Obblighi a carico di Istituti di pagamento e dei fornitori di servizi AISP

Nell'ambito della prestazione dei servizi di pagamento, se per i controlli di vigilanza prudenziale vige il principio dell'*home country control*, per cui, in ambito comunitario, all'attività transfrontaliera si applicano sostanzialmente le norme dello stato di appartenenza, con riguardo alla disciplina legislativa in materia di antiriciclaggio vige il principio opposto: le norme del diritto nazionale – che in Italia sono più rigorose di quelle di *"armonizzazione minima"* imposte dalla direttiva comunitaria vigente – trovano applicazione anche nei confronti degli IP esteri operanti in Italia con proprie succursali, con soggetti convenzionati, con agenti mandatari comunque denominati o in libera prestazione di servizi.

Il Testo unico bancario (TUB), al Titolo V-ter, include gli IP tra i soggetti ai quali è riservata la prestazione dei servizi di pagamento, nel cui ambito sono ricompresi anche gli istituti di moneta elettronica, le banche, gli uffici postali, nonché la Banca Centrale Europea e le banche centrali nazionali (se non agiscono in veste di autorità monetarie) e le pubbliche amministrazioni statali, regionali e locali (se non agiscono in veste di autorità pubbliche). Gli IP autorizzati in Italia sono iscritti dalla Banca d'Italia in un apposito elenco ove si indica la tipologia dei servizi autorizzati e le succursali ed agenti di cui ciascun istituto si avvale. Con l'osservanza di determinate procedure di notificazione, gli stessi possono svolgere attività transfrontaliera nell'intera area comunitaria, prestandovi servizi ammessi al mutuo riconoscimento, tramite proprie succursali ovvero senza costituirvi uno stabile insediamento, vale a dire in regime di libera prestazione di servizi (LPS). Corrispondentemente, nel rispetto di analoghe procedure, gli IP degli altri Stati comunitari possono operare in Italia tramite succursali o in LPS.

Al fine di meglio comprendere la corretta applicazione della disciplina antiriciclaggio alla prestazione dei servizi di pagamento appare opportuno innanzitutto tracciare un quadro generale delle attività che gli IP possono essere autorizzati ad esercitare e delle diverse modalità di svolgimento delle stesse. In particolare, la conoscenza delle modalità di contatto con gli utenti dei servizi costituisce un necessario presupposto per stabilire su quali soggetti ricadano le diverse fasi in cui gli adempimenti

antiriciclaggio possono scomporsi in concreto.

Tra le peculiarità operative degli Istituti che assumono rilevanza ai fini dell'antiriciclaggio si segnalano: la presenza di operazioni di pagamento complesse, il tradizionale ricorso a soggetti esterni, ai quali è demandato il contatto diretto con il cliente (intermediari-*partner* convenzionati, reti di agenti e altri soggetti convenzionati) e la prestazione in tempo reale di molti servizi.[1] Si tratta di caratteristiche che, in particolare, possono rendere difficoltosa l'esecuzione dell'adeguata verifica del cliente, a tal punto da rendere necessaria l'individuazione di idonee procedure operative nonché seguire e sfruttare al meglio l'evoluzione tecnologica.

La normativa antiriciclaggio non intende tuttavia interferire sull'autonomia delle scelte organizzative dei destinatari degli obblighi, anche se alcuni requisiti organizzativi funzionali alla prevenzione del riciclaggio sono obbligatori.

In particolare occorre:

- istituire una funzione antiriciclaggio incaricata di sovrintendere all'attività e nominarne il responsabile; è ammessa l'esternalizzazione e l'attribuzione della responsabilità della funzione a un amministratore privo di deleghe operative (o all'amministratore unico);
- disporre di un'unità di revisione interna e, ove non prevista, assegnare i relativi compiti a un amministratore privo di deleghe operative (o all'amministratore unico);
- formalizzare la responsabilità per la segnalazione delle operazioni sospette;
- definire chiaramente ruoli, compiti e responsabilità nonché stabilire procedure intese a garantire l'osservanza degli obblighi antiriciclaggio;
- prevedere e attuare programmi organici, di addestramento e formazione del personale dipendente (specie se a più diretto contatto con la clientela) e dei collaboratori esterni legati da vincolo

[1] Per un esaustivo quadro della disciplina degli Istituti di pagamento si veda il titolo V-*ter* del Testo Unico Bancario.

contrattuale (strumento formale: stesura del programma).

- responsabilizzare e controllare il personale dipendente e i collaboratori esterni (strumento: calendarizzare controlli ispettivi periodici oltre a quelli senza preavviso).

È importante inoltre segnalare che la funzione antiriciclaggio all'interno degli Istituti di pagamento deve godere di assoluta indipendenza ed essere dotata di risorse qualitativamente e quantitativamente adeguate, deve verificare nel continuo che le procedure aziendali siano coerenti e con l'obiettivo di prevenire e contrastare la violazione della normativa esterna (leggi e norme regolamentari) e interna all'Istituto.

