Pubblicazione Trimestrale
ISSN: 2279-9737

Rivista di Diritto Bancario

dottrina
e giurisprudenza
commentata

Ottobre/Dicembre

2020

rivista.dirittobancario.it

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

2020 | 2021

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

NORME PER LA VALUTAZIONE E LA PUBBLICAZIONE

La Rivista di Diritto Bancario seleziona i contributi oggetto di pubblicazione sulla base delle norme seguenti.

I contributi proposti alla Rivista per la pubblicazione vengono assegnati dal sistema informatico a due valutatori, sorteggiati all'interno di un elenco di ordinari, associati e ricercatori in materie giuridiche, estratti da una lista periodicamente soggetta a rinnovamento.

I contributi sono anonimizzati prima dell'invio ai valutatori. Le schede di valutazione sono inviate agli autori previa anonimizzazione.

Qualora uno o entrambi i valutatori esprimano un parere favorevole alla pubblicazione subordinato all'introduzione di modifiche aggiunte e correzioni, la direzione esecutiva verifica che l'autore abbia apportato le modifiche richieste.

Qualora entrambi i valutatori esprimano parere negativo alla pubblicazione, il contributo viene rifiutato. Qualora solo uno dei valutatori esprima parere negativo alla pubblicazione, il contributo è sottoposto al Comitato Esecutivo, il quale assume la decisione finale in ordine alla pubblicazione previo parere di un componente della Direzione scelto ratione materiae.

2020 | 2021

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

SEDE DELLA REDAZIONE

Università degli Studi di Trento, Facoltà di Giurisprudenza, via Verdi 53,
(38122) Trento – tel. 0461 283836

2020 | 2021

FRANCESCO CIRAOLO

Open Banking, Open Problems. Aspetti controversi del nuovo modello dei "sistemi bancari aperti".

SOMMARIO: 1. Innovazione tecnologica, *unbundling* dei servizi finanziari e disintermediazione. Verso un nuovo assetto del mercato bancario. – 2. Gli aspetti problematici del nuovo modello operativo dell'*open banking*. Definizione dell'ambito dell'indagine. – 3. PSD2, *open banking* e concorrenza. – 4. PSD2, *open banking* e tutela dei dati personali. – 5. PSD2, *open banking* e sicurezza delle transazioni. La responsabilità dei nuovi prestatori di servizi di pagamento. – 6. Considerazioni conclusive.

1. *Innovazione tecnologica,* unbundling *dei servizi finanziari e disintermediazione. Verso un nuovo assetto del mercato bancario.*

Le innovazioni tecnologiche degli ultimi anni hanno avuto, com'è noto, un impatto di straordinaria importanza sul sistema finanziario, tale da determinare un significativo ridimensionamento del ruolo degli intermediari tradizionali e da imporre, al contempo, la ricerca di nuovi equilibri complessivi.

Il settore dei servizi di pagamento, in particolare, è sempre stato estremamente permeabile alle novità, grazie anche alla fattiva partecipazione dell'industria finanziaria a processi di (ri-) regolamentazione che presuppongono, per la peculiare natura della materia trattata, uno stretto connubio tra aspetti giuridici e profili tecnici[1]. In tal senso, dunque, non rappresenta un'eccezione neanche il

---

L'autore è membro dell'Arbitro Bancario Finanziario, Collegio di Palermo. Le opinioni espresse nel presente scritto hanno carattere personale e non rappresentano la posizione dell'organismo di appartenenza.

[1] Immediato, al riguardo, è il riferimento alla realizzazione, a partire dai primi anni duemila, della *Single Euro Payment Area* (SEPA), cui ha fornito un decisivo contributo anche l'industria bancaria europea, attraverso lo *European Payment Council*. Com'è noto, infatti, tale organismo ha definito gli *standard* tecnici e procedurali relativi a strumenti di pagamento armonizzati, elaborando in particolare il *SEPA Cards Framework* (ossia lo schema per i pagamenti a mezzo carta), il *SEPA Credit Transfer Rulebook* (per i bonifici) e il *SEPA Direct Debit Rulebook* (per gli addebiti diretti). Le regole giuridiche armonizzate in materia di prestazione di servizi di pagamento, dettate dalla dir. 2007/64/CE (PSD), si sarebbero dunque innestate su regole tecniche e procedure già condivise tra gli operatori del settore. Sui distinti

fenomeno, di stretta attualità, dell'*open banking*, che ha trovato recente riconoscimento normativo, in sede europea, ad opera della direttiva UE 2015/2366 del 25 novembre 2015 (c.d. PSD2), recepita in Italia con d. lgs. n. 218/2017 (in vigore dal 13 gennaio 2018).

Sia pure in mancanza di una definizione univoca – formulata facendo perno, a seconda dell'angolo di osservazione prescelto, ora sui profili giuridico-normativi, ora sugli aspetti tecnologico-operativi, altre volte su quelli più prettamente aziendalistici –, quello dei "sistemi bancari aperti" è considerato, volendo mutuare un'espressione dilagante in letteratura, come un nuovo "paradigma" operativo, caratterizzato dall'accessibilità, da parte di specifiche categorie di soggetti (i c.d. *Third-Party Providers*, TPPs) ed in funzione dell'erogazione di nuove tipologie di servizi di pagamento (i servizi di disposizione di ordini di pagamento e i servizi di informazione sui conti, sui quali v. *infra*, par. 2), dei dati dei conti di pagamento intrattenuti dagli utenti presso banche o altri enti autorizzati (i c.d. prestatori di servizi di pagamento di radicamento dei conti).

Si evince subito, sin da queste prime battute, la portata rivoluzionaria dell'argomento in discussione: le banche perdono, per la prima volta, il monopolio sui dati dei propri correntisti, per effetto di un obbligo normativo (la c.d. *access to account rule*, in gergo *XS2A rule*), che impone loro di condividerli con altri soggetti, in nome dell'innovazione, dell'efficienza e dello sviluppo competitivo del mercato dei servizi di pagamento[2].

Il punto appare, per le implicazioni che ne discendono, di rilevanza tutt'altro che secondaria. Non soltanto perché testimonia la sopravvenuta modifica del tradizionale rapporto tra banche e clienti,

---

passaggi temporali in cui si è articolato il progetto SEPA e sulle relative criticità, di recente, F. PORTA, *Obiettivi e strumenti della PSD2*, in F. MAIMERI, M. MANCINI (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, Banca d'Italia, *Quaderni di Ricerca Giuridica*, 2019, n. 87, 24 ss.

[2] Considerato, infatti, che le banche non hanno alcun incentivo a condividere i dati dei propri clienti con altre imprese in grado di offrire ulteriori servizi a valore aggiunto, l'introduzione di un obbligo di accesso ai conti a favore di terze parti mira ad assicurare maggiore competizione nel mercato dei servizi di pagamento e a stimolare l'innovazione (S. VEZZOSO, *Fintech, access to data, and the role of competition policy*, 2018, 35, reperibile all'indirizzo *https://ssrn.com/abstract=3106594*).

risultando le prime ormai private di un "privilegio" (il controllo esclusivo dei dati bancari dei clienti) sul quale hanno sempre basato la propria operatività e costruito anche i propri vantaggi competitivi[3], ma anche e soprattutto perché rimanda, allargando lo sguardo all'intero mercato di riferimento, ad un fenomeno di ancor più ampia portata, rappresentato dall'attuale tendenza alla "disintermediazione" degli istituti bancari (espressione con la quale si intende alludere alla progressiva marginalizzazione di questi ultimi rispetto a settori di mercato nei quali hanno trovato ingresso nuovi operatori – dalle *start up FinTech* alle c.d. *Big Tech* – specializzati nell'erogazione di servizi finanziari di ultima generazione)[4]. In termini più generali, dunque, l'*open banking* può ritenersi emblematico del processo di trasformazione in atto nel settore bancario-finanziario, ove al classico modello di banca che produce e distribuisce i propri servizi mantenendo il controllo sull'intera filiera produttiva, si contrappone la sempre maggiore "disarticolazione" (*unbundling*) della catena del valore dell'intermediazione finanziaria in più segmenti, ciascuno dei quali è occupato da soggetti in grado di offrire specifici prodotti e/o servizi ("disintermediando", appunto, gli operatori tradizionali), basati sulle nuove tecnologie digitali[5].

[3] Al riguardo, è stato sottolineato che l'effetto più significativo delle nuove disposizioni normative consiste nel venir meno del «monopolio degli istituti di credito sui dati bancari dei clienti, frutto di investimenti, relazioni con la clientela e regole molto stringenti», come anche della stessa «esclusività del rapporto con la clientela», con ciò determinandosi una significativa trasformazione dell'operatività bancaria (A. ARGENTATI, *Le banche nel nuovo scenario competitivo. FinTech, il paradigma dell'Open banking e la minaccia delle big tech companies*, in *Merc. conc. reg*., 2018, 453).

[4] Sul fenomeno della disintermediazione in ambito finanziario v. G. PITRUZZELLA, *FinTech e i nuovi scenari competitivi nel settore finanziario, creditizio, assicurativo*, in *Bancaria*, 2018, n. 6, 23 ss.

[5] Invero, è oggi possibile riprodurre per via digitale intere componenti dell'attività bancaria tipica (si pensi, ad es., all'erogazione del credito in modalità *peer to peer*), che possono essere pertanto prestate, nel rispetto delle riserve di attività, anche da soggetti non bancari (ciò che lascia presagire a taluni la fine del sistema bancocentrico, o quanto meno della banca *full service*, per come sino ad oggi conosciuta). In altri casi, invece, il fenomeno assume una diversa configurazione, nel senso che i nuovi *competitors* si concentrano su singole fasi della filiera produttiva di specifiche tipologie di servizi/prodotti del ramo finanziario, come accade, ad es., nell'ambito dei servizi di pagamento: la catena procedimentale dei pagamenti, infatti,

Quale possa essere l'impatto di simili cambiamenti sulla configurazione del sistema bancario è presto a dirsi, né tali valutazioni costituiscono – è opportuno precisarlo – l'oggetto del presente lavoro. Ci si limiterà ad osservare, pertanto, che le banche stanno subendo enormi pressioni concorrenziali da parte di soggetti che, avvantaggiati dalle loro elevate competenze tecnologiche, da strutture operative più snelle e da vincoli regolamentari assai meno stringenti, invadono ed erodono le aree di competenza degli intermediari tradizionali, obbligandoli a ripensare i propri modelli di *business* e a valutare nuove strategie imprenditoriali, finalizzate a controbilanciare gli effetti (perdita di quote di mercato, riduzione dei margini di redditività e profittabilità, ecc.) del processo di disintermediazione in atto[6]. Tra chi presagisce drasticamente la definitiva eclissi della banca tradizionale,

---

prevede oggi – come sarà meglio precisato a breve la partecipazione di nuovi soggetti (i già citati TPPs) ad una specifica fase della stessa, vale a dire la disposizione dell'ordine di pagamento (eseguito poi dall'intermediario detentore del conto), ovvero, con diversa e assai più limitata portata, la fornitura di informazioni relative ai conti (in chiave strumentale anche all'eventuale esecuzione di successive operazioni di trasferimento di fondi). In arg., v. M. CARNEY, *The Promise of FinTech - Something New Under the Sun?*, Speech of the Governor of the Bank of England, Chair of the Financial Stability Board, Deutsche Bundesbank G20 Conference *Digitising finance, financial inclusion and financial literacy*, Wiesbaden, 25 gennaio 2017, 3 ss. (si può consultare su *https://www.bankofengland.co.uk/speech/2017/the-promise-of-fintech-something-new-under-the-sun*); D. GAMMALDI, C. IACOMINI, *Mutamenti del mercato dopo la PSD2*, in F. MAIMERI, M. MANCINI (a cura di), *Le nuove frontiere*, cit., 140; da ultimo, sulla disaggregazione e riaggregazione delle attività finanziarie in nuovi sistemi di creazione del valore, A. OMARINI, *La digital banking transformation: dall'unbundling al re-bundling, verso nuovi modelli di intermediazione*, in *Bancaria*, 2020, n. 1.

[6] D. MILANESI, *A New Banking Paradigm: The State of Open Banking in Europe, The United Kingdom, and the United States*, Stanford-Vienna TTLF Working Paper No 29, 2017, 140 ss. (*http://ttlf.stanford.edu*). V. anche F. ZUNZUNEGUI, *Digitalisation of payment services*, Ibero-American Institute for Law and Finance, Working Paper Series 5/2018, 7 ss. (reperibile su *https://ssrn.com/abstract=3256281*), il quale sottolinea la convergenza tra i *business models* di banche e *FinTech* e la sempre maggiore integrazione tra la *FinTech industry* e la tradizionale industria finanziaria. Più in generale, sui possibili scenari evolutivi innescati dalle relazioni tra banche e *FinTech firms*, v. BCBS, *Sound Practises. Implications of fintech developments for banks and bank supervisors*, febbraio 2018, 15 ss. (*www.bis.org*); C. SCHENA, A. TANDA, C. ARLOTTA, G. POTENZA, *Lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, in CONSOB, *Quaderni FinTech*, n. 1, 2018, 85 ss.

destinata a soccombere di fronte alle aggressioni dei nuovi *competitors* (per scomparire del tutto, secondo gli scenari più estremi, o per trasformarsi sempre più in una piattaforma dedicata alla vendita di prodotti e servizi erogati da terzi[7]), e chi ritiene, invece, che la forza dirompente delle imprese *FinTech* giungerà ad un naturale esaurimento, nel momento stesso in cui gli intermediari storici saranno in grado, all'esito di un più o meno lungo processo di modernizzazione, di colmare il *gap* tecnologico che li separa dai nuovi[8], si situano coloro che evidenziano, piuttosto, le opportunità offerte da varie forme di alleanza strategica tra i vecchi e i nuovi operatori[9].

