Luglio 2020

PSD2: gli ostacoli all'operatività dei TPP alla luce dei chiarimenti dell'EBA

Antonio Di Giorgio e Bianca Mascagni, Annunziata & Conso

1. Introduzione

Il 4 giugno scorso, la European Banking Authority ("**EBA**") ha pubblicato una *opinion* volta a fornire chiarimenti in merito ai possibili ostacoli che i prestatori di servizi di pagamento di radicamento del conto, quali ad esempio banche, istituti di credito e istituti di pagamenti (complessivamente, "**ASPSP**") pongono all'offerta dei servizi informativi e di pagamento offerti dalle c.d. "terze parti" ("**Third Party Providers**" o "**TPP**") abilitate e dà indicazioni sulla corretta applicazione della regolamentazione tecnica di degli orientamenti EBA di attuazione delle disposizioni della PSD2 in materia di accesso ai conti.

Tale parere è stato redatto alla luce dei diversi quesiti ricevuti dagli operatori del mercato e sulla base dei modelli operativi adottati sino ad ora nel settore sulla base delle disposizioni della seconda direttiva sui servizi di pagamento[1] ("**PSD2**" o "**Direttiva**") e alle norme tecniche di regolamentazione sulla "*strong customer authentication*" ("**SCA**") e sulla comunicazione comune e sicura ("**CSC**") emanati in attuazione della Direttiva[2] ("**RTS**").

Come è noto, uno dei profili di innovazione della PSD2 ha, difatti, riguardato l'introduzione di due nuovi servizi e di due nuovi prestatori di sevizi di pagamento abilitati a prestare (esclusivamente) tali servizi, ovvero i TPP. I due servizi di nuova introduzione e i nuovi prestatori sono (i) il servizio di informazioni sui conti fornito dai c.d. AISP[3], e (ii) il servizio di disposizione di ordine di pagamento fornito dai c.d. PISP[4]. La Direttiva consente agli utenti dei servizi di pagamento di utilizzare tali nuovi servizi, e impone agli ASPSP, presso i quali gli utenti detengono i propri conti di pagamento, di

[1] Direttiva (UE) 2015/2366.
[2] Regolamento Delegato (UE) 2018/389.
[3] Il servizio di accesso ai conti permette agli AISP di accedere ai conti di pagamento degli utenti per fornire servizi informativi aggregati sui conti correnti dello stesso, anche se intrattenuti con istituti finanziari diversi.
[4] Il servizio di disposizione di ordini di pagamento permette ai PISP di accedere ai conti di pagamento degli utenti per fornire servizi dispositivi (i.e. invio di bonifici bancari) richiesti e autorizzati dagli stessi.

stabilire apposite interfacce di accesso attraverso le quali i TPP (*i.e.* PISP o AISP) possono, in sicurezza, accedere ai conti di pagamento dei clienti[5].

In tale ambito, l'articolo 32, paragrafo 3, degli RTS richiede agli ASPSP, che hanno implementato un'interfaccia dedicata[6], di garantire che tale interfaccia non crei ostacoli alla fornitura dei servizi da parte di PISP e AISP.

Il parere dell'EBA, oggetto del presente contributo, interviene proprio per meglio chiarire il menzionato articolo degli RTS e per rispondere alle richieste avanzate dagli operatori in merito al considerare o meno determinate pratiche di mercato come ostacoli alla fornitura dei servizi di pagamento. In particolare, il parere analizza una serie di pratiche individuate dall'Autorità sul mercato, chiarendo per ciascuna quali comportamenti degli ASPSP possano essere considerati in linea con lo spirito della Direttiva e degli RTS, e quali, al contrario, debbano essere censurati.

Oltre a rispondere e a chiarire i quesiti posti dal mercato, l'opinion dell'EBA si rivolge direttamente alle autorità competenti degli Stati Membri, invitandole a prestare particolare attenzione, nell'ambito dei controlli svolti, alla tematica ivi analizzata e ad adottare le azioni necessarie per garantire la conformità delle interfacce offerte dagli ASPSP al dettato normativo e, qualora vengano individuati ostacoli, per garantire che gli ASPSP interessati li rimuovano nel più breve tempo possibile. EBA controllerà il modo in cui l'autorità competente di ciascun Stato Membro terrà in considerazione i chiarimenti forniti, adottando le azioni necessarie qualora individui delle incongruenze nell'applicazione delle disposizioni rilevanti.

