* ideale per furti d'identità e frodi informatiche. Alla luce dei trasferimenti *online*, del ricorso a relazioni commerciali con società *offshore,* potrebbe essere opportuno imporre processi rafforzati di compliance KYC e *Henanced Due Diligence.*

Situazione dissimile, invece, per ciò che concerne gli obblighi di controllo costante dell'andamento del rapporto contrattuale. Infatti, con riferimento al servizio di disposizione di ordini di pagamento (PISP), il monitoraggio delle disposizioni di trasferimento di mezzi di pagamento[27], dato il limitato patrimonio informativo di cui dispone, si esaurisce nell'analisi di congruità e ragionevolezza delle disposizioni impartite dal cliente rispetto alla sua posizione economico finanziaria, desumibile dalle informazioni fornite dal cliente stesso oppure ricavate attraverso fonti esterne o documenti indipendenti. La fonte informativa del PISP è limitata alle informazioni relative alle disposizioni impartite e a quelle fornite nella fase preliminare all'instaurazione del rapporto contrattuale. Invece, l'intermediario presso cui è radicato il conto, deputato all'esecuzione dell'ordine di trasferimento dei mezzi di pagamento, può vedere la disponibilità finanziaria del cliente, la situazione economico finanziaria e l'origine dei fondi sulla base anche della complessiva operatività storicizzata.

Dal presupposto che la base informativa PISP è meno ampia di quella dell'ASPSP, alla segnalazione di operazione sospetta effettuata dal PISP, potrebbe non seguire la segnalazione dell'intermediario presso il quale il conto è radicato, mentre non potrebbe legittimamente essere il contrario. Infatti, dalla più ampia base informativa di cui dispone l'intermediario di radicamento discende un sospetto maggiormente qualificato, rispetto al quale l'analisi del PISP non può che essere parziale. Stesso discorso quando l'oggetto dell'analisi si sposta dall'ammontare dell'operazione di pagamento eseguita per mezzo dell'ordine del PISP al destinatario del pagamento.

Per quanto riguarda l'AISP, l'aggregazione delle informazioni potrebbe dare la possibilità di rilevare incongruenze complessive rispetto al profilo economico e finanziario del cliente, restituendo un quadro complessivo non solo al cliente ma anche all'Autorità di Vigilanza.

5. *CDD and Risk Factors Guidelines di EBA*

Il 5 febbraio 2020, le ESA decidevano di mettere in consultazio-

[27] Che il prestatore, dietro indicazioni del titolare del conto, fornisce all'intermediario dove il conto è radicato.

ne[28] alcune *Guidelines* sui fattori di rischio e sulla *customer due diligence*[29], dedicando la *Sectoral Guideline* 18 a PISP e AISP, destinatari anche del Titolo I *General Guidelines*.

In via preliminare, EBA afferma che PISP e AISP sono da considerare "*obliged entities*" ai sensi della AMLD e sono, quindi, tenuti a adottare misure adeguate per identificare e valutare il ML/FT risk, ancorché il livello associato alle loro attività appare limitato. La premessa è che l'*open banking* e l'attività dell'AISP, in particolare, siano potenziali strumenti di coordinamento dei *mule-rings*. Il primo risultato che ottengono è quello di prendere una posizione decisa nei confronti di entrambe le categorie di *third party providers* da considerarsi soggetti obbligati ai sensi dell'art. 3, co. 2, lett. a) IVAMLD 2015/849.

Come suesposto, in sede di consultazione emersero dubbi in merito alla possibilità di non considerare gli AISP quali soggetti obbligati AML, poiché tra le informazioni che questi sono tenuti a fornire per ottenere la registrazione[30] è omessa la policy AML, in conformità con le eccezioni previste per i fornitori di AIS ai sensi dell'art. 33 PSD2.

In questo contesto, la *Guideline* 18 espone le comuni aspettative sui *compliance efforts* di AISP e PISP, con particolare riguardo agli obblighi di monitoraggio, di norma nella forma di *semplified due diligence* SDD. Le misure di *semplified due diligence* che potrebbero trovare applicazione sono l'affidamento sull'origine dei fondi come prova dell'identità del cliente ove le credenziali del conto di pagamento siano conosciute, e il conto sia detenuto in un *EEA-regulated* PSP; alla presunzione della natura e dello scopo del rapporto continuativo; alla postposizione della verifica dell'identità del cliente a data certa dopo l'instaurazione del rapporto continuativo.