Come noto, invero, l'attività di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo si fonda su tre pilastri: la conoscenza del cliente (attuata tramite la c.d. "adeguata verifica"); la tracciabilità delle operazioni (attuata tramite la registrazione e la conservazione dei relativi dati, utilizzando l'Archivio Unico Informatico o le altre modalità consentite); la segnalazione delle operazioni sospette (che costituisce il fine ultimo della complessiva attività di prevenzione).

L'adeguata verifica si colloca pertanto nell'ambito dei capisaldi della prevenzione nelle due diramazioni di profilatura in classi di rischio e monitoraggio costante. Il criterio dell'*approccio basato sul rischio* - espressione del principio di proporzionalità - dovrebbe teoricamente consentire di commisurare discrezionalmente l'adempimento degli obblighi all'effettivo rischio di riciclaggio desumibile dalla natura della controparte, dal tipo di attività esercitata e dall'area geografica di riferimento. Il principio incontra, peraltro, significative limitazioni nelle numerose disposizioni tassative previste dalla normativa.[2] In base a tale principio, l'Istituto può proporzionare l'adempimento degli obblighi alle proprie dimensioni e all'entità e tipologia dei rischi cui è concretamente esposta l'attività svolta. Questa operazione presuppone una puntuale "*mappatura*" dei rischi in concreto verificabili, la definizione di un modello antiriciclaggio aziendale di mitigazione dei rischi e un periodico esercizio di autovalutazione della funzionalità del modello,

[2] Per un ulteriore approfondimento sul tema si veda: G. CASTALDI, N. GOMES in *Istituti di pagamento e Imel adempimenti antiriciclaggio*, aprile 2017, Associazione Italiana Prestatori di Servizi di Pagamento.

delle vulnerabilità e dei possibili interventi migliorativi.

Si ricorda inoltre che gli Istituti di pagamento e di moneta elettronica, al pari degli altri prestatori di servizi di pagamento, possono ampliare la propria capacità operativa mediante la definizione di accordi di promozione e conclusione di contratti. È ammessa infatti la delega a terzi di numerose fasi dell'adeguata verifica, salvo sempre il monitoraggio costante, attraverso "collaboratori esterni" ai quali è possibile demandare l'identificazione dei clienti e l'acquisizione dei relativi documenti. Tra tali collaboratori sono ricompresi (per ciò che concerne la normativa e i provvedimenti attualmente vigenti) sia gli agenti ex. art. 128-quater del T.U.B. sia un'ulteriore e non ben definita categoria di *"soggetti convenzionati"* che viene individuata nel nuovo decreto AML. Tuttavia, se da un lato l'utilizzo di una rete di agenti o di altri collaboratori esterni consente di allargare la capillarità e incrementare la tempestività dell'offerta dei servizi, dall'altro comporta una serie di rischi aggiuntivi, ivi compreso quello di coinvolgimento in vicende di riciclaggio o finanziamento del terrorismo. Pertanto, anche l'utilizzo e la distribuzione di strumenti di pagamento elettronici, che di per sé rappresenta un'attività a basso rischio di riciclaggio, richiede misure rafforzate di adeguata verifica nel momento in cui i rapporti o le operazioni coinvolgano collaboratori esterni, paesi terzi ad alto rischio o l'ampia categoria delle PEP.

L'introduzione della PSD2 ha in aggiunta importato una profonda rivoluzione all'interno del settore dei servizi di pagamento riversando effetti non poco rilevanti sulla disciplina di *anti-money loundering*. Nell'ottica di un marcato aumento della concorrenza, infatti, la normativa ha introdotto nuovi soggetti idonei alla prestazione di servizi di pagamento e, per ciò che concerne tale breve contributo, ha configurato nei conti di pagamento delle *facilities* strumentali alla fornitura all'utente finale di tali nuovi servizi on-line.

A tal proposito, l'*Account Information Service Provider* (AISP) – quale soggetto disciplinato dalla PSD2 – offre all'utente finale il quadro aggregato della propria situazione finanziaria, delle entrate e delle uscite di fondi, senza limitazioni o ostacoli derivanti dal fatto di detenere conti di pagamento presso uno o più prestatori di servizi di radicamento di conto. Con detto servizio sarà possibile imporre a questi ultimi, noti con l'acronimo ASPSP (*Accounting Service Payment Service Provider*), di consentire l'accesso alle terze parti per reperire informazioni sul conto. Il perimetro di operatività è pertanto strettamente connesso

ai servizi di pagamento, alla disponibilità di conti on line e alla necessaria autorizzazione da parte del cliente finale.[3] Si tratta, in sostanza, di condividere un patrimonio di dati e informazioni che sono stati in passato considerati in dotazione esclusiva della banca o dell'istituto di pagamento presso cui è detenuto il conto. La PSD2 focalizza l'attenzione intorno a tali Third Party Provider (TPP) che rappresentano quindi i nuovi attori disposti a muoversi lungo il palcoscenico dei servizi di pagamento.