Alla luce delle considerazioni dell'EBA, il presente contributo rappresenta un'analisi delle "pratiche del mercato" considerate di ostacolo alla prestazione dei servizi di PISP e AISP, suddivise per aree di rilevanza.

2. Il reindirizzamento: un ostacolo all'operatività dei PISP?

In primo luogo, EBA analizza, in via generale, la pratica del reindirizzamento obbligatorio, già affrontata dall'Autorità[7] in passato, facendo luce su quali siano i casi in

[5] Ai sensi dell'art. 31 degli RTS, i prestatori di servizi di pagamento di radicamento del conto, gli ASPSP, possono scegliere, nella predisposizione delle interfacce di accesso alle terze parti, di creare delle interfacce dedicate, ovvero se consentire ai TPP di servirsi delle interfacce già predisposte dall'ASPSP ed utilizzate per l'autenticazione e la comunicazione con gli utenti dei servizi di pagamento del prestatore di servizi di pagamento di radicamento del conto stesso.

[6] In tal caso si fa riferimento esclusivamente a quegli ASPSP che, ai sensi del menzionato art. 31 degli RTS., hanno deciso di avvalersi della prima opzione ivi indicata e, pertanto hanno provveduto alla predisposizione di un'interfaccia dedicata esclusivamente alla comunicazione con i TPP, senza permettere a questi ultimi di avvalersi delle interfacce già predisposte dall'ASPSP ed utilizzate per l'autenticazione e la comunicazione con i propri utenti.

[7] Si veda il parere dell'EBA sull'attuazione dell'RTS (EBA-Op-2018-04) e gli orientamenti dell'EBA sull'esenzione dal meccanismo di emergenza ai sensi dell'articolo 33, paragrafo 6, del RTS (EBA/GL/2018/07).

cui tale pratica possa essere considerata di ostacolo all'attività dei TPP, e in particolare dei PISP. Le questioni sollevate dal mercato in questo contesto si riferiscono in particolare allo scenario in cui il reindirizzamento sia l'unico metodo attraverso il quale gli utenti possano autenticarsi presso il proprio ASPSP, e di conseguenza, sia un passaggio necessario anche per l'utilizzo dei servizi forniti dai TPP.

A parere di EBA, la censura della pratica deve limitarsi ai soli casi in cui il reindirizzamento venga implementato dal prestatore di radicamento del conto (*i.e.* ASPSP) in modo da creare inutili complicazioni nella c.d. *user experience* dell'utente, rendendo l'accesso ai servizi forniti dai TPP più difficoltoso e macchinoso rispetto alla normale navigazione ed esecuzione di pagamenti attraverso i canali propri dell'ASPSP, ad esempio attraverso la richiesta di informazioni ulteriori rispetto a quelle richieste per l'accesso diretto o all'inizializzazione di un pagamento attraverso il proprio conto di pagamento.

Sempre in tema di reindirizzamento obbligatorio, gli operatori del settore hanno riscontrato che tale pratica rappresenta un ostacolo per i TPP, in particolare con riferimento ai pagamenti inizializzati dagli utenti presso i c.d. *point-of-sale*: la possibilità di autenticarsi attraverso l'interfaccia dell'ASPSP richiede che il pagamento avvenga attraverso l'utilizzo di un *web browser* o di una *mobile app,* che reindirizzi per l'appunto l'utente sul sito *web* o sull'applicazione del proprio istituto di credito, limitando, così, la capacità dei TPP di progettare nuovi modi in cui i clienti possono avviare i propri pagamenti. In tal modo i PISP possono competere con gli emittenti di carte di pagamento, solo con riferimento ai pagamenti *online*. L'operatività di un PISP presso un punto di vendita fisico richiederebbe necessariamente la predisposizione da parte degli ASPSP di meccanismi di autenticazione disaccoppiati o incorporati nello strumento di pagamento fornito agi utenti direttamente dai PISP (*i.e.* una *mobile app* creata dal PISP che permetta i pagamenti presso rivenditori convenzionati).