L'AML/CFT *system* di PISP e AISP dovrebbe essere impostato in modo tale da rilevare attività transazionali sospette o insolite. Anche senza detenere informazioni significative sul cliente, PISP e AISP dovrebbero usare le proprie informazioni per rilevare operazioni sospette.

L'applicazione della *due diligence* in forma semplificata sembra essere suggerita da due circostanze limitative del livello di rischio di riciclaggio: i PISP, pur essendo coinvolti nella *payment chain* non eseguono la transazione di pagamento e non detengono i fondi del PSU; gli AISP non sono coinvolti nella *payment chain* e non detengono i fondi del PSU.

[28] Fino al 15 maggio del 2020.

[29] *Consultation Paper Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ("The Risk Factors Guidelines"), amending Guidelines JC/2017/37.*

[30] Ai sensi delle *Guidelines* 11 luglio 2017.

La *Guideline* 18, inoltre, fornisce 3 categorie di *additional risk factors* specifiche per PIS e AIS. Per la categoria *Customer risk factors,* si fa riferimento al cliente che trasferisce i fondi da diversi conti di pagamento verso lo stesso beneficiario per un elevato ammontare totale e senza una chiara logica economica razionale, oppure le ipotesi di sospetto di elusione di soglie[31]; al cliente che riceve o invia fondi verso Paesi ad alto rischio o verso PEP. Per la categoria *Distribution channel risk factors* si fa rinvio alle ESAs' Opinion sull'uso di soluzioni innovative per i processi di CDD[32]. L'ultima categoria, *Country or geographical risk factor,* comprende le ipotesi in cui il cliente utilizza diversi conti detenuti presso diversi ASPSP. In particolare, per i PISP rileva il cliente che avvia un pagamento verso un Paese ad alto rischio, per gli AISP, il cliente che aggrega conti in Paesi ad alto rischio. In senso contrario, il cliente che avvia una *payment transaction* verso un Paese EEA o aggrega conti detenuti in questi paesi, o che presenti comunque obblighi non meno stringenti di quelli della IV AMLD, sono da considerarsi fattori che potenzialmente possono ridurre il rischio di ML/FT.

L'esito della consultazione e l'attuale versione delle Guidelines su *CDD e risk factors*[33] considera i TPP obbligati a valutare il ML/FT risk, applicare misure di CDD adeguate e la *policy* AML, formare il personale. Il *draft* è stato approvato senza modifiche sostanziali della *Guideline* 18.

Questo senz'altro avrà un effetto diretto sulle *business lines* dei TPP che dovranno necessariamente offrire strumenti di monitoraggio delle transazioni come parte integrante del *core business*.

L'efficace segmentazione del servizio di pagamento e la valorizzazione del ruolo dei TPP non possono prescindere dall'adozione di protocolli di condivisione dei dati tra i diversi intermediari e da auspicabili forme di collaborazione tra questi al fine di evitare inutili duplicazioni degli obblighi quando già è la tecnologia a garantire l'univoca identificazione del PSU. Al contempo si auspica un intervento delle Autorità di Vigilanza volto a definire le linee per l'autovalutazione del rischio di ML/FT e le procedure di collaborazione attiva al fine di non sommergere la UIF di segnalazioni sterili, basate su analisi parziali e non integrate tra PSP e TPP.

A bank only has insight into transactions that involve its own accounts. A TPP, by contrast, has insight into sets of transactions performed through multiple

[31] Ad es. perché si rilevano entrate ricorrenti diverse dal salario o dallo stipendio, molto vicine alle CDD *threshold* e coincidenti con trasferimenti in uscita, ravvisandosi quindi la tipica attività del *money mule.*

[32] JC 2017 81.

[33] Si rinvia la consultazione su, www.eba.europa.eu.

banks, which provides it with an overall view of those banks. As a result, a TPP may be better placed than a single bank to assess whether specific transactions are unusual in the area of money laundering or terrorist financing. A TPP must notify the Financial Intelligence Unit (UIF Banca d'Italia) of any and all unusual transactions. TPPs must meet the transaction monitoring requirements.