LA RESPONSABILITÀ DELLA BANCA E DEI THIRD PARTY PROVIDERS (TPPS) PER OPERAZIONI FRAUDOLENTE ALLE SOGLIE DELLA RIFORMA DELLA "PSD2"

THE LIABILITY OF THE BANK AND THIRD PARTY PROVIDERS (TPPS) FOR FRAUDULENT TRANSACTIONS ON THE THRESHOLD OF "PSD2" REFORM

Actualidad Jurídica Iberoamericana Nº 18, febrero 2023, ISSN: 2386-4567, pp. 1738-1765

Martina
PICCINNO

ARTICOLO CONSEGNATO: 14 de octubre de 2022
ARTICOLO APPROBATO: 5 de diciembre de 2022

ABSTRACT: L'evoluzione tecnologica che sta interessando il settore dei servizi di pagamento digitali impone un costante adeguamento delle normative ai canoni di efficienza, velocità e sicurezza. L'incremento dei servizi offerti e degli intermediari coinvolti è foriero di nuove opportunità ma di altrettanti rischi la cui allocazione diviene cruciale per tutelare la fiducia degli utenti nei nuovi sistemi. Per tale motivo la PSD2 ha focalizzato l'attenzione proprio sui rapporti a valle delle operazioni di pagamento, individuando le responsabilità di utenti, operatori tradizionali e nuovi *players* (TPPs). Lo sforzo, tuttavia, non è stato sufficiente: il dinamismo che connota il settore, in una ai sempre piú aggiornati e subdoli sistemi di frode, ne mettono a repentaglio la tenuta e obbligano ad un ripensamento della struttura delle responsabilità, quantomeno nel senso di tenere in considerazione quali sopravvenienze possono essere concretamente gestite e da chi.

PAROLE CHIAVE: PSD2; Third Party Provider; riforma disciplina servizi di pagamento; operazioni fraudolente; riparto di responsabilità tra operatori tradizionali e Third Party Providers.

ABSTRACT: *The technological evolution that is affecting the digital payment services sector requires constant adaptation of regulations to the standards of efficiency, speed and security. The increase in the services offered and the intermediaries involved is a harbinger of new opportunities but also of new risks, the allocation of which becomes crucial in order to protect users' confidence in the new systems. This is why PSD2 has focused precisely on the relationships downstream of payment transactions, identifying the responsibilities of users, traditional operators and new players (TPPs). The effort, however, has not been sufficient: the dynamism that characterises the sector, in the midst of the ever more up-to-date and devious fraud systems, jeopardising its resilience, obliges a rethinking of the structure of responsibilities, at least in the sense of taking into account which contingencies can be concretely managed and by whom.*

KEY WORDS: *PSD2; Third Party Provider; reform of payment services regulation; fraudulent transactions; allocation of responsibilities between traditional players and Third Party Providers.*

SOMMARIO.- I. ALLE SOGLIE DELLA RIFORMA DELLA PSD2: MOTIVAZIONI E AUSPICI. – II. LA SICUREZZA COME OBIETTIVO PRINCIPE DELLA PSD2: LE OPERAZIONI NON AUTORIZZATE. – III. I THIRD PARTY PROVIDERS QUALI NUOVI OPERATORI DEL MERCATO. – IV. I PISP: NATURA E COSTRUZIONE DEL NUOVO RAPPORTO "A TRE FATTORI". – V. LA STRUTTURA DELLA RESPONSABILITÀ DEI PISP IN CASO DI OPERAZIONI FRAUDOLENTE. – VI. BREVI RIFLESSIONI CONCLUSIVE.