A tal proposito, EBA chiarisce che né la PSD2, né gli RTS, obbligano gli ASPSP ad implementare sistemi di autenticazione specifici volti a consentire pagamenti attraverso l'utilizzo dei servizi forniti dai PISP, predisponendo procedure *ad hoc* ulteriori rispetto a quelle create per i pagamenti eseguiti presso il prestatore di radicamento del conto. Ai sensi della normativa applicabile, un PISP ha il solo diritto di avviare le stesse transazioni che l'ASPSP offre ai propri utenti, con la conseguenza che se un ASPSP dovesse offrire ai propri clienti la possibilità di effettuare pagamenti istantanei presso specifici *point-of-sales*, l'ASPSP dovrebbe anche consentire ai propri clienti di avviare pagamenti istantanei, entro gli stessi limiti di importo, presso specifici *point-of-sales* utilizzando i servizi forniti dai PISP.

3. *Strong customer authentication* e selezione del conto per le transazioni effettuate dai PISP

Ai sensi dell'art. 97, paragrafo 1, lett. a), b) e c) della PSD2[8], un utente che vuole disporre un bonifico attraverso l'utilizzo dell'*internet banking* o della *mobile app* del proprio istituto di credito è tenuto ad immettere le proprie credenziali di autenticazione due volte: la prima per accedere all'interfaccia operativo scelto, la seconda per disporre l'ordine di bonifico. Laddove lo stesso utente decida di effettuare un pagamento avvalendosi del servizio di disposizione di ordine di pagamento fornito da un PISP, se il PISP trasmette all'ASPSP tutte le informazioni necessarie per avviare il pagamento - compreso il numero di conto o l'IBAN del conto da addebitare - tale duplicazione, a parere di EBA, risulta un ostacolo all'operatività della terza parte. Ciò, a meno che l'ASPSP non sia in grado di dimostrare che tale richiesta è dovuta a ragioni di sicurezza debitamente giustificate e dimostrabili (i.e. il sospetto di frode per una particolare transazione).

Caso diverso quello in cui le informazioni relative al conto di pagamento da addebitare non vengiano trasmesse all'ASPSP dal PISP, al momento della richiesta di avvio del pagamento. Nel caso in cui, quindi, sia lo stesso utente a dover selezionare presso il proprio istituto di credito il conto da addebitare nell'ambito di una transazione effettuata avvalendosi dell'utilizzo di un PISP, la richiesta di doppia autenticazione - una per accedere all'elenco dei conti di pagamento e una seconda per autenticare il pagamento - non costituisce un ostacolo censurabile.

In tal caso, ci si trova però di fronte ad una differente problematica sollevata dal mercato che riguarda, nello specifico, la pratica secondo cui, per l'utilizzo dei servizi forniti dai TPP, all'utente venga richiesto di inserire manualmente il proprio IBAN. L'EBA riconosce che tale pratica costituisce un impedimento censurabile nel caso di TPP autorizzati per la prestazione del servizio di accesso ai conti e debitamente accordati, a cura dell'utente, all'accesso delle informazioni relative a tutti i conti dallo stesso detenuti presso uno o più istituti di credito. In tal caso, il TPP può inviare all'ASPSP una richiesta separata per l'accesso al conto o, a seconda dei casi, per l'avvio del pagamento, con i relativi dettagli del conto.

Diverso è il caso dei PISP autorizzati esclusivamente al servizio di disposizione di ordini di pagamento: ai sensi della PSD2, un PISP non è autorizzato ad accedere all'elenco di tutti i conti di pagamento dell'utente[9]. Tuttavia, se il PISP non comunica all'ASPSP l'IBAN del conto da addebitare e l'utente si trova a doverlo selezionare manualmente

[8] L'art. 97, paragrafo 1 della PSD2 dispone che "*Gli Stati membri provvedono a che un prestatore di servizi di pagamento applichi l'autenticazione forte del cliente quando il pagatore:*
a) accede al suo conto di pagamento on line;
b) dispone un'operazione di pagamento elettronico;
c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi."