Al momento, è probabilmente questa la direzione intrapresa dal mercato, registrandosi numerosi casi di *partnership* tra banche e imprese *FinTech* (non di rado destinate a sfociare in rapporti partecipativi) concluse in un'ottica di reciproci vantaggi, vale a dire per consentire alle prime di accedere a soluzioni tecnologicamente più avanzate e sviluppare prodotti e servizi innovativi a costi vantaggiosi (avviando un processo di trasformazione digitale che le stesse, con le proprie sole forze, non riuscirebbero a compiere in tempi accettabili), alle seconde di estendere il proprio raggio di operatività alla vastissima

[7] In argomento, D. GIROMPINI, *PSD2 e Open Banking. Nuovi modelli di business e ruolo delle banche,* in *Bancaria*, 2018, n. 1, 70 ss.; D. MILANESI, *A New Banking Paradigm*, cit., 159 ss., ove un confronto anche con il diverso modello di *bank as a marketplace*; M. ZACHARIADIS, P. OZCAN, *The API Economy and Digital Transformation in Financial Services: The Case of Open Banking*, SWIFT Institute Working Paper No. 2016-001, 10 ss.

[8] Ritengono alcuni studiosi, d'altronde, che il vantaggio competitivo offerto dalla tecnologia sia destinato a rilevare solo nel breve termine (G. BARBA NAVARRETTI, G. CALZOLARI, A.F. POZZOLO, *FinTech and Banks: Friends or Foes?*, in *European Economy*, 2017, 2, 16). È indubbio, nondimeno, che il salto tecnologico appare estremamente faticoso per molti istituti, ostacolati nei processi di riorganizzazione interna e di ammodernamento da strutture, procedure e dotazioni di personale (o, più in generale, da una cultura aziendale) non sempre adeguati rispetto a tale obiettivo.

[9] M. SCHIEPPATI, *Banche, «pensare come Google»?*, in *Bancaria*, 2017, n. 3, 60. Anche l'ultima *Indagine FinTech nel sistema finanziario italiano* (Banca d'Italia, dicembre 2019) conferma la crescita degli investimenti *FinTech* nel settore bancario, il 14% dei quali è rappresentato da forme di cooperazione tra istituti tradizionali e imprese *FinTech*, prevalentemente secondo la modalità della *partnership*, sovente in combinazione con incubatori, acceleratori, distretti, o con l'acquisizione di partecipazioni. Significativa, peraltro, l'affermazione secondo la quale proprio l'*open banking* e la PSD2 hanno dato impulso alla realizzazione di progetti innovativi e di più ampio respiro, volti alla creazione di nuovi ecosistemi digitali (p. 7).

platea, altrimenti non facilmente raggiungibile, dei clienti degli istituti bancari[10].

2. *Gli aspetti problematici del nuovo modello operativo dell'*open banking*. Definizione dell'ambito dell'indagine.*

Nel contesto sopra tratteggiato si collocano i servizi di pagamento riconducibili all'alveo concettuale e operativo dell'*open banking*.

Al riguardo, giova precisare che, muovendo dalla necessità di ammodernare il quadro giuridico in materia di pagamenti al dettaglio – in considerazione delle numerose innovazioni tecnologiche che hanno interessato il settore, dell'affermarsi di nuovi servizi e dell'ingresso sul mercato di nuovi operatori, non rientranti nell'ambito di applicazione della precedente disciplina –, la PSD2 ha dettato le condizioni normative per un mercato dei pagamenti maggiormente integrato, basato su regole chiare, moderne e di uniforme applicazione, che possa fungere da propulsore per la crescita economica dell'intera Unione[11].

In questa logica sono state introdotte le disposizioni relative alle nuove tipologie di servizi di pagamento, volte a garantire l'apertura del mercato ad alcune categorie di operatori (i c.d. *Third-Party Providers*, TPPs) già presenti nel settore dei pagamenti via *Internet*, ma non ancora provvisti di una specifica disciplina (con evidenti rischi, che il legislatore ha inteso dunque neutralizzare, sia per gli utenti che per

[10] D. GAMMALDI, C. IACOMINI, *Mutamenti del mercato dopo la PSD2,* cit.; M.-T. PARACAMPO, FinTech, *evoluzioni tecnologiche e sfide per il settore bancario tra prospettive di cambiamento ed interventi regolamentari. Fenomenologia di un processo* in fieri, in M.-T. PARACAMPO (a cura di), *FINTECH. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, vol. II, Torino, 2019, 27. Sul punto v. anche il recente *EBA Report on the Impact of Fintech on Payment Institutions' and E-Money Institutions' Business Model*, luglio 2019, 14 ss.

[11] Cfr. 5° e 7° considerando. Merita peraltro sottolineare come, sposando gli attuali orientamenti regolamentari in materia di *FinTech*, anche le scelte normative della PSD2 si fondino sui principi della *neutralità* rispetto ai profili tecnologici (le definizioni contenute nella direttiva non sono infatti vincolate dal riferimento a specifiche soluzioni tecniche, in modo da poter ricomprendere anche eventuali nuove fattispecie) e della *proporzionalità* (l'azione regolamentare e di vigilanza è infatti commisurata alle specifiche attività poste in essere dai diversi operatori e ai relativi rischi).

l'ordinato funzionamento del mercato[12]): i prestatori di servizi di disposizione di ordini di pagamento (o *Payment Initiation Service Providers*, PISPs) e i prestatori di servizi di informazione sui conti (*Account Information Service Providers*, AISPs)[13].

Più in dettaglio, i servizi del primo tipo consentono al prestatore (PISP) di disporre un pagamento, per conto dell'utente, a valere su un conto intrattenuto da quest'ultimo presso un altro intermediario (il prestatore di servizi di pagamento di radicamento del conto, o *Account Servicing Payment Service Provider*, ASPSP), assicurando contestualmente al beneficiario del pagamento che lo stesso è stato disposto[14]. In termini tecnici, essi consentono di effettuare bonifici *on line* attraverso «*un software che fa da ponte tra il sito web del commerciante e la piattaforma di online banking della banca del pagatore*» [15], ponendosi, dunque, come una valida e più economica alternativa ai tradizionali pagamenti con carta (per effettuare transazioni su *Internet*, infatti, l'utente deve solo possedere un conto corrente con accesso remoto, mentre il commerciante non è obbligato ad aderire ad un *card scheme* e a sopportare i relativi costi)[16].

Gli *Account Information Services*, invece, nascono con l'obiettivo di fornire all'utente informazioni consolidate relative ai conti che lo stesso intrattiene presso altri intermediari (*i.e.*, uno o più prestatori di servizi di pagamento di radicamento del conto), consentendogli di avere un

[12] Primaria esigenza delle nuove disposizioni è, infatti, quella di garantire ai consumatori un elevato livello di protezione (tenuto conto che i rischi di sicurezza dei pagamenti elettronici sono aumentati in proporzione alla complessità tecnica e alla diffusione dei nuovi strumenti e servizi di pagamento), a sua volta necessario per rafforzare la fiducia dei medesimi nel buon funzionamento del mercato dei pagamenti (cfr. 6° considerando PSD2).

[13] La ragione della revisione della PSD sarebbe da rinvenire, invero, nella necessità di regolamentare tali soggetti (così, FSB, *Financial Stability Implications from FinTech*, 27 giugno 2017, 25), fermo restando che l'erogazione dei nuovi *payment services* non è preclusa ai tradizionali prestatori di servizi di pagamento (cfr. 33° considerando PSD2).

[14] Il beneficiario viene in tal modo incentivato ad una pronta esecuzione della propria prestazione, ad es. la consegna di un bene o l'erogazione di un servizio (29° considerando PSD2).

[15] V. 27° considerando PSD2.

[16] F. CIRAOLO, *La prestazione di servizi di pagamento nell'era del* FinTech *e dell'*Open Banking, in M.-T. PARACAMPO (a cura di), *FINTECH. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, cit., 227.

quadro generale della propria situazione finanziaria e delle proprie abitudini di spesa. In sostanza, accedendo al servizio tramite un'apposita piattaforma *online*, l'utente può ricevere un'informativa completa e organizzata su tutti i propri conti di pagamento e assumere, di conseguenza, decisioni consapevoli in merito all'efficiente gestione delle proprie risorse[17].

Lo svolgimento dei nuovi servizi di pagamento presuppone, dunque, l'accesso diretto del fornitore (PISP o AISP) ai conti "esterni" del proprio cliente, senza che il prestatore di servizi di pagamento di radicamento del conto del pagatore (ASPSP) possa opporvisi, quanto meno ove non ricorra un giustificato motivo oggettivo (ed essendo anzi previsto che gli ordini di pagamento trasmessi mediante un PISP, o le richieste di dati trasmesse mediante un AISP, vengano trattati dall'ASPSP *«senza discriminazioni»* rispetto agli ordini o alle richieste provenienti direttamente dal cliente).

Significativa appare, dunque, l'attrazione delle attività in esame nell'alveo dei servizi di pagamento (con conseguente estensione del relativo regime normativo, sia pure mitigata dal principio di proporzionalità[18]), se solo si osserva come le stesse, diversamente dalle

[17] Curiosamente, la definizione italiana di «*servizio di informazione sui conti*» (art. 1, comma 1, lett. b-*ter*), d. lgs. n. 11/2010) non prevede, a differenza di quella offerta dalla PSD2, che le informazioni fornite dall'AISP debbano essere aggregate o consolidate, lasciando ipotizzare che anche la dazione di una singola informazione relativa ad uno specifico conto di pagamento possa integrare la prestazione del servizio. Al riguardo, tuttavia, è stato opportunamente osservato che la qualificazione di un servizio come AIS richiede necessariamente una forma di consolidamento delle informazioni, anche se attinenti ad un unico conto (M. CATENACCI, C. FORNASARO, *PSD2: i prestatori di servizi di informazione sui conti (AISPS)*, aprile 2018, 3-4, disponibile su *www.diritto bancario.it*).

[18] Si consideri che il PISP non può detenere in alcuna fase della catena del pagamento i fondi del pagatore, quanto meno se autorizzato ad esercitare esclusivamente tale nuovo servizio di pagamento (cfr. 31° considerando e art. 66.3, lett. *a*, PSD2). L'attività dei PISPs non comporta, dunque, quella trasformazione delle scadenze (con i connessi rischi di liquidità) che è tipica degli intermediari bancari, con conseguenze anche in termini di requisiti prudenziali e di vigilanza minimi a carico di tali operatori (come anche degli AISPs, per i quali valgono analoghe considerazioni). Sarebbe infatti sproporzionato imporre ai TPPs che prestino in via esclusiva i servizi di disposizione di ordine di pagamento e di informazione sui conti, senza mai detenere fondi dei clienti, requisiti di fondi propri, potendo risultare sufficiente, affinché gli stessi siano in grado di fare fronte alle responsabilità derivanti dall'esercizio delle loro attività, un'assicurazione obbligatoria per responsabilità

altre fattispecie incluse nella medesima categoria (v. all. I alla PSD2), non si traducono nella gestione di conti di pagamento, né nell'esecuzione di operazioni di prelievo/versamento su conti o di pagamento mediante moneta scritturale (ovvero, secondo altra impostazione, nella gestione di flussi finanziari o nella detenzione di fondi degli utenti[19]). I PISs, invero, danno mero impulso ad un'operazione di pagamento che verrà eseguita da soggetti diversi, mentre gli AISs sono connotati da una valenza prettamente informativa, assumendo, al più, carattere puramente strumentale rispetto ad eventuali movimentazioni di fondi che l'utente decidesse di effettuare in un secondo tempo, dopo avere verificato le disponibilità sul proprio conto[20].

La scelta del legislatore europeo, dunque, trova spiegazione nella volontà di assicurare un'adeguata cornice normativa, comprensiva di efficaci forme di controllo, ad attività che, sfruttando le potenzialità insite nelle nuove tecnologie, risultano fondamentali per lo sviluppo dei pagamenti elettronici (obiettivo a sua volta necessario, come già ricordato, per sostenere la crescita economica e sociale nell'Unione),

civile professionale, o analoga garanzia (v. 35° considerando e art. 5, par. 2 e 3, PSD2). I criteri e gli indicatori per stabilire l'importo minimo di tale assicurazione o garanzia sono stati definiti dall'EBA negli *Orientamenti* del 12 settembre 2017 (EBA/GL/2017/08).

[19] D. GAMMALDI, C. IACOMINI, *Mutamenti del mercato dopo la PSD2*, in F. MAIMERI, M. MANCINI (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, cit., 128.

[20] Su un piano analogo, e per questo motivo associata spesso al fenomeno dell'*open banking*, si colloca la possibilità per gli emittenti carte di pagamento (CBPIIs, *card-based payment instrument issuers*) di ottenere dall'ASPSP la conferma (sotto forma di semplice risposta affermativa o negativa) della disponibilità, sul conto del pagatore, dell'importo necessario a dare esecuzione ad un pagamento a mezzo carta, a condizione che il conto sia accessibile *on line* e che il pagatore abbia prestato il proprio consenso (art. 65 PSD2; art. 5-*bis* d. lgs. n. 11/2010). Le disposizioni sul *fund checking* appaiono particolarmente innovative, poiché agevolano l'emissione di strumenti di pagamento *card-based* (in particolare, carte di debito) anche da parte di enti che non gestiscono il conto dell'utilizzatore, rendendo accessibili all'emittente alcune (limitate) informazioni relative ai conti aperti presso altri intermediari, al pari di quanto accade nel caso dei PISs e degli AISs. Diversamente da questi ultimi, tuttavia, il servizio di conferma di disponibilità di fondi non rappresenta un nuovo tipo di servizio di pagamento, ma un'attività che può essere svolta soltanto dagli intermediari già autorizzati ad emettere strumenti di pagamento basati su carta, funzionale rispetto all'utilizzo dei medesimi.

ma necessitano, al contempo, di regole che garantiscano l'efficacia e la sicurezza delle transazioni, nonché la protezione dei fondi e dei dati personali dei soggetti coinvolti, evidentemente esposti, per effetto dell'esercizio delle attività medesime, a maggiori rischi di attacchi esterni[21].