I. ALLE SOGLIE DELLA RIFORMA DELLA PSD2: MOTIVAZIONI E AUSPICI.

Il 10 maggio 2022 la Commissione Europea ha aperto una consultazione (con scadenza 2 agosto 2022) affinché tutti gli operatori del mercato – compresi privati cittadini – potessero esprimere la propria opinione in merito ad una possibile revisione della direttiva 2015/2366/UE, cd. PSD2 ("*Second Payment Services Directive*"). L'iniziativa si inserisce nell'alveo della strategia della Commissione Europea in materia di finanza digitale avente come priorità una proposta legislativa sulla cd. "*open finance*". In verità, ciò che per semplicità viene definito "consultazione sulla PSD3" consta di tre progetti distinti: una consultazione pubblica, aperta a chi ha conoscenze base del mercato dei pagamenti e delle relative leggi, e due "*targeted consultations*" rivolte a *stakeholders* professionali: la prima "*on the review of PSD2*" e la seconda "*on the open finance framework*". I due temi sono intimamente collegati; la finanza aperta[1], infatti, promuove l'accesso da parte di fornitori di servizi terzi ai dati (aziendali e dei consumatori) dei clienti (imprese e consumatori) – detenuti principalmente, ma non solo, da intermediari del settore finanziario – con il consenso di questi ultimi, per una vasta gamma di servizi finanziari (inclusi prestiti, credito al consumo, investimenti e pensioni). Inoltre, permette una piú ampia integrazione dei dati finanziari con i settori non finanziari, come la sanità e la pubblica amministrazione, e per questo rappresenta il passo successivo della politica europea di "*open access*", inaugurata a seguito dell'adozione delle procedure di "*open banking*" introdotte proprio dalla PSD2 attualmente in revisione.

Dopo soli quattro anni dall'entrata in vigore della Seconda Direttiva sui Servizi di Pagamenti (ed a tre dalla messa in atto del sistema di sicurezza anti frode "*Strong Customer Authentication*"), l'Unione Europea interroga gli utilizzatori e promotori dei servizi di pagamento in merito al raggiungimento degli obiettivi prefissati (cd. "*backward-looking*") – misurandone costi e benefici, efficacia e efficienza – e si

1 Per la proposta sulla "*open finance*" si veda European Commission: "Consultation document, targeted consultation on open finance framework and data sharing in the financial sector", disponibile al sito *ec.europa.eu/info/publications/finance-consultations-2022-open-finance_en*.

• Martina Piccinno
Dottoranda di ricerca in "Diritto dei consumi" – Università degli studi di Perugia
martinapiccinno01@gmail.com

interroga sulla eventuale obsolescenza dei suoi contenuti (cd. "*forward-looking*")[2], mirando a riempire le lacune e correggere eventuali storture.

L'inarrestabile stagione di riforme che vive la disciplina dei servizi di pagamento e, di conseguenza, la contrattazione bancaria, trova giustificazione nell'impatto che la rivoluzione tecnologica, supportata dalla transizione digitale, ha generato sugli stessi, oggetto di una nuova metodica che prende il nome di "*FinTech*"[3]. In un settore in cui, *ictu oculi*, lo sviluppo corre piú veloce delle regole, si impone la ricerca non facile di un equilibrio tra adeguamento normativo alle nuove tecnologie, tutela della concorrenza e del mercato e stabilizzazione dei sistemi finanziari.

Ciò a maggior ragione dopo la pandemia da Covid-19 che ha messo in "*stand-by*" il mondo "reale" in favore di quello virtuale, dando un forte impulso al settore dell' "e-*commerce*". Il consumatore, inizialmente scettico rispetto ai metodi di pagamento diversi dal contante, si è riversato sui cd. "e-*payments*" (pagamenti mediante internet) e "*m-payments*" (pagamenti tramite dispositivo mobile), consentendo da un lato l'accesso al mercato di nuovi "intermediari", prestatori di servizi (operanti al di fuori del circuito bancario), ma allo stesso tempo accelerando l'esigenza di interventi normativi europei che tutelino gli utenti e sopperiscano alla notevole frammentazione delle discipline nazionali di settore. In questo contesto, la direttiva in questione interviene abrogando la precedente direttiva 2007/64/CE (PSD1)[4], considerata già obsoleta al momento della sua attuazione[5], e si fa carico di predisporre regole uniformi in ordine ai pagamenti elettronici in tutta l'Eurozona, che amplino il paniere di servizi messi a disposizione dell'utenza, e a prevedere livelli di sicurezza tali da prevenire l'utilizzo fraudolento dei sistemi di pagamento.

2 E lo fa a mezzo di un questionario suddiviso per sezioni (*Payment Methods*, *Digital Payment*, *Blocking Funds*, ecc.), tra le quali, al punto 4.6, spicca quella a titolo "*Fraud*". Per la consultazione si veda European Commission: "Consultation document public consultation on the review of the revised payment services directive (psd2) and on open finance", in *ec.europa.eu/info/publications/finance-consultations-2022-psd2-review-open-finance_en*.