[9] Tali informazioni vanno oltre l'ambito dei dati cui i PISP hanno diritto ad accedere ai sensi dell'articolo 66, paragrafo 4, lettera b), della PSD2 e dell'articolo 36, paragrafo 1, lettera b), degli RTS.

dall'interfaccia del proprio istituto di credito, l'ASPSP è obbligatoriamente tenuto a comunicare al PISP tale informazione.

4. Frequenza della richiesta di autenticazione nell'ambito del servizio di accesso ai conti

Come già ricordato nel precedente paragrafo, la PSD2 richiede l'applicazione delle procedure di *strong cutomer authentication* ogni volta che un utente decida di accedere al proprio conto o ai propri conti di pagamento *online*, sia direttamente attraverso le interfacce messe a disposizione dagli istituti di credito di radicamento del conto, sia tramite un AISP. L'art. 10 degli RTS prevede un'esenzione dall'obbligo di applicare la SCA per ogni accesso, qualora l'utente si avvalga di un AISP e attraverso l'interfaccia messa a disposizione di quest'ultimo possa visualizzare solo una serie limitata di dati (*i.e.* solo il saldo e/o le operazioni di pagamento eseguite negli ultimi 90 giorni). Tuttavia, anche in virtù della menzionata esenzione, la normativa richiede l'applicazione della *strong customer authentication* almeno ogni 90 giorni, al fine di permettere all'utente di rinnovare la propria scelta di avvalersi del servizio di accesso ai conti e permettere agli AISP di visualizzare tali informazioni.

A tal riguardo, alcuni operatori del mercato hanno espresso la preoccupazione che l'obbligo di ri-autenticazione da parte degli utenti ogni 90 giorni, possa avere un impatto negativo sul servizio promosso dagli AISP, in particolare in quei casi di utilizzo da parte di utenti detentori di più conti di pagamento presso diversi istituti di credito. In tal caso, difatti, l'utente è tenuto a ad autenticarsi presso ciascun ASPSP affinché l'AISP possa continuare ad avere accesso ai dati di tutti conto selezionati.

A parere dell'EBA, l'obbligo di ri-autenticazione ogni 90 giorni, rappresenta un adeguato equilibrio tra gli obiettivi di agevolazione della concorrenza perseguiti dalla PSD2 e la facilità d'utilizzo dei servizi promossi dai TPP da parte dei consumatori, da un lato, e di garanzia dei necessari presidi di la sicurezza, dall'altro. Il requisito dei 90 giorni non è quindi di per sé un ostacolo. Pertanto, al fine di ridurre al minimo eventuali complicazioni relative alla *user experience* degli utenti rispetto all'utilizzo delle applicazioni fornite dagli AISP, EBA, nell'ambito del parere oggetto di commento, invita le autorità competenti di ciascun Stato Membro ad incoraggiare i prestatori di servizi di pagamento di radicamento del conto ad avvalersi dell'esenzione di cui all'articolo 10, permettendo l'accesso continuo da parte degli AISP per un periodo di 90 giorni, prima di richiedere nuovamente l'autenticazione da parte dell'utente.

Inoltre, EBA chiarisce che l'obbligo, e la conseguente responsabilità, di provvedere all'esecuzione da parte degli utenti delle procedure di autenticazione forte, spettano agli ASPSP e non alle terze parti (TPP), che possono però essere delegate a tale compito attraverso appositi accordi di esternalizzazione conformi alla normativa applicabile[10].

[10] Linee guida dell'EBA sugli accordi di esternalizzazione (EBA/GL/2019/02).

5. Controlli aggiuntivi sul consenso e registrazioni supplementari

Da ultimo, nel parere oggetto di commento, EBA fornisce un chiarimento in merito ad una delle questioni più dibattute sin dal momento della pubblicazione della PSD2 sulle novità dalla stessa introdotte. Gli istituti di credito, trovatisi improvvisamente a doversi relazionarsi con i nuovi servizi di pagamento e con i *third parties providers*, si sono chiesti se, per motivi di tutela della propria clientela, fosse possibile proporre ai propri utenti un consenso iniziale e generale, una sorta di "Opt-in", rispetto all'utilizzo dei servizi promossi dalle terze parti, sulla base del quale rifiutare a priori le richieste di interazione dei TPP.