Emerge, da queste ultime considerazioni, l'ampio ventaglio di problematiche giuridiche che interessano la materia in esame, alcune delle quali possono considerarsi tipiche della generalità delle attività (finanziarie) ad alto impatto tecnologico, altre, invece, sono più direttamente riconducibili allo specifico tema oggetto di studio.

Ora, tralasciando gli aspetti di carattere più generale (*i.e.*, quelli legati all'esplosione del *FinTech* e alle relative questioni regolatorie e di supervisione[22]), la dottrina che sino a questo momento si è occupata del fenomeno dell'*open banking* pare avere concentrato l'attenzione su alcuni specifici filoni d'indagine, riferibili, in particolare, a tre distinte macro-tematiche (ognuna delle quali a sua volta frazionabile in ulteriori rivoli): *i)* apertura del mercato a nuovi operatori e profili di diritto della concorrenza; *ii)* tutela della riservatezza dei dati dei titolari dei conti di pagamento, in relazione all'accessibilità dei medesimi da parte di soggetti terzi; *iii)* caratteri dell'attività di impresa dei nuovi operatori e connessi profili di responsabilità civilistica, specie in rapporto alla mancata adozione dei necessari presidi di sicurezza a tutela dei clienti.

Gli studi finora condotti hanno dunque privilegiato un approccio "settoriale" alla materia, quasi sempre tralasciando una visione d'insieme che tenesse conto delle necessarie intersezioni tra le diverse aree di indagine. È appena il caso di rilevare, ad esempio, che l'ingresso nel mercato di nuovi prestatori di servizi di pagamento, certamente apprezzabile in chiave pro-concorrenziale e di stimolo all'innovazione,

[21] V. PROFETA, *I Third Party Provider: profili soggettivi e oggettivi*, in F. MAIMERI, M. MANCINI (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, cit., 51-53.

[22] Per una completa panoramica delle problematiche inerenti al *FinTech*, si rinvia all'esaustiva opera di M.-T. PARACAMPO (a cura di), *FINTECH. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, cit., cui *adde* E. CORAPI, R. LENER, *I diversi settori del Fintech. Problemi e prospettive*, Milano, 2019; F. FIMMANÒ, G. FALCONE (a cura di), *FinTech*, Napoli, 2019; G. FINOCCHIARO, V. FALCE, *Fintech: Diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, Bologna, 2019; da ultimo, M. CIAN, C. SANDEI, *Diritto del Fintech*, Milano, 2020.

richiede altresì che venga definito con accuratezza il regime delle rispettive responsabilità, ricollegandosi inevitabilmente, come già accennato, ad un incremento dei rischi di frode e di violazione/uso improprio di dati riservati. E ancora, la puntuale individuazione dei limiti entro i quali può essere legittimamente effettuato il trattamento dei dati personali dei titolari dei conti, da parte dei soggetti terzi autorizzati ad accedervi, finisce per avere un rilevante impatto sulla conformazione (e sul grado di concorrenzialità) del mercato dei servizi finanziari, specie se si considera che su quest'ultimo si sono da tempo affacciati, accanto ad operatori di dimensioni contenute, anche i grandi colossi della tecnologia (attratti dalla possibilità di sfruttare, attraverso le proprie avanzate capacità di *data analytics*, anche l'ingente mole di informazioni riveniente dall'esercizio dei nuovi *payment services*, al fine di ampliare/rafforzare l'offerta di altri servizi, finanziari e non)[23].

Si possono in altri termini ravvisare, nella materia in oggetto, una serie di *trade-offs* tra i diversi obiettivi della regolamentazione (ad es., tra apertura del mercato a nuovi operatori ed esigenze di sicurezza nella prestazione dei nuovi servizi, o tra promozione dell'innovazione e protezione dei dati personali dei titolari dei conti di pagamento), che rendono assai difficoltosa, per lo studioso di discipline gius-economiche, una valutazione complessiva della disciplina dell'*open banking*.

Muovendo da tali premesse, ci si prefigge di analizzare, in questa sede, le problematiche di maggior respiro attinenti al nuovo modello dei sistemi bancari aperti (*i.e.*, tutela della concorrenza, tutela della *privacy*, responsabilità dei nuovi prestatori di servizi di pagamento), con l'obiettivo di sviluppare alcune riflessioni – ognuna delle quali meritevole senz'altro di ulteriore approfondimento – circa l'adeguatezza delle risposte offerte sul piano legislativo e di individuare, conseguentemente, quei profili di criticità che necessiterebbero di un intervento correttivo.

[23] È stato puntualizzato, del resto, come la catena del valore dei servizi bancari e finanziari venga oggi «contesa "sull'ultimo miglio", quello relativo alla relazione con il cliente, al fine di acquisirne i dati e sviluppare servizi aggiuntivi» (A. PERRAZZELLI, *Intervento* alla sessione di apertura del Salone dei Pagamenti, *Payvolution*, Milano, 6 novembre 2019, 2, reperibile su *www.bancaditalia.it*). E proprio i dati sui pagamenti, utilizzabili per ricostruire le abitudini di spesa e personali dei clienti e per la profilazione dei medesimi, appaiono particolarmente preziosi.

3. *PSD2,* open banking *e concorrenza.*

Non v'è dubbio che tra i principali obiettivi della PSD2 risieda anche quello di garantire maggiore concorrenzialità al mercato dei servizi di pagamento, favorendo l'ingresso di nuovi operatori e migliorando, per tale via, il «tono competitivo di un settore a lungo percepito come una foresta pietrificata»[24].

Proseguendo lungo il solco già tracciato dalla prima PSD, che ha introdotto, accanto alle preesistenti categorie, una nuova famiglia di prestatori di servizi di pagamento (gli istituti di pagamento), la PSD2 pone le basi normative per l'apertura del mercato ad ulteriori soggetti, definendo una cornice regolamentare chiara ed uniforme, che renda possibile, come già accennato, la più ampia diffusione di nuovi servizi/mezzi di pagamento, in un contesto di adeguate tutele per l'utente.

L'ammodernamento del quadro normativo dovrebbe, pertanto, generare efficienze nel sistema dei pagamenti complessivamente inteso e garantire agli utenti un più ampio ventaglio di scelte (considerato che agevola il lancio di servizi e metodi di pagamento innovativi, di facile utilizzo, nonché sicuri), alimentando, in tal modo, la fiducia dei consumatori verso un mercato ritenuto essenziale per lo sviluppo delle attività economiche e sociali dell'UE[25].

Le nuove disposizioni in materia di libero accesso ai conti si rivelano evidentemente strumentali al raggiungimento di tali obiettivi. Si è già detto, del resto, che l'imposizione di un obbligo normativo come la *XS2A rule* permette, in concreto, di superare le naturali resistenze delle banche ad aprire la "scatola nera" dei dati dei propri clienti e a perdere,

[24] Così, A. ARGENTATI, *Le banche nel nuovo scenario competitivo*, cit., 448. La dottrina, d'altro canto, ha evidenziato come il settore in esame sia caratterizzato dalla presenza di *lock-in effects*, alte barriere all'entrata, abuso di potere dagli *incumbents* e altri comportamenti anti-competitivi, cui l'introduzione della *access to account rule* può oggi porre rimedio: O. BORGOGNO, G. COLANGELO, *Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule*, Stanford-Vienna European Union Law Working Paper No 35, 2018, in part. 7 e 19-20 (può leggersi su *https://ssrn.com/abstract=3251584*).

[25] Cfr. 6° e 7° considerando PSD2.

contestualmente, quel rapporto esclusivo con i medesimi sul quale si edifica, com'è noto, larga parte del loro *business*[26].

Sotto diverso profilo, inoltre, le regole sull'accesso ai conti, per come strutturate, consentono di esonerare da responsabilità i correntisti rispetto alla violazione dell'obbligo, sancito già dalla PSD (e replicato dalla PSD2), di non comunicare a terzi quei dati riservati (tipicamente, le credenziali di accesso ai servizi di pagamento o le *password* dispositive) richiesti per la fruizione dei servizi di *internet banking* e per il compimento delle operazioni di pagamento, posto che tale condotta è ritenuta indicativa di una grave negligenza, atta a fondare la responsabilità dell'utente per eventuali transazioni non autorizzate (v. *infra*, par. 5). Le norme in esame, dunque, agevolano, nella sostanza, l'esercizio di attività che risulterebbero altrimenti ostacolate dalla presenza dei divieti sopra indicati.

Sebbene le regole sull'accesso ai conti appaiano fortemente indirizzate a promuovere la concorrenza nel settore dei pagamenti *on line*, l'interprete deve comunque confrontarsi, sotto tale aspetto, con alcune questioni di non agevole soluzione.

La prima riguarda, in particolare, l'individuazione degli strumenti di intervento attivabili dalle autorità *antitrust* a fronte di possibili comportamenti anti-concorrenziali degli ASPSPs, volti a negare o ad ostacolare l'accesso ai conti dei clienti da parte di TTPs debitamente autorizzati (dai titolari dei conti stessi)[27].

A tal riguardo, frequente appare il richiamo, negli studi che si sono occupati dell'argomento, ai principi della nota *essential facility doctrine*, evocata in ragione del fatto che lo svolgimento dei nuovi servizi di pagamento non potrebbe prescindere dall'accesso ad una "infrastruttura" (la rete dei conti correnti) ritenuta insostituibile e sostanzialmente non duplicabile, controllata da soggetti con un forte

[26] V. *supra*, note 2 e 3. Sul timore delle banche di vedersi relegate a mere *dumb pipes* (ossia semplici depositarie dei fondi dei propri clienti, private della relazione diretta con gli stessi), per effetto dell'ingresso sul mercato di operatori in grado di offrire direttamente alla clientela moderni servizi a valore aggiunto, v. O. BORGOGNO, G. COLANGELO, *op. cit.*, 10.

[27] Anticipando quanto sarà più dettagliatamente specificato nel par. 4, si precisa che l'esercizio delle attività dei TPPs postula necessariamente il consenso esplicito del cliente, sussistendo il quale il fornitore terzo è autorizzato ad accedere ai conti accesi presso un ASPSP, indipendentemente dalla stipula di un accordo contrattuale con quest'ultimo.

potere di mercato (le imprese bancarie tradizionali)[28]. L'introduzione di una regola legale di accesso ai conti, invero, garantirebbe ai TPPs la possibilità stessa di esistere, dando stimolo alla concorrenza in mercati contigui rispetto a quello di fornitura dei servizi di amministrazione dei conti di pagamento.

In quest'ottica, quindi, alcuni Autori giungono ad affermare che «i conti di pagamento nel loro insieme finiscono con il rivestire il ruolo di un'*essential facility* e la previsione di un'obbligatoria accessibilità consente di garantire la piena concorrenza tra tutti i prestatori di servizi di pagamento, anche non bancari, che operano sulla rete dei conti nell'interesse dell'utente finale dei servizi»[29], mentre altri si limitano ad osservare, con maggior prudenza, come «il "sistema dei conti di pagamento" assurge al ruolo di "infrastruttura essenziale" *sui generis*, con rilevanti impatti sul sistema di relazioni tra gli operatori»[30].

In senso opposto, tuttavia, v'è anche chi ritiene che il legislatore europeo abbia inteso individuare nei conti di pagamento delle *facilities* "necessarie" per la fornitura ai consumatori di nuove tipologie di servizi *intenet-based*, ma non per questo "essenziali" ai medesimi fini, quanto

---

[28] Vale la pena di rammentare, in breve, che le condizioni in presenza delle quali un'impresa in posizione dominante si considera obbligata, secondo la dottrina richiamata nel testo, a mettere a disposizione di terzi una risorsa dalla stessa controllata sono: *a)* che detta risorsa sia effettivamente insostituibile o non duplicabile; *b)* che l'accesso alla *essential facility* sia necessario per un'effettiva concorrenza in un mercato a valle; *c)* che il rifiuto di garantire l'accesso alla risorsa determini l'eliminazione della concorrenza nel mercato a valle; *d)* che da tale rifiuto possa derivare un pregiudizio per i consumatori (COMMISSIONE EUROPEA, *Orientamenti sulle priorità della Commissione nell'applicazione dell'articolo 82 del Trattato CE al comportamento abusivo delle imprese dominanti volto all'esclusione dei concorrenti*, 2009). In dottrina, *ex multis*, D. DURANTE, G.G. MOGLIA, A. NICITA, *La nozione di* essential facility *tra regolamentazione e antitrust. La costruzione di un test*, in *Merc. conc. reg.*, 2001, 257; M. SIRAGUSA, M. BERETTA, *La dottrina delle* essential facilities *nel diritto comunitario ed italiano della concorrenza*, in *Contr. Impr. Eur.*, 1999, 260; S. BASTIANON, *A proposito della dottrina delle* essential facilities. *Tutela della concorrenza o tutela dell'iniziativa economica?* in *Merc. conc. reg.*, 1999, 149.

[29] V. PROFETA, *op. cit.*, 65.

[30] Così, R. MENZELLA, *Il ruolo dei big data e il mobile payment*, in F. MAIMERI, M. MANCINI (a cura di), *Le nuove frontiere*, cit., 152-3. Accennano ad «una sorta di *essential facility*», intesa come infrastruttura funzionale allo sviluppo di un ecosistema aperto per i pagamenti *retail*, anche D. GAMMALDI, C. IACOMINI, *Mutamenti del mercato dopo la PSD2*, cit., 139.

meno non nella (restrittiva) accezione del termine comunemente accolta dal diritto della concorrenza[31]; ed ancora, chi sostiene che richiamare, nella specie, l'accesso ad una *essential facility* risulti sostanzialmente fuorviante, sussistendo, oltre ad alcune significative differenze con le classiche figure di riferimento[32], notevoli difficoltà nell'individuare gli esatti confini del mercato rilevante (con evidenti conseguenze in merito alla possibilità di ravvisare in capo alle banche *incumbents* una posizione dominante e, quindi, alla configurabilità stessa di eventuali condotte abusive)[33].

A fronte di così spiccate divergenze dottrinarie, ed in assenza, allo stato, di un consolidato orientamento delle autorità competenti (dovuto alla mancata analisi di casi concreti), non resta che concludere che la violazione dell'obbligo di garantire l'accesso ai conti, seppur rilevante, in astratto, ai fini dell'attivazione dei tradizionali rimedi civilistici, ben più difficilmente può risultare sanzionabile sul piano *antitrust*, quanto meno sotto il profilo, sin qui esaminato, dello sfruttamento abusivo di una posizione dominante[34].

---

[31] A. BURCHI, S. MEZZACAPO, P. MUSILE TANZI, V. TROIANO, *Financial Data Aggregation e Account Information Services. Questioni regolamentari e profili di business*, in CONSOB, *Quaderni* FinTech, n. 4, 2019, 18-19.

[32] In particolare, la *XS2A rule* non richiederebbe alcun compenso per l'accesso ai dati dei conti, né alcun accordo contrattuale tra TPP e ASPSP, essendo sufficiente, per poter accedere ai conti di pagamento, il solo consenso del titolare (F. DI PORTO, G. GHIDINI, '*I Access Your Data, You Access Mine'. Requiring Data Reciprocity in Payment Services*, 2019, 12 ss., reperibile su *https://ssrn.com/abstract=3407294*).

[33] Ed invero, ponendo specificamente l'attenzione sui dati dei clienti, è stato affermato che se le autorità *antitrust* decidessero di includere nella definizione di mercato rilevante, malgrado le indicazioni più restrittive della PSD2 (artt. 66 e 67), «data other than just the customer accounts' payment history, such as behavioral data from internet search, social network, and comparison sites pertaining to the bank's client», sarebbe difficile, rispetto a tali dati, teorizzarne la natura di *essential facility*, come sarebbe altresì legittimo revocare in dubbio «the monopolistic power of incumbent banks». Viceversa, ove le Autorità identificassero «each and every customer's account data as a separate relevant market; or consider that not only payment data but all data about a given customer or a bunch of customers make a separate relevant market (…) banks would easily be deemed dominant and any refusal to provide access to such data be prohibited as abusive» (F. DI PORTO, G. GHIDINI, *op. cit.*).

[34] In termini dubitativi v., ad es., Vito MELI, *Opportunità e sfide per la concorrenza nella disciplina dei servizi di pagamento*, in M.C. PAGLIETTI, M.I. VANGELISTI, *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli*

In un quadro ancora così incerto, ulteriori fattori di complicazione discendono, poi, dall'eterogenea natura dei nuovi *competitors* delle banche (intese come prestatrici dei servizi di pagamento tradizionali), tra i quali, come già sottolineato, non si annoverano unicamente piccole o medie imprese del ramo *FinTech*[35], ma anche soggetti di enormi dimensioni e dalla smisurata potenza economica, quali le *Big Tech companies*, in grado di alterare profondamente le dinamiche competitive e l'attuale assetto del mercato bancario. È evidente, del resto, che questi ultimi non soltanto godono già, in determinati settori, di un innegabile vantaggio competitivo (in termini di bacini di utenza, di dotazioni tecnologiche e di mezzi finanziari), utilizzabile per affermarsi rapidamente anche nel mercato dei servizi di pagamento, ma possono altresì occupare, nei relativi mercati di provenienza, una posizione egemone, tale da prospettare un inedito conflitto tra «intermediari bancari, da un lato, non in posizione dominante sul proprio mercato, ma sottoposti all'obbligo di dare accesso ai conti dei propri clienti, e operatori digitali, dall'altro, che proprio grazie a quell'obbligo normativo si espandono nel mercato dei pagamenti, forti della posizione di forza detenuta altrove»[36].

Ora, se è fondata, come pare anche a chi scrive, l'affermazione secondo cui i colossi del *Tech* sono fortemente interessati al mercato dei servizi di pagamento (o bancari-finanziari, più in generale) non

interessi nella PSD2, Roma, 2020, 141-142, il quale, muovendo dal presupposto che la particolare posizione che ciascuna banca detiene sui conti dei propri clienti sia in qualche modo assimilabile ad una posizione di monopolio, ipotizza che alcuni comportamenti individuali possano anche ricondursi all'abuso di posizione dominante, sebbene la mancanza di precedenti in tal senso renda il tema assai controverso.

[35] Enti rispetto ai quali è stata peraltro ventilata l'applicazione, in caso di condotte ostruzionistiche da parte delle banche *incumbents*, della normativa sulle pratiche commerciali scorrette, nei limiti in cui può essere estesa anche al settore *B2B* (A. ARGENTATI, *Le banche nel nuovo scenario competitivo*, cit., 458).

[36] In questi termini A. ARGENTATI, *Le banche nel nuovo scenario competitivo*, cit., 459, con espresso riferimento alla posizione dominante di *Google* nei servizi di ricerca *on line*, di *Facebook* nei *social network* e di *Amazon* nell'intermediazione nel commercio elettronico. In prospettiva analoga v. anche V. MELI, *op. cit.*, ove si sottolinea, in particolare, l'urgenza di approfondire il dibattito «su come inquadrare nell'analisi antitrust non l'attività specifica di ciascuno di tali operatori bensì l'enorme volume di informazioni che essi detengono, i *big data*, che può avere una valenza trasversale nei mercati».

tanto (o non solo) per espandere la propria attività nel settore dell'intermediazione finanziaria, quanto «per trattenere i clienti nel loro spazio virtuale (anche quando effettuano un pagamento o chiedono un prestito) e naturalmente per arricchire il loro patrimonio già inestimabile di dati (che, a differenza delle banche, non devono condividere con nessuno)»[37], appare lecito interrogarsi anche circa la necessità di adottare strumenti che consentano di riequilibrare la relazione competitiva tra banche e *Big Tech.*

Su questi temi, ancora poco esplorati, ha iniziato a confrontarsi parte della dottrina, muovendo specificamente dal presupposto che le norme della PSD2 vietano sì, in linea di principio, lo sfruttamento dei dati dei conti da parte dei TPPs per scopi *diversi* dall'erogazione dei servizi di pagamento dagli stessi prestati[38], ma non sembrano impedire, tuttavia, che i dati e le informazioni acquisiti nell'espletamento dei servizi in questione possano essere ulteriormente utilizzati e/o incrociati dal *provider* con altri dati relativi all'utente (come quelli ricavabili, ad es., dalla navigazione su *Internet* o dall'analisi delle abitudini di spesa del soggetto interessato), ai fini di una prestazione mirata, più efficiente e maggiormente personalizzata dei servizi medesimi, con benefiche ripercussioni anche per l'innovazione[39].

Sulla base di tale assunto, una fra le più interessanti questioni che sono state prospettate riguarda quindi l'opportunità di prevedere, a favore delle banche detentrici dei conti di pagamento, una clausola di reciprocità nei confronti dei c.d. *big data conglomerates* che abbiano deciso di agire anche come TPPs (ossia, nello specifico, come prestatori di *payment initiation services* o di *account information services*), beneficiando della *access to account rule*. Se è vero, infatti, che nulla sembra precludere a tali soggetti, quanto meno ai fini di un miglioramento dei servizi di pagamento erogati, la possibilità di

[37] V. ancora A. ARGENTATI, *Le banche nel nuovo scenario competitivo*, cit., 456.

[38] V. *infra*, par. 4.

[39] Cfr. F. DI PORTO, G. GHIDINI, '*I Access Your Data, You Access Mine',* cit., 16, ove si legge: «In other words, Fintechs are *not* prevented from 'using, storing and accessing' account data *if* they want to use them to enhance, make the payment initiation service more agreeable, efficient and consumer-centric. By allowing them to run big data analytics on those data (made possible thanks to the use, storing and accessing) Fintechs are put in a position to ameliorate the paying experience of consumers by targeting their needs and further enhance innovation».

elaborare, sfruttando le loro avanzate capacità di *data analytics*, le informazioni rivenienti dall'accesso ai conti, incrociandole anche con i dati di diversa natura di cui gli stessi già ampiamente dispongono, potrebbe rivelarsi opportuno, in un'ottica di livellamento del terreno di gioco e di promozione dell'efficienza e dell'innovazione nel settore dei pagamenti, garantire anche alle banche detentrici dei conti "aperti" la possibilità di un accesso (autorizzato dai soggetti interessati) ai dati non finanziari dei clienti posseduti dalle *Big Tech* (*i.e.*, i dati comportamentali tratti da ricerche, *social networks*, siti di comparazione, ecc.), sia pur ponendo analoghe limitazioni nell'impiego dei dati suddetti (ossia circoscrivendone l'utilizzo al solo scopo di una più efficiente prestazione dei medesimi servizi di pagamento digitali)[40].

Un'ipotesi che, se confermata, sconterebbe certamente alcune difficoltà sul piano sia normativo che applicativo (esattamente rispetto a quali imprese, e quali specifiche condizioni, garantire agli ASPSPs la sopra descritta condizione di reciprocità? E limitatamente a quali specifiche tipologie di dati non finanziari dovrebbe essere esteso l'accesso in favore delle banche?), ma che potrebbe efficacemente controbilanciare, nondimeno, quel vantaggio competitivo altrimenti attribuito alle *Big Tech companies*, stimolando altresì gli operatori tradizionali a sviluppare competenze e abilità (*data analytics*) di cui gli stessi non risultano, allo stato, ancora adeguatamente provvisti, per potersi poi presentare sul mercato come *competitors* più efficienti e più temibili.

4. *PSD2,* open banking *e tutela dei dati personali.*

Ulteriore ventaglio di problemi innescati dalle regole sull'*open banking* riguarda la tutela dei dati personali registrati nei conti di pagamento.

Considerato, infatti, che l'esercizio dei nuovi servizi di pagamento postula l'accesso *ab externo* ai conti di pagamento e ai dati ivi contenuti (con i limiti cui si farà cenno nel prosieguo), sorge ovviamente l'esigenza di proteggere gli interessati da un uso illegittimo dei suddetti dati da parte dei TPPs o di terzi (si immagini il caso di un attacco ai

[40] Il tema è ampiamente sviluppato da F. DI PORTO, G. GHIDINI, '*I Access Your Data, You Access Mine',* cit., 22 ss.

sistemi informatici di un PISP o di un AISP), oltre che dal rischio di frodi perpetrate abusando di informazioni personali e riservate (basti pensare alla ricca casistica delle operazioni di pagamento non autorizzate, commesse mediante utilizzo illecito delle credenziali di sicurezza rilasciate al titolare di un determinato strumento di pagamento).

A dispetto dell'indubbia rilevanza pratica del problema, la PSD2 detta, sul punto, regole piuttosto scarne, limitandosi sostanzialmente a vietare un uso dei dati dei correntisti *diverso* da quello direttamente correlato all'attività tipica dei TPPs. In estrema sintesi, infatti, secondo le attuali disposizioni di legge: *i)* il PISP non chiede al pagatore dati diversi da quelli necessari a prestare il servizio di disposizione di ordini di pagamento, non usa e non conserva dati e non vi accede per fini diversi dalla prestazione del servizio, né conserva dati sensibili relativi ai pagamenti eseguiti dal pagatore; *ii)* l'AISP accede alle sole informazioni sui conti di pagamento designati e sulle operazioni di pagamento eseguite su detti conti, senza richiedere dati sensibili relativi ai pagamenti, inoltre non usa e non conserva dati, né vi accede per fini diversi dalla prestazione del servizio di informazione sui conti[41].

Va peraltro segnalato che, con disposizione di carattere generale, riferita alla protezione dei dati personali nel contesto della prestazione di ogni tipo di servizio di pagamento (compresi, dunque, quelli erogati dai TPPs), sia l'art. 94 della PSD2 che l'art. 29 del d. lgs. n. 11/2010 prevedono che: *i)* è consentito il trattamento dei dati personali da parte di sistemi di pagamento e di prestatori di servizi di pagamento, conformemente alla vigente normativa in tema di *data protection*, se necessario per garantire la prevenzione, l'indagine e l'individuazione dei casi di frode nei pagamenti; *ii)* i prestatori di servizi di pagamento hanno accesso, trattano e conservano i dati personali necessari alla prestazione dei rispettivi servizi, solo dietro consenso esplicito dell'utente dei servizi di pagamento.

Relativamente ai punti trattati, dunque, l'impianto della PSD2 risulta alquanto asciutto, ma soprattutto sprovvisto, per altro verso, di regole idonee a garantire un efficace coordinamento con la normativa generale in materia di protezione dei dati personali (in atto, Regolamento UE 2016/679, c.d. GDPR), della quale si assume l'applicazione anche nel

[41] Artt. 66.3 e 67.2 PSD2; artt. 5-*ter* e 5-*quater* d. lgs. n. 11/2010.

contesto della prestazione dei servizi di pagamento[42]. E invero, la coesistenza dei due plessi normativi non appare affatto semplice, sollevando una serie di questioni interpretative che, in difetto di un adeguato raccordo tra le disposizioni in esame – preordinate, peraltro, al raggiungimento di finalità non del tutto coincidenti[43] –, non sembrano trovare agevole risposta.

Attenta dottrina, pertanto, ha prontamente messo in luce come la PSD2 lasci aperti numerosi interrogativi, densi di riflessi anche sul piano pratico e applicativo[44]. In questo senso, ad es., non soltanto viene in rilievo la differenza di significato attribuibile, nei due gruppi di norme, a concetti apparentemente identici (si pensi, ad es., alla diversa portata che rivestono, nei due ambiti disciplinari in considerazione, le

[42] V. 89° considerando PSD2, ove si specifica che, qualora vi sia trattamento di dati personali da parte di prestatori di servizi di pagamento, è opportuno che siano indicati lo scopo specifico e le pertinenti basi giuridiche, che vi sia conformità con i requisiti normativi di sicurezza, che siano rispettati i basilari principi di necessità, proporzionalità, limitazione delle finalità e proporzionalità nel periodo di conservazione dei dati. Il 90° considerando, inoltre, precisa che la direttiva rispetta i diritti fondamentali e osserva i principi stabiliti dalla Carta dei diritti fondamentali dell'Unione Europea, tra cui anche il diritto alla protezione dei dati personali.