3 Al fine di non sviare il discorso dal tema cardine, per approfondimenti sulla *Fintech* si rinvia, *ex multis*, a Falcone, G.: "Contratti bancari e fintech", in *Contratti bancari* (a cura di E. Capobianco), Wolters Kluwer, Milano, 2021, pp. 613 ss.; Paracampo, M. (a cura di): "Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari", ed. 2°, Giappichelli, Torino, 2017; Schena, C., Tanda, A., Arlotta, C. e Potenza, G.: "Lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale", in *CONSOB*, *Quaderno Fintech*, num. 1°, marzo 2018. Per un approccio anche comparatistico si veda, Cian, M. e Sandei, C.: "Diritto del Fintech", Cedam-Wolters Kluwer, Padova, 2020.

4 E che, a sua volta, era tassello del piú ampio progetto europeo SEPA, "*Single Euro Payments Area*", promosso da Commissione e Sistema Europeo delle Banche Centrali (SEBC) e volto a modificare la struttura del mercato dei pagamenti attraverso due leve: definizione di schemi di pagamento utilizzabili in modo uniforme in tutta l'area, cd. "*SEPA for instruments*"; (ii) adeguamento delle infrastrutture per la compensazione e il regolamento dei pagamenti con l'obiettivo di assicurare la raggiungibilità di tutte le potenziali controparti europee, cd. "*SEPA for infrastructures*". Un progetto in parte naufragato (per approfondire le ragioni di insuccesso si veda Bott, J.: "The Single Euro Payments Area: New Alliances Required to Tip the Market", *ECRI Research Report*, num. 10°, luglio 2009).

5 Come ricorda giustamente Vanini, S.: "L'attuazione in Italia della seconda direttiva sui servizi di pagamento nel mercato interno: le innovazioni introdotte dal d.lgs. 15 dicembre 2017, n. 21", *Nuove leggi civ. comm.*, num. 4°, 2018, p. 840, proprio per tale motivo la Commissione Europea aveva deciso di adottare nel 2012 il Libro verde intitolato «Verso un mercato europeo integrato dei pagamenti tramite carte, Internet e telefono mobile» in cui auspicava un intervento tempestivo nella suddetta materia.

In Italia la normativa viene recepita *in extremis* dal d.lgs. 15 dicembre 2017, n. 218 che, a sua volta, apporta modifiche tanto al Titolo VI del t.u.b. («Trasparenza delle condizioni contrattuali e dei rapporti con i clienti») quanto, e specialmente, al d.lgs. 27 gennaio 2010, n. 11 già attuativo della PSD1.

In breve, gli obiettivi prefissati mirano a rendere semplice e, soprattutto, sicuro l'uso dei pagamenti *online*, in contrasto alle frodi informatiche, e ad un rafforzamento dei diritti degli utenti fino alla promozione di servizi di pagamento innovativi ed efficienti[6]. Dai primi riscontri emersi dalla consultazione pare che la Direttiva abbia imboccato la strada giusta: la maggior parte dei *feedback* ricevuti, specialmente dai clienti *retail*, si mostra soddisfatta dei risultati raggiunti al punto da ritenere inutile un suo "*restiling*"[7]. La tesi, tuttavia, non convince pienamente gli "addetti ai lavori" i quali evidenziano la presenza di alcune lacune come, ad esempio, la carenza di armonizzazione degli *standards* per lo scambio di informazioni tra intermediari, l'esclusione di alcuni nuovi operatori di supporto all'erogazione dei servizi di pagamento dalla disciplina della direttive o, ancora, manifestano una preferenza verso una regolamentazione che non aggiunga tecnicismi, bensí operi per principi, venendo incontro ad un mercato dinamico in perpetua evoluzione[8].