L'art. 32, paragrafo 3, degli RTS[11] menziona esplicitamente come potenziale ostacolo all'operatività dei TPP, la richiesta di "*ulteriori verifiche del consenso dato dagli utenti dei servizi di pagamento ai PISP e agli AISP*". L'EBA ha già in precedenza[12] chiarito che l'obbligo in capo ai TPP è limitato a garantire di aver ottenuto il consenso esplicito da parte degli utenti, in conformità, rispettivamente, dell'art. 66, paragrafo 2 e, dell'art. 67, paragrafo 2, lettera a), della PSD2. A tal fine, gli ASPSP non devono, e non possono, verificare il consenso dato dagli utenti ai PISP e agli AISP: pertanto, chiarisce EBA, anche un consenso generale richiesto *ex ante* dagli ASPSP per consentire agli utenti di avvalersi dei servizi di AISP e PISP deve considerarsi un ostacolo ai sensi dell'art. 32, paragrafo 3, degli RTS.

EBA sottolinea inoltre che, come già indicato al considerando 69 della PSD2, i termini e le condizioni contrattuali proposti alla propria clientela dagli ASPSP "*non dovrebbero contenere disposizioni che rendano più difficile, in qualsiasi modo, l'utilizzo dei servizi di pagamento di altri prestatori di servizi di pagamento autorizzati o registrati ai sensi della Direttiva*".

È fatta salva la possibilità per ciascun utente di richiedere al proprio prestatore di servizi di pagamento di radicamento del conto di negare l'accesso al proprio, o ai propri conti di pagamento, a uno o più specifici TPP.

---

[11] L'art. 32, paragrafo 3, degli RTS dispone che "*I prestatori di servizi di pagamento di radicamento del conto che abbiano predisposto un'interfaccia dedicata provvedono affinché tale interfaccia non crei ostacoli alla prestazione dei servizi di disposizione di ordine di pagamento e di informazione sui conti. Detti ostacoli possono consistere, tra l'altro, nell'impedire l'utilizzo da parte dei prestatori di servizi di pagamento di cui all'articolo 30, paragrafo 1, delle credenziali rilasciate dai prestatori di servizi di pagamento di radicamento del conto ai loro clienti, nell'imporre il reindirizzamento verso l'autenticazione o altre funzioni del prestatore di servizi di pagamento di radicamento del conto, nel richiedere autorizzazioni e registrazioni aggiuntive rispetto a quelle previste dagli articoli 11, 14 e 15 della direttiva (UE) 2015/2366 o nel richiedere ulteriori verifiche del consenso dato dagli utenti dei servizi di pa*gamento ai prestatori di servizi di disposizione di ordine di pagamento e di servizi di informazione sui conti".

[12] Si veda il parere dell'EBA sull'attuazione dell'RTS (EBA-Op-2018-04) e gli orientamenti dell'EBA sull'esenzione dal meccanismo di emergenza ai sensi dell'articolo 33, paragrafo 6, del RTS (EBA/GL/2018/07).

Le medesime considerazioni vengono richiamate da EBA con riferimento alle pratiche poste in essere dai prestatori di servizi di pagamento di radicamento del conto con riferimento alla richiesta, ai TPP, di esperire procedure di registrazione supplementari per l'accesso all'interfaccia dell'ASPSP e alle informazioni dei conti di pagamento degli utenti di quest'ultimo.

Anche in tal caso la normativa sembra essere chiara: l'art. 32, paragrafo 3, degli RTS menziona espressamente come potenziale ostacolo all'operatività dei TPP "*la richiesta di autorizzazioni e registrazioni supplementari oltre a quelle previste dagli articoli 11, 14 e 15 della PSD2*", e pertanto il conseguimento delle necessarie autorizzazioni ed iscrizioni negli appositi registri da parte delle autorità competenti.