[43] Il GDPR, infatti, tutela il diritto di ogni persona fisica alla protezione dei propri dati personali, stabilendo che il trattamento degli stessi è consentito, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato (il quale ha sempre il diritto di essere adeguatamente informato sul modo in cui i propri dati sono trattati, di controllare l'accesso ai medesimi e di trasmettere i dati già forniti ad un titolare del trattamento ad altro titolare del trattamento). La PSD2, e le disposizioni sull'*open banking* in particolare, appaiono maggiormente focalizzate, invece, sulla necessità di garantire un'apertura concorrenziale del mercato dei servizi di pagamento a nuovi intermediari (TPPs), obiettivo che presuppone tuttavia, come più volte accennato, la contestuale tutela dei dati dei titolari dei conti (non necessariamente persone fisiche), compatibilmente con la disciplina di carattere generale.

[44] Il riferimento è a M. RABITTI, A. SCIARRONE ALIBRANDI, *I servizi di pagamento tra PSD2 e GDPR: open banking e conseguenze per la clientela*, in F. CAPRIGLIONE, Liber amicorum *Guido Alpa*, Cedam, 2019, 726-727.

nozioni di *«dati sensibili»*[45] o di *«consenso esplicito»* dell'utente[46]), ma dubbi non meno significativi emergono anche in merito alla protezione da accordare alle c.d. *silent parties* (nella specie, i beneficiari dei pagamenti), i cui dati personali possono essere trattati, seppur in difetto di consenso dall'interessato, durante lo svolgimento delle attività dei TPPs[47]; ai criteri da utilizzare per stabilire chi, tra il prestatore di servizi di pagamento di radicamento del conto e il TPP, rivesta il ruolo di *«titolare del trattamento»* e chi, invece, sia qualificabile come *«responsabile del trattamento»*[48]; o ancora, ai criteri che possano

[45] Si osservi, al riguardo, che la PSD2 preclude ai TPPs di trattare, conservare e addirittura richiedere (per i soli AISPs) *«dati sensibili»* degli utenti (genericamente intesi, ai sensi dell'art. 4, n. 32, come dati relativi ai pagamenti che possono essere utilizzati per commettere frodi, incluse le credenziali di sicurezza personalizzate), con l'evidente intento di sterilizzare i rischi di azioni fraudolente in danno della clientela e rafforzare i presidi di sicurezza, mentre il GDPR sposa la logica, più ampia, della protezione dei dati personali più delicati (e perciò qualificati come *«sensibili»*), concernenti l'origine razziale o etnica, le convinzioni politiche o religiose, la salute, l'orientamento sessuale degli individui, ecc.

[46] Il consenso esplicito previsto dalla PSD2 per l'accesso, la trattazione e la conservazione dei dati personali relativi alla prestazione dei servizi di pagamento (art. 94) è, infatti, riferito e limitato alla sola prestazione dei servizi medesimi (e alla stessa funzionale), laddove il consenso previsto dal GDPR ha portata e valenza più generale, riguardando ogni dato dell'utente, ovvero ogni possibilità di utilizzo dei dati che il titolare del trattamento è autorizzato a porre in essere, nel rispetto dei limiti di legge. In argomento si vedano le riflessioni di A. BURCHI, S. MEZZACAPO, P. MUSILE TANZI, V. TROIANO, *Financial Data Aggregation e Account Information Services.*, cit., 33 ss., ove si precisa che la previsione del *«consenso esplicito»*, da parte della PSD2, mira ad offrire all'utente dei servizi di pagamento una protezione rafforzata, rappresentando un requisito aggiuntivo di natura contrattuale, in virtù del quale il PSP è tenuto ad informare il cliente della raccolta e del successivo trattamento dei dati personali necessari alla prestazione del servizio, mentre l'utente deve esplicitamente acconsentire al trattamento per tali specifiche finalità, ai sensi e per gli specifici effetti della normativa di settore.

[47] Sul punto si è espresso, com'è noto, lo *European Data Protection Board* (EDPB), che, in una lettera indirizzata al Parlamento europeo in data 5 luglio 2018, ha chiarito che l'interesse legittimo del titolare del trattamento o di un terzo (art. 6, comma 1, lett. *f*, GDPR) costituisce una base legale sufficiente per il trattamento dei dati della parte silente, purché vengano rispettati i principi di minimizzazione, limitazione e trasparenza e i dati vengano utilizzati solo per tale finalità di trattamento.

[48] Sostiene ad es. D. HELGADOTTIR, *The Interaction between Directive 2015/2366 (EU) on Payment Services (PSD2) and Regulation (EU) 2016/679 on General Data Protection (GDPR) Concerning Third Party Providers*, 12 dicembre 2019, 16 (*https://ssrn.com/abstract=3455428*), che, «when a bank receives data from another

sovrintendere alla distribuzione di responsabilità tra prestatore di servizi di pagamento di radicamento del conto e TPP a fronte di un illecito utilizzo dei dati del cliente, specie in assenza di appositi accordi contrattuali tra tali soggetti[49].

Da ciò si evince quanto possa essere delicata l'applicazione delle regole sulla protezione dei dati personali alla prestazione dei servizi di pagamento, tanto più che, in tale ambito, le prime si intersecano altresì con le disposizioni in tema di trasparenza e di sicurezza dei

bank or institution and is processing the data under its own terms, then the bank is a processor. So, in this regard, if data moves from the bank to a TPP, the bank is the controller and the TPP (AISP or PISP) is a processor instructed by the data controller». Altri hanno invece osservato che, laddove manchi un rapporto contrattuale tra ASPSP e TPP, esteso sino a stabilire chi fra i soggetti coinvolti sia il titolare e chi il responsabile del trattamento (art. 28 GDPR), con previsione anche delle rispettive responsabilità in caso di frode, utilizzo illecito dei dati o *data breach*, entrambi i soggetti potrebbero essere ritenuti titolari del trattamento (fermo restando che, ai sensi del GDPR, è titolare del trattamento chi effettua l'uso secondario degli stessi, ossia il TPP, allorquando utilizza i dati ai fini degli adempimenti dei propri obblighi contrattuali): M. RABITTI, A. SCIARRONE ALIBRANDI, *op. cit.*, 730-731; v. anche EUROPEAN BANKING FEDERATION, *Guidance for implementation of the revised Payment Services Directive*, dicembre 2019, 84.

[49] D. HELGADOTTIR, *op. cit.*, 9. È stato peraltro sollevato il dubbio se una banca possa rifiutare l'accesso ai dati dei propri correntisti ad una terza parte che non sia ritenuta in grado di garantirne la riservatezza: gli obblighi di condivisione dei dati connessi al regime di *open banking*, invero, sembrano anche in questo caso confliggere insanabilmente con i doveri di protezione dell'interessato, imposti dal GDPR (B. RUSSO, *Tecnologie digitali e tutela dei dati personali: quali possibili impatti sulla PSD2?*, in questa *Rivista.*, 2019, I, 287-288). Di certo, il problema non pare trovare soluzione nel disposto dell'art. 68.5 PSD2 (ove si stabilisce espressamente che l'accesso del TPP ad un conto di pagamento – che deve sempre avvenire, si badi, in modo equo e non discriminatorio - può essere negato solo per motivi *«obiettivamente giustificati e debitamente comprovati connessi all'accesso fraudolento o non autorizzato al conto di pagamento»* da parte del *provider* terzo), a meno che non si voglia accedere ad un'interpretazione estensiva della norma, che non sembra tuttavia argomentabile in modo convincente.

pagamenti[50], con un impatto che finisce per estendersi, per alcuni rilevanti aspetti, anche all'organizzazione interna degli intermediari[51].

Ora, sebbene in questa sede non sia possibile analizzare diffusamente ciascuno dei punti sopra menzionati, vi è uno specifico profilo, evocato dalla complessa relazione tra necessità di protezione dei dati personali dell'utente ed esigenze di sviluppo del mercato dei pagamenti digitali, su cui merita soffermare l'attenzione.

In particolare, muovendo dall'assunto, cui già si è accennato, che il mercato dei nuovi servizi di pagamento sollecita gli interessi delle *Big*

[50] Sotto il primo profilo (trasparenza), invero, la PSD2 prevede che l'utente sia informato del trattamento dei propri dati personali, in conformità alle disposizioni generali; sotto il secondo (sicurezza) rileva, invece, la necessaria adozione di mezzi di comunicazione sicura tra intermediari, attraverso i quali possano essere scambiate informazioni relative ai servizi di pagamento, nel rispetto dei criteri stabiliti dal Regolamento Delegato UE n. 2018/389 della Commissione, contenente regole sull'autenticazione forte del cliente e sugli *standard* aperti di comunicazione comuni e sicuri. A quest'ultimo aspetto si ricollega la convergenza, ai fini sopra citati, verso quella particolare soluzione tecnologica rappresentata dalle APIs (*Application Programming Interfaces*), programmi che permettono la comunicazione tra le banche e i soggetti terzi che chiedono l'accesso al conto dei clienti, secondo canoni di interoperabilità e di sicurezza (v. 93° considerando PSD2). Le APIs garantiscono che solo le funzioni (e i dati) per cui il cliente abbia dato un esplicito consenso siano a disposizione dei TPPs, ma prospettano, al contempo, diverse problematiche relative al loro effettivo grado di standardizzazione e interoperabilità (v. M. RABITTI, A. SCIARRONE ALIBRANDI, *op. cit.*, 718 ss.; COMMISSIONE EUROPEA, *FinTech Action plan*, 8 marzo 2018; O. BORGOGNO, *Regimi di condivisione dei dati ed interoperabilità: il ruolo e la disciplina delle A.P.I.*, in *Diritto dell'informazione e dell'informatica*, 2019, II, 689 ss.).

[51] Si pensi, ad es., alle misure organizzative che gli intermediari sono tenuti ad adottare per garantire la sicurezza e gestire eventuali incidenti operativi e di sicurezza. In quest'ottica, la PSD2 prevede che i PSP debbano, sin dalla fase di autorizzazione allo svolgimento delle proprie attività, adottare misure di monitoraggio e gestione degli incidenti relativi alla sicurezza e dei reclami dei clienti relativi alla sicurezza (art. 5, comma 1, lett. *f*), nonché redigere un documento relativo alla politica di sicurezza, comprendente una valutazione dettagliata dei rischi relativi ai servizi di pagamento offerti e una descrizione delle misure di controllo e di mitigazione adottate per tutelare gli utenti contro i rischi in materia di sicurezza, compresi frode e uso illegale di dati sensibili e personali (art. 5, comma 1, lett. *j*). In argomento rilevano, peraltro, le linee-guida adottate dall'EBA in attuazione dell'art. 5.5 PSD2 (EBA/GL/2017/09 dell'11 luglio 2017), nonché gli *Orientamenti* EBA in materia di segnalazione di gravi incidenti del 19 dicembre 2017 e quelli sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento del 12 gennaio 2018, richiamati anche nelle disposizioni di vigilanza della Banca d'Italia.

Tech companies anche in ragione della possibilità di acquisire grandi quantità di dati relativi ai conti di pagamento (immaginabili come una sorta di materia prima a partire dalla quale è possibile costruire, tramite sofisticati processi di aggregazione e rielaborazione, servizi ad elevato valore aggiunto), è interessante interrogarsi sulla reale estensione dei limiti all'utilizzo dei dati medesimi, per come effettivamente imposti dall'ordinamento.

Già si è detto, ad esempio, che il divieto di sfruttare ulteriormente a fini commerciali i dati acquisiti dai TPPs nello svolgimento dei nuovi servizi di pagamento non sembra precludere, alle imprese che ne abbiano la capacità e le competenze, la combinazione degli stessi con altre informazioni relative agli utenti (ad es., *behavioral data*), in funzione di una prestazione maggiormente "targettizzata" dei servizi medesimi (v. *supra*, par. 3). A ben considerare, infatti, in simili casi si rimarrebbe nell'ambito di un uso dei dati personali del cliente ai fini della (migliore) erogazione degli stessi servizi rispetto ai quali l'originario trattamento era stato autorizzato dall'interessato.

Il dubbio che può sorgere, tuttavia, è se sia concepibile l'uso dei dati dei conti anche per scopi diversi e ulteriori rispetto a quelli sopra descritti, e segnatamente in vista della prestazione di servizi (finanziari e non) distinti da quelli nel contesto dei quali tali dati siano stati già acquisiti e trattati.

Forti sono, in questo senso, le suggestioni che provengono da altri ordinamenti, come ad es. quello statunitense, là dove i servizi di *consumer financial data aggregation*, particolarmente affini a quelli di informazioni sui conti, si caratterizzano, al contempo, per un raggio di operatività ben più ampio rispetto a questi ultimi, dal momento che si traducono nell'aggregazione di un vasto *set* di informazioni di natura finanziaria riferite ai clienti (*i.e.*, non solo quelle registrate sui conti di pagamento e/o relative alle operazioni di pagamento ad essi associate, ma anche quelle concernenti prestiti, carte di credito o investimenti in strumenti o prodotti finanziari), poi utilizzate anche ai fini della vendita ai medesimi clienti di prodotti e servizi del ramo finanziario (creditizi, di investimento, assicurativi o previdenziali), individuati come adeguati alle loro specifiche caratteristiche ed esigenze personali[52].

[52] A. BURCHI, S. MEZZACAPO, P. MUSILE TANZI, V. TROIANO, *op. cit.*, 9. Altro esempio potrebbe essere rappresentato dall'esperienza maturata nel Regno Unito, la

Il quesito che si pone all'interprete, in altri termini, è stabilire se il divieto per i TPPs (e per gli AISPs in particolare) di sfruttare i dati dei conti per scopi (commerciali) diversi dalla prestazione dei propri servizi tipici sia o meno compatibile con un ulteriore trattamento dei medesimi dati, in funzione dell'erogazione al cliente, che abbia prestato il proprio consenso, di servizi di diversa natura[53].

Al riguardo, sebbene il tenore letterale delle disposizioni di riferimento (art. 66-7 PSD2) induca, a prima vista, ad offrire al quesito risposta negativa (lasciando intravedere l'esistenza di un divieto assoluto, a carico dei TPPs, di ulteriori trattamenti dei dati personali dei titolari dei conti), appare difficile, ad una più attenta analisi, non concordare con quella dottrina secondo la quale un'interpretazione eccessivamente restrittiva del testo normativo si porrebbe palesemente in contrasto con le disposizioni del GDPR, che non sembrano affatto escludere, nella specie, la liceità di trattamenti ulteriori di dati già raccolti.

Nulla, invero, sul piano giuridico sembra impedire ad un utente di poter autorizzare il trattamento e l'utilizzo ulteriore dei propri dati personali registrati in uno o più conti di pagamento, nell'ottica della successiva fruizione, nel proprio interesse, di altri prodotti e servizi a valore aggiunto, che presuppongano l'uso di tali informazioni[54].

---

cui normativa autorizza i *Price Comparison Websites* ad agire come PISP o AISP, offrendo anche servizi di tipo bancario (E. COLOMBARI, R. TEDESCHI, *Regolamentazione e apertura volontaria: breve guida all'open banking in Italia e all'estero*, s.d., 9, reperibile su *www.prometeia.it*).

[53] I dati raccolti dai TPPs, ad es., potrebbero essere analizzati, elaborati e trasmessi ad imprese terze, ai fini dell'erogazione di ulteriori servizi o attività, come valutazione del merito creditizio, pianificazione finanziaria, consulenza in materia di investimenti, previdenziale o assicurativa, o dell'adempimento degli obblighi di valutazione dell'adeguatezza/appropriatezza nel contesto ed in funzione della prestazione dei servizi di investimento (A. BURCHI, S. MEZZACAPO, P. MUSILE TANZI, V. TROIANO, *op. cit.*, 35 ss.). Si tratta, d'altro canto, di servizi il cui corretto espletamento presuppone l'uso di informazioni affidabili e aggiornate, quali potrebbero essere anche quelle rivenienti dai conti di pagamento.

[54] A. BURCHI, S. MEZZACAPO, P. MUSILE TANZI, V. TROIANO, *op. cit.*, 139. Nello stesso senso anche D. HELGADOTTIR, *op. cit.*, 22 ss., e, incidentalmente, S. VEZZOSO, *op. cit.*, 32, secondo la quale «Upon customer's consent, AISPs can then share the data with other companies such as price comparison websites that offer additional services that the customer may benefit from». Posto, tuttavia, che le banche sopportano ingenti costi per la manutenzione della rete dei conti, resta aperto il

In altri termini, fermo restando il divieto per i TPPs di utilizzare, nel proprio interesse e per proprio conto, i dati personali dei clienti per scopi diversi da quelli per i quali gli stessi sono stati raccolti (ciò che appare conforme al generale principio della limitazione delle finalità del trattamento, espresso dall'art. 5, par. 1, lett. *b*, GDPR), non v'è motivo di ritenere che il titolare dei dati non sia libero di conferire (anche) al TPP un distinto mandato per un loro ulteriore trattamento, funzionale alla prestazione di servizi di diversa natura (e dunque preordinato, anche in questo caso, al conseguimento di specifiche e predeterminate finalità)[55]. In simili ipotesi, d'altronde, non si configurerebbe alcuna violazione del divieto espresso dagli artt. 66 e 67 PSD2 (che resta pienamente operativo, nei limiti sopra specificati), bensì l'esercizio di un diritto soggettivo all'uso dei propri dati, riconosciuto dalle disposizioni generali in materia di *data protection* (GDPR) in conformità alle quali deve essere letta e applicata la normativa di settore (PSD2).

Certamente, non sfugge a chi scrive che l'ambiguità del dato normativo, amplificata dall'insufficiente raccordo tra PSD2 e GDPR, rischia di indebolire tale interpretazione, per quanto fondata su valide argomentazioni, anche di carattere sistematico. Nondimeno, ciò che appare interessante osservare è che ove la stessa, nel tempo, dovesse risultare confermata, le conseguenze sulla complessiva configurazione e sui possibili sviluppi del mercato finanziario (ivi comprese le implicazioni sul piano della regolamentazione e della supervisione) apparirebbero quanto mai rilevanti. Il patrimonio di dati racchiuso nei conti di pagamento, invero, non rappresenterebbe più soltanto il fondamento necessario per la prestazione dei nuovi servizi di pagamento, per come disciplinati dalla PSD2, ma una preziosissima base informativa per la fornitura di servizi ulteriori e diversi, il cui

problema delle condizioni alle quali debba essere consentito l'ulteriore utilizzo dei dati dei clienti: la previsione di un diritto di accesso gratuito agli stessi da parte dei TPPs, infatti, sarebbe stata controbilanciata dalla PSD2 attraverso l'imposizione di specifiche limitazioni, sicché un utilizzo dei dati di pagamento per finalità diverse dovrebbe essere disciplinato, secondo alcuni, da specifici accordi contrattuali tra la banca e il fornitore terzo (D. GAMMALDI, C. IACOMINI, *Mutamenti del mercato dopo la PSD2*, cit., 139).

[55] La base giuridica dell'ulteriore trattamento sarebbe dunque rappresentata, nella specie, dal consenso dell'interessato, ai sensi dell'art.6, comma 1, lett. *a)*, GDPR.

esercizio postula una conoscenza quanto più completa e approfondita della situazione economico-finanziaria dell'utente. Per tale via, ad esempio, si potrebbe determinare – come dianzi accennato – la trasformazione degli AISs da servizi meramente informativi a servizi di analisi, elaborazione e condivisione con imprese terze dei dati raccolti e trattati, in chiave strumentale rispetto ad un'efficiente e corretta erogazione di servizi *lato sensu* finanziari, spazianti dalla valutazione del merito creditizio alla gestione di portafogli, dalla consulenza finanziaria a quella patrimoniale o assicurativa, ecc.[56]

In questa prospettiva, dunque, la stessa nozione di *open banking* acquisirebbe una nuova e più ampia dimensione, posto che le soluzioni tecnologiche (APIs) e normative (PSD2) che ne sono alla base potrebbero incoraggiare la realizzazione di progetti che sconfinano dalla specifica area tematica dei servizi di pagamento, per dare luogo ad ulteriori ed innovative modalità di interazione tra i vari attori presenti nel sistema finanziario, con ulteriore stimolo alla competizione, all'innovazione e al benessere dei consumatori.

5. *PSD2,* open banking *e sicurezza delle transazioni. La responsabilità dei nuovi prestatori di servizi di pagamento*.

Un ultimo tema sul quale occorre soffermare l'attenzione è quello della responsabilità dei TPPs, in relazione alla prestazione dei nuovi servizi di pagamento.

La rilevanza dell'argomento non può sfuggire, se solo si pensa che l'inserimento di fornitori terzi nella "catena procedimentale" di ogni operazione di pagamento intermediato[57] implica, come già precisato, un notevole incremento dei punti di accesso ai conti, con maggiori rischi di *data breach*, di frodi informatiche e di abusi in danno dei correntisti.

Certamente, i diversi ruoli che, a livello operativo, i predetti soggetti sono chiamati a svolgere incidono anche sul piano delle rispettive

[56] V. *supra*, nt. 53.

[57] La dimensione procedimentale delle operazioni di pagamento mediate da intermediari, intese come pluralità di atti e fatti preordinati alla soddisfazione del creditore e alla liberazione del debitore, è frequentemente evidenziata in letteratura (v. ad es. M. ONZA, *Gli strumenti di pagamento nel contesto dei pagamenti on line*, in *Dir. banc. fin.*, 2017, 679; V. DE STASIO, *Ordine di pagamento non autorizzato e restituzione della moneta*, Milano, 2016, 64).

responsabilità: se gli AISPs, infatti, si limitano a fornire un servizio a carattere eminentemente informativo (salve le possibilità di futuro sviluppo immaginate *sub* 4), i cui rischi sono essenzialmente limitati all'accesso abusivo ai dati personali immagazzinati nei conti (e all'illecita captazione degli stessi), i PISPs, pur non detenendo fondi dell'utente e non amministrando conti di pagamento[58], operano dando impulso a vere e proprie operazioni di pagamento (*sub specie* di bonifici) a valere sui conti del cliente, sicché al pericolo di accesso indebito alle informazioni ivi contenute si somma quello, maggiormente rilevante (e oggetto, difatti, di apposite previsioni normative), di transazioni inesatte o addirittura fraudolente, imputabili a errori o falle nell'organizzazione dello specifico servizio di pagamento[59].

Negli anni, il tema delle operazioni di pagamento non autorizzate si è dovuto misurare con la rapida evoluzione dei sistemi di pagamento e con il correlato incremento dei rischi di frode, specie in relazione all'uso di strumenti o di modalità di pagamento innovativi, basati sulle più sofisticate tecnologie digitali (si pensi solo all'ampia gamma dei metodi di pagamento via *Internet*, o alla crescente diffusione dei c.d. *mobile payments*). Ciò a significare che tanto il processo di produzione

[58] Ovviamente, là dove prestino esclusivamente tale servizio (31° considerando PSD2).

[59] Analogo problema non sussiste, evidentemente, con riferimento all'attività degli AISPs, di per sé finalizzata, come già osservato, a fornire informazioni al cliente circa la situazione dei propri conti e a consentirgli una migliore pianificazione delle proprie spese e risorse. Rileva invece, sotto altro profilo cui si può solo accennare, l'eventuale responsabilità di soggetti diversi dai PSPs sin qui considerati, come, ad es., i gestori delle applicazioni informatiche utilizzate tramite dispositivi mobili dai fruitori di servizi di pagamento per l'esecuzione di transazioni *on line*, o i produttori di *smart objects* abilitati a funzioni di pagamento. Il coinvolgimento di tali soggetti nelle operazioni di pagamento potrebbe, peraltro, introdurre degli elementi di debolezza nell'apparato di sicurezza delineato dalla PSD2, compromettendo la fiducia degli utenti nell'integrità dell'intero sistema e il suo stesso funzionamento (F. PORTA, *op. cit.*, 33, nt. 32). Più in generale, sulla difficoltà di «identificare il soggetto da cui dipende l'esattezza della prestazione (e, specularmente, da cui dipende l'inadempimento o l'adempimento inesatto)», nel contesto di attività di impresa caratterizzate dalla scomposizione e parcellizzazione della filiera del valore (e, quindi, da prestazioni soggettivamente e tecnologicamente complesse), v. R. NATOLI, *Frazionamento della filiera produttiva e regole del contratto*, in *Riv. trim. dir. econ.*, 2019, 287 ss.

delle regole, quanto la fase di interpretazione e applicazione delle medesime, non possono prescindere da un'adeguata comprensione dei complessi aspetti tecnologici – inevitabilmente ostici per il giurista – sottesi all'esecuzione delle operazioni di pagamento.

Rinviando, sul punto, alle trattazioni specialistiche, basterà qui rilevare che, in materia di responsabilità per operazioni di pagamento non autorizzate, la PSD2 ricalca sostanzialmente le medesime scelte normative operate dalla precedente dir. 2007/64/CE, riproponendo un criterio di suddivisione delle stesse fra utente e prestatore di servizi di pagamento, basato essenzialmente sulle rispettive capacità di prevenire e/o gestire determinati rischi (ciascuna delle parti, in pratica, è tenuta a sopportare le conseguenze degli eventi che ricadono in modo più diretto nella propria sfera di controllo)[60].

In quest'ottica, il legislatore ha stabilito che: *i)* le perdite relative ad operazioni non autorizzate compiute prima della denuncia di furto, smarrimento o appropriazione indebita dello strumento di pagamento gravano sul titolare dello stesso nei limiti di un massimale fissato in 50 euro, che non trova tuttavia applicazione ove questi abbia agito in modo fraudolento, o non abbia adempiuto, con dolo o con grave negligenza, i doveri posti a suo carico dalla legge (*i.e.*, utilizzare lo strumento di pagamento conformemente alle condizioni che ne disciplinano l'uso, adottando, in particolare, ogni ragionevole misura per proteggere le credenziali di sicurezza personalizzate e notificando senza indugio al prestatore dei servizi di pagamento, o al soggetto specificato da quest'ultimo, lo smarrimento, il furto, l'appropriazione indebita o l'utilizzo non autorizzato dello strumento di pagamento)[61]; *ii)*

[60] Sul tema, di recente, M.C. PAGLIETTI, *Questioni in materia di prova nei casi di pagamenti non autorizzati*, in M.C. PAGLIETTI, M.I. VANGELISTI, *Innovazione e regole nei pagamenti digitali*, cit., 43 ss., ove ulteriori riferimenti bibliografici, anche alla letteratura straniera.

[61] A tali previsioni, già presenti nella precedente disciplina, la PSD2 aggiunge quella secondo cui la franchigia non va applicata se lo smarrimento, il furto o l'appropriazione indebita dello strumento di pagamento non potevano essere notati dal pagatore prima di un pagamento (salvo il caso in cui lo stesso abbia agito in modo fraudolento), o se la perdita è stata causata da atti o omissioni di dipendenti, agenti o succursali di un fornitore di servizi di pagamento o di un ente cui sono state esternalizzate le attività (art. 74, par. 1, PSD2; art. 12, comma 2-*ter*, d. lgs. n. 11/2010). Sulle difficoltà interpretative poste da tali disposizioni, mi sia concesso rinviare a F. CIRAOLO, *Pagamento fraudolento con carta di credito e ripartizione*

successivamente alla denuncia, le perdite gravano interamente sul prestatore di servizi di pagamento (tenuto, da quel momento, a impedire ogni possibile uso non autorizzato dello strumento), salvo il caso in cui l'utilizzatore abbia agito in modo fraudolento.

A tali regole fa eco un peculiare regime probatorio, secondo il quale, in caso di contestazione di una specifica operazione di pagamento, per sottrarsi al rimborso del relativo importo[62] il prestatore di servizi di pagamento deve in primo luogo dimostrare che essa è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze di guasti tecnici o altri inconvenienti, per poi offrire l'ulteriore prova della frode o della grave negligenza da parte dell'utente[63].

Si badi, peraltro, che la prova dell'assoluta correttezza, sotto il profilo tecnico, delle operazioni eseguite, nonché della grave negligenza del cliente, non vale necessariamente ad esonerare il prestatore di servizi di pagamento da ogni responsabilità, dovendo questi rispondere anche della sicurezza e dell'affidabilità del servizio nei confronti dell'utenza, in virtù sia di quanto stabilito dalla normativa di settore, sia, più in generale, degli obblighi di diligenza professionale qualificata gravanti *ex lege* sull'intermediario (art. 1176, comma 2, c.c.). In questa logica si spiega, dunque, l'obbligo per ogni prestatore di servizi di pagamento di adottare i presidi di sicurezza e gli accorgimenti tecnici più evoluti al fine di prevenire eventuali frodi, già sancito per via dottrinaria e giurisprudenziale[64], ed oggi espressamente previsto,

delle responsabilità. Dagli orientamenti attuali alla revisione della PSD, in *Dir. banc. fin.*, 2017, 186 ss. In giurisprudenza, v. invece ABF, Coll. coord., dec. n. 24366/19.

[62] Le disposizioni in materia prevedono, più in dettaglio, che il cliente debba contestare l'operazione entro il termine di 13 mesi dalla data di addebito e che l'intermediario debba provvedere al rimborso del relativo importo al più tardi entro la fine della successiva giornata operativa, salvo che non sussista un motivato sospetto di frode (art. 73 PSD2; art. 11 d. lgs. n. 11/2010).

[63] La mancata prova della corretta autenticazione/esecuzione dell'operazione di pagamento da parte dell'intermediario è sufficiente, dunque, a fondarne la responsabilità, rendendo superfluo l'esame dei profili di colpevolezza dell'utente: in questo senso v. ad es. ABF Bari, n. 14456/18 e n. 24806/18; ABF, Coll. coord., n. 22475/19.

[64] La giurisprudenza di legittimità ha già da tempo chiarito che, quand'anche il cliente omettesse di rispettare determinati obblighi comportamentali, la banca rimarrebbe comunque tenuta ad osservare, nell'erogazione dei propri servizi, la diligenza qualificata del *bonus argentarius*, da valutare tenendo conto dei rischi

sotto certi aspetti, anche in sede normativa (il riferimento è all'obbligo di adottare, in una serie di casi specificamente indicati, le c.d. procedure di autenticazione forte del cliente, in difetto delle quali il pagatore non è tenuto a sopportare alcuna conseguenza finanziaria, salvo che abbia agito in modo fraudolento[65]).

Ebbene, il quadro normativo sopra rappresentato è stato sostanzialmente esteso anche agli operativi attivi nel nuovo ecosistema dell'*open banking*, stabilendo, in particolare, che quando l'operazione di pagamento è disposta mediante un PISP, spetta a quest'ultimo dimostrare che, «*nell'ambito delle sue competenze*», la stessa è stata autenticata, correttamente registrata ed eseguita e che non ha subito le conseguenze di guasti o altri inconvenienti legati al servizio, nonché fornire, se del caso, gli elementi di prova che dimostrino la frode o la grave negligenza dell'utente[66].

Sul punto si ripresentano, pertanto, le medesime difficoltà interpretative e applicative (con palesi ricadute anche sul piano del contenzioso) emerse già nel precedente regime disciplinare, specie con riferimento all'accertamento della sussistenza di un elemento generico

professionali tipici dell'attività esercitata (Cass., n. 13777/09 e n. 806/16). In applicazione di tale principio, dunque, il giudice deve sempre valutare se l'intermediario abbia o meno adottato le misure necessarie a garantire la sicurezza del servizio di pagamento offerto al cliente (Cass., n. 2950/17 e n. 9158/18, richiamate anche da ABF, Coll. coord., n. 24366/19, al fine di sancire l'obbligo dei PSPs di predisporre un sistema di *sms alert*, quale basilare presidio di sicurezza volto a consentire al cliente di bloccare tempestivamente l'uso non autorizzato del proprio strumento di pagamento).

[65] Art. 74.2 PSD2; art. 12, comma 2-*bis*, d. lgs. n. 11/2010. Si rammenta brevemente che l'autenticazione forte consiste in una procedura che consente al PSP di verificare l'identità di un utente o la validità dell'uso di uno strumento di pagamento (compreso l'uso delle credenziali di sicurezza personalizzate), basata sull'impiego di due o più elementi tra loro indipendenti (classificabili nelle categorie «*qualcosa che solo l'utente conosce*», ad es. una *password*, «*qualcosa che solo l'utente possiede*», ad es. un *token*, «*qualcosa che caratterizza l'utente*», ad es. un dato biometrico) e concepita in modo da assicurare la riservatezza dei dati di identificazione. La *strong authentication* è prevista per i casi in cui il pagatore: *a*) accede al suo conto di pagamento *on line*; *b*) dispone un'operazione di pagamento elettronico; *c*) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La procedura e le relative esenzioni (ad es., per pagamenti *contactless* di basso importo) sono disciplinate dal Regolamento delegato (UE) 27 novembre 2017, n. 2018/389.

[66] Art. 72 PSD2; art. 10 d. lgs. n. 11/2010.

e privo di significato univoco – inevitabilmente destinato, pertanto, ad essere plasmato in base alla sensibilità del singolo operatore del diritto – qual è la grave negligenza dell'utente[67].

Gli aspetti di maggiore novità concernono, tuttavia, la definizione dei rapporti tra i prestatori di servizi di pagamento di radicamento dei conti e i PISPs, con specifico riferimento alle ipotesi in cui le operazioni di pagamento siano state disposte tramite questi ultimi. L'intervento di un *provider* terzo, legittimato ad inserirsi nel rapporto tra ente detentore del conto di pagamento e soggetto pagatore, rende infatti necessario stabilire quale, tra i predetti prestatori di servizi di pagamento, sia responsabile di eventuali transazioni fraudolente (come anche inesatte, o ineseguite) in danno dell'utente.

Al riguardo, le soluzioni escogitate dal legislatore europeo sono palesemente ispirate ad un *favor* verso l'utente, volto ad ingenerare fiducia nell'uso dei nuovi strumenti di pagamento e ad assicurare, più in generale, l'ordinato ed efficiente funzionamento del mercato dei servizi di pagamento. Anche per le ipotesi di intervento del PISP, infatti, vale la regola generale secondo la quale chi assume di essere stato danneggiato da un pagamento non autorizzato o fraudolento ha diritto ad ottenere il rimborso della relativa somma, che dovrà essere eseguito (non dal PISP, ma) dall'ASPSP entro la giornata operativa successiva alla richiesta, salvo che non sussista un ragionevole sospetto di frode. Il PISP, tuttavia, dovrà immediatamente rimborsare all'intermediario presso il quale è radicato il conto l'importo dell'operazione contestata, nonché risarcire quest'ultimo anche per le

[67] V. ancora F. CIRAOLO, *Pagamento fraudolento con carta di credito*, cit., 184 ss. Di recente è stato osservato, peraltro, che l'evoluzione tecnologica nel settore dei pagamenti (oggi effettuabili sempre più frequentemente anche in modalità *contactless* o mediante uso di *smart objects*, con conseguente incremento del pericolo di intercettazione abusiva del flusso di dati che circola attraverso tali supporti) comporta una riduzione dei margini entro i quali è possibile riconoscere la colpa grave dell'utente, dal quale non si può certo esigere la piena comprensione del funzionamento e dei rischi propri di strumenti presentati come di facile utilizzo, ma tecnologicamente assai complessi (potendosi pretendere, al più, che non vengano mai disattivate dall'utente le tutele *standard* predisposte negli strumenti di pagamento utilizzati): L. MIOTTO, M. SPERANZIN, *I pagamenti elettronici*, in M. CIAN, C. SANDEI, *Diritto del Fintech*, cit., 187 ss.

perdite subite[68].

Ora, per quanto possa risultare apprezzabile la scelta di garantire in ogni caso all'utente l'immediato (ancorché non definitivo[69]) rimborso, da parte del prestatore di servizi di pagamento di radicamento del conto, dell'importo di un'operazione di pagamento disconosciuta (esonerandolo, quindi, dall'individuazione del soggetto effettivamente responsabile di eventuali malfunzionamenti nel sistema di autenticazione, autorizzazione, esecuzione e registrazione della transazione)[70], non può non rilevarsi come le predette soluzioni normative lascino comunque in ombra alcuni importanti aspetti della relazione tra gli intermediari intervenuti nella catena del pagamento. Aspetti che avrebbero meritato di essere definiti con maggiore puntualità specialmente nell'ordinamento nazionale, all'interno del quale la PSD2 ha avuto, come vedremo, un'infelice e non del tutto fedele trasposizione.

Al riguardo, è stato infatti affermato che i rapporti tra PISP e ASPSP sembrerebbero articolati, nella normativa italiana, secondo una sequenza procedimentale che contempla una prima fase a carattere sommario (legata all'urgenza, stabilita per legge, di provvedere al massimo entro una giornata lavorativa), durante la quale il primo è

[68] Art. 74.2 PSD2; art. 11, comma 2-*bis*, d. lgs. n. 11/2010. Si noti peraltro che, in punto di responsabilità dei PSPs, la normativa europea ammette altresì la possibilità di un'ulteriore *«compensazione finanziaria»*, in conformità alla legge applicabile al contratto stipulato dal pagatore con il prestatore di servizi di pagamento o con il PISP (art. 73.3 PSD2). Si può immaginare, pertanto, che il PISP possa essere chiamato a rifondere all'ASPSP anche la "perdita" rappresentata dalla suddetta *«compensazione finanziaria»*.

[69] V. art. 11, comma 3, d. lgs. n. 11/2010, ai cui sensi il rimborso non preclude al PSP la possibilità di dimostrare, anche in un momento successivo, che l'operazione era stata regolarmente autorizzata e pretendere quindi dall'utente la restituzione dell'importo inizialmente riconosciutogli.

[70] Osserva al riguardo G. BERTI DE MARINIS, *La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD2*, in *Dir. banc. fin.*, 2018, 645, come l'individuazione del primo e diretto interlocutore dell'utente nel soggetto presso il quale è acceso il conto di pagamento non soltanto risponde ad esigenze di rapidità e semplificazione, ma risulta anche coerente con gli obblighi di cui all'art. 6-*bis* d. lgs. n. 11/2010, che riconoscono all'ASPSP la possibilità di negare ai TPPs l'accesso ai conti di pagamento dei propri clienti, per comprovate e giustificate ragioni connesse ad un accesso fraudolento o non autorizzato.

tenuto a corrispondere al secondo, dietro semplice richiesta, l'importo dell'operazione contestata dal cliente (salva la possibilità di sottrarsi a tale obbligo, dimostrando, entro lo stesso ridottissimo termine, la piena regolarità tecnica dell'operazione di pagamento disposta suo tramite, per la parte di sua competenza[71]), cui farebbe seguito una seconda (ed eventuale) fase di merito, nel contesto della quale potrebbe trovare più adeguato spazio l'esercizio delle azioni per il risarcimento delle maggiori *«perdite»* subite dal prestatore di servizi di pagamento di radicamento del conto (salva, ovviamente, la necessità di individuazione e quantificazione delle medesime[72]), o delle azioni di regresso tra intermediari[73].

Si tratta di una soluzione interpretativa che aspira a restituire coerenza ad una disciplina non del tutto lineare, ma che si scontra, nondimeno, con ostacoli di varia natura.

Il primo è rappresentato dal tenore letterale delle norme di

[71] La norma sembra basata, pertanto, su una sorta di presunzione di responsabilità del PISP (analogamente a quanto previsto dall'art. 72.1 PSD2 e dall'art. 10, comma 1-*bis*, d. lgs. n. 11/2010), obbligato al rimborso immediato, a meno che non riesca a provare che l'operazione, nella parte posta sotto il suo controllo diretto, è stata correttamente autorizzata, autenticata ed eseguita, senza guasti o inconvenienti di sorta (sul punto v. anche *infra*, nt. 77). Non è invece previsto che, nei rapporti interni tra intermediari, il PISP possa sottrarsi al rimborso adducendo un ragionevole sospetto di frode (argomento utilizzabile invece dall'ASPSP nei confronti del pagatore).

[72] V. *supra*, n. 68.

[73] Così, R. FERRETTI, *Operazioni di pagamento non autorizzate. Il riparto di responsabilità tra PISP e AISP*, intervento al Convegno *L'attuazione della seconda direttiva sui servizi di pagamento e open banking*, Bergamo, 19 ottobre 2019 (materiale consultato per cortesia dell'autore), con impostazione condivisa anche da L. MIOTTO, M. SPERANZIN, *I pagamenti elettronici*, cit., 193, nt. 84. In punto di regresso fra i prestatori di servizi di pagamento rilevano le disposizioni dell'art. 92 PSD2, che prevedono l'ipotesi di una *«compensazione»*, là dove il prestatore di servizi di pagamento responsabile dell'operazione non autorizzata non si sia avvalso di mezzi di autenticazione forte del cliente, nonché la possibilità di *«ulteriori compensazioni finanziarie»*, determinate conformemente agli accordi conclusi tra intermediari e alla legislazione applicabile agli stessi. La prima parte norma, peraltro, è stata recepita nell'ordinamento italiano attraverso l'oscura disposizione secondo cui, se la responsabilità di un'operazione di pagamento è attribuibile ad altro intermediario coinvolto o interposto nell'esecuzione della stessa, è prevista, oltre al risarcimento delle perdite e degli importi versati, anche *«una compensazione degli importi qualora gli intermediari non si avvalgano dell'autenticazione forte del cliente»* (art. 27, comma 1, d. lgs. n. 11/2010, da ultimo modificato con d. lgs. n. 36/2020).

riferimento, là dove si specifica che, qualora l'ASPSP chieda, oltre al rimborso dell'importo restituito all'utente, anche il risarcimento del danno per le perdite subite, il PISP, *se responsabile dell'operazione non autorizzata*, debba provvedere in tal senso, al più tardi entro il giorno successivo (senza necessità di alcuna costituzione in mora). Sembra, dunque, che anche l'obbligo risarcitorio debba essere adempiuto, dietro richiesta dell'ASPSP, in modo tempestivo (e non già all'esito di una successiva fase di merito), sebbene non possa non rilevarsi, in senso critico, come l'accertamento della responsabilità del PISP (elemento su cui dovrebbe comunque fondarsi la pretesa azionata) appaia difficilmente compatibile, in caso di contrasto tra gli intermediari intervenuti nell'operazione, con un limite temporale così ristretto[74]. Sul punto, dunque, le norme in esame meriterebbero di essere formulate con maggior chiarezza, avvertendosi, in particolare, l'esigenza di indicazioni più dettagliate in merito al *modo* e al *tempo* in cui debba essere fornita la prova della responsabilità del PISP.