L'ingresso dei nuovi operatori ha consentito di ricondurre sotto la generica definizione di PSP (Payment Service Provider) tanto gli istituti di pagamento tradizionali quanto gli AISP e, più in generale, i TPP, contribuendo positivamente al problema dell'inquadramento giuridico nella disciplina di prevenzione del riciclaggio e contrasto al terrorismo. Invero, essendo espressamente equiparati dalla PSD2 ad Istituti di pagamento e IMEL nonché, i loro servizi, espressamente annoverati dall'art. 1, comma 2, lettera h) septies 1 del T.U.B, tali nuovi soggetti rientrano a pieno titolo nel *genus* dei prestatori di servizi di pagamento e, come tali, necessariamente obbligati al rispetto della normativa prevista dal d.lgs. 231 del 2007. È stato inoltre più volte specificato che i *payment service providers*, pur non essendo espressamente menzionati tra i soggetti obbligati al rispetto degli obblighi di antiriciclaggio, rientrino nella più ampia categoria delle *financial institutions* che comprendono, tra le varie, le attività risultanti dall'allegato I della CRD 2013/36, nel quale (al punto 4) figurano i *payment services provider* così come definiti dalla PSD. Considerata dunque l'introduzione e la piena riconducibilità da parte della PSD2 dei nuovi servizi di AISP e PISP al *genus* dei PSP, è evidente che tali nuovi attori debbano essere considerati soggetti inevitabilmente obbligati ai fini di antiriciclaggio.[4]

L'estensione delle norme e dei presidi di AML appare necessaria in quanto i *Third Party Provider* operano in un contesto tecnologico incredibilmente fertile per il proliferare di *cyber threats*, al punto da imporre una revisione periodica del *legal framework* finalizzata alla ricerca e alla neutralizzazione delle

[3] V. *A. Burchi, S. Mezzacapo, P. Musile Tanzi, V. Troiano,* Financial Data Aggregation e Account Information Services, Questioni regolamentari e profili di business, Quaderno FinTech n. 4, marzo 2019, Consob.

[4] V. file:///C:/Users/Lenovo/Desktop/SIWP-No-2015-001-AML-Risks-of-the-Third-Party-Payment-Providers_FINAL.pdf

nuove minacce.

Nello specifico, in tema di *risk assessment*, già la IV direttiva AML ha richiesto agli Stati membri di assicurare che i soggetti obbligati, inclusi i TPP, procedano agli *step* necessari ad identificare e valutare il rischio di riciclaggio e finanziamento del terrorismo prendendo in considerazione i fattori di rischio indicati dalla normativa. Gli *step* richiesti dipenderanno dalla natura e dalle dimensioni dei soggetti obbligati e le valutazioni del rischio richiederanno di essere documentate e rese disponibili alle autorità di vigilanza.

Se però, da una parte, l'estensione della normativa può comportare una riduzione sostanziosa del rischio di riciclaggio, dall'altra rischia di aggravare e, conseguentemente, danneggiare le procedure e l'operatività dei nuovi soggetti autorizzati. A tal proposito, nell'ambito degli adempimenti di adeguata verifica della clientela o, come altrimenti definita, di *Customer due diligence*, non sempre risulta facile chiarire le condizioni secondo cui possono essere adottati controlli e verifiche semplificati. Infatti, in qualità di soggetti obbligati, i TPP devono prendere in considerazione le misure di *Customer due diligence* adottando, nei casi di incertezza, comportamenti tendenzialmente conformi alla normativa più stringente. È chiaro tuttavia che un'eccessiva regolamentazione non può che contrastare l'impeto innovativo apportato dalla PSD2, essendo innegabile, sotto questo aspetto, che gli obblighi di AML siano idonei ad erigere barriere all'ingresso del mercato per i TPP e i loro *business model*. Imporre misure di *Customer due diligence* anche ai TPP significa essenzialmente raddoppiare la procedura di adeguata verifica già prevista per i prestatori di servizi di pagamento di radicamento di conto (ASPSP), rendendo un obbligo di questo tipo niente più che un ostacolo insormontabile alla piena efficacia della nuova normativa inerente i servizi di pagamento.

Nondimeno, la normativa europea in tema di antiriciclaggio prende in considerazione queste situazioni reputando appropriato permettere ai clienti, la cui identificazione è stata portata a termine altrove, di essere "presentati" ai nuovi soggetti obbligati ed evitare così di ripetere le procedure di adeguata verifica che comporterebbero inefficienza e ritardi nello sviluppo dei modelli di business. Tale sistema circoscriverà la responsabilità finale per la *Customer due diligence* in capo all'Istituto di pagamento o alla banca alla quale il cliente è stato "introdotto" nel caso in cui le operazioni di pagamento coinvolgano un AISP o un PISP.