Ciò nonostante, EBA riconosce che alcune procedure di registrazione potrebbero essere tecnicamente necessarie per consentire una comunicazione sicura tra TPP e ASPSP, senza che esse costituiscano necessariamente un ostacolo. Tuttavia, le registrazioni supplementari richieste dall'ASPSP affinché i TPP possano accedere ai conti di pagamento degli utenti, o all'interfaccia degli ASPSP, rispetto a quanto tecnicamente necessario per garantire un accesso sicuro ai conti di pagamento, devono ritenersi un impedimento censurabile.

6. Considerazioni conclusive

Le questioni e i quesiti sollevati dal mercato che EBA si è trovata ad affrontare e (tentare di) risolvere nell'ambito dell'*opinion* oggetto di commento, testimoniano la portata innovativa della PSD2, che non si ferma all'introduzione dei due nuovi servizi di pagamento, ma riguarda, più in generale, il cambiamento architetturale e tecnologico introdotto dalle disposizioni degli RTS in materia di API, i rapporti tra banche e soggetti non bancari e le misure di sicurezza a tutela del cliente; tutte circostanze che hanno ridisegnato il *framework* dei servizi di pagamento europei. Il termine utilizzato per riferirsi a tale rivoluzione bancaria digitale è *"open banking"*, fenomeno attraverso il quale la prestazione dei servizi di pagamento e la gestione dei conti non è più prerogativa di banche e istituzioni finanziarie, ma permette ad altri nuovi *player* di mercato di accaparrarsi parte della clientela facendo leva sull'innovazione tecnologica (i c.d. operatori del *fintech*).

L'utente finale beneficia così di un numero maggiore di servizi, testimoni dell'evoluzione dei bisogni e delle esigenze della clientela, e di una maggiore integrazione dei servizi bancari nell'ecosistema digitale. È necessario però assicurarsi, che tale apertura del settore dei pagamenti, da un lato, sia realizzata in concreto e, dall'altro, non porti una diminuzione dei presidi posti a tutela della trasparenza e della sicurezza dei pagamenti della clientela.

É a questo che mira l'intervento di EBA. E ciò non può che realizzarsi attraverso il costante sforzo delle autorità competenti dei singoli Stati Membri, prime destinatarie dell'*opinion* dell'EBA, ma anche degli operatori più grandi del settore (*i.e.* gli istituti di

credito), sempre più consapevoli di operare in un mercato in crescente concorrenza e primi "vigilanti" delle minime misure di sicurezza dei pagamenti all'interno dello stesso.

La garanzia dei presidi a tutela della trasparenza e della sicurezza dei pagamenti della clientela, da sola, forse, non è sufficiente a rassicurare i consumatori in merito all'utilizzo dei nuovi servizi promossi dai TPP e dalla Direttiva. Il mercato dei servizi di pagamento digitali, difatti, sconta ancora la forte diffidenza dei consumatori che non conoscono gli strumenti di pagamento elettronici utilizzabili per gli acquisti *online*, le modalità di utilizzo e gli operatori che li offrono. A tale fine, come detto, rilevante può essere l'impegno da parte delle autorità di vigilanza dei singoli Stati Membri, non soltanto nell'ottica di controllo e vigilanza della tutela dei consumatori, ma altresì nell'attività di sensibilizzazione ai nuovi strumenti di pagamento digitale e alle caratteristiche di sicurezza dagli stessi garantite.

A riguardo, si segnala un documento di recente pubblicato dalla Banca d'Italia, che si rivolge, per l'appunto, "*a tutti coloro che comprano beni o servizi online e vogliono capire meglio come funzionano i pagamenti sul web*" e sono interessati a documentarsi in merito ai vantaggi, ai rischi e alle regole di funzionamento dei pagamenti digitali[13]. Il documento propone una spiegazione semplice e fruibile dei servizi offerti da PISP e AISP e permette al lettore (o meglio il consumatore, fruitore del servizio) di acquisire gli strumenti per orientarsi con consapevolezza tra i nuovi servizi offerti dal mercato dei pagamenti.

[13] Si veda "I pagamenti nel commercio elettronico: una mappa per orientarsi", documento pubblicato dalla Banca d'Italia in data 15 giugno 2020.