Il secondo si ricollega, invece, ad un'evidente difformità tra la normativa nazionale e la PSD2. L'ipotizzata articolazione dei rapporti tra prestatori di servizi di pagamento secondo una sequenza logica (e temporale) che contrappone il rimborso (immediato e non condizionato alla responsabilità del PISP) dell'importo dell'operazione fraudolenta al risarcimento del danno *«anche per le perdite subite»* (in questo caso, subordinatamente alla responsabilità del PISP), invero, non sembra trovare riscontro nel testo della direttiva: quest'ultima, infatti, pare semmai orientata verso una soluzione maggiormente unitaria, prevedendo che il PISP, se responsabile dell'operazione non autorizzata, debba immediatamente risarcire l'ASPSP, su richiesta di quest'ultimo, per le *«perdite subite o gli importi pagati in conseguenza del rimborso al pagatore, compreso l'importo dell'operazione di pagamento non autorizzata»*[75] (di tal che la scissione tra fase sommaria,

[74] Anche in questo caso si assisterebbe, dunque, ad un'inversione dell'onere della prova, analogamente a quanto osservato *supra,* nt. 71. Il PISP sarebbe infatti tenuto al risarcimento, fatta salva la possibilità di dimostrare la piena regolarità dell'operazione contestata e di chiedere, in tal caso, la restituzione di quanto eventualmente versato all'ASPSP.

[75] Art. 74.2 PSD2. Come evidenziato in dottrina, quindi, in punto di operazioni di pagamento non autorizzate la normativa europea opera una netta distinzione, dotata di maggiore coerenza sul piano sistematico, tra rimedi restitutori (azionabili nel

relativa al mero rimborso, e fase di merito, preordinata alla definizione di ulteriori pretese risarcitorie, non risulta contemplata dalle norme europee). Indipendentemente da quale possa ritenersi la soluzione più efficiente, tale discrasia andrebbe eliminata, considerato che la PSD2 detta norme di piena armonizzazione, vietando agli Stati membri di mantenere o introdurre disposizioni di diverso tenore (art. 107).

La terza ed ultima difficoltà – per vero, di carattere più generale – concerne, infine, le concrete modalità di erogazione dei servizi dei TPPs, le quali non presuppongono necessariamente, come già si è osservato (par. 2), la conclusione di alcun accordo contrattuale con gli ASPSPs[76]. È evidente, infatti, che all'interno di un regolamento negoziale potrebbe trovare naturale ed opportuna collocazione anche la suddivisione delle responsabilità per operazioni non autorizzate (o non correttamente eseguite), prevenendo l'insorgere di controversie fra i diversi prestatori di servizi di pagamento coinvolti nell'operazione (o agevolandone la soluzione)[77] ed aumentando, al contempo, la fiducia

rapporto tra utente e ASPSP, in ragione della non imputabilità al pagatore dell'ordine di trasferimento dei fondi) e rimedi risarcitori (applicabili, per converso, nei rapporti interni tra ASPSP e PISP, in conseguenza di una responsabilità per inadempimento o per fatto illecito in capo al secondo). La legge italiana, invece, attua un'inopportuna sovrapposizione fra detti rimedi (v. art. 11, comma 2-*bis*, d. lgs. n. 11/2010, ove si prevede che il PISP debba sia *rimborsare* che *risarcire* l'ASPSP), ingenerando, peraltro, il rischio di *overcompensation* a carico del PISP, nelle ipotesi di un recupero parziale, da parte dell'ASPSP, dei fondi trasferiti e non conteggiabili all'utente nel rapporto di conto corrente: V. DE STASIO, *Riparto di responsabilità e restituzioni nei pagamenti non autorizzati*, in M.C. PAGLIETTI, M.I. VANGELISTI, *Innovazione e regole nei pagamenti digitali*, cit., 40 ss.

[76] La ragione per la quale la legge non subordina l'attività dei TPPs alla conclusione di un rapporto contrattuale con gli AISPSs è stata ravvisata nell'esigenza di evitare che gli enti detentori dei conti - caratterizzati da forti incentivi a non cooperare con i nuovi operatori, onde non perdere la relazione privilegiata con la clientela - pongano in essere condotte discriminatorie nei confronti di questi ultimi, imponendo condizioni contrattuali che possano frustrare il raggiungimento degli obiettivi pro-concorrenziali perseguiti dalla PSD2 (G. COLANGELO, O. BORGOGNO, *op. cit.*, 15).

[77] Problematica può rivelarsi, in concreto, l'attuazione della disposizione secondo cui, in caso di operazioni non autorizzate, il PISP è tenuto a dimostrare che, *«nell'ambito delle sue competenze»*, le stesse sono state autenticate, correttamente registrate ed eseguite. Può infatti presumersi che non sia sempre agevole accertare che la frode, la falla di natura tecnica o l'errore nel procedimento di pagamento sia riferibile a quello specifico segmento dell'operazione posto sotto il controllo diretto

reciproca fra i medesimi e la certezza giuridica dei rispettivi rapporti[78].

Dalle superiori osservazioni traspare, dunque, quanto faticosa possa risultare la ricostruzione esegetica delle norme in esame. Nondimeno, una lettura coerente delle medesime può tentarsi, a nostro avviso, nei termini che seguono: *i)* là dove l'ASPSP ritenga il PISP responsabile di un'operazione di pagamento non autorizzata, disposta suo tramite, potrà pretendere dallo stesso la restituzione dell'importo rimborsato al cliente, le spese connesse all'esecuzione dell'operazione e il risarcimento degli ulteriori danni subiti (nella misura stabilita per via contrattuale, o altrimenti documentati); *ii)* il PISP dovrà ottemperare alla richiesta entro un giorno lavorativo, a meno che non offra, entro lo stesso termine, la prova della piena regolarità del segmento di operazione posto sotto il suo diretto controllo; *iii)* nulla osta, tuttavia, a che il PISP possa dimostrare anche in un secondo tempo la propria mancanza di responsabilità, fornendo la prova, inizialmente non reperita, della corretta esecuzione dell'operazione per quanto di sua competenza e pretendendo quindi la restituzione, a titolo di indebito, di quanto inizialmente versato all'ASPSP.

In conclusione, pur con tutte le perplessità suscitate dall'infelice formulazione del testo di legge, la definizione dei rapporti tra PISP e ASPSP sembra doversi ritenere affidata ad una prima fase caratterizzata da una sostanziale inversione dell'onere della prova (posto, di fatto, a carico del primo), fatta salva, nondimeno, la possibilità di un successivo e più approfondito accertamento delle effettive responsabilità, ai fini del regolamento dei rispettivi obblighi di natura economica (ed in questo senso può condividersi, dunque, l'idea di un'articolazione bifasica della procedura volta alla corretta ripartizione delle responsabilità fra gli intermediari).

---

del PISP (74° considerando PSD2). Ciò anche alla luce della previsione secondo la quale al PISP è consentito fare ricorso alle medesime procedure di autenticazione fornite dall'ASPSP (art. 97, par. 5, PSD2; art. 10-*bis*, comma 5, d. lgs. n. 11/2010), cui potrebbe risultare imputabile, pertanto, un eventuale malfunzionamento delle medesime.

[78] F. CASCINELLI, V. PISTONI, G. ZANETTI, *La Direttiva (UE) 2015/2366 relativa si servizi di pagamento nel mercato interno*, luglio 2016, 14, reperibile su *www.diritto bancario.it*, ove si ipotizza che i PSPs possano regolare per via contrattuale la ripartizione delle rispettive responsabilità, tenendo conto degli *standard* tecnici specificamente adottati.

6. *Considerazioni conclusive*.

L'innovazione tecnologica è divenuta, negli ultimi anni, un fattore di cambiamento dirompente nel settore finanziario, la cui portata non può certo ritenersi limitata all'incessante realizzazione di prodotti o servizi di ultima generazione, ma coinvolge, in modo assai più profondo, l'intero assetto del mercato finanziario. Ed invero, se gli intermediari tradizionali, sottoposti a sempre maggiori pressioni concorrenziali, sono oggi costretti a ricercare nuovi modelli di *business*, anche le autorità di settore devono sforzarsi, dal canto loro, di adeguare i propri compiti di regolamentazione e di vigilanza ad un contesto radicalmente mutato, che pone nuove ed inedite sfide.

Il settore dei servizi di pagamento rappresenta, come si è potuto osservare nelle pagine precedenti, una delle punte più avanzate di tale fenomeno, poiché al progresso tecnologico che ha guidato l'evoluzione dei sistemi di pagamento si è aggiunta la risposta offerta sul piano normativo dal legislatore europeo, ben consapevole che una materia così rilevante ai fini dello sviluppo dell'intero sistema economico e sociale non sarebbe potuta restare priva di un quadro regolamentare unitario, moderno e adeguato a supportare il processo di integrazione del mercato interno.

Eppure, come si è cercato di evidenziare nel corso di questo scritto, per quanto apprezzabili siano stati gli sforzi a livello legislativo, gli obiettivi sopra indicati possono dirsi solo in parte raggiunti.

Al di là delle immancabili lacune o ambiguità nel testo delle disposizioni normative, invero, il dato che maggiormente emerge da un'analisi complessiva della disciplina dei servizi di pagamento è la difficoltà di governare efficacemente una materia magmatica e sfuggente come quella in esame, che impone non soltanto di adeguare le norme esistenti alle nuove soluzioni di tipo tecnologico (compito già di per sé estremamente impegnativo, considerati i tempi di reazione del legislatore e le difficoltà nell'inquadrare le nuove fattispecie all'interno delle categorie già note), ma di contemperare altresì molteplici esigenze, attinenti ai piani – distinti, ma complementari - della tutela del consumatore, della sicurezza dei pagamenti, della responsabilità degli intermediari, della concorrenza leale e della protezione dei dati personali.

Viene peraltro in rilevo, attraverso tale ultima considerazione,

un'ulteriore problematica che connota la materia in oggetto: il rischio di una sovrapposizione – e finanche di un conflitto – di competenze tra le distinte autorità (europee e nazionali) preposte a ciascuno degli ambiti sopra indicati. Si pensi, per citare un solo esempio, alle ipotesi in cui il titolare di un conto di pagamento subisca gli effetti di una transazione fraudolenta, a seguito dell'illecita captazione delle proprie credenziali riservate: fattispecie assai frequente nella pratica, nella quale si compendiano aspetti relativi alla corretta esecuzione degli obblighi relativi alla prestazione dei servizi di pagamento, sotto lo specifico profilo (di competenza della Banca d'Italia) dell'adozione di adeguate misure organizzative e di sicurezza, e aspetti relativi alla tutela dei dati personali (di competenza del Garante della Privacy)[79]. Né pare potersi del tutto tralasciare, per altro verso, il ruolo degli enti che svolgono funzioni di controllo nei settori in cui operano i soggetti che, a vario titolo, offrono servizi tecnici a supporto dei sistemi di pagamento (si pensi, ad es., alle società di telecomunicazioni)[80].

È forse in queste ultime considerazioni, tuttavia, che può essere ricercata, in parte, la soluzione ai problemi di cui sopra si è discusso. Come da più parti rilevato, infatti, la complessità della materia – che coniuga numerosità delle fonti e compresenza di molteplici attori, delineando un quadro estremamente articolato, tanto sul piano oggettivo quanto su quello soggettivo – esige un'azione coordinata fra le diverse autorità interessate, ispirata al principio di leale collaborazione, affinché, mantenendo un costante dialogo con il mercato, possano essere elaborate soluzioni concordate e quanto più possibile razionali. Il raccordo fra le autorità potrebbe condurre, ad es., ad elaborare un linguaggio intersettoriale realmente unitario e condiviso, a garantire l'uniforme e coerente interpretazione ed

[79] I riflessi di tale situazione sono peraltro evidenti anche sul piano processuale, posto che le controversie giudiziarie in tema di operazioni di pagamento non autorizzate sono state spesso incardinate dall'attore lamentando non già la violazione della disciplina dei servizi di pagamento, bensì della normativa sulla *privacy*.

[80] D. GAMMALDI, C. IACOMINI, *Mutamenti del mercato dopo la PSD2*, cit., 141 citano, al riguardo, le autorità preposte al controllo delle infrastrutture di telecomunicazioni, in ragione della rilevanza delle *Telco* nell'offerta dei servizi di mobilità, menzionando altresì l'Agenzia per l'Italia Digitale (AgID), quale ente incaricato di riconoscere i c.d. QTSPs (operatori che rilasciano i certificati digitali che consentono l'identificazione dei TPPs) di cui al Reg. UE/910/2014 sull'identità digitale.

applicazione dei testi normativi, a definire con maggiore precisione gli ambiti di applicazione delle disposizioni rilevanti, a coordinare e rendere più efficienti i controlli, a razionalizzare gli adempimenti a carico degli operatori.

In altri termini, a creare le condizioni per un ecosistema regolamentare puntuale, coerente e completo, ma al contempo flessibile, come appare necessario per potere governare una fase di continui cambiamenti come quella in corso.