Si deve, dunque, riconoscere alla PSD2 un contributo significativo nell'incremento dei livelli di innovazione, competitività e sicurezza. Proprio per questo i necessari miglioramenti e chiarimenti nei diversi profili non devono

6 Per una ricostruzione completa di tutti gli aspetti della direttiva PSD2 si vedano, tra gli altri, Porta, F.: "Obiettivi e strumenti della PSD2", in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale* (a cura di F. Maimeri e M. Mancini), in *Quaderni di Ricerca Giuridica della Consulenza Legale della Banca di Italia*, num. 87°, settembre 2019, pp. 21 ss.; Geva, B.: "Payment Transactions under the E.U. Second Payment Services Directive - An Outsider's View", *54 Texas International Law Journal*, 2019, pp. 211 ss.; Marasa', F.: "Servizi di pagamento e responsabilità degli intermediari", Giuffrè, Milano, 2020, in particolare pp. 17 ss.; Sciarrone Alibrandi, A.: "Impostazione sistematica della Direttiva PSD2", in *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2* (a cura di M.C. Paglietti e M.I. Vangelisti), RomaTre-Press, Roma, 2020, pp. 13 ss., la quale si concentra nel descrivere i principi portanti della direttiva individuati nel controverso (almeno in ambito bancario-finanziario) principio di proporzionalità ed in quello di trasparenza.

7 Per completezza, si precisa che i dati relativi alla partecipazione alla consultazione *ut supra*, nonché alcune delle risposte fornire da operatori del mercato e da utenti, sono disponibili al sito *ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/F_en.* Tra i documenti consultabili è presente il "*Factual summary report PSD2 and open finance public consultation*" che riporta l'esito della consultazione pubblica. In sintesi, la categoria piú numerosa a rispondere al questionario risulta essere quella dei privati cittadini europei, seguita da imprese e associazioni di imprese (in particolare del settore bancario e assicurativo). Tra i Paesi europei, il maggior riscontro si è ottenuto dalla Germania. Per quanto sinora detto, risulta che lo strumento di pagamento preferito dalla maggioranza, anche *online*, resta la carta di credito. I "*digital wallet*" cosí come gli *m-payments* destano, invece, ancora perplessità nel 23% di coloro che hanno risposto. Negativo, invece, il giudizio sulla trasparenza informativa, soprattutto in tema di costo delle commissioni ("*fee per transaction*"). Coloro che desiderano maggiori informazioni (39%) vorrebbero conoscere il tempo esatto di esecuzione, l'importo preciso delle commissioni per ogni fase della transazione, le condizioni del pagamento e ricevere qualche tipo di conferma che il sito web non sia fraudolento e sul tasso di cambio di riferimento per transazioni con l'estero.

8 Tra i vari pareri consultabili si suggerisce, per completezza di veduta, quello rilasciato da Abi (Associazione Bancaria Italiana): "Call for evidence", agosto 2022, disponibile in *ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/F33, agosto 2022*.

sostituirsi alla precedente regolamentazione bensí inserirsi nel quadro normativo generale esistente.

II. LA SICUREZZA COME OBIETTIVO PRINCIPE DELLA PSD2: LE OPERAZIONI NON AUTORIZZATE.

Si conceda un'affermazione banale: se è indiscusso che il settore *tech* offre opportunità tendenzialmente illimitate, pagamenti sempre piú veloci e a costi ridotti, perché limita al minimo l'intermediazione (intesa nella sua accezione tradizionale), è ancor piú vero che presta facilmente il fianco a sempre nuove forme di frodi informatiche e ad un conseguente uso illegale di dati sensibili, che minano alle fondamenta la fiducia dei consumatori in questi nuovi sistemi. Basti pensare alle ormai note "intrusioni" non autorizzate all'interno dei conti di pagamento, con furti di denaro e di dati personali (attraverso tecniche note come: "*phishing*", "*man in the browser*" o "*man in the middle*", "*smishing*" e "*vishing*") che popolano le decisioni dei giudici di merito italiani, dell'Arbitro Bancario e Finanziario (ABF) e anche, in determinati casi, della Corte di Giustizia Europea[9].

La consapevolezza di aumento esponenziale del rischio si palesa nella stessa direttiva al Considerando 7, nel quale la sicurezza viene elevata a «condizione fondamentale per il buon funzionamento del relativo mercato». Se risulta impossibile azzerare il rischio legato alle nuove figure di pagamento e di *players* del settore, in quanto fisiologico elemento della complessità del sistema, questo può essere gestito e minimizzato nella sua fase patologica attraverso politiche di "*risk allocation*". Ed è ciò a cui l'impianto complessivo della PSD2 mira, attraverso la implementazione degli *standards* di sicurezza richiesti e, soprattutto, sforzandosi di allocare in modo equilibrato le responsabilità da operazioni non autorizzate tra attori tradizionali e nuovi *players*.

La direttiva, infatti, interviene nella fase e*x ante*, cioè precedente alla frode, al fine di prevenire l'insorgenza della stessa a mezzo di meccanismi tecnici di sicurezza e, di conseguenza, attraverso l'imposizione di precisi adempimento in capo agli operatori del mercato (compito a cui finora ha adempiuto, nonostante i limiti dell'obsolescenza tecnologica della regola). Sotto tale profilo, si presenta di estremo rilievo l'introduzione del sistema di sicurezza di autenticazione rafforzata, *Strong Costumer Authentication* (SCA), definita dall'art. 4, n. 30, dir. 2015/2366/UE[10]

9 Si pensi, ad esempio, a Corte di Giustizia UE, 11 novembre 2020 (C-287/19), DenizBank AG c/ Verein für Konsumenteninformation, in *curia.europa.eu*, con nota di Dalmartello, A.: "Il sistema europeo dei servizi di pagamento e i pagamenti anonimi "*contactless*", *Nuove leggi civ. comm.*, num. 4°, 2021, pp. 837 ss., e di Marasa', F.: "I pagamenti contactless nel sistema della PSD2", *Banca borsa tit. cred.*, num. 2°, 2022, pp. 149 ss., a tema operazioni non autorizzate a mezzo servizi *contactless* (NFC).

10 Recepito dall'art. 1, co. 1, lett. q-*ter*, del d.lgs. n. 11 del 2010, ed implementata dal regolamento attuativo 2018/389/UE.

come «un'autenticazione basata sull'uso di due o piú elementi classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione». Attraverso credenziali di accesso univoche, dinamiche e multifattore, generate con i dati di cui sopra (anche di natura biometrica)[11] e fornite al solo cliente, la banca contrassegna la singola operazione di pagamento per uno specifico importo e beneficiario (cd. "*Dynamic Linking*"), verifica la riconducibilità dell'attività alla volontà del cliente medesimo di cui accerta l'identità, negando al tempo stesso a terzi non autorizzati intrusioni illecite; e ciò nel caso di utilizzo del conto *online*, di operazioni di pagamento elettronico o di effettuazione di qualunque operazione a distanza che rechi in sé un rischio di frode[12]. L'ottica su cui si struttura detta disciplina è di inevitabile *favor* per l'utente, nella logica propria dei rapporti asimmetrici di consolidata esperienza europea. In linea con questo principio la SCA diviene per il prestatore di servizi di pagamento un vero e proprio onere che lo obbliga a munirsi di dispositivi e software atti a generare il codice monouso di autenticazione[13]. Il suo mancato impiego, salvo casi espressamente previsti per legge[14], costituisce la base per una piú sfavorevole modulazione della

11 Si veda, a tal proposito, Eba, European Banking Authority: "Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2", 21 giugno 2019, in *eba.europa.eu/eba-publishes-an-opinion-on-the-elements-of-strong-customer-authentication-under-psd2*.

12 Tale è la dicitura dell'art. 97, par. 1, della direttiva PSD2, recepito dall'art. 10 *bis* del d.lgs. n. 11 del 2010. Gli artt. 97 e 98 disciplinano l'applicazione della SCA e sono coadiuvati nel dettaglio dagli artt. 27-29 del regolamento di attuazione 2018/389/UE.

13 Un onere che non solo aiuta a proteggere dalle frodi ma, rendendo piú difficoltoso e lungo l'accesso al conto, induce l'utente «ad una piú accorta riflessione sull'operazione economica», cosí che quest'ultima risulti davvero espressione della «genuina volontà negoziale del soggetto pagatore» (Berti De Marinis, G.M.: "La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD2", *Dir. banc. merc. fin*., num. 4°, 2018, p. 655).

14 A tal proposito, l'art. 98 della direttiva PSD2 permette all'EBA, «in stretta cooperazione con la BCE e previa consultazione di tutti i portatori di interessi» di specificare i casi che sono esenti dalla SCA, sulla base di: «a) il livello del rischio connesso al servizio prestato; b) l'importo, la frequenza dell'operazione, o entrambi; c) il canale di pagamento utilizzato per l'esecuzione dell'operazione» o, semplicemente, perché a basso rischio di frode. In questo senso è orientato il capo III del regolamento di attuazione, 2018/389/UE, rubricato "Esenzioni dall'Autenticazione Forte del cliente" che, ad esempio, all'art. 11, dispensa dall'uso del suddetto sistema di sicurezza nelle forme di pagamento "*contactless*", ove vengano rispettati alcuni requisiti, tra i quali il piú significativo riguarda l'importo massimo della transazione che non deve superare i 50 euro in totale (proprio tale presupposto, secondo DigitalEurope: "DIGITALEUROPE's response to Call for Evidence on Payment Services-Review of EU Rules", 26 luglio 2022, p. 4, disponibile *al sito digitaleurope.org/resources/digitaleuropes-response-to-the-digital-decade-consultation*, durante la crisi pandemica ha rappresentato «*a good example of striking the right balance between innovation and security*»); all'art. 12, prevede l'esenzione con riferimento ai pagamenti effettuati presso terminali non custoditi aventi ad oggetto il pagamento di tariffe di trasporto o di parcheggio o, all'art. 16, per le operazioni di pagamento a distanza di importi singoli o aggregati poco significativi (per approfondimenti si veda Berti De Marinis, G.M.: "La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD2", cit., pp. 649 ss.; Rispoli Farina, M.: "La *strong customer authentication* e la responsabilità dei prestatori dei servizi di pagamento", *I-Lex*, num. 12°, 2019, pp. 105 ss.). Infatti, se detto tipo di autenticazione manifesta evidenti vantaggi in ambito di sicurezza e controllo verso intromissioni abusive sui conti, allo stesso tempo irrigidisce le procedure di pagamento, rendendole macchinose e articolate e rischia di dissuadere molti utenti (in particolare i piú scettici verso forme di pagamento diverse dal contante) dal loro utilizzo, ingenerando ciò che viene definito "rischio di abbandono della transazione". Una preoccupazione che non ha lasciato indifferenti gli operatori del mercato i quali, in occasione della consultazione pubblica di cui si è già fatto cenno, hanno espresso, quasi all'unanimità, la loro contrarietà all'estensione operativa della SCA

riparto di responsabilità nei confronti della banca in ipotesi di operazioni non autorizzate (art. 92, par. 1, dir. 2015/2366/UE e art. 12, co. 2 *bis*, d.lgs. 11/2010)[15].

La direttiva, infatti, si occupa, altresí , di regolare la fase e*x post* in cui l'incursione illecita nel conto di pagamento è già avvenuta e, quindi, non resta che ripartire le responsabilità nei rapporti a valle tra banca, clienti ed eventuali terze parti. Un gioco di equilibri, quest'ultimo, che in Italia ha acceso un dibattito (dagli sviluppi complessi e dall'esito ancora incerto) proprio con riferimento alla natura della responsabilità della banca in caso di operazioni fraudolente. Questa, in qualità di operatore tradizionale presso cui è radicato il conto del cliente ed a cui è rivolta l'introduzione dei sempre piú stringenti requisiti di sicurezza, si pone come primo baluardo a difesa di usi abusivi dei sistemi tecnologici, rientrando la conservazione dei codici di accesso del cliente tra gli obblighi di diligenza professionale (obblighi di "protezione" che trovano applicazione anche nell'*home banking*). La violazione degli stessi però viene interpretata da dottrina e giurisprudenza in modo estremamente ondivago, oscillando tra responsabilità contrattuale per mancata diligenza del *bonus argentarius*, ed e*xtra* contrattuale da attività pericolosa (art. 2050 c.c.), tra responsabilità aggravata, oggettiva e, persino, da *status*. Tutte queste tesi, però, restituiscono l'immagine unica di una responsabilità sempre piú sbilanciata dal lato dell'intermediario il quale è chiamato a sopportare *ex lege* gravosi oneri probatori e, spesso nella pratica, a rispondere di frodi informatiche dovute a cause sconosciute (i cd. "altri inconvenienti" di cui art. 10 d.lgs. 11/2010)[16]. Di contro, si

proponendo, di contro, una riduzione delle ipotesi di suo utilizzo [Abi: "Call for evidence", cit., suggerisce di non modificare l'architettura e le disposizioni generali della stessa ma, allo stesso tempo, di valutarne la esclusione per alcuni settori come quello della beneficenza, della sanità e dei trasporti; dello stesso avviso Banco Bilbao, nel "feedback" rilasciato il 1° agosto 2022, sulla pagina ufficiale della Commissione Europea (consultabile al sito *ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/F3332125_en*), il quale fa notare che «l'attrito in alcune transazioni di *e-commerce* sarebbe aumentato»; allo stesso modo nel *feedback* del 27 luglio 2022 (in *ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/F3330023_en*), Enel Spa, lamenta la futura installazione di *PIN-pad* nelle stazioni di ricarica delle macchine elettriche che avrebbe come unico esito l'aumento dei costi di installazione ed il conseguente incremento del prezzo finale al consumo, scoraggiando l'uso degli autoveicoli provvisti di questa nuova tecnologia e la creazione di infrastrutture pubbliche di ricarica. Chiede, pertanto, la rimozione della SCA per detto tipo di operazione, suggerendo di inserire la categoria delle transazioni di ricarica nell'art. 12 del regolamento di attuazione, al pari dei pagamenti di parcheggi e trasporti pubblici; la medesima esenzione dalla SCA è richiesta nel parere rilasciato il 1° agosto 2022 (*ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/F3332123_en*), dalla Global Business Travel Association con riferimento alle transazioni nel settore dei viaggi d'affari, colpite in modo marginale dalle frodi però affaticate da tale sistema di sicurezza perché basate, solitamente, su acquisti rapidi tramite *account* aziendali, il cui numero di telefono, necessario per la verifica SCA, non è associato al singolo impiegato bensì all'impresa].

15 L'art. 12, co. 2 *bis*, d.lgs. 11/2010 afferma che «se il prestatore di servizi di pagamento del pagatore non esige un'autenticazione forte del cliente, il pagatore non sopporta alcuna conseguenza finanziaria salvo qualora abbia agito in modo fraudolento», introducendo una vera e propria sanzione per la banca secondo una responsabilità che si può definire "oggettiva", con l'unica esimente della frode; ciò comporta che il prestatore sarà responsabile anche nelle ipotesi di dolo o colpa grave della condotta dell'utente. Un *proportionality check* dell'adeguatezza della sanzione che a Paglietti, M.C.: "Questioni in materia di prova di pagamenti non autorizzati", in *Innovazione e regole nei pagamenti digitali* (a cura di M.C. Paglietti e M.I. Vangelisti), Romatre-Press, Roma, 2020, pp. 56 s., considerando la *ratio* e gli interessi che la norma di diritto sostanziale violata protegge.

16 La tematica è molto complessa e necessiterebbe una trattazione sistematica che, tuttavia, tocca solo in parte l'attuale oggetto di riflessione. Per una ricostruzione attenta e completa si rinvia, quindi, a Marasa' F.:

assottiglia il perimetro della colpa grave di cui risponde il cliente. Detta presunzione di legge a sfavore dell'intermediario esprime ragioni di opportunità e di efficienza allocativa del rischio: l'avvenimento "frode", infatti, ricade nel rischio d'impresa e la banca rappresenta il "*best risk bearer*" o "*cheapest cost avoider*"[17], secondo una concezione che vede quest'ultima come soggetto capace di assorbire i costi dell'illecito e ripartirli sulla massa di utenti (cd. giustificazione social-commerciale).

Come si vedrà di seguito non è possibile restare indifferenti rispetto all'architettura assunta dalla responsabilità del prestatore del servizio, stanti le ricadute che la stessa produce anche sul modello di riparto di responsabilità in ipotesi di frodi informatiche su transazioni in cui sono intervenuti i Third Party Provider.

III. I THIRD PARTY PROVIDERS QUALI NUOVI OPERATORI DEL MERCATO.

Occorre precisare che il *favor* che la direttiva palesa per il cliente non esime quest'ultimo dal rispetto di alcuni obblighi di condotta. Al dovere dell'intermediario di salvaguardare l'accesso esclusivo alle proprie credenziali, corrisponde un correlato obbligo di questi a custodire le stesse e gli strumenti di pagamento, con diligenza ed in conformità alle previsioni contrattuali[18].

Tale sistema, già presente nella PSD1, mirava a responsabilizzare l'utente dei servizi digitali ponendo a suo carico il rischio rientrante nella propria sfera di controllo. Tuttavia, l'eccessivo rigore del dettato normativo diveniva un ostacolo quando il cliente, al fine di effettuare i pagamenti a mezzo di servizi digitali rapidi e poco costosi, cedeva le sue credenziali di accesso al conto a operatori terzi non finanziari (come, per esempio, Google Wallet, PayPal, Apple Pay, Samsung Pay, Amazon Pay). Questa modalità operativa (cd. "*screen scraping*")[19] non solo

"Servizi di pagamento" cit., pp. 100 ss., e ivi altra dottrina, cosí come a Antonucci, A.: "I contratti bancari on line", in *Contratti bancari* (a cura di E. Capobianco), Wolters Kluwer, Milano, 2021, pp. 585 ss.; Caggiano, A.: "Pagamenti non autorizzati tra responsabilità e restituzioni. Una rilettura del d. legisl. 11/2010 e lo scenario delle nuove tecnologie", *Riv. dir. civ.*, num. 2°, 2016, pp. 10459 ss.; Maffeis, D.: " Ordini di pagamento e di investimento on line nella giurisprudenza di merito e nella fonte persuasiva dinamica dell'ABF", *Riv. dir. civ.*, num. 5°, 2013, pp. 1273 ss.; Sulla responsabilità della banca per "altri inconvenienti" si ricorda ABF, Coll. Coord., 7 ottobre 2020, n. 17280, in *arbitrobancariofinanziario.it*.; quest'ultimi rientrano nel concetto di «danno da ignoto tecnologico» [Paglietti, M.C.: "Questioni in materia di prova" cit., p. 51].

17 La ragion d'essere di questa lettura è spiegata chiaramente in ABF, Coll. Coord., 26 ottobre 2012, n. 3498, in *arbitrobancariofinanziario.it*. In generale, l'ABF, nonostante la presenza di varie correnti di pensiero al suo interno, ha sempre cercato nelle sue decisioni di vagliare con estrema attenzione il rispetto degli obblighi di diligenza professionale, valutando con particolare rigore l'adempimento degli oneri probatori *ex* art. 72 PSD2 e *ex* art. 10, co. 1 e 2, d.lgs. 11/2010 (ABF, Coll. Coord., 10 ottobre 2019, n. 22745, in *arbitrobancariofinanziario.it*). Si veda, ad esempio, Sica, S. e Sabatino, B.M.: "Disintermediazione finanziaria e tutela del cliente e dell'utilizzatore", *Dir. inf.*, num. 1°, 2021, pp. 1 ss. ma anche Frau, R.:, "Home banking, phising e responsabilità civile della banca", *Resp. civ. prev.*, num. 2°, 2019, p. 622 ss.

18 Con riferimento agli obblighi dell'utente si vedano l'art. 69 della direttiva 2015/2366/UE e l'art. 7 del d.lgs. 11/2010 aggiornato.

19 Quale processo di raccolta dei dati di visualizzazione dello schermo da un'applicazione a un'altra, in modo che quest'ultima possa visualizzarla. Pratica attualmente vietata dalla PSD2 che, nel contesto *de quo*,

impediva alla banca di conoscere il vero autore/promotore della transazione ma, soprattutto, violava l'obbligo contrattuale in capo al cliente di non divulgazione a terzi delle proprie credenziali di sicurezza. Come conseguenza, in caso di contestazione da parte dell'utente per operazioni non autorizzate, questi poteva perdere il diritto al rimborso perché considerato responsabile dell'intromissione illecita.

Per ovviare a tale situazione di incertezza giuridica, lesiva tanto dell'utente quanto degli stessi operatori, era necessario identificare, regolamentare (e responsabilizzare) i nuovi attori abilitati all'erogazione di tali servizi. Il compito viene assolto dalla PSD2 la quale, in un'ottica di promozione di una sana concorrenza e di armonizzazione normativa (teoricamente massima), regola l'ingresso nel mercato dei cd. Third Party Providers, erogatori di servizi funzionali all'esecuzione del pagamento che si interpongono nel rapporto banca-cliente per facilitare le transazioni *online*. Questi sono sostanzialmente riconducibili a due categorie: il PISP ("*Payment Initiation Service Provider*"), ossia il «servizio di disposizione di ordine di pagamento» «che dispone l'ordine di pagamento su richiesta dell'utente di servizi di pagamento relativamente ad un conto di pagamento detenuto presso un altro prestatore di servizi di pagamento» e l'AISP ("*Account information Service Provider*"), «servizio di informazione sui conti» inteso quale «aggregatore *online* di informazioni (saldi e transazioni) relