«Il diritto dell'economia» issn 1123-3036, anno 69, n. 110 (1 2023) pp. 211-250

Articoli e saggi

I *Third Party Providers* e l'accesso ai conti bancari nella disciplina giuridica dei servizi di pagamento: problemi e prospettive

Roberta lo Conte

Sommario: 1. Premessa. – 2. I servizi sottoposti a riserva introdotti dalla Direttiva UE/2015/2366. – 3. La disciplina giuridica europea e nazionale dei *Third Party Payment Providers*. – 4. I *Card based payment instrument issuers*. – 5. Le modalità di accesso ai conti e il Regolamento delegato (UE) 2018/389. – 6. La disciplina del consenso per l'esecuzione delle operazioni di pagamento. – 7. Le novità in materia di responsabilità dei prestatori di servizi di pagamento. – 8. Il ruolo delle banche nel nuovo mercato dei pagamenti. – 9. Gli ostacoli all'attività dei *Third Party Providers* e i chiarimenti dell'EBA. – 10. I lavori di revisione della PSD2. – 11. Considerazioni conclusive.

1. *Premessa*

L'attuale disciplina giuridica dei servizi di pagamento pone numerose questioni che riguardano la tutela degli utenti di tali servizi e il regime di responsabilità degli intermediari che svolgono le attività di prestazione dei servizi di pagamento, in un delicato bilanciamento tra perseguimento degli interessi pubblici e autonomia degli operatori del mercato di riferimento. Partendo dalle innovazioni introdotte dalla direttiva 2015/2366/UE (c.d. *Payment service directive 2* - PSD2), attuata in Italia con il d.lgs. 15 dicembre 2017, n. 218[1], il presente contributo intende esaminare in particolare la disciplina relativa ai *Third Party Providers* (TPPs), i nuovi intermediari prestatori del servizio di disposizione di ordini di pagamento (*Payment initiation service* - PIS) e di informazione sui conti (*Account information service* - AIS). La Direttiva si inserisce in un programma di

[1] Direttiva 2015/2366 del Parlamento Europeo e del Consiglio del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno.

armonizzazione delle regole di funzionamento del mercato dei pagamenti al dettaglio, avviato già con la Direttiva 2007/64/CE (c.d. PSD) recepita nel nostro ordinamento con il d.lgs. 27 gennaio 2010, n. 11[2].

Lo sviluppo della tecnologia e la diffusione di pagamenti via *Internet* e tramite dispositivi *mobile* hanno infatti determinato la necessità di un nuovo intervento legislativo comunitario in materia di servizi di pagamento[3]. La nuova Direttiva ha l'obiettivo di promuovere i pagamenti digitali regolando uniformemente i nuovi tipi di servizi di pagamento offerti da soggetti già operanti sul mercato, non regolati dal primo atto comunitario. Essa mira a soddisfare le esigenze di tutela degli utenti di servizi di pagamento garantendo trasparenza, sicurezza, protezione dei dati personali e responsabilità[4]. L'Italia ha attuato la Direttiva con il d.lgs. 15 dicembre 2017, n. 218[5], intervenendo con importanti modifiche e integrazioni alle disposizioni contenute sia nel d.lgs. n. 11/2010 sia nel Testo unico bancario (TUB)[6].

Le novità più importanti sono quelle relative ai servizi di informazione sui conti di pagamento *online* (*Account Information Services* – AIS), ai servizi di conferma disponibilità fondi previsti nel caso di pagamenti effettuati con carte di debito emesse da un operatore diverso rispetto a quello presso il quale si detiene il conto (cioè il CISP), e quelle legate ai servizi di disposizione di ordini di pagamento *online* (*Payment Initiation Services* – PIS) che consentono di avviare un pagamento *online* tramite un prestatore di servizi di pagamento diverso da quello presso il quale si detiene il conto: questi servizi, diffusi nella prassi del settore del commercio elettronico già prima dell'adozione della seconda Direttiva, trovano oggi in questa normativa espressa disciplina e definizione[7]. Si tratta di attività che vengono erogate attraverso la modalità dell'*Open Banking,* con lo scambio, tramite le API software, di dati tra i vari soggetti in modo libero e veloce[8].

---

[2] Direttiva 2007/64/CE del Parlamento Europeo e del Consiglio del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno.

[3] . L.G. Chiusolo, M. Doria, M.I. Vangelisti, *L'assetto istituzionale del sistema dei pagamenti in Italia*, in Aa.Vv., *Economia dei sistemi di pagamento*, Bologna, 2005, 83 ss.

[4] Considerando 3 e 7 Direttiva 2015/2366/UE.D. Girompini, *PSD2 e Open Banking. Nuovi modelli di business e ruolo delle banche*, in *Bancaria*, 2018, 1, 70.

[5] Pubblicato in G.U. 13 gennaio 2018, n. 10.

[6] In particolare, è stato necessario modificare il Capo II-*bis* del titolo VI del Testo Unico bancario e il provvedimento di Banca d'Italia "Trasparenza delle operazioni e dei servizi bancari e finanziari – correttezza delle relazioni tra intermediari e clienti" di luglio 2009, in particolare la sezione VI "Servizi di pagamento". Queste modifiche, attuative della PSD2, sono state apportate con il provvedimento della Banca d'Italia del 19 marzo 2019 e sono applicate a partire dal 1° gennaio 2020, unitamente alle modifiche apportate dal provvedimento di Banca d'Italia di giugno 2019, attuative della direttiva 2014/92/UE (*Payment Accounts Directive*, c.d. PAD).

[7] L. Miotto, M. Speranzin, *I pagamenti elettronici*, in *Diritto del Fintech*, a cura di Cian, Sandei, Padova, 2020, 163 ss.

[8] G. Gimigliano, G. Nava*, L'inquadramento giuridico dei Mobile payment: profili ricostruttivi e distonie regolamentari*, in *Smart cities e diritto dell'innovazione*, a cura di G. Olivieri e V. Falce, Milano, 2016, 190 ss.; L.

Con l'implementazione della seconda *Payment Services Directive*, banche, utenti e il mondo delle *fintech* sono divenuti quindi i protagonisti di un cambiamento storico nell›erogazione di servizi finanziari e bancari che avviene lungo due direttrici fondamentali: lo scambio e la trasmissione di informazioni e la diversificazione dei soggetti che si trovano ad erogare servizi al mercato.

Anche se le maggiori novità hanno riguardato i prestatori di servizi di pagamento, la portata rivoluzionaria della PSD2 non si esaurisce, tuttavia, nel mondo *payment services*. Il cambiamento introdotto dalle disposizioni in materia di API, rapporti tra banche e soggetti non bancari e misure di sicurezza poste a tutela del cliente, hanno ridisegnato profondamente il settore dei servizi bancari europei. Storicamente, i servizi di pagamento e la gestione dei conti sono stati erogati da banche e istituzioni finanziarie attraverso la struttura di una filiera completa. Dalla raccolta del denaro, all'erogazione di mutui e finanziamenti, alla gestione dei servizi di pagamento, fino al contatto con il cliente per il tramite delle filiali (o, anche, tramite *home banking*): è stata la banca tradizionale ad aver gestito tutti questi servizi.

Le recenti novità normative hanno introdotto invece, sostanziali cambiamenti nei modelli di *business* di banche, introducendo nuovi *player*s di mercato che pongono in essere le loro attività facendo leva sul cambiamento tecnologico[9]. Si tratterà in questa sede dell'analisi dettagliata del funzionamento dei nuovi servizi di pagamento e si analizzeranno tutti i meccanismi posti a presidio della tutela del mercato e dei singoli utenti. Emergerà dunque che, dai rapporti tra *fintech* e banche, allo sviluppo di nuove offerte di prodotti e servizi da parte di soggetti istituzionali e nuovi operatori saranno molte le sfide da affrontare con la finalità di cogliere appieno le potenzialità della rivoluzione apportata dalla PSD2, avendo riguardo sempre agli obiettivi della tutela del cliente e del buon funzionamento del mercato di riferimento[10].

2. *I servizi sottoposti a riserva introdotti dalla Direttiva UE/2015/2366*

La PSD2 ha introdotto la regolamentazione di due nuove categorie di attività: i servizi di disposizione di ordine di pagamento e i servizi di informazione sui conti. Si tratta di servizi di pagamento soggetti a riserva che vengono elencati

Miotto, M. Speranzin, *I pagamenti elettronici*, in *Diritto del Fintech*, a cura di Cian, Sandei, Padova, 2020, 180 ss.

[9] Tale veloce evoluzione tecnologica comporta anche la necessità di un'interpretazione evolutiva delle tradizionali categorie giuridiche codicistiche, applicate ai nuovi strumenti (ad esempio, con riguardo alla natura giuridica della c.d. moneta elettronica v. D. Siclari, *Legislazione della nuova economia e disciplina codicistica: la moneta elettronica*, in *Banca, borsa, tit. cred.*, 2005, I, 4, 466 ss.).

[10] Con particolare riferimento al tema della responsabilità degli intermediari che svolgono l'attività di prestazione di servizi di pagamento v., di recente, F. Marasà, *Servizi di pagamento e responsabilità degli intermediari*, Milano, 2020.

ai numeri 7 e 8 dell'Allegato I della Direttiva[11]. Come già accadeva nella PSD1, la nuova normativa non dà nel catalogo delle definizioni un'esplicazione univoca delle caratteristiche del servizio di pagamento, inteso come contratto: rinviando all'Allegato I, offre soltanto un'elencazione di attività commerciali tipiche ripartite in otto categorie che vengono classificate come servizi di pagamento[12]. L'art. 4 della nuova Direttiva detta una specifica definizione per i nuovi servizi di pagamento: in particolare per «servizio di disposizione di ordine di pagamento» si intende quello in base al quale si «dispone l'ordine di pagamento su richiesta dell'utente di servizi di pagamento relativamente a un conto di pagamento detenuto presso un altro prestatore di servizi di pagamento»[13]. Questo tipo di prestazione, conosciuta anche come *Payment initiation service* (PIS), permette al prestatore di servizi di pagamento di avviare un'operazione di pagamento sulla base di un ordine che il prestatore stesso impartisce e che autorizza il proprio cliente a movimentare il proprio conto anche se detenuto presso un prestatore diverso. Si tratta dunque di un servizio informatico che offre una soluzione di pagamento elettronico alternativa e a costi inferiori rispetto a quella delle carte: permette infatti di connettere il sito web del commerciante con la piattaforma *online banking* della banca del pagatore per disporre pagamenti online tramite bonifico[14].

Il secondo servizio, quello di informazione sui conti, noto anche come *Account information service* (AIS), è il «servizio online che fornisce informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento»[15]. Questo consente al prestatore di accedere a tutti i conti di pagamento del proprio cliente anche se stabiliti presso altri prestatori, al fine di poter acquisire informazioni di pagamento e poter fornire al richiedente una panoramica della propria situazione finanziaria in qualsiasi momento[16]. Per entrambi i servizi, il prestatore opera su un conto di pagamento online attivato presso un altro prestatore di servizi di pagamento (c.d. presta-

[11] V. Profeta, *I Third Party Providers: profili soggettivi ed oggettivi*, in F. Maimeri, M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, Quaderni di ricerca giuridica della Banca d'Italia, n. 87, Settembre 2019, 49 ss.

[12] V. Profeta, *I Third Party Providers: profili soggettivi ed oggettivi*, cit. 49 ss.

[13] V. l'art. 4.15 della Direttiva PSD2.

[14] S. Moneti, *Mobile payments: gli sviluppi del mercato e l'inquadramento normativo*, in *Analisi giuridica dell'economia*, 2015, 101 ss.; E. Cervone, *Strumenti di pagamento innovativi, interoperabilità e neutralità tecnologica: quali regole e quale governance per un mercato sicuro, efficiente ed innovativo*, in *Riv. trim. dir. econ.*, 2016, 41.

[15] Si veda art. 4.16 Direttiva PSD2; A. Antonucci, *Mercati dei pagamenti: le dimensioni del digitale, in Riv. dir. banc.*, *www.dirittobancario.it,* 18, 2018; E. Cervone, *Strumenti di pagamento innovativi, interoperabilità e neutralità tecnologica: quali regole e quale governance per un mercato sicuro, efficiente ed innovativo*, in *Riv. trim. diritto dell'economia*, 2016, 73 ss.

[16] M. Catenacci, C. Fornasaro, *PSD2: i prestatori di servizi d'informazione sui conti (AISPS*), in *Dir. Banc.,* 2018, 4, 16 ss.

tore di servizi di pagamento di radicamento del conto) che gestisce il conto del medesimo cliente[17]. L'art. 4.16 prevede una limitazione a svolgere questi servizi solo in relazione ai conti accessibili online. Nonostante una previsione del genere manchi in relazione alla definizione del servizio di disposizione d'ordine di pagamento, dalla disposizione contenuta nell'art. 66 comma 1 della Direttiva emerge indirettamente che anche questo servizio può essere svolto soltanto sui conti[18]. Dunque, dato che le prestazioni in esame vengono espletate esclusivamente in maniera telematica, ne consegue che non possono essere utilizzate per eseguire operazioni relative a conti di pagamento ad operatività tradizionale. Attraverso la previsione di un diritto in capo al pagatore di avvalersi di un prestatore di servizi di disposizione di ordine di pagamento (art. 66, comma 1, PSD2) e del diritto di ricorrere a servizi che consentono l'accesso alle informazioni sui conti elencati al punto 8 dell'Allegato I (art. 67, comma 1 PSD2), il legislatore europeo ha concretizzato la sua volontà di promuovere l'utilizzo di bonifici in forma digitale[19].

Si metta in evidenza che entrambi i nuovi servizi PIS e AIS non comportano la custodia e la gestione dei fondi con cui si esegue il pagamento: l'ordine di pagamento impartito da un PISP dà soltanto avvio ad un'operazione eseguita tra diversi prestatori[20]. Il servizio di fornitura di informazioni su dati contenuti nei conti di pagamento ha un carattere del tutto accessorio rispetto alla principale attività di pagamento. Nonostante ciò, la categorizzazione di questi servizi tra quelli "di pagamento", con tutte le conseguenze che ne derivano, risponde all'interesse pubblico di monitorare lo svolgimento delle attività che ne sono oggetto; la tecnologia che le contraddistingue infatti, pone la necessità di garantire livelli alti di sicurezza informativa al fine sia di tutelare i fondi, sia di proteggere i dati relativi ai pagamenti che vengono resi conoscibili a terzi individui diversi dal titolare del conto e dal prestatore presso il quale il conto stesso è radicato[21]. Da ciò nasce la riserva di attività, strettamente collegata dunque al carattere preponderante che assume la tecnologia nella categoria dei servizi di pagamento digitalizzati che si avvalgono della moneta scritturale. Il procedimento di pagamento neces-

[17] Art. 4.17 Direttiva PSD2.

[18] Tale disposizione esclude il diritto del pagatore di avvalersi di un prestatore di servizi di disposizione di ordine di pagamento qualora il conto di pagamento "non sia accessibile online"; A. Antonucci*, Mercati dei pagamenti: le dimensioni del digitale*, in *Riv. dir. banc.,* 2018, 18.

[19] V. Profeta, *I Third Party Providers: profili soggettivi ed oggettivi*, in F. Maimeri, M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale, Quaderni di ricerca giuridica della Banca d'Itali*a, n. 87, Settembre 2019, 51 ss.

[20] Per un approfondimento sull'aspetto procedimentale del pagamento eseguito attraverso un intermediario professionale v. A. Sciarrone Alibrandi, *Il diritto del sistema finanziario*, in Aa.Vv., *Diritto commerciale*, a cura di M. Cian, Torino, 2013, 319 ss.

[21] In dottrina V. Di Stasio, *Ordine di pagamento non autorizzato e restituzione della moneta*, Milano, 2016, 45 ss.; A. Sciarrone Alibrandi, *Il diritto del sistema finanziario,* in Aa.Vv., *Diritto commerciale*, a cura di M. Cian, Torino, 2013, 319;

sita, dal punto di vista soggettivo, della presenza attiva di più intermediari specializzati per lo svolgimento di attività diverse e funzionali all'esecuzione del pagamento[22]. Tuttavia, questi nuovi strumenti elettronici consentono di dare istantaneità ai procedimenti di pagamento.

D'altro canto, dato che i nuovi servizi possono in tal modo comportare un indebito accesso al conto di pagamento con pregiudizio per i fondi, la nuova disciplina è volta a potenziare i presidi di sicurezza informatica dei pagamenti elettronici ed a monitorare le frodi: è attribuita *all'European Banking Authority* (EBA)[23] la competenza di definire standard tecnici di comunicazione sicura tra i *Third Party Providers* (TPPs) e i prestatori di servizi di pagamento di radicamento del conto, che tengano conto della incessante evoluzione tecnologica. La Direttiva poi si preoccupa di regolare il riparto del rischio dell'inadempimento del pagamento o della sua esecuzione non autorizzata con l'introduzione in capo all'utente, di un diritto al rimborso (salvo in caso di frode) da far valere nei confronti del prestatore del servizio di radicamento del conto: a causa delle difficoltà che si riscontrano nell'individuazione del soggetto responsabile fra quelli coinvolti a vario titolo nell'operazione di pagamento, è sul gestore del conto che grava il rischio della contestazione del pagamento[24].

La nuova disciplina vuole così assicurare un'efficienza procedimentale complessiva dei servizi di pagamento aumentando la fiducia dei consumatori verso il sempre più diffuso utilizzo dei nuovi strumenti elettronici.

3. *La disciplina giuridica europea e nazionale dei* Third Party Payment Providers

I *Third Party Payment Providers* (TPPs), termine col quale si indicano i soggetti che forniscono questa nuova tipologia di servizi, in virtù della Direttiva PSD2, al fine di svolgere la propria attività, devono ottenere l'autorizzazione amministrativa, come accade per gli istituti di pagamento. I TPPs si distinguono

[22] M. Onza, *Gli strumenti di pagamento nel contesto dei pagamenti online*, in *Diritto bancario*, 4/2017, 679; V. Profeta, *I Third Party Providers: profili soggettivi ed oggettivi*, in F. Maimeri, M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale, Quaderni di ricerca giuridica della Banca d'Italia,* n. 87, Settembre 2019, 51 ss.

[23] L'European Banking Authority (EBA) ha il ruolo di regolatore di secondo livello e di promotore del coordinamento tra le diverse Autorità nazionali.

[24] È salvo il suo diritto ad ottenere, a prima richiesta, lo stesso rimborso dal PISP; con riferimento agli AIS, il Considerando n. 28 della Direttiva n. 2015/2366 sottolinea che "…*tali servizi dovrebbero essere trattati nella presente direttiva al fine di garantire ai consumatori una protezione adeguata relativamente ai dati di pagamento e contabili nonché la certezza giuridica legata allo status di prestatore di servizi di informazione sui conti*"; M. Catenacci, C. Fornasaro, *PSD2: i prestatori di servizi d'informazione sui conti (AISPS*), in *Dir. Banc*., 4/2018, 73 ss.

in PISPs (*Payment initiation service providers*) che forniscono i servizi di ordine di pagamento e AISPs (*Account information service providers)* che forniscono informazioni sui conti[25]. L'art. 37 della Direttiva contiene il divieto di prestare servizi di pagamento per le persone fisiche o giuridiche che non siano prestatori di servizi di pagamento[26] e, tra i prestatori disciplina esclusivamente gli istituti di pagamento dettando le regole da seguire per l'ottenimento dell'autorizzazione amministrativa[27]. Sono previsti diversi requisiti per ottenere l'autorizzazione o la registrazione allo svolgimento in forma isolata del servizio di disposizione di ordine di pagamento e di quello di informazione sui conti: chi intende svolgere soltanto servizi PIS è tenuto ad avere un capitale iniziale di euro, anziché di euro 125.000 previsto per gli istituti di pagamento ed è obbligato ad attuare un'assicurazione per la responsabilità civile professionale che sia valida in tutti i territori in cui offrono i servizi in presenza del compimento di operazioni non autorizzate e/o in caso di mancata o tardiva esecuzione di operazioni di pagamento e per l'esercizio dell'azione di regresso da parte di altri soggetti prestatori di servizi di pagamento (art. 92)[28]. L'art. 33 della Direttiva prevede che, in caso di prestazione del servizio online di informazione sui conti, le imprese, anche individuali, devono presentare una domanda di registrazione e possedere un'analoga assicurazione per la responsabilità civile professionale che copra le pretese risarcitorie collegate ai danni causati al prestatore di servizi di pagamento di radicamento del conto o all'utente dei servizi di pagamento dall'accesso o derivanti dall'uso non autorizzato o fraudolento delle informazioni del conto di pagamento[29].

L'art. 5.4 della PSD2 affida all'EBA la definizione dei criteri per stabilire l'importo monetario minimo dell'assicurazione per la responsabilità civile professionale in relazione ai servizi PIS e AIS[30]: questi sono stabiliti in base al rischio

[25] Alla generale categoria dei TPPs sono riconducibili anche i prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta, cd. CBPIIs (Card based payment instrument issuers), limitatamente allo svolgimento del servizio di conferma della disponibilità di fondi.

[26] Sono salvi i servizi espressamente esclusi dall'ambito di applicazione della medesima Direttiva; art. 37, comma 1, e art. 3, lett. k), PSD2; la Direttiva 2007/64 prevedeva analogo divieto (art. 29).

[27] L'art. 1 della PSD2 elenca: (a) enti creditizi; b) istituti di moneta elettronica; c) uffici postali; d) istituti di pagamento; e) BCE e banche centrali nazionali; f) Stati membri e rispettive autorità regionali o locali ove non agiscano in quanto autorità pubbliche; M. Pimpinella, G. Carrafiello, L'evoluzione normativo-regolamentare nel settore dei pagamenti: PSD2 e Regolamento MIF, Milano, 2016, 169 ss.

[28] V. Profeta, *I Third Party Providers: profili soggettivi ed oggettivi*, in F. Maimeri, M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale, Quaderni di ricerca giuridica della Banca d'Italia*, n. 87, Settembre 2019, 56 ss.

[29] Secondo l'art. 7 della Direttiva, gli istituti che svolgono soltanto servizi informativi non sono tenuti al possesso di un capitale iniziale né ad indicare i soggetti partecipanti al capitale; Guideline EBA/GL/2017/09, dell'11 luglio 2017, 4.2, che prevedono quale soggetto richiedente la registrazione per lo svolgimento dei soli servizi del n. 8, o la persona fisica o quella giuridica.

[30] Il 7 luglio 2017 l'EBA ha pubblicato il Rapporto finale (GL/2017/08) contenente "*Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee under Article 5(4) of Directive (EU) 2015/2366 (PSD2)*"; per un approfondimento v. C. Marseg-

dell'impresa, allo svolgimento contestuale di altri servizi di pagamento o di altre attività e al volume delle attività stesse che, mentre per il servizio di disposizione di ordini di pagamento è ragguagliato al valore delle operazioni disposte, per il servizio di informazione dipende dal numero dei clienti che utilizzano i servizi di informazione sui conti. Per di più, questo nuovo ruolo normativo dell'EBA, non previsto nella PSD1, è fondamentale in quanto permette di uniformare in tutti i Paesi dell'Unione Europea le caratteristiche della polizza assicurativa[31]. Necessario per il rilascio dell'autorizzazione per lo svolgimento del PIS e per la registrazione per lo svolgimento dell'AIS, è il documento relativo alla politica di sicurezza che il richiedente deve fornire all'Autorità di vigilanza, contenente i rischi connessi a tutti i servizi offerti (inclusi i rischi derivanti da frode e uso illegale di dati sensibili) e la descrizione dell'organizzazione dei presidi di controllo e di sicurezza[32].

Molta attenzione è prestata dalla PSD2 all'organizzazione della sicurezza informatica, sia per la tutela dell'integrità dell'attività dell'intermediario, sia per la tutela dei diritti personali e patrimoniali degli utenti, a partire dalla prima fase di valutazione dei requisiti necessari per l'ottenimento dell'autorizzazione da parte dell'intermediario e poi durante lo svolgimento dell'attività di vigilanza: ciò rappresenta una novità importante rispetto alla prima Direttiva PSD1 in quanto manifesta il progresso e la rivoluzione tecnologica che ha investito negli ultimi anni gli intermediari[33]. Durante il procedimento di valutazione di questi profili l'Autorità di vigilanza designata può esercitare una vera e propria discrezionalità tecnica. L'art. 14, ai commi 1 e 2, della PSD2, prevede che l'autorizzazione rilasciata per l'esecuzione dei servizi di disposizione comporti l'iscrizione dell'istituto richiedente e dei relativi agenti, in un pubblico registro, consultabile liberamente ed accessibile online, tenuto presso lo Stato membro di origine. Lo stesso accade per tutti i provvedimenti di revoca delle autorizzazioni e delle esenzioni[34], nonché per le persone fisiche o giuridiche, iscritte nel medesimo registro per lo svolgi-

---

lia, *Responsabilità civile: furto della tessera di Bancomat e concorso di colpa tra l'utilizzatore e l'intermediario,* in *Nuova Giur. Civ.*, 2020, 3, 561 ss.

[31] Attraverso tale polizza, gli istituti che svolgono i nuovi servizi sopperiscono alla minore dotazione patrimoniale così da provvedere alla copertura finanziaria per le eventuali ipotesi di responsabilità civile derivanti dai danni eventualmente arrecati, nell'esecuzione dei loro servizi, ai clienti, ai prestatori che forniscono e amministrano i conti di pagamento o ai terzi; M.M. Pimpinella, G. Carrafiello, *L'evoluzione normativo-regolamentare nel settore dei pagamenti: PSD2 e Regolamento MIF,* 2016, 64 ss.; E. Zeppieri, *L'implementazione in Italia della nuova direttiva sui servizi di pagamento*, in *Dir. Bancario*, 2018, 45 ss.

[32] Art. 5, comma 1, lett. j., della Direttiva PSD2.

[33] La Direttiva ha conferito all'EBA il mandato ad adottare 6 technical standards, 4 set di guidelines e un registro; v. i *Considerando* nn. 107 e 108 della PSD2; I. D'Ambrosio, *La tutela del consumatore nei pagamenti elettronici e la nuova Direttiva europea PSD2,* in *Notariato,* 2019, 6, 676 ss.;

[34] L'art. 14, par. 3, PSD2 letteralmente indica "*la revoca… di esenzioni concesse a norma degli articoli 32 o 33*"; v. M. Rispoli Farina, *Informazione e servizi di pagamento*, in *Analisi giuridica dell'economia*, I, 2015, 175 ss.; A. Sciarrone Alibrandi, *Il diritto del sistema finanziario*, in Aa.Vv., *Diritto commerciale*, a cura di M. Cian, Torino, 2013, 319 ss.

mento dei soli servizi di informazione sui conti. Di nuova istituzione è il registro elettronico detenuto dall'*European Banking Authority,* pubblicato sul sito web e consultabile liberamente, nel quale si raccolgono tutte le informazioni contenute nei vari registri nazionali. È del 13 dicembre 2017 la pubblicazione da parte dell'EBA di un Rapporto finale contenente il progetto di norme tecniche di regolamentazione che definiscono i requisiti tecnici relativi allo sviluppo, alla gestione e al mantenimento del registro elettronico centrale e all'accesso alle informazioni ivi contenute; è un documento consultabile gratuitamente online e diretto a garantire al cittadino un accesso facile e un'agevole ricerca delle informazioni[35].

Gli artt. 23 e 24 della Direttiva statuiscono che anche gli istituti di pagamento che svolgono il ruolo di TPPs[36], sono soggetti alla vigilanza informativa ed ispettiva delle Autorità nazionali competenti nonché alle disposizioni di *soft law* e ai provvedimenti amministrativi a carattere vincolante delle stesse[37]. Le Autorità possono dunque adottare provvedimenti di revoca o sospensione dell'autorizzazione quando ricorrono alcune condizioni previste all'art. 13 della PSD2 e comminare sanzioni amministrative nei confronti degli intermediari o di coloro che controllano l'attività degli istituti di pagamento che hanno commesso infrazioni alle disposizioni legislative, regolamentari o amministrative. I prestatori di servizi di informazioni sui conti sono sottoposti anch'essi alla vigilanza dell'Autorità competente ma al contempo sono esentati dal rispettare le disposizioni relative al capitale iniziale e al capitale di funzionamento e quelle concernenti il ricorso ad agenti attraverso cui vengono esternalizzate le attività[38].

Passando all'analisi della normativa nazionale dei servizi di pagamento, si ricordi, come già sopra accennato, che la PSD2 è stata recepita in Italia con il d.lgs. n. 218/2017, che ha aggiornato sia il Testo Unico Bancario[39], sia il d.lgs. n. 10/2011[40]: il primo nelle parti relative agli istituti di pagamento (Titolo V-*ter*) ed alla trasparenza dei rapporti dei prestatori di servizi di pagamento con i clienti (Titolo VI); il secondo per la parte relativa ai profili concernenti i rapporti contrattuali tra i prestatori di servizi di pagamento e i clienti. Il legislatore italiano

[35] EBA/RTS/2017/10; I. D'Ambrosio, *La tutela del consumatore nei pagamenti elettronici e la nuova Direttiva europea PSD2*, in *Notariato*, 2019, 6, 676 ss.

[36] Compresi gli AISPs registrati.

[37] Rispettivamente art. 23, comma 1, par. 2, lett. a) e b) 24) e art. 23, comma 1, par. 2 lett. c).

[38] V. Profeta, *I Third Party Providers: profili soggettivi ed oggettivi*, in F. Maimeri, M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale, Quaderni di ricerca giuridica della Banca d'Italia,* n. 87, Settembre 2019, 58 ss.; R. Ferrari, *L'era del FinTech: La rivoluzione digitale nei servizi finanziari*, Milano, 2016, 203 ss.

[39] Decreto legislativo 1° settembre 1993, n. 385.

[40] Il medesimo decreto legislativo contiene le norme di attuazione del Regolamento (UE) n. 751/2015 del Parlamento europeo e del Consiglio, del 29 aprile 2015, relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta; M. Onza, *Gli strumenti di pagamento nel contesto dei pagamenti online,* in *Diritto bancario,* 2017, 4, 679 ss.

ha avuto pochi spazi di discrezionalità in quanto si è in presenza di una Direttiva di armonizzazione massima, diretta a garantire una uniforme applicazione della normativa in tutta l'Unione Europea. È stata così ampliata la definizione normativa dei servizi di pagamento che ricomprende anche il servizio di disposizione di ordini di pagamento e quello di informazione sui conti[41] riservati ora ai prestatori di servizi di pagamento[42]: si tratta di una riserva penalmente presidiata dalla fattispecie prevista dall'art. 131-*ter* del T.U.B che punisce con la reclusione da sei mesi a quattro anni e con la multa da 2.066 euro a 10.329 euro chiunque presta servizi di pagamento in violazione della riserva ex art. 114-*sexies* senza essere autorizzato ai sensi dell'art. 114-*novies.* L'art. 131-*ter* individua l'abusivismo nell'assenza dell'autorizzazione disciplinata dall'art. 114-*novies:* ciò fa sì che si applichi tale fattispecie penale anche all'esercizio abusivo della prestazione di servizi di informazione sui conti[43].

La PSD2 qualifica il provvedimento di accesso allo svolgimento di questi servizi come una registrazione, e non come autorizzazione mentre la disciplina italiana di recepimento richiede anche per gli AISPs la verifica del possesso dei requisiti tecnici che deve essere effettuata dalla Banca d'Italia attraverso una valutazione tecnico-discrezionale[44]: l'Autorità è portata a verificare (attraverso un accertamento tecnico discrezionale posto in essere utilizzando parametri da essa individuati) la presenza di requisiti tecnici specifici in capo ai richiedenti e non ad effettuare esclusivamente una semplice ricognizione di elementi oggettivi necessari alla registrazione del prestatore[45]. Tale operazione si svolge attraverso un esame preliminare di procedure e documenti relativi a: programmi di attività del tipo di servizi di pagamento; al piano aziendale; alla procedura di monitoraggio e gestione degli incidenti relativi alla sicurezza; alla procedura di archiviazione, monitoraggio e gestione dei dati sensibili sui pagamenti; al documento relativo alla politica di sicurezza, la copertura assicurativa o la stipula di una garanzia per la responsabilità nei confronti del prestatore di servizi di pagamento di radicamento del conto o dell'utente dei servizi di pagamento derivante dall'accesso non autorizzato o fraudolento alle informazioni del conto di pagamento o dall'uso non autorizzato o fraudolento delle stesse[46]. La Banca d'Italia con il Provvedi-

[41] Art. 1, lett. h septies 1, nn.7) e 8) T.U.B.

[42] Art. 114-*sexies* T.U.B; E. Zeppieri, *L'implementazione in Italia della nuova direttiva sui servizi di pagamento*, 2018, in *www.dirittobancario.it*.

[43] Par. 1, sez. I, capo III, Disposizioni di vigilanza della Banca d'Italia, 23 luglio 2019, (nt. 16), 32.

[44] Il provvedimento adottato resta pertanto contrassegnato dall'esercizio di una discrezionalità tecnica nell'accertamento dei requisiti di iscrizione che, in Italia, caratterizza i provvedimenti autorizzativi.

[45] M. Catenacci, V. Sanna*, La disciplina degli AISP nelle nuove disposizioni di vigilanza della Banca d'Italia*, 2019, in *www.dirittobancario.it*.

[46] M. Mancini, M. Rispoli, V. Santoro, A. Sciarrone Alibrandi, O. Troiano (a cura di), *La nuova disciplina dei servizi di pagamento*, Torino, 2011, 48 ss.

mento del 23 luglio 2019, recante modifiche alle disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica in attuazione della Direttiva UE/2015/2366, ha qualificato il proprio provvedimento non come "registrazione" ma come "autorizzazione" anche in relazione a quei prestatori che svolgono servizi di informazioni sui conti[47]. Il recepimento della PSD2 non ha modificato i requisiti per il rilascio dell'autorizzazione allo svolgimento dei servizi di pagamento (inclusi quelli di disposizione di ordini di pagamento indicati nell'art. 114 *novies*, comma 1, TUB): unica novità è stata l'introduzione, nell'art. 114 *novies*, comma 1-*bis*, TUB., per gli istituti che intendono svolgere i nuovi servizi, dell'obbligo di stipulare una polizza di assicurazione della responsabilità civile o analoga forma di garanzia per i danni arrecati nell'esercizio dell'attività derivanti da condotte proprie o di terzi. Anche se, secondo l'interpretazione letterale dell'art. 114 *novie*s, comma 1 *bis*, tale obbligo sembrerebbe riferito espressamente soltanto agli istituti che svolgono il servizio di disposizione di ordini di pagamento, in realtà questo deve ritenersi applicabile anche agli AISPs[48].

In relazione alle indicazioni contenute nell'art. 5 della PSD2, la normativa italiana di recepimento ha mostrato inizialmente una lacuna, successivamente colmata dall'EBA: il decreto legislativo, infatti, non ha preso in considerazione i requisiti per l'autorizzazione, specificatamente quelli concernenti la politica di sicurezza, la prevenzione dei rischi relativi ai servizi offerti, il monitoraggio e la gestione degli incidenti relativi alla sicurezza e i reclami dei clienti[49]. Il provvedimento emanato dall'EBA, dell'11 luglio 2017, al quale rinviano anche le norme di carattere secondario messe in consultazione dalla Banca d'Italia, ha permesso il superamento di tale deficit al fine di garantire l'uniformità applicativa della Direttiva circa i requisiti di sicurezza informatica necessari per la tutela dell'intermediario e degli utenti dei servizi di pagamento[50].

La sicurezza rappresenta per la PSD2 e per i successivi orientamenti dell'EBA, uno dei temi più importanti tale da incidere sull'organizzazione amministrativa degli istituti di pagamento[51]. In tale ambito, infatti, il Provvedimento della Banca d'Italia del 23 luglio 2019, ha previsto un rafforzamento di tutte le misure orga-

---

[47] Si veda F. Cascinelli, V. Pistoni, G. Zanetti, *La Direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno,* luglio 2016, 14 ss., in www.dirittobancario.it.

[48] V. Disposizioni di vigilanza della Banca d'Italia, 23 luglio 2019, nt. 16, 55.

[49] L. Miotto, M. Speranzin, *I pagamenti elettronici*, in *Diritto del Fintech*, a cura di Cian, Sandei, Padova, 2020, 140 ss.

[50] EBA/GL/2017/09 dell'11 luglio 2017, in attuazione dell'art. 5.5 della PSD2.

[51] Orientamenti finali in materia di segnalazione dei gravi incidenti ai sensi della direttiva 2015/2366/UE (PSD2), emanati dall'EBA il 19 dicembre 2017; Orientamenti finali sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento ai sensi della direttiva 2015/2366/UE (PSD2), emanati dall'EBA il 12 gennaio 2018; V. Profeta, *I Third Party Providers: profili soggettivi ed oggettivi*, in F. Maimeri, M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale, Quaderni di ricerca giuridica della Banca d'Italia*, n. 87, Settembre 2019, 49 ss.

nizzative degli istituti di pagamento al fine di presidiare tutti i rischi, in particolare quelli collegati alla sicurezza dei pagamenti; ad esempio il citato Provvedimento richiede agli istituti di pagamento l'adozione di procedure e sistemi idonei a: tutelare la sicurezza, l'integrità e la riservatezza delle informazioni; archiviare e gestire i dati sensibili relativi ai pagamenti, con i limiti di accesso; acquisire dati statistici relativi ai risultati della gestione, alle operazioni di pagamento effettuate e alle frodi[52].

L'art. 114 *novies* del TUB., statuisce che, in relazione ai nuovi istituti di pagamento aventi sede in Italia dove svolgono una parte della loro attività di erogazione di servizi di pagamento, spetta alla Banca d'Italia il rilascio dell'autorizzazione, la verifica del possesso continuo di dei requisiti (attraverso l'azione di vigilanza) e la tenuta dell'albo nazionale, consultabile liberamente online[53]. Quest'ultimo rende pubblici ora anche i dati identificativi della polizza assicurativa o della analoga garanzia ormai obbligatoria per gli istituti di pagamento che svolgono attività di disposizione di ordini di pagamento. Per i soggetti che prestano esclusivamente servizi di informazione sui conti, è prevista l'iscrizione in una sezione speciale dell'albo degli istituti di pagamento. In base alle disposizioni contenute nella PSD2, gli AISPs debbono possedere requisiti semplificati per l'iscrizione nell'albo rispetto a quelli imposti agli altri istituti di pagamento: non è richiesta infatti l'indicazione di un capitale o il possesso di determinate qualità in capo ai titolari di azioni[54].

L'art. 114-*novies* TUB indica quale forma giuridica necessaria per lo svolgimento di queste attività quella in società, sia essa per azioni, in accomandita per azioni, a responsabilità limitata o cooperativa mentre la Direttiva prevedere l'estensione alle persone fisiche la registrazione per lo svolgimento del servizio di informazione sui conti[55]. L'art. 114-*septiesdecies* TUB riassume il regime normativo degli istituti che svolgono soltanto servizi informativi sui conti e contiene due categorie di disposizioni. Il primo gruppo di disposizioni detta una disciplina riguardante gli istituti che svolgono soltanto le attività di informazione: questi non possono svolgere anche attività accessorie di concessione di credito e di prestazione di garanzia o di gestione di sistemi di pagamento ma possono svolgere altre attività di impronta imprenditoriale soggette a valutazione dalla Banca

---

[52] A. Messore, *La nuova disciplina dei servizi di pagamento digitali prestati dai Third Party Providers*, in Nuove *Leggi Civ. Comm.,* 2020, 2, 511.

[53] Art. 114-*novies*, comma 1, lett. b) e art. 114-*septies* T.U.B.

[54] Gli AISPs non sono soggetti ad una mera registrazione nell'albo data la necessaria attività valutativa tecnico discrezionale rimessa alla Banca d'Italia per accertare il possesso dei requisiti di iscrizione all'albo; F. Ciraolo, *I servizi di pagamento nell'era FinTech*, in M.T. Paracampo (a cura di), *Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari,* Torino, 2017, 188 ss.

[55] Di ciò tengono conto anche gli orientamenti EBA; M. Mancini, M. Rispoli, V. Santoro, A. Sciarrone Alibrandi, O. Troiano (a cura di), *La nuova disciplina dei servizi di pagamento*, Torino, 2011, 72 ss.

d'Italia ai fini dell'autorizzazione[56]. Questi soggetti, se costituiti in forma societaria, non sono destinatari delle norme di tutela sulle partecipazioni azionarie[57] e di quelle concernenti i conti di pagamento e il patrimonio destinato[58], in quanto gli istituti che svolgono soltanto servizi di informazione sui conti non detengono fondi dei clienti. Ancora, agli istituti che svolgono soltanto le attività di informazione non si applicano le disposizioni relative alla trasparenza nei rapporti contrattuali con i clienti e non possono ottenere dalla Banca d'Italia un regime di esenzione totale o parziale da alcune disposizioni che valgono per gli istituti di pagamento[59].

Il secondo gruppo di disposizioni è quello contenuto nell'art. 114 *septiesdecies* TUB, ricompreso nell'ambito del Titolo VI del TUB che ne prevede espressamente l'applicazione agli istituti che svolgono i servizi di informazione sui conti[60]. Tutte le altre disposizioni del Testo Unico, in quanto non espressamente richiamate, sarebbero applicabili soltanto se compatibili con la peculiarità del servizio di informazione sui conti, che al pari di quello di disposizione di ordine di pagamento, non comporta la tenuta di conti di pagamento e/o la gestione di fondi. In questo modo, gli AISPs, così come tutti gli istituti di pagamento, sono soggetti all'azione di vigilanza della Banca d'Italia prevista dall'art. 114-*quaterdecies* TUB e soggiacciono alle sanzioni amministrative contenute nel Titolo VIII, irrogabili dalla stessa Banca d'Italia, anche se tali disposizioni non sono richiamate nell'art. 114-*septiesdecies*[61].

Interessante è la disciplina della "trasparenza contrattuale" regolata dal Titolo VI TUB e che si applica sia agli AISPs che ai PISPs, sottoposti automaticamente alla vigilanza della Banca d'Italia che ha il potere di acquisire informazioni, eseguire ispezioni e adottare le misure inibitorie previste dall'art. 128-*ter* TUB in caso di irregolarità nel comportamento di questi istituti[62]. Secondo l'o-

---

[56] Artt. 114-*octies* T.U.B. e 114-*novies*, commi 4 e 5 T.U.B.

[57] Né tantomeno quelle relative ai requisiti di onorabilità dei partecipanti al capitale, art. 114-*undecies*, commi 1 e 1-*ter* T.U.B.;

[58] Artt. 114-*duodecies* e 114-*terdecies* T.U.B.

[59] Artt. 114-*undecies*, commi 1 e 114-*sexiesdecies* T.U.B.; v. S. Vanini, *L'attuazione in Italia della seconda Direttiva sui servizi di pagamento nel mercato interno: le innovazioni introdotte da d.lgs. 15 dicembre 2017, n. 218,* in *Le nuove leggi civili e commerciali,* 2018, 4, 866 ss..

[60] Tale articolo contiene delle esenzioni per tali soggetti che quindi non possono concedere credito, prestare garanzie, gestire sistemi di pagamento, nonché le altre attività accessorie alla prestazione di servizi di pagamento (art. 114 octies T.U.B.); A. Messore, *La nuova disciplina dei servizi di pagamento digitali prestati dai Third Party Providers,* in *Nuove Leggi Civ*. Comm., 2020, 2, 511 ss.

[61] Si veda V. Profeta, *I Third Party Providers: profili soggettivi ed oggettivi*, in F. Maimeri, M. Mancini (a cura di)*, Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale, Quaderni di ricerca giuridica della Banca d'Italia*, n. 87, Settembre 2019, 55 ss.

[62] Al riguardo rileva dunque l'art. 34 d.lgs. n. 11/2010, che, in recepimento del Titolo III della PSD2, introduce nel Titolo VI del T.U.B., il nuovo Capo II bis, dedicato specificamente alla disciplina sulla trasparenza dei servizi di pagamento. La Banca d'Italia, nell'ambito della delega ex artt. 126-*bis* ss. T.U.B, con il provvedimento del 19 marzo 2019, in tema di Trasparenza delle operazioni e dei servizi bancari e finanziari e correttezza delle relazioni tra intermediari e clienti detta regole di forma e contenuto per i contratti quadro relativi ai ser-

riginario art. 128-*bis* TUB, i nuovi istituti di pagamento erano tenuti obbligatoriamente ad aderire ai sistemi di risoluzione stragiudiziale delle controversie con la clientela; disciplina modificata di recente dal d.lgs n. 36/2020, recante «Disposizioni correttive ed integrative del decreto legislativo di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno, nonché di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta». L'art. 1 di tale decreto, infatti, ha introdotto alcune modifiche di aggiornamento al TUB; in particolare: la lettera b) del comma 1, intervenendo sull'articolo 114-*septiesdecies* del TUB relativo ai prestatori del servizio di informazione sui conti, ha inciso sulla disciplina da applicare ai soggetti che prestano il servizio in via esclusiva con eliminazione del riferimento all'articolo 128-*bis* del TUB, riguardante appunto i sistemi di risoluzione stragiudiziale delle controversie con la clientela. L'art. 2, comma 1, lettera a) del recente decreto ha apportato invece modifiche all'articolo 27 del d.lgs. n. 11/2010, con la previsione di un diritto di regresso che sorge nel caso in cui la responsabilità di un prestatore di servizi di pagamento sia attribuibile a un altro prestatore degli stessi servizi o ad un altro soggetto interposto nell'esecuzione dell'operazione. Secondo questa disposizione, il secondo prestatore di pagamento è tenuto a risarcire il primo prestatore di servizi di pagamento in caso di perdite o di importi versati con riferimento a operazioni di pagamento non autorizzate e con riferimento alla inesatta, tardiva o mancata esecuzione delle operazioni di pagamento[63].

4. *I* Card based payment *instrument issuers*

Accanto ai nuovi servizi di pagamento appena illustrati, un'altra importante novità introdotta dalla PSD2 riguarda il cosiddetto "*fund checking*", ossia il controllo della disponibilità dei fondi.

La Direttiva introduce infatti la possibilità per i prestatori di servizi di pagamento basati su carta, i c.d. CBPIIs (*Card based payment instrument issuers*) di ricevere conferma della disponibilità dei fondi a fronte di operazioni di pagamen-

vizi di pagamento, nonché gli obblighi informativi degli intermediari di servizi di pagamento, distinti a seconda che le operazioni di pagamento rientrino o meno in un contratto quadro (sez. VI); D. Girompini, *PSD2 e Open Banking. Nuovi modelli di business e ruolo delle banche,* in *Bancaria*, 2018, fasc. 1, 70 ss.

[63] V. Art. 27, comma 1, d.lgs. n. 11/2010 aggiornato. La novella legislativa ha voluto aggiungere quindi, tra le ipotesi di regresso, anche quella riconducibile all'articolo 25-*bis* del decreto, relativa alla responsabilità in caso di prestazione dei servizi di disposizione di ordine di pagamento per la mancata, inesatta o tardiva esecuzione dell'operazione di pagamento. Da ultimo, la lettera b) del comma 1 è intervenuta sull'articolo 34-*bis* del d.lgs. n. 11/2010, che disciplina il limite alle commissioni interbancarie applicate alle operazioni di pagamento nazionali effettuate con carta di debito dai consumatori.

to richieste dal pagatore tramite piattaforma online. Tale possibilità è essenziale per la gestione e la riduzione del rischio di credito. Il servizio di conferma di disponibilità di fondi (che non ha una sua autonomia nell'elenco dei servizi contenuto nell'Allegato I) non può costituire un'attività esclusiva di un prestatore di servizi di pagamento; al contrario può essere svolto soltanto dai prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta, assumendo un carattere strumentale[64].

Questa nuova modalità di controllo della disponibilità dei fondi si divide in vari step: si parte dalla sottoscrizione di un contratto tra il pagatore e il *Card Issuer Service Provider*; il pagatore effettua un'operazione di pagamento tramite piattaforma online a favore di un soggetto terzo beneficiario; *l'Account Servicing Payment Service Provider* del beneficiario a questo punto si rivolge al CISP per richiedere conferma della disponibilità dei fondi necessari per il completamento dell'operazione il quale si rivolge a sua volta all' l'*Account Servicing Payment Service Provider* del pagatore[65]. Quest'ultimo, che non può trasmettere alcuna informazione di natura qualitativa o quantitativa, tramite una semplice conferma o un diniego si esprime sulla disponibilità dei fondi ed il CISP ne informerà l*'Account Servicing Payment Service Provider* del beneficiario. Il prestatore che svolge tale tipo di servizio ha in comune con il PISP e l'AISP il fatto che per eseguire il proprio servizio ha accesso al conto di pagamento del cliente acceso presso un altro prestatore soltanto con il consenso esplicito del cliente stesso[66].

5. *Le modalità di accesso ai conti e il Regolamento delegato (UE) 2018/389*

Aspetto cruciale della Direttiva, è quello riguardante la disciplina delle modalità di accesso ai conti: si tratta di una normativa dettagliata alla quale debbono attenersi i vari soggetti coinvolti nell'operazione di pagamento ossia PISPs e AISPs e prestatori di radicamento del conto, al fine di non mettere a rischio la sicurezza dei fondi e dei dati di pagamento[67]. Le parti dell'operazione sono tenute

---

[64] G. Ardizzi, S. Emiliozzi, J. Marcucci, L. Monteforte *News and consumer card payments, presentato al Workshop della Banca d'Italia Harnessing Big Data & Machine Learning Technology for Central Banks*, 26-27 marzo 2018.

[65] V. V. Aprigliano, G. Ardizzi, L. Monteforte, *Using the payment system data to forecast the Italian GDP, Banca d'Italia – Working Papers (Temi di discussione)* 2017, n. 1098; V. Falce, *Il funzionamento dei sistemi di pagamento al dettaglio. Ancora in materia di commissioni interbancarie,* in *Armonizzazione europea dei servizi di pagamento e attuazione della direttiva 2007/64/CE*, a cura di M. Rispoli Farina, Milano 2009, 531 ss.

[66] V. Falce, *Dalla self-regulation al payment package. Storia delle commissioni interbancarie*, in www.dimt.it, 2015.

[67] Queste misure si applicano anche all'operazione di conferma della disponibilità di fondi su richiesta di un prestatore di servizi di pagamento emittente strumenti di pagamento basati su carta; C. Giussani, *Verso*

a comunicare tra loro in maniera sicura «conformemente all'articolo 98, paragrafo 1, lett. d)» della PSD2, rispettando le norme tecniche volte a: assicurare un livello adeguato di sicurezza per gli utenti e i prestatori di servizi di pagamento mediante l'adozione di requisiti efficaci basati sul rischio; assicurare la sicurezza dei fondi e dei dati personali degli utenti; garantire un'equa concorrenza tra i prestatori di servizi di pagamento; assicurare la neutralità dei modelli tecnologici; permettere lo sviluppo di mezzi di pagamento accessibili e innovativi. La regolamentazione della PSD2 è basata sul criterio della "neutralità tecnologica": vengono fissati alcuni principi da rispettare attraverso la standardizzazione ed indicati una serie di obiettivi da raggiungere nell'esecuzione dell'operazione di pagamento[68].

È stato il Regolamento delegato (UE) 2018/389 della Commissione del 27 novembre 2017 a definire tutti i requisiti degli standard aperti che si devono rispettare per assicurare comunicazioni sicure ai fini dell'identificazione, dell'autenticazione, della notifica, della trasmissione di informazioni e dell'attuazione delle misure di sicurezza, tra i prestatori di servizi di pagamento di radicamento del conto, i prestatori di servizi di disposizione di ordine di pagamento, di informazione sui conti, i pagatori, i beneficiari ed altri[69]. L'interoperabilità tra i diversi sistemi è utilizzata per garantire la diffusione degli strumenti di pagamento elettronico tra pagatori, beneficiari e relativi prestatori di servizi di pagamento; gli standard tecnici danno la possibilità all'industria di svilupparsi ed innovarsi tramite l'utilizzo della tecnologia avanzata.

Il Regolamento citato ribadisce l'obbligo[70], per i prestatori di servizi di pagamento, di applicare l'autenticazione forte del cliente in tre casi: quando il pagatore accede al conto del cliente online; quando dispone un'operazione di pagamento elettronico; quando effettua azioni a distanza con il rischio di frode nei pagamenti. Questo provvedimento disciplina ed individua anche alcune fattispecie che sono

---

una maggiore integrazione del mercato dei pagamenti al dettaglio: raggiunto il compromesso sul testo della proposta di direttiva sui pagamenti elettronici (c.d. PSD 2), in *Eurojus*, 14 settembre 2015.

[68] Sul tema della neutralità tecnologica v. Strumenti di pagamento innovativi, interoperabilità e neutralità tecnologica: quali regole e quale governance per un mercato sicuro, efficiente ed innovativo, in *Riv. trim. diritto dell'economia*, 2016, 61 secondo il quale "neutralità tecnologica è sinonimo del termine "standard di prestazione", che sono gli standard che descrivono il risultato previsto, ma non impongono una data tecnologia. Neutralità tecnologica significa, dunque, che i regolatori dovrebbero astenersi dall'usare la regolazione come mezzo per strutturare il mercato in un certo modo. In un mercato altamente competitivo, i regolatori dovrebbero impegnarsi a non scegliere i "vincitori tecnologici".

[69] Come precisato nei Considerando 29 e 30 del regolamento delegato della Commissione, esso si basa sul progetto di norme tecniche di regolamentazione che l'European Banking Authority (come previsto dall'art. 98, par. 4, comma primo, PSD2) ha presentato alla Commissione dopo aver svolto consultazioni pubbliche aperte e trasparenti sul progetto presentato, aver analizzato i potenziali costi e benefici della disciplina e richiesto il parere del gruppo delle parti interessate nel settore bancario, istituito dall'art. 37 del regolamento (UE) n. 1093/2010.

[70] Previsto già dall'art. 97, comma 1, PSD2; V. Meli, *Gli interventi dell'Autorità nei sistemi di pagamento, Relazione al Convegno Antitrust di Trento*, 16-18 ottobre 2015.

esenti dall'autenticazione forte: si tratta di casi che, in basi ad alcuni parametri[71], sono considerati a basso rischio di frode; è il prestatore, in presenza di tali fattispecie, a dover effettuare una valutazione del grado di rischio che in concreto potrebbe interessare l'operazione[72] utilizzando degli indici enunciati dal legislatore comunitario e precisamente nell'art. 18 del Regolamento di attuazione 2018/389/UE.

I prestatori di servizi, per applicare questi regimi di esenzione sono tenuti a monitorare tutte le operazioni (attraverso specifici meccanismi e avvalendosi anche qui di numerosi indici indicati nel Regolamento medesimo[73]) al fine di captare le attività di pagamento poste in essere senza autorizzazione o in maniera fraudolenta. Dopodiché gli stessi devono adempiere all'obbligo di trasmettere i dati rilevati alle autorità competenti e all'EBA. Questo continuo controllo dei dati di pagamento permette da un lato, una concreta valutazione del rischio di sicurezza relativo all'istituto di pagamento per l'applicazione di adeguate misure preventive di sicurezza; dall'altro, di captare i campanelli di allarme di eventuali disfunzioni generalizzare che possono essere evitate attuando un aggiornamento e integrazione della disciplina relativa alle misure di sicurezza che sono risultate inadeguate a prevenire il compimento di illeciti[74].

Il Regolamento (UE) 2018/389 ha fissato anche i requisiti dell'interfaccia informatica necessari per i prestatori di servizi di pagamento di radicamento del conto online per permettere ai nuovi IP di accedere ai conti dall'esterno. Secondo l'art. 30, par. 1 e 2, questo tipo di interoperabilità deve consentire l'identificazione del TPP, deve permettere al prestatore di servizi di informazione sui conti e al prestatore di servizi di disposizione di ordine di pagamento di comunicare con il PSP di radicamento del conto in maniera sicura e di disporre gli ordini di pagamento e ricevere tutte le informazioni accessibili ai prestatori di servizi di pagamento di radicamento del conto sull'esecuzione dell'operazione di pagamento[75].

---

[71] Ossia in relazione alla tipologia di operazione, alle modalità con le quali la stessa è compiuta, ai beneficiari del pagamento o all'importo dell'operazione; v. M. Mancini, *Commento all'art. 1, comma 1, lettere q e s,* in *La nuova disciplina dei servizi di pagamento*, a cura di M. Mancini, M. Rispoli Farina, V. Santoro, A. Sciarrone Alibrandi e O. Troiano, Torino, 2011, 26 ss.

[72] C.d. *targeted authentication*.

[73] Ad es.: l'essere il pagamento in presenza o a distanza; in base al valore medio delle operazioni; con autenticazione forte o esenzione; C. Brescia Morra, *Il diritto delle banche,* Milano, 2016, 83 ss.

[74] G. Berti De Marinis, *La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD2*, in *Diritto della borsa e del mercato finanziario*, 2018, 4, 649 ss.

[75] La struttura informatica utilizzata per il dialogo con i TPPs deve avere lo stesso livello di disponibilità e di prestazione delle interfacce messe a disposizione dell'utente per accedere direttamente al proprio conto online. Condotte di ostacolo possono essere ravvisate ad esempio quando si impedisce l'utilizzo da parte dei TPPs delle credenziali rilasciate dai prestatori di servizi di pagamento di radicamento del conto ai loro clienti; per un ulteriore approfondimento v. Valcke, N. Vandezande, N. Van deVelde, *The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4*, in *Swift institute working paperno*. 2015-001, 2015, 45 ss.

Gli *Account servicing payment service providers* (ASPSPs) ossia i prestatori di radicamento del conto devono predisporre misure di emergenza nel caso in cui vi sia una indisponibilità non programmata dell'interfaccia o in caso di guasto dei sistemi[76] (art. 33, Reg. Cit.): i TPPs possono così anche accedere alla stessa interfaccia messa a disposizione dei clienti in caso di prestazioni inadeguate da parte di quella per loro predisposta. Si tratta di una modalità che viene definita una *fallback option.* Secondo l'art. 33, par. 6 del Regolamento citato, le Autorità nazionali, previa consultazione con l'EBA, possono esentare gli ASPSPs dal dotarsi di queste misure di emergenza se le interfacce rispettano alcune condizioni indicate nello stesso articolo[77]. Per garantire un'applicazione uniforme di questi criteri fissati nell'art. 33, par. 6 del Regolamento, l'EBA ha poi elaborato le *Guidelines on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of Regulation (EU) 2018/89.*

Altra modalità di accesso al conto del pagatore è quella indiretta[78], che consente l'autenticazione e la comunicazione con il prestatore di servizi di pagamento di radicamento del conto: i prestatori che gestiscono il conto di pagamento possono consentire agli istituti che svolgono i nuovi servizi, di utilizzare le interfacce disponibili all'accesso online da parte dei titolari dei conti[79]. Le parti osservano tecniche di crittografia avanzate per assicurare la tutela della riservatezza dei dati durante lo scambio degli stessi via web[80]. Attraverso ciò si è voluta garantire la sicurezza dei fondi e dei dati di pagamento che vengono minacciati da condotte di frode informatica[81]. La disciplina nazionale che ha recepito la Direttiva PSD2 fa un rinvio alle norme tecniche di regolamentazione adottate dalla Commissione europea[82] al fine di individuare i metodi per attuare una comunicazione sicura: a tali norme soggiacciono sia i prestatori di servizi di pagamento di radicamento del conto, sia i prestatori di servizi di disposizione di ordine di pagamento e di informazione sui conti. L'art. 6-*bis* del d.lgs. n. 11/2020 ha previsto anche l'introduzione di alcuni limiti all'accesso ai conti di pagamento da parte dei terzi prestatori di servizi di pagamento: il prestatore di servizi di pagamento di radica-

[76] Art. 33 Regolamento UE.

[77] Ad esempio, è prevista la sperimentazione sul campo per almeno tre mesi.

[78] Si veda il Considerando n. 32 del Regolamento; KPMG, PSD2: a game changer?, ottobre 2018.

[79] Art. 31 Regolamento UE.

[80] Ogni sessione di comunicazione deve avere una durata breve; v. C. Schena, A. Tanda, C. Arlotta, G. Potenza, *Lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, Consob, 2018; F. Fiordelisi, P. Schwizer, M.G. Soana, *The determinants of reputational risk in the banking sector*, in *Journal of Banking and Finance,* 2013, 1359-1371.

[81] A ciò si ricollega anche l'esigenza di monitorare il malfunzionamento dei sistemi operativi dei vari istituti in funzione preventiva del compimento dell'illecito; C. Schena, A. Tanda, C. Arlotta, G. Potenza, *Lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, Consob, 2018.

[82] artt. 5-*ter*, comma 2, lett. d), e comma 3, lett. a), nonché art. 5-*quater*, comma 2, lett. c), e comma 3, lett. a), d.lgs. n. 11/2010.

mento del conto può rifiutare l'accesso soltanto in presenza di giustificate ragioni relative all'accesso fraudolento o non autorizzato al conto di pagamento da parte dei prestatori di servizi di informazione sui conti o di disposizione di ordine di pagamento[83], anche in caso di ordini di pagamento fraudolenti o non autorizzati. In tali circostanze, il prestatore di radicamento del conto deve, prima di inoltrare il rifiuto, informare i TPPs, dando atto dei motivi che hanno condotto al rifiuto (salvo che si tratti di motivi legati all'ordine pubblico o di pubblica sicurezza[84] o altri connessi all'applicazione delle disposizioni in materia di riciclaggio e finanziamento del terrorismo). Il diniego di accesso al conto così corredato deve essere immediatamente comunicato anche alla Banca d'Italia, competente ad effettuare le sue valutazioni e ad adottare tutte le misure che ritiene opportune[85].

6. *La disciplina del consenso per l'esecuzione delle operazioni di pagamento*

L'accesso ai conti si verifica per i *TTPs* previo un esplicito consenso del pagatore, o dell'utente in caso di servizio di informazione sui conti, a svolgere i nuovi servizi di pagamento[86]: ciò può avvenire (e avviene il più delle volte) attraverso dispositivi informatici, data appunto la natura informatica dell'attività e delle modalità con cui tali soggetti interagiscono con gli utenti[87]. Al fine di stabilire le modalità attraverso cui il consenso per l'esecuzione della singola operazione di pagamento deve essere prestato, si prevede l'introduzione di queste nel contratto quadro che regola lo svolgimento del servizio. Nel dettaglio, il consenso esplicito deve riguardare: l'importo del pagamento, il beneficiario dello stesso, ogni dato relativo all'operazione e la disponibilità a fornire al beneficiario qualunque informazione ottenuta nella prestazione del servizio di disposizione di ordine di pagamento[88]. L'art. 62, comma 2, PSD2, dispone che «il consenso ad eseguire un'operazione di pagamento può anche essere prestato tramite … il prestato-

[83] Compresi i casi di ordini di pagamento fraudolenti o non autorizzati.

[84] M. Catenacci, C. Fornasaro, *PSD2: i prestatori di servizi d'informazione sui conti (AISPS*), in *Dir. Banc.*, 2018, 4, 37 ss.; V. Profeta, *I Third Party Providers: profili soggettivi ed oggettivi*, in F. Maimeri, M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale, Quaderni di ricerca giuridica della Banca d'Italia,* n. 87, Settembre 2019, 53 ss.

[85] Art. 6-*bis*, comma 2, d.lgs. n. 10/2011.

[86] Artt. 5-*ter*, comma 2, lett. c), e 5-*quater*, comma 2, lett. a), d.lgs. n. 11/2010; V. Profeta, *I Third Party Providers: profili soggettivi ed oggettivi*, in F. Maimeri, M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale, Quaderni di ricerca giuridica della Banca d'Italia*, n. 87, Settembre 2019, 69 ss.

[87] Per un'analisi della disciplina della responsabilità degli intermediari per l'esecuzione del pagamento in assenza del consenso dell'utente e per la mancata, inesatta o tardiva esecuzione dell'operazione v. la già ricordata monografia di F. Marasà, *Servizi di pagamento e responsabilità degli intermediari*, cit.

[88] I dati non possono essere modificati dal prestatore che dispone l'ordine.

re di servizi di disposizione di ordine di pagamento»: in questo caso, il prestatore di servizi di pagamento di radicamento del conto non dovrà richiedere altre verifiche circa il consenso dato dagli utenti ai prestatori disponenti l'ordine di pagamento e a quelli che svolgono il servizio di informazione sui conti[89]. Il prestatore di radicamento del conto è tenuto a presumere, per via dell'autenticazione e della presenza di credenziali di accesso al conto, che il TTP agisca sulla base dell'esplicito consenso del cliente, senza dovere svolgere indagini e verifiche sulla relazione contrattuale tra quest'ultimo e il cliente.

L'art. 6-*bis*, comma 1, d.lgs. n. 11/2010 prevede che l'accesso al conto può essere rifiutato in virtù del fatto che l'ordine di pagamento non venga autorizzato dal titolare del conto (circostanza della quale ne è a conoscenza il gestore del conto); ciò si realizza nel momento in cui l'utente, propenso a revocare il consenso alla prestazione dei TTPs, ne informa il prestatore del radicamento del conto, il quale a sua volta da comunicazione della revoca al Terzo Provider[90]. Le ipotesi di accesso non autorizzato al conto, con possibilità di determinare un legittimo rifiuto di colloquio da parte del prestatore di radicamento del conto, vengono assimilate, dallo stesso art. 6-*bis*, alle ipotesi di ordini di pagamento fraudolenti o non autorizzati[91]. La disciplina nazionale dispone che il consenso di cui si parla, può essere revocato in qualsiasi momento, attraverso la procedura concordata nel contratto quadro generale o in quello relativo a singole operazioni di pagamento, ma ciò deve avvenire prima che l'ordine di pagamento diventi irrevocabile ai sensi dell'art. 17 del d.lgs. n. 11/20103 [92]. Quest'ultimo, modificato dal recepimento della Direttiva PSD2, statuisce che il pagatore non può revocare l'ordine di pagamento dopo aver prestato il proprio consenso a disporre l'operazione di pagamento al prestatore di servizi di disposizione di ordine di pagamento e, ancora, che, decorsi i termini previsti dalla legge, l'ordine di pagamento può essere revocato solo se la revoca è stata concordata dal cliente con tutti i prestatori di servizi coinvolti nell'operazione[93]. Infine, se l'utente ha richiesto l'aiuto di un prestatore di servizi di disposizione d'ordine di pagamento, occorrerà, oltre ad una "negoziazione" della revoca con il prestatore di radicamento del conto, anche il consenso del *Payment Initiation Service Provider*[94]. Tutte le operazioni di paga-

[89] Art. 32, comma 3, reg. delegato (UE) n. 2018/389.

[90] Art. 6-*bis*, comma 3, d.lgs. n. 10/2011; M.M. Pimpinella, G. Carrafiello, *L'evoluzione normativo-regolamentare nel settore dei pagamenti*, Milano, 2016, 10 ss.

[91] L'individuazione di questi comporta un'attenta valutazione delle ipotesi in cui il consenso all'operazione di pagamento correttamente prestato sia stato successivamente revocato dall'utente; M. Rispoli Farina, *Informazione e servizi di pagamento, in Analisi Giuridica dell'Economia*, 2015, 175-200.

[92] Art. 5, comma 4, d.lgs. n. 11/2010.

[93] Art. 17, comma 2, d.lgs. n. 11/2010; V. Antoro, *I conti di pagamento degli istituti di pagamento,* in *Giur. comm.*, 2008, 84 ss.; Aa.Vv., *FINTECH. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari,* a cura di Paracampo, Torino, 2017, 83 ss.

[94] Art. 17, comma 5, d.lgs. n. 11/2010.

mento che vengono realizzate dopo la revoca del consenso prestato, sono ritenute non autorizzate con conseguente impossibilità per il TTP di accedere al conto.

7. *Le novità in materia di responsabilità dei prestatori di servizi di pagamento*

Alla luce dei mutamenti operati con la Direttiva 2366/2015 (PSD2), ci si chiede se possono rilevarsi cambiamenti in relazione al regime della responsabilità civile dei prestatori di servizi di pagamento. In realtà, la Direttiva PSD2 ha confermato il regime di responsabilità gravante sui prestatori, contenuto dapprima nel d.lgs. n. 11/2010 e successivamente modificato ed integrato dal d.lgs. n. 218/2017[95]. In particolare, gli artt. 10 e 11 del d.lgs. n. 11/2010, in origine delineavano i profili di una responsabilità dei prestatori di servizi di pagamento: secondo tali disposizioni, queste avevano l'obbligo di assicurarsi che tutti i dispositivi personalizzati forniti alla clientela non fossero mai accessibili a soggetti diversi dal loro legittimo titolare. Ancora, era previsto, in caso di disconoscimento dell'operazione da parte dell'autore, un rimborso immediato a favore dell'utilizzatore di questi servizi, tranne che nel caso in cui vi fosse stato un sospetto motivato di frode e fatta salva la possibilità per l'intermediario, di dimostrare successivamente che non era previsto alcun diritto al rimborso per l'utilizzatore[96].

L'originario art. 10 prevedeva un onere della prova in capo al prestatore: qualora l'utilizzatore dei servizi di pagamento negasse di aver dato l'autorizzazione per un'operazione già eseguita, ovvero sostenesse che la stessa era stata eseguita in maniera scorretta, era dunque onere del prestatore stesso provare l'esito positivo dell'operazione. Allo stesso modo, l'utilizzo di uno strumento di pagamento offerto dall'intermediario non rendeva automaticamente legittima l'operazione in parola e non dimostrava che il cliente avesse agito con frode o che questi non avesse adempiuto agli obblighi di utilizzo conforme degli strumenti da lui posseduti, con dolo o colpa grave[97].

Il d.lgs. n. 218/2017, di attuazione della direttiva PSD2, rafforza ancora di più quell'onere della prova gravante sui soggetti intermediari: l'art. 10 del d.lgs. n. 11/2010, così come modificato, sancisce infatti che è onere del prestatore dei servi-

[95] Per un approfondimento v. I.A. Caggiano, *Pagamenti non autorizzati tra responsabilità e restituzioni. Una rilettura del d.lgs. 11/2010 e lo scenario delle nuove tecnologie*, in *Riv. Dir. Civ.,* 2016, 2, 2938 ss.

[96] R. Frau, *Operazioni di home banking disconosciute dal correntista e responsabilità semioggettiva della banca,* in *Responsabilità civile e previdenza*, 2017, 3, 855 ss.; P. Montella, *L'autenticazione ad accesso forte (Strong customer Authentication) e la responsabilità del Prestatore del servizio di pagamento alla luce delle modifiche al d.lgs. n. 11 del 27 dicembre 2010,* in *De Iustitia*, 124 ss.

[97] P. Montella, *La Direttiva PSD2: obiettivi della revisione e principali tratti di novità*, in *Innovazione e diritto*, 129 ss.

zi di pagamento, compreso il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente, al fine di far pagare a quest'ultimo il prezzo di un'operazione non autorizzata[98]. Anche l'art. 11 ha subito dei cambiamenti conseguentemente al recepimento della Direttiva PSD2: questo attualmente non si limita più a prevedere in maniera generica un obbligo del rimborso dei fondi illecitamente sottratti all'utente, ma ne puntualizza determinati aspetti: il rimborso dovrà avvenire entro il giorno in cui si è svolta l'operazione o entro quello successivo. Si ribadisce la possibilità per il prestatore di servizi che deve effettuare il rimborso di dimostrare che l'operazione a questi impartita è avvenuta su disposizione del cliente intestatario dei fondi, con diritto alla ripetizione delle somme già elargite[99]. Mentre nel previgente sistema l'utilizzatore del servizio di pagamento in caso di utilizzo illecito dello strumento in suo possesso, era sottoposto esclusivamente ad una franchigia di un importo pari a 150 euro, per le operazioni poste in essere prima della comunicazione del furto o dello smarrimento dello strumento al prestatore del servizio di pagamento, con la nuova Direttiva PSD2 che ha introdotto la *Strong Customer Authentication*[100], all'utilizzatore resta comunque il diritto alla restituzione integrale dell'importo che gli è stato addebitato senza autorizzazione, allorquando il prestatore di pagamenti non abbia adempiuto all'obbligo di esigere un'autenticazione forte del cliente. In tal caso, anche il soggetto beneficiario del pagamento dovrà rispondere dell'indebito utilizzo dello strumento qualora non abbia adempiuto all'obbligo di richiedere l'autenticazione forte del pagatore. Negli altri casi, (esclusi quelli in cui abbia agito fraudolentemente o in cui non abbia adempiuto gli obblighi di cui all'art. 7 del d.lgs. n. 11/2010 con dolo o colpa grave) il pagatore può sopportare, perdite relative ad operazioni di pagamento che non siano state autorizzate derivanti dall'indebito utilizzo dello strumento di pagamento a seguito di furto, appropriazione indebita o smarrimento, per una somma non superiore a 50 euro[101].

Alla luce di ciò, la colonna portante della garanzia costituita da un sistema di accesso forte, sarebbe la difficoltà consistente nella violazione di un tale sistema, per effetto del quale il legislatore nazionale, sulle linee di quanto stabilito dalla normativa europea, ha previsto a carico del prestatore, il rimborso immediato e

[98] *Si vedano M. Rispoli Farina, Informazione e servizi di pagamento, in Analisi* giuridica dell'economia, I, 2015, 175 ss.; G. Gabassi, S. Langer, *Obblighi informativi nel settore sei servizi di pagamento. Considerazioni diatopiche tra diritto nazionale italiano e austriaco e diacroniche tra PSD e PSD2*, in *Contratto e Impresa*, 2018, 2, 650 ss.

[99] C. Corvese, G. Gimigliano (a cura di), *Profili interdisciplinari del commercio elettronico*, Siena, 2016, 37 ss.

[100] Si vedano G. Casali, *I contratti del software: qualificazione, responsabilità e garanzie*, *in I Contratti*, vol. IV, 2014, 389 ss.; R. Frau, *Operazioni di home banking disconosciute dal correntista e responsabilità* semioggettiva della banca, in *Responsabilità civile e previdenza*, vol. 3, 2017, 855 ss.

[101] Circa la dottrina in materia che ha cercato di tratteggiare con maggior precisione "la diligenza del buon banchiere", v. G. Ferri, *La diligenza del buon banchiere*, in *Banca, Borsa e Titoli di credito*, vol. I, 1958, 1 ss.

integrale da aversi «[…] in ogni caso al più tardi entro la fine della giornata operativa successiva a quella in cui prende atto dell'operazione o riceve una comunicazione in merito. Ove per l'esecuzione dell'operazione sia stato addebitato un conto di pagamento, il prestatore di servizi di pagamento riporta il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo, assicurando che la data valuta dell'accredito non sia successiva a quella dell'addebito dell'importo»[102]: nel caso di violazione anche di tali procedure sul pagatore non graverà alcuna perdita. Si evidenzia a questo punto come, dato l'obbligo per coloro che offrono servizi di pagamento di utilizzare per la loro attività interfacce web che permettano un'autenticazione forte del cliente, sia divenuto di gran lunga più facile per l'utilizzatore di tali strumenti ottenere il rimborso delle somme che gli sono stata sottratte illecitamente[103].

La responsabilità del prestatore del servizio così come quella di altri soggetti, quali i prestatori del servizio di radicamento del conto o di coloro che forniscono informazioni collegate al servizio reso, è diventata dunque, con la nuova Direttiva PSD2, di tipo oggettivo a causa della difficoltà per i soggetti menzionati di fornire la prova di un eventuale dolo o colpa grave in capo all'utilizzatore.

8. *Il ruolo delle banche nel nuovo mercato dei pagamenti*

A fronte dei significativi cambiamenti che hanno interessato il mercato dei pagamenti, è opportuno fare qualche considerazione sugli attori principali del settore, ossia le banche.

Queste, con l'entrata in vigore della PSD2, si sono trovati, il più delle volte, a far i conti con il rischio di "disintermediazione", con conseguente perdita di una relazione privilegiata di lunga data e una progressiva compromissione della capacità di preservare un'efficace relazione con il cliente[104]. È indubbio poi che l'emergenza sanitaria ha accelerato la trasformazione digitale del settore bancario e di conseguenza anche del modo in cui i clienti interagiscono con le banche, spingendo anche coloro più legati ai servizi tradizionali ad aprirsi al Fintech[105].

---

[102] Art. 11, d.lgs. 11/2010; M. Doria, V. Fucile, A. Tarola*, La sorveglianza sui sistemi di pagamento,* in *Quad. Giuri. Comm.,* a cura di Carriero e Santoro, 2005, 83 ss.

[103] Si vedano G. Berti De Marinis., *La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD2,* in *Diritto della banca e del mercato finanziario*, vol. 4, 2018, 639 ss.; V. Coppola*, Il contratto di servizi di pagamento: inquadramento generale e profili di responsabilità*, in *Innovazione e Diritto,* Napoli, 2014, 3, 38 ss.

[104] *Per una comparazione v. R. Barontini, Innovazione e rischio di credito durante la crisi finanziaria, in Bancaria*, 2015, 2, 83 ss.

[105] Si veda EDP, *L'impatto del COVID-19 sul mondo delle banche e dei pagamenti,* 2021 su https://www.lineaed it/news/51068/limpatto-del-covid-19-sul-mondo-delle-banche-e-dei pagamenti/.

Le banche, dinanzi a questi cambiamenti, tendono sempre di più ad adottare un approccio basato sui vantaggi offerti dalle novità introdotte dalla PSD2: mediante una collaborazione diretta con i TPPs e Fintech, queste avranno la possibilità di rafforzare i processi di fidelizzazione della clientela mediante l'introduzione nella loro offerta, di servizi che sarebbero difficili da costruire al loro interno o che non sarebbero applicabili a tutti i clienti[106].

In tal senso, la PSD2 ha dato la possibilità di ridefinire il concetto di *customer experience* in linea con le nuove esigenze dei clienti, fulcro della competitività delle banche, le quali sono state indotte ad elaborare un nuovo posizionamento strategico nel mercato, partendo dal porre in essere una serie di comportamenti[107]. Una certa attenzione è stata data all'individuazione dei margini prodotti, alla stima dei ricavi aggiuntivi che derivano dall'utilizzo di informazioni circa il comportamento della clientela per indirizzare offerte di servizi a valore aggiunto, all'ottimizzazione dei modelli di *pricing*, alla valutazione delle opportunità di crescita derivanti dal funzionamento del business e all'individuazione del livello di innovazione che si intende introdurre nella propria organizzazione[108]. Per comprendere i possibili posizionamenti di mercato, occorre considerare due elementi, in grado di influenzare in maniera significativa lo sviluppo dei ricavi commissionali: lo sviluppo di servizi a valore aggiunto e l'apertura dei dati e la data *monetisation,* che indicano rispettivamente il *quantum* di investimenti in innovazione e sviluppo dell'offerta che permette alle banche di differenziarsi dalla concorrenza e il grado di apertura degli operatori nella capacità di gestire informazioni comportamentali riferite alla clientela[109].

Dalla combinazione di questi due elementi è dunque possibile individuare quattro ruoli che le banche possono assumere nel nuovo contesto, ossia:

- il ruolo di *compliant player*, assunto dalle banche che considerano l'adeguamento alla PSD2 come un semplice obbligo di conformità al nuovo quadro normativo, concentrando tutti i loro investimenti nell'adeguamento delle procedure, dei processi e dei contratti, lasciando invariata la propria offerta e apportando eventuali modifiche solo in termini di *pricing;*

---

[106] A. Argentati, *Le banche nel nuovo scenario competitivo. FinTech, il paradigma Open banking e la minaccia delle big tech companies*, in *Mercato Concorrenza Regole*, 2018, 441 ss.; A. Berger, L. Klapper, R. Turk-Ariss, *Bank competition and financial stability*, in *Journal of Financial Services Research*, 2009, 849 ss.

[107] Si vedano S. Rossi, *Idee per il futuro del sistema finanziario italiano*, Intervento, Courmayeur, 23 settembre 2017; Banca Centrale Europea, *Guida alla valutazione delle domande di autorizzazione all'esercizio dell'attività bancaria degli enti creditizi fintec*h, marzo 2018, 3.

[108] V. Capriglione, A. Sacco Ginevri, *Metamorfosi della governance bancaria*, Torino, 2019, 85 ss.

[109] Maggiore sarà il quantitativo di informazioni disponibili, più facilmente si riuscirà a creare modelli di business innovativi e digitali; G. Gabbi, *Definizione, misurazione e gestione del rischio reputazionale negli intermediari finanziari,* in *Banca Impresa e Società*, 2004, 51-80.

- il ruolo di aggregatore, che permette agli operatori di configurarsi come soggetti abilitati ad integrare le informazioni ed attuare operazioni di pagamento a valere anche sui conti correnti della concorrenza e di porre in essere anche investimenti di carattere commerciale diretti a sviluppare nuovi servizi a valore aggiunto[110];
- il ruolo di piattaforma, che presuppone necessarie competenze specifiche in ambito tech, sicurezza e *analytics* ed in virtù del quale gli attori predispongono di un'adeguata capacità di investimento impiegata per lo più in infrastrutture informatiche e sicurezza per la creazione di un ambiente pienamente *compliant* al nuovo quadro normativo e fondato base strutturali innovative[111]. Lo sviluppo di questi modelli, che gestiscono anche i contenuti informativi dei pagamenti, permette di integrare l'offerta di servizi tradizionali di pagamento verso la propria clientela con servizi digitali, aprendo così il target anche ad altri operatori o banche[112];
- infine, il ruolo di aggregatore come piattaforma, che, assunto principalmente dagli operatori che si trovano a gestire grandi volumi di affari con una clientela significativa nel mercato di riferimento e trasversale e che utilizzano le proprie capacità di investimento in tecnologie e marketing, permette a questi soggetti di offrire servizi anche ad operatori minori in cerca di un *payment engine* "performante" e pienamente allineato alla normativa. Essenziali, in tal caso, sono i vantaggi che derivano dalla collaborazione diretta con le terze parti e con altri istituti finanziari e dalla condivisione di conoscenze e di tecnologie innovative con le stesse[113].

Dalla suddivisione effettuata emerge che, se l'operatore decidesse di andare oltre il semplice adeguamento alla PSD2, essenziale è l'interazione con i TPPs: in tal caso essenziali solo le *Application Programming Interfaces* (API), interfacce aperte che consentono di interagire con programmi altrimenti inaccessibili e che, offrendo concrete modalità per il miglioramento dei programmi e dei servizi offerti, favoriscono l'instaurazione di relazioni di collaborazione tra *players* nel mercato dei pagamenti, consentono alle banche di raggiungere mercati in nuove

[110] Gli aggregatori valutano spesso la possibilità di giungere a partnership con terze parti al fine di ridurre i costi di sviluppo e di innovazione; A. Sciarrone Alibrandi, *Le banche e il sistema dei pagamenti*, in A. Brozzetti (a cura di), *Riflessioni su banche e attività bancaria, immaginando il "futuribile". Atti del convegno «Banche e attività bancaria nel TUB: qualche riflessione su un ventennio di regolamentazione, immaginando il "futuribile" (per dirla con Franco Belli)»* tenutosi a Siena il 19-20 settembre 2014, Milano, 2015.

[111] C.d. open ABI.

[112] M. Porzio, *La disciplina generale dei contratti bancari*, in C. Angelici, F. Belli, G.L. Greco, M. Porzio, M. Rispoli Farina (a cura di), *I contratti delle banche*, Torino, 2003, 77 ss.

[113] A. Antonucci, *Mercati dei pagamenti: le dimensioni del digitale*, in *Riv. dir. banc., www.dirittobancario.it*, 18, 2018; A. Sciarrone Alibrandi, *Il diritto del sistema finanziario*, in Aa.Vv., *Diritto commerciale*, a cura di M. Cian, Torino, 2013, 319 ss.

porzioni geografiche e permettono la personalizzazione dei prodotti e servizi in base alle specifiche esigenze dei clienti[114].

A seguito della nuova disciplina europea e nazionale sui pagamenti, le banche, mentre da un lato potrebbero decidere di limitarsi a rendere accessibili ai TPPs i conti dei propri clienti, dall'altro potrebbero optare per la conversione in piattaforma, garantendo oltre i servizi tradizionali, anche i servizi integrati prestati da soggetti terzi. Le banche sono così tenute a rendere semplice e celere l'offerta di servizi ai propri clienti: obiettivo della novella legislativa è appunto quello di innalzare, tramite un rinnovamento del business bancario, il livello della competitività tra i vari operatori del mercato dei pagamenti, a beneficio dei consumatori finali[115].

L'ingresso delle terze parti, autorizzate ad operare nel mercato dei pagamenti, e lo sviluppo di nuovi servizi comporta così il superamento dell'interfaccia di pagamento gestita solitamente dalla banca o dal provider di carte di pagamento, consentendo che l'esperienza del cliente venga gestita *end-to-end* dal retailer/operatore che vende i propri prodotti/servizi[116]. In questo senso non si esclude che gli Over the Top e quindi i grandi colossi del *marketing* e delle tecnologie di consumo come Facebook, Amazon, Google, possano sviluppare sempre di più le proprie piattaforme ed offrire ai pubblici servizi finanziari erogati dalle banche, arrivando a dominare così i nuovi servizi Fintech, dal momento che la loro impronta nel settore finanziario è in crescita[117].

9. *Gli ostacoli all'attività dei* Third Party Providers *e i chiarimenti dell'EBA*

La *European Banking Authority* (EBA) ha pubblicato il 4 giugno 2020 una prima *Opinion* volta a fornire chiarimenti in merito agli ostacoli che i prestatori di servizi di pagamento di radicamento del conto (banche, istituti di credito e isti-

[114] Nello specifico, le API permettono quindi lo scambio sicuro di dati tra diverse applicazioni e una connessione tra i conti degli utenti e le applicazioni dei TPPs. In questo modo gli AISP sono in grado di conoscere informazioni relative ai conti di pagamento detenuti dall'utente presso uno o più ASPSP, mentre i PISP possono disporre ordini di pagamento a valere sui conti detenuti presso uno o più ASPSP; ITASEC19, *Terza Conferenza Italiana sulla Cyber Security, Sicurezza, privacy, normative: come farli coesistere in ambito Fintech?, Intervento del Capo del Dipartimento Mercati e sistemi di pagamento della Banca d'Italia*, Paolo Marullo Reedtz, Pisa, 14 febbraio 2019.

[115] R. Frau, *Operazioni di home banking disconosciute dal correntista e responsabilità semioggettiva della banca,* in *Responsabilità civile e previdenza*, 2017, 3, 855 ss.

[116] A. Guaccero, *Automazione dei processi e dei servizi, imputazione e responsabilità,* in *Diritto del Fintech*, a cura di M. Cian e Sandei, Milano, 2020, 60 ss.

[117] Sulla promozione di pagamenti elettronici sicuri, efficienti e competitivi v. Libro verde della Commissione europea "*Verso un mercato europeo integrato dei pagamenti tramite carte, internet e telefono mobile" dell'11.1.2012; EBA, Discussion Paper on the EBA's approach to financial technology (FinTech*), 4 August 2017 su https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1919160/7a1b9cda-10ad-4315-91ce-d798230ebd84/EBA%20Discussion%20Paper%20on%20Fintech%20%28EBA-DP-2017-02%29.pdf?retry=1.

tuti di pagamenti (ASPSP) pongono all'offerta dei servizi informativi e di pagamento offerti dalle terze parti abilitate: tale documento dà indicazioni sulla corretta applicazione della regolamentazione tecnica di degli orientamenti EBA di attuazione delle disposizioni della PSD2 in materia di accesso ai conti. Si tratta di un parere redatto sulla base dei modelli operativi adottati in virtù della Direttiva PSD2 in questa sede analizzata e delle norme tecniche di regolamentazione sulla "*strong customer authentication"* (SCA) e sulla comunicazione comune e sicura (CSC) emanati in attuazione della Direttiva (RTS)[118].

In relazione al principale profilo innovativo della PSD2, riguardante appunto l'introduzione di due nuovi servizi e di due nuovi prestatori di sevizi di pagamento abilitati a prestare tali servizi, ovvero i TPP, il parere dell'EBA è intervenuto a chiarire meglio il contenuto dell'art. 32, paragrafo 3, degli RTS che prevede che gli ASPSP, che abbiano implementato un'interfaccia dedicata, debbano garantire che tale interfaccia non ostacoli la fornitura dei servizi da parte di PISP e AISP. Ciò al fine di rispondere a tutte le richieste provenienti dagli operatori in merito alla definizione di determinate pratiche di mercato come ostacoli alla fornitura dei servizi di pagamento medesimi[119].

Una prima analisi dell'EBA ha riguardato i casi in cui la pratica del reindirizzamento può essere vista come un ostacolo all'attività dei TPPs, in particolare dei PISPs, in uno scenario in cui il reindirizzamento stesso è l'unico metodo attraverso il quale gli utenti possono autenticarsi presso il proprio ASPSP.

Secondo l'Autorità, il reindirizzamento può rappresentare un ostacolo se implementato in modo da creare attriti nella *user experience* del cliente, rendendo l'accesso ai servizi dei TPPs più difficoltoso rispetto alla esecuzione normale dei pagamenti attraverso i canali propri dell'ASPSP. Per gli operatori del settore, tale pratica rappresenta un ostacolo per i TPPs, soprattutto per i pagamenti inizializzati dagli utenti presso i c.d. *point-of-sale*: l'autenticazione tramite l'interfaccia dell'ASPSP fa sì che il pagamento venga effettuato attraverso l'utilizzo di un web browser o di una App che reindirizzano l'utente sul sito web o sull'apposita App del proprio istituto di credito; si limita così la capacità dei TPP di organizzare nuove modalità di pagamento per i clienti e i PISP si trovano a competere con i soggetti emittenti di carte di pagamento solo con riferimento ai pagamenti online[120].

L'operatività di un *Payment Initiation Service Provider* presso un punto di vendita fisico richiederebbe agli ASPSP, di predisporre di meccanismi di auten-

[118] Regolamento Delegato (UE) 2018/389.

[119] Si fa riferimento esclusivamente a quegli ASPSP che, ai sensi del menzionato art. 31 degli RTS., hanno deciso di avvalersi della prima opzione qui indicata e, pertanto hanno provveduto alla predisposizione di un'interfaccia dedicata esclusivamente alla comunicazione con i TP

[120] 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).

ticazione insiti nello strumento di pagamento fornito agli utenti dai PISP[121]: sul punto l'EBA ha chiarito che gli ASPSP non sono obbligati ad implementare sistemi di autenticazione specifici volti a consentire pagamenti attraverso l'utilizzo dei servizi forniti dai PISP, predisponendo apposite procedure rispetto a quelle create per i pagamenti eseguiti presso il prestatore di radicamento del conto[122]. Nessun obbligo in tal senso è infatti previsto dalla PSD2 e dagli RTS. Un PISP ha il diritto di avviare le medesime transazioni che sono offerte dall'ASPSP ai propri utenti; un ASPSP, nel momento in cui si trovi ad offrire ai propri clienti la possibilità di effettuare pagamenti istantanei presso specifici point of sales, dovrebbe anche consentire ai clienti stessi l'avviamento di pagamenti istantanei (con gli stessi limiti d'importo) presso specifici *point-of-sales* utilizzando i servizi forniti dai PISP[123].

L'EBA ha poi chiarito che in quasi tutti gli scenari, un solo flusso di *Strong Customer Authentication* (SCA) sarebbe sufficiente affinché l'utente possa autenticarsi verso la propria banca quando utilizza i servizi di TPPs autorizzati. Secondo la disciplina contenuta nella PSD2, un utente, al fine di effettuare un bonifico attraverso l'utilizzo dell'internet banking o della mobile app del proprio istituto di credito, è tenuto ad introdurre due volte le proprie credenziali di autenticazione: la prima per accedere all'interfaccia operativa scelta, la seconda per disporre l'ordine di bonifico[124]. Nel momento in cui l'utente decida di effettuare un pagamento attraverso il servizio fornito da un PISP, se il PISP trasmette all'ASPSP tutte le informazioni necessarie per avviare il pagamento (numero di conto o l'IBAN del conto da addebitare), tale duplicazione, risulta essere per l'EBA un ostacolo all'operatività della terza parte, se l'ASPSP non dimostra che la richiesta è dettata da ragioni di sicurezza facilmente dimostrabili[125].

Diversa è la situazione nel caso in cui tutte le informazioni relative al conto di pagamento da addebitare non vengano trasmesse, al momento della richiesta di avvio del pagamento, all'ASPSP dal PISP: in tale circostanza è lo stesso utente che deve selezionare presso il proprio istituto di credito il conto da addebitare attraver-

[121] Ad esempio, tramite una mobile App; EBA, *Guidelines on the exemption from the contingency mechanism under the RTS on SCA and CSC*, pubblicate il 4 dicembre 2018.

[122] R. Frau, *Operazioni di home banking disconosciute dal correntista e responsabilità semioggettiva della banca,* in *Responsabilità civile e previdenza*, 2017, 3, 855 ss.; V. Profeta*, I Third Party Providers: profili soggettivi ed oggettivi*, in F. Maimeri, M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale, Quaderni di ricerca giuridica della Banca d'Italia*, n. 87, Settembre 2019, 55 ss.

[123] A. Di Giorgio, B. Mascagni, *PSD2: gli ostacoli all'operatività dei TPPs alla luce dei chiarimenti dell'EBA*, in *www.dirittobancario.it*, 2020.

[124] art. 97, paragrafo 1, lett. a), b) e c) della PSD2 il quale 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 online; 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 abus*i".

[125] A. Vivoli, *PSD2 a che punto siamo? Capire dove si annida l'inefficienza*, in *www.riskcompliance.it*, 2020.

so una transazione effettuata tramite l'utilizzo di un PISP; pertanto la richiesta di due autenticazioni, una per accedere all'elenco dei conti di pagamento e l'altro per autenticare il pagamento stesso, non costituisce ostacolo censurabile[126]. La problematica che emerge in questo contesto è un'altra, e riguarda in particolare la pratica secondo la quale, al fine di utilizzare i servizi forniti dalle terze parti, all'utente venga chiesto di inserire il proprio IBAN. Nella sua *Opinion* l'EBA riconosce tale pratica come un impedimento censurabile nel caso di TPPs autorizzati alla prestazione del servizio di accesso ai conti e accordati, a cura dell'utente, all'accesso delle informazioni relative a tutti i conti dallo stesso detenuti presso uno o più istituti di credito; il TPP può così inviare all'ASPSP un'apposita richiesta per l'accesso al conto o per l'avvio del pagamento, con tutti i dettagli del conto medesimo.

Diversa ancora, è la situazione dei PISP autorizzati esclusivamente al servizio di disposizione di ordini di pagamento: ai sensi della Direttiva, un PISP non è autorizzato ad accedere all'elenco di tutti i conti di pagamento dell'utente. L'ASPSP ha l'obbligo di comunicare al PISP l'IBAN del conto da addebitare, se quest'ultimo non lo comunica all'ASPSP e l'utente deve selezionarlo in maniera manuale dall'interfaccia dell'istituto di credito[127].

In relazione alla richiesta di autenticazione nell'ambito del servizio di accesso ai conti, si ricordi che la normativa della PSD2 prevede l'applicazione delle procedure di SCA quando un utente accede al proprio conto o ai propri conti di pagamento online, sia attraverso le interfacce messe a disposizione dagli istituti di credito di radicamento del conto, sia tramite un AISP. Se l'utente si avvale di un AISP e attraverso la relativa interfaccia può visualizzare solo una serie limitata di dati, l'art. 10 degli RTS prevede un'esenzione dall'obbligo di applicare la SCA per ogni accesso. Nonostante ciò, si richiede l'applicazione della *Strong Customer Authentication* almeno ogni 90 giorni per permettere all'utente di rinnovare la propria scelta di avvalersi del servizio di accesso ai conti e permettere agli AISP di visualizzare le informazioni[128].

Secondo alcuni operatori del mercato, l'obbligo di riautenticazione da parte degli utenti ogni 90 giorni, avrebbe potuto incidere negativamente sul servizio promosso dagli AISP, come nel caso di utilizzo da parte di utenti che possiedono più conti di pagamento presso istituti di credito diversi; l'utente deve auten-

[126] V. Profeta, *I Third Party Providers: profili soggettivi ed oggettivi*, in F. Maimeri, M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale, Quaderni di ricerca giuridica della Banca d'Italia*, n. 87, Settembre 2019, 60 ss.

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

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

ticarsi presso ciascun ASPSP per permettere all'AISP di accedere ai dati di tutti i conti selezionati[129].

A tal riguardo, l'EBA nel parere in oggetto si è pronunciata stabilendo che la riautenticazione ogni 90 giorni, non è affatto un ostacolo ma un punto di equilibrio tra le finalità di agevolazione della concorrenza perseguite dalla PSD2 e la facilità d'utilizzo dei servizi dei TPPs da parte dei consumatori. Per l'EBA, le autorità competenti di ciascun Stato Membro debbono incoraggiare i prestatori di servizi di pagamento di radicamento del conto ad avvalersi dell'esenzione ex art. 10, permettendo così un accesso continuato agli AISP per un periodo di 90 giorni, prima di richiedere una nuova autenticazione all'utente: ciò al fine di evitare eventuali complicazioni per gli utenti stessi in relazione all'uso delle applicazioni degli AISP[130].

Per l'Autorità gli ASPSP e non i TTPs hanno l'obbligo di provvedere all'esecuzione da parte degli utenti delle procedure di autenticazione forte; le terze parti però possono essere delegate a procedere in tal senso attraverso appositi accordi di esternalizzazione conformi alla normativa applicabile.

Ultimo aspetto toccato dall'EBA nella sua *Opinion* del 4 giugno 2020 è quello relativo ai controlli aggiuntivi sul consenso, questione tra le più dibattute sin dal momento della pubblicazione della PSD2. Gli istituti di credito operanti sul mercato, infatti, si sono chiesti se fosse possibile proporre ai propri utenti un unico consenso iniziale e generale rispetto all'utilizzo dei servizi offerti dalle terze parti. Secondo l'art. 32, paragrafo 3, degli RTS la richiesta di "*ulteriori verifiche del consenso dato dagli utenti dei servizi di pagamento ai PISP e agli AISP*" sarebbe un potenziale ostacolo all'operatività dei TPP. Con un precedente parere sull'attuazione dell'RTS l'EBA, ha già chiarito che l'obbligo dei TPPs è diretto a garantire l'ottenimento del consenso esplicito da parte degli utenti secondo quanto previsto dall'art. 66, paragrafo 2 e, dell'art. 67, paragrafo 2, lett. a), della PSD2; gli ASPSP non devono verificare il consenso dato dagli utenti ai PISP e agli AISP e viene messo in evidenza che, anche un consenso generale richiesto dagli ASPSP agli utenti *ex ante*, è da considerarsi un ostacolo ai sensi dell'art. 32, paragrafo 3, degli RTS[131].

Per l'Authority, i termini e le condizioni contrattuali che gli ASPSP propongono alla propria clientela «non dovrebbero contenere disposizioni che rendano più difficile, in qualsiasi modo, l'utilizzo dei servizi di pagamento di altri presta-

[129] A. Di Giorgio, B. Mascagni, *PSD2: gli ostacoli all'operatività dei TPP alla luce dei chiarimenti dell'EBA,* in *www.dirittobancario.it*, 2020.

[130] A. Vivoli, *PSD2 a che punto siamo? Capire dove si annida l'inefficienza*, www.riskcompliance.it, 2020; D. Girompini, *PSD2 e Open Banking. Nuovi modelli di business e ruolo delle banche*, in Bancaria, 2018, fasc. 1, 70 ss.

[131] A. Vivoli, *PSD2 a che punto siamo? Capire dove si annida l'inefficienza,* in *www.riskcompliance.it*, 2020.

tori di servizi di pagamento autorizzati o registrati ai sensi della Direttiva»[132]. Il prestatore di servizi di pagamento di radicamento del conto può, previa richiesta del proprio utente, negare l'accesso ai conti di pagamento del cliente, a uno o più TPPs. Il medesimo ragionamento viene fatto dall'EBA in relazione alle pratiche poste in essere dai prestatori di servizi di pagamento di radicamento del conto ed in particolare con riferimento alla richiesta, ai TPP, dell'espletamento di procedure di registrazione supplementari per l'accesso all'interfaccia dell'ASPSP e alle informazioni dei conti di pagamento degli utenti di quest'ultimo[133].

In proposito, l'EBA evidenzia come l'art. 32, paragrafo 3, degli RTS menziona tra gli ostacoli potenziali all'attività dei TPP anche eventuali «autorizzazioni e registrazioni supplementari oltre a quelle previste dagli articoli 11, 14 e 15 della PSD2». Non si è in presenza di ostacoli quando alcuni processi di registrazione sono tecnicamente necessari per consentire una comunicazione sicura con la banca: si pensi al caso in cui sia necessaria una preregistrazione dell'app del TPP per consentire una comunicazione sicura con l'App di autenticazione della banca e tale registrazione viene elaborata in modo tempestivo non creando rallentamenti inutili per il cliente finale[134].

10. *I lavori di revisione della PSD2*

La Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015, prevede all'art. 108 una clausola di revisione ai sensi della quale la Commissione è tenuta a presentare al Parlamento europeo, al Consiglio, alla BCE e al Comitato economico e sociale europeo una relazione sull'applicazione e sull''impatto della PSD2. Il 20 ottobre 2021, la Commissione ha presentato all'Autorità Bancaria Europea una *Call for Advice* (CfA) avente la l'obiettivo di raccogliere informazioni sull'applicazione e sull'impatto della PSD2 e di identificare, tramite analisi degli sviluppi di mercato, tutti gli aspetti sui quali sarebbe necessario un intervento nell'ambito della revisione della PSD2[135].

Il 23 giugno 2022, l'EBA ha pubblicato le proprie risposte alla CfA della Commissione con l'*Opinion of the European Banking Authority on its technical*

---

[132] *Considerando* 69 della PSD2.

[133] A. Vivoli, *PSD2 a che punto siamo? Il percorso a ostacoli dell'Open Banking alla luce dell'Opinion EBA del 4 giugno 2020*, in *www.riskcompliance.it*, 2020.

[134] 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); A. Di Giorgio, B. Mascagni, *PSD2: gli ostacoli all'operatività dei TPP alla luce dei chiarimenti dell'EBA,* in *www.dirittobancario.it*, 2020.

[135] Commissione Europea, *Call for advice to the European Banking Authority (EBA) regarding the review of Directive (EU) 2015/2366 (PSD2*), in *www.ec.europa.eu*.

advice on the review of Directive (EU) 2015/2366 on payment services in the internal market, divisa in 9 sezioni e contenente l'osservazione dell'EBA in risposta alle 28 domande poste dalla Commissione[136].

In primis, a seguito di incertezze relative all'interpretazione dei vari servizi di pagamento sorte tra gli operatori del mercato, l'EBA ritiene che, sebbene i servizi di pagamento elencati nell'Allegato I della PSD2 assicurino neutralità dal punto di vista tecnologico e di business, potrebbe essere necessario chiarire gli elementi distintivi tra l'esecuzione di bonifici e il servizio di rimessa di denaro. Infatti, anche se in alcuni casi i modelli di business utilizzati nel mercato sono simili, i due servizi di pagamento soggetti ad un trattamento normativo differenziato[137]. Secondo l'EBA, al fine di distinguere i due servizi, potrebbe essere necessario chiarire che l'esecuzione di bonifici debba essere accompagnata dall'apertura di un conto a nome dell'utente di servizi di pagamento.

Dai numeri 3 e 4 dell'Allegato I della PSD2, emerge che le operazioni di pagamento ivi disciplinate sono sostanzialmente identiche tra loro e si differenziato esclusivamente per il fatto che i servizi di cui al numero 4 dell'Allegato I prevedono l'esistenza di una linea di credito accordata all'utente di servizi di pagamento. Secondo l'EBA, tali servizi potrebbero essere accorpati in un servizio di pagamento unico. Al contrario, i servizi di emissione di strumenti di pagamento e di convenzionamento di operazioni di pagamento (c.d. *acquiring*) presentano caratteristiche diverse tra loro e dovrebbero costituire, per tale motivo, due servizi di pagamento distinti e autonomi.

In relazione all'ambito di applicazione della PSD2, l'Autorità europea ha analizzato, tra tutti, il servizio di informazione sui conti, riscontrando la necessità di fornire chiarimenti in merito alle attività che un prestatore di tale servizio può svolgere; in particolare, è auspicabile valutare se lo stesso possa fornire informazioni consolidate sui conti di pagamento in maniera esclusiva all'utente di servizi di pagamento o anche direttamente a terzi, previo espresso consenso dell'utente. L'EBA, manifestando una preferenza per la seconda opzione, ritiene necessario un chiarimento di tale aspetto all'interno della Direttiva stessa[138].

Circa l'ambito di applicazione negativo della PSD2, sono state numerose le richieste di chiarimenti pervenute all'Autorità in relazione in particolare alla cosiddetta *limited network exemption*, ossia l'esenzione sui servizi prestati sulla base di stru-

[136] https://www.dirittobancario.it/art/modifiche-alla-psd2-sui-servizi-di-pagamento-le-proposte-delleba/.

[137] Ad esempio, diversi sono i requisiti in tema di capitale iniziale e fondi propri per gli istituti di pagamento (IP) che offrono tali servizi; v. E. Zeppieri, *Revisione della PSD2: analisi dell'Opinion EBA*, in www.dirittobancario.it, 2022.

[138] Ciò è già stato dall'EBA nelle proprie Q&A in risposta alle domande degli operatori del mercato e, in particolare, nella Q&A 4098.

menti a spendibilità limitata. Lo scorso febbraio l'EBA nei suoi Orientamenti sull'esclusione relativa alle reti limitate a norma della direttiva relativa ai servizi di pagamento nel mercato interno, ha chiarito che, gli strumenti di pagamento che permettono al detentore di acquistare beni o servizi esclusivamente nei locali dell'emittente, possono essere utilizzati soltanto in locali fisici e non i punti vendita online[139].

I suddetti Orientamenti hanno analizzato dunque molte delle questioni sollevate dal mercato sull'esenzione in questione, e pertanto l'EBA propone di includere gli stessi nella Direttiva o di ricevere un mandato dagli organi europei per la redazione di norme tecniche di regolamentazione.

Sull'esenzione relativa alle operazioni di pagamento effettuate tramite un agente commerciale, l'EBA ha mostrato ancora la presenza di una serie di carenze e lacune nel testo della Direttiva ed ha in particolare evidenziato la necessità di chiarire alcuni di questi aspetti all'interno dell'atto europeo; è stato notato infatti che gli agenti commerciali sono spesso identificati sulla base di disposizioni di diritto nazionale divergenti tra loro. La dicitura "negoziare o concludere" non appare abbastanza esaustiva soprattutto in caso di contratti conclusi digitalmente; ancora sarebbe del tutto certo che un soggetto che a seguito dell'accettazione del pagamento consegni beni per conto del venditore, possa beneficiare dell'esenzione in esame. Permangono infine dubbi da chiarire sull'applicabilità o meno dell'esenzione ai c.d. *escrow agent* e ad alcune piattaforme[140].

È stata ravvisata altresì la necessità di fornire delucidazioni anche con riferimento alla cosiddetta esenzione sugli ATM (*Automatic Teller Machine*) indipendenti ex art. 3 della PSD2. L'EBA ha sottolineato infatti la presenza di lacune in relazione al caso in cui un gestore di ATM agisce per conto di un prestatore di servizi di pagamento (PSP) in qualità di emittente di carte di pagamento. Non è affatto chiaro se in queste circostanze sia necessaria la conclusione di un accordo negoziale tra il gestore di ATM ed il singolo PSP emittente di carte di pagamento o se, di contro, possa essere sufficiente la conclusione di un mero contratto quadro con uno schema di carte di pagamento.

In relazione al servizio *cash-in-shop*, che consente all'utente di servizi di pagamento di prelevare contante dall'esercente con la propria carta senza effettuare alcun acquisto, l'Autorità europea ha messo in evidenza che mentre per alcuni operatori del mercato il fenomeno potrebbe essere ricondotto al servizio di *acquiring*[141], assimilabile al *cash-back*, per altri, ricadrebbe nell'esenzione ex art. 3 della PSD2 sugli ATM indipendenti. È stato così proposto dall'EBA di chiari-

[139] https://www.dirittobancario.it/art/psd2-linee-guida-eba-sugli-strumenti-di-pagamento-utilizzabili-in-modo-limitato/.

[140] E. Zeppieri, *Revisione della PSD2: analisi dell'Opinion EBA*, in *www.dirittobancario.it*, 2022.

[141] Convenzionamento di operazioni di pagamento; M. M. Pimpinella, G. Carrafiello, *L'evoluzione normativo-regolamentare nel settore dei pagamenti*, Milano, 2016, 9 ss.

re se tali servizi rientrino nell'ambito di applicazione positivo della PSD2 e chi, in tal caso, debba essere considerato l'effettivo prestatore del servizio o se, invece, debbano essere esclusi dall'ambito di applicazione della Direttiva in ragione del minor rischio loro connesso.

Criticità sono state riscontrate con l'*Opinion* in esame, anche in riferimento alle operazioni *one-leg* riguardanti la *Strong Customer Authentication*, e, in particolare, al fatto che alcuni al fine di eludere l'obbligo di effettuare la SCA concludono contratti per l'accettazione dei pagamenti con *acquirers* avente base in Stati terzi, laddove tale misura di sicurezza non è richiesta. Tale prassi per l'EBA, sembrerebbe non essere consentita dalla PSD2[142].

Quanto agli schemi di carte di pagamento, l'Autorità ha osservato come questi rivestono particolare importanza per il rispetto degli obblighi principali previsti dalla PSD2, in particolare l'applicazione della SCA. Gli schemi di carte di pagamento forniscono protocolli di comunicazione usati dai PSP per effettuare l'autenticazione forte ed eventuali malfunzionamenti potrebbero avere effetti significativi sul rispetto della misura di sicurezza medesima. Anche gli esercenti svolgono a tal riguardo un ruolo molto importante. Premesso quanto sopra, l'EBA suggerisce di prevedere nella Direttiva specifici obblighi in capo agli schemi di carte di pagamento e agli esercenti al fine di assicurare un'adeguata applicazione della SCA[143].

Anche per i servizi di *payment gateway*, nonostante sia stata ravvisata la necessità di non ricomprenderli del tutto nell'ambito di applicazione della Direttiva essendo servizi di natura tecnica, l'*European Authority* propone di introdurre delle modifiche che prevedano alcune disposizioni specifiche loro applicabili.

Con riferimento ai prestatori di servizi di portafoglio digitale (*e-wallet*), quest'ultima ha ritenuto invece che l'emissione di un token collegato ad uno strumento di pagamento o al conto di pagamento dell'utente di servizi di pagamento costituisca emissione di uno strumento di pagamento; tale attività, pertanto, rientrerebbe già ora nell'ambito di applicazione della PSD2[144].

---

[142] P. Montella, *L'autenticazione ad accesso forte (Strong customer Authentication) e la responsabilità del Prestatore del servizio di pagamento alla luce delle modifiche al d.lgs. n. 11 del 27 dicembre 201*0, in *De Iustitia*, 124 ss.; V. Falce, *Dalla self regulation a/ payment package. Storia delle commissioni interbancarie*, in *Analisi giuridica dell'economi*a, 1, 2015, 55 ss.; M.R. Farina, *Responsabilità degli intermediari bancari e finanziari e sistemi di internet banking: aggressione informatica e protezione del cliente*, in C.G. Corvese, G. Gimigliano, *Profili interdisciplinari del commercio elettronico*, Pisa, 2016, 97 ss.

[143] E. Zeppieri, *Revisione della PSD2: analisi dell'Opinion EBA*, in www.dirittobancario.it, 2022; EBA, *Guidelines on the exemption from the contingency mechanism under the RTS on SCA and CSC*, pubblicate il 4 dicembre 2018.

[144] R. Pardolesi e A. Davola, *«Smart contract»: lusinghe ed equivoci dell'innovazione purchessia*, in *Foro Italiano*, 4, V, 2019, 83 ss.; R. Ferrari, *L'era del Fintech. La rivoluzione digitale nei servizi finanziari*, Milano, 2016, 17 ss.

Novità rilevanti hanno interessato poi l'autenticazione forte del cliente in relazione alla quale l'EBA ha esaminato varie aree che potrebbero essere oggetto di modifiche e puntualizzazioni. Con specifico riguardo ai casi di esternalizzazione, nonostante in via generale sia previsto che la responsabilità per la corretta applicazione della SCA ricada sul PSP che ha emesso le credenziali di sicurezza personalizzate dello strumento di pagamento, l'Autorità ha proposto di indicare in maniera più chiara nella Direttiva i soggetti responsabili nei casi di esternalizzazione e/o delega a terzi per l'applicazione della SCA: proprio nelle Q&A 4047 e 4651, l'EBA ha evidenziato, rispettivamente, che i PSP possono utilizzare la tecnologia fornita da soggetti terzi[145]al fine di supportare l'applicazione della SCA, mentre i PSP possono utilizzare credenziali biometriche registrate nel singolo dispositivo, previa verifica del rispetto dei requisiti di sicurezza. Tuttavia, è stata registrata l'assenza in alcuni casi di un vero rapporto contrattuale tra il PSP ed il produttore del dispositivo mobile; quest'ultimo a volte possiede il controllo sulla corretta applicazione della SCA. Questo meccanismo sembra comportare significative criticità nel momento in cui il PSP non si trovi a non operare un adeguato controllo sulle misure di sicurezza utilizzate ed il rispetto dei requisiti previsti dalla PSD2 e dalle norme tecniche di regolamentazione. Per questi motivi per l'EBA sarebbe auspicabile indicare chiaramente nella Direttiva se l'utilizzo di queste tecnologie fornite da terzi richieda un accordo di esternalizzazione o meno. Ciò è valido anche per la delega da parte di PSP a PISP e AISP[146].

Altro profilo di interesse riguarda l'applicabilità di quanto contenuto nel Considerando 95 della PSD2, ai sensi del quale la sicurezza dei pagamenti elettronici è fondamentale per garantire la protezione degli utenti del commercio elettronico. I servizi di pagamento offerti elettronicamente devono risultare sicuri e affidabili, e devono essere prestati tramite l'adozione di tecnologie che siano in grado di garantire l'autenticazione sicura dell'utente, riducendo così il rischio di frode. Dalla disciplina però non sembrerebbe ravvisarsi la necessità di garantire lo stesso livello di protezione per tutte le operazioni di pagamento eseguite con modalità diverse rispetto all'uso di dispositivi elettronici[147]. Queste esclusioni sono state oggetto di chiarimenti da parte dell'Autorità europea: con riferimento all'esclusione dell'applicazione della SCA per le operazioni disposte dagli esercenti (*Merchant Initiated Transaction*, MIT), l'EBA suggerisce di introdurre nell'atto comunitario alcune previsioni che contenessero: una definizione chiara di MIT, la disciplina del mandato elettronico per le operazioni disposte dal beneficiario/

[145] Ad esempio, smartphone per la rilevazione dell'impronta digitale.

[146] E. Zeppieri, *Revisione della PSD2: analisi dell'Opinion EBA*, in *www.dirittobancario.it*, 2022.

[147] Si fa riferimento ad operazioni di pagamento su supporto cartaceo, ordini per corrispondenza o ordini telefonici; M. Fava, *Strong customer authentication, A business perspective*, Relazione tenuta al Convegno «Recepimento PSD2 e novità sui servizi dì pagamento», Milano, 28 marzo 2018.

esercente che chiarisca così l'applicabilità della SCA alla creazione del mandato, i limiti al numero di operazioni di pagamento da eseguire e infine chiarimenti sul rapporto tra MIT e addebiti diretti.

Previsioni specifiche, al contempo, dovrebbero essere introdotte per la tematica degli ordini per corrispondenza e gli ordini telefonici (*Mail Order or Telephone Order*, MOTO)[148]. Secondo l'EBA, infatti, dovrebbero essere introdotta una definizione chiara di MOTO all'interno della Direttiva, diretta a limitare il più possibile l'ambito di applicazione dell'esenzione dalla SCA. Ad una più ampia definizione, corrisponderebbe un più elevato rischio di frode[149].

Circa la responsabilità per mancata applicazione della SCA, secondo l'EBA, la Commissione dovrebbe introdurre delle misure più efficaci al fine di assicurare un'applicazione più ferrea disposizioni in tema di SCA e prevedere che, in tutti i casi in cui la SCA e altre misure di sicurezza non vengano applicate a causa della mancata adozione da parte dell'esercente di soluzioni adeguate, la responsabilità in caso di operazioni di pagamento non autorizzate passi dal PSP del beneficiario all'esercente[150].

Per concludere, nella sua recente *Opinion* del 2022, l'*European Authority* ha indicato la necessità di introdurre chiarimenti con riferimento alla classificazione delle operazioni di rimborso e della conseguente applicabilità a queste della SCA. Più in particolare, ci si è chiesti se un rimborso costituisca un'operazione di pagamento autonoma e indipendente o se si tratti di un semplice diritto degli esercenti nell'ambito del servizio di *acquiring*: è stato così chiarito che, il rimborso disposto da un esercente-pagatore, rappresenta un'operazione di pagamento elettronico e, per tale motivo, il PSP dell'esercente dovrebbe applicare la SCA, a condizione che non sia applicabile un'esenzione[151].

11. *Considerazioni conclusive*

A seguito dell'analisi della recente disciplina relativa ai servizi di pagamento, sembrerebbe emergere che le leggi europee di ultima generazione si pongono con maggior forza in un'ottica di tutelare l'utilizzatore di servizi di pagamento, oltre-

[148] Numerose sono state le Q&A pubblicate dall'EBA sul tema.

[149] Per l'EBA sarebbe auspicabile prevedere dei requisiti di sicurezza minimi. L'Autorità ha evidenziato come spesso le operazioni di pagamento vengano classificate come MIT e MOTO al solo scopo di eludere l'obbligo di applicazione della SCA. L'introduzione di definizioni e previsioni specifiche dovrebbe eliminare o almeno ridurre tale prassi; M. Fava, *Strong customer authentication, A business perspective*, cit.

[150] E. Zeppieri, *Revisione della PSD2: analisi dell'Opinion EBA*, in *www.dirittobancario.it*, 2022.

[151] EBA, Q&A 4855.

ché di protezione del risparmio che i clienti depositano nei conti di pagamento ai fini di un utilizzo corretto e consapevole degli stessi.

L'analisi puntuale condotta dall'EBA, sia sui potenziali ostacoli nella prestazione di servizi di disposizione di ordini di pagamento o informativi sui conti, sia sui vari aspetti e lacune contenute nella PSD2 che meritano di essere attenzionate in una prospettiva di revisione della Direttiva stessa, sembrerebbe al contempo essere diretta principalmente alle Autorità di vigilanza nazionali che hanno il compito di vigilare sulla conformità delle interfacce di accesso ai conti predisposte dalle banche ai requisiti tecnici regolamentari, seguendo i chiarimenti contenuti nella *Opinion* del 2020. In tale contesto, tale "guida" ha avuto la finalità di garantire una corretta funzionalità dell'*open banking*, fenomeno attraverso il quale, soprattutto nell'era post pandemica, la prestazione dei servizi di pagamento e la gestione dei conti non vengono più affidate esclusivamente alle banche ed alle istituzioni finanziarie, ma a nuovi *player* del mercato che hanno sempre di più la possibilità di fidelizzare parte della clientela tramite l'utilizzo di strumenti tecnologici. Questo importante documento ha trovato un pieno e positivo riscontro da parte dell'*European Third Party Providers Association* (ETPPA)[152], associazione formata da Fintech di derivazione non bancaria che offrono servizi AIS o PIS.

Il cliente finale beneficia così di un numero maggiore di servizi nel settore dei pagamenti: risulta pertanto necessario assicurarsi sia che tale estensione si realizzi in concreto, sia che garantisca in ogni caso una piena tutela della trasparenza e della sicurezza dei pagamenti effettuati dagli utenti. Ciò può realizzarsi soltanto attraverso le attività delle Autorità competenti dei singoli Stati Membri, importanti non soltanto ai fini del controllo e della vigilanza della tutela dei consumatori, ma anche per sensibilizzare l'utilizzo dei nuovi strumenti di pagamento digitale[153].

Sempre di più negli ultimi tempi si sta assistendo all'evoluzione delle banche come vere e proprie piattaforme di servizi integrati che si propongono come TPP rispetto ai *competitors*[154]. A partire dal 2020 infatti, numerosi istituti di credito hanno provveduto ad integrarsi con TPP, consentendo così anche ai propri clienti di raccogliere informazioni e attuare operazioni favorendo, allo stesso tempo, la creazione di nuove forme di cooperazione, anche con *startup* innovative[155].

A tal proposito l'EBA, in un contesto di piena diffusione delle banche digitali, auspica sempre di più un intervento delle Autorità che possa comportare il

---

[152] V. *www.etppa.org*.

[153] Il documento pubblicato dalla Banca d'Italia il 15 giugno 2020, rubricato "I pagamenti nel commercio elettronico: una mappa per orientarsi" contiene delle linee guida per tutti i soggetti "che comprano beni o servizi online e vogliono capire meglio come funzionano i pagamenti sul web".

[154] Banca 5 è stata la prima banca italiana ad operare come TPP: *www.banca5.com*.

[155] M. Fava, *Strong customer authentication, A business perspective*, Relazione tenuta al Convegno «Recepimento PSD2 e novità sui servizi dì pagamento», Milano, 28 marzo 2018.

superamento degli ostacoli richiamati e che possa dare maggiore chiarezza ad una normativa che presenta tutt'ora alcuni punti dubbi «al fine di creare un sistema dei pagamenti europeo "open" digitale e sicuro, nel quale il cliente possa liberamente utilizzare gli strumenti che ritiene più adatti alle sue esigenze»[156].

È dunque possibile affermare che la PSD2 ha portato con sé tutti gli elementi necessari a trasformare il mercato dei servizi bancari, rendendolo "*open*". Utili senza ombra di dubbio sono state le lezioni apprese da settori e mercati che sono stati già impattati dalle normative europee come, ad esempio, nel settore delle telecomunicazioni o quello dell'energia. La liberalizzazione del settore bancario potrà arrecare sfide non troppo dissimili da quelle portate dai *Mobile Virtual Network Operator* nella telefonia mobile, che offrono servizi dedicati a specifichi segmenti di clientela attraverso l'utilizzo di *billing e provisioning* di operatori *core*.

Nonostante ciò, è persistente la probabilità che i nuovi soggetti, attori del mercato derivanti dal recepimento della normativa europea, siano comunque di estrazione bancaria (come è accaduto nella prima fase delle normative relative agli istituti di pagamento e degli IMEL): per evitare, dunque, che le aperture del mercato avvengano solo attraverso il proliferare dei soli soggetti afferenti al mondo bancario, sarà necessario che tutte le normative future di attuazione della PSD2 siano dirette a tutelare i nuovi soggetti che entrano nel mercato stesso anche con posizioni asimmetriche, in un'ottica di tutela anche degli utenti/consumatori[157].

Il rischio concreto per l'utente di tali servizi collegato alle banche e ai nuovi soggetti riguarda, *in primis*, la frode nell'utilizzo delle credenziali di autenticazione, che questi soggetti possono porre in essere direttamente o indirettamente tramite altre figure. I rischi sempre più elevati (tra i quali ad esempio il "phishing" o l'hackeraggio) stanno contribuendo a diffondere una diffidenza generale verso le nuove tecnologie, causata anche dalle difficoltà di individuare e perseguire gli autori degli illeciti che spesso operano in Paesi extra-UE. Per tale motivo, l'elevazione degli standard minimi di sicurezza dei clienti e dei loro dati e la previsione della *Strong Customer Authentication* costituiscono senza ombra di dubbio il fulcro di tutta dell'architettura della PSD2[158].

Il cambiamento normativo deve dunque portare con sé una trasformazione sistemica del mondo dei servizi di pagamento. Le banche potranno sviluppare ulteriori modelli di business cogliendo quelle che sono le potenzialità di un

---

[156] Così A. Di Giorgio, B. Mascagni, *PSD2: gli ostacoli all'operatività dei TPP alla luce dei chiarimenti dell'EBA*, in *www.dirittobancario.it*, 2020.

[157] A.M. Benedetti, *La difesa del consumatore dal contratto e la natura 'ambigua' dei recessi di pentimento*, in *Annuario del contratto*, Torino, 2011, 3 ss.

[158] L. Ammannati, *Il paradigma del consumatore nell'era digitale: consumatore digitale o digitalizzazione del consumatore?*, in *Riv. trim. dir. ec.*, 2019, 24 ss.; E. Zeppieri, *L'implementazione in Italia della nuova direttiva sui servizi di pagamento*, in *Dir. banc.*, 2018, 10 ss.

mercato sempre più presidiato da *players* innovativi e, dal canto loro, le *fintech* potranno beneficiare di un'apertura strutturale del mondo dei servizi bancari per fornire al cliente prodotti e servizi del tutto innovativi. Il miglioramento dei livelli di sicurezza per come prescritti e promossi dal quadro normativo di riferimento, che sono alla base delle offerte contrattuali del settore dei pagamenti, dovrà essere una scelta "obbligata" dell'operatore del mercato e sarà «uno degli elementi sui cui fondare la concorrenza tra le imprese di settore»[159].

[159] Così R. Motroni, *La PSD2 tra soggetti e oggetto della tutela*, in *Il diritto dell'economia*, 2019, 2, 421.

I Third Party Providers *e l'accesso ai conti bancari nella disciplina giuridica dei servizi di pagamento: problemi e prospettive*

Partendo dalle innovazioni introdotte dalla direttiva 2015/2366/UE (c.d. *Payment service directive 2* - PSD2), attuata in Italia con il d.lgs. 15 dicembre 2017, n. 218, il presente saggio intende esaminare in particolare la disciplina relativa ai *Third Party Providers* (TPPs), i nuovi intermediari prestatori del servizio di disposizione di ordini di pagamento (*Payment initiation service* - PIS) e di informazione sui conti (*Account information service* - AIS). L'attuale disciplina giuridica pone numerose questioni che riguardano la tutela degli utenti dei servizi di pagamento e il regime di responsabilità degli intermediari che svolgono le attività di prestazione di tali servizi, in un delicato ma necessario, ancorché mutevole, bilanciamento tra perseguimento degli interessi pubblici e autonomia degli operatori del mercato di riferimento.

Starting from the innovations introduced by the directive 2015/2366/UE (so-called Payment service directive 2 - PSD2), implemented in Italy with the legislative decree 15 December 2017, n. 218, this essay intends to examine in particular the regulations relating to Third Party Providers (TPPs), the new intermediaries providing the service of provision of payment orders (Payment initiation service - PIS) and information on accounts (Account information service - AIS). The current legal framework raises numerous issues concerning the protection of users of payment services and the liability regime of intermediaries who carry out the activities of providing such services, in a delicate but necessary, albeit changing, balance between the pursuit of public interests and autonomy of the operators in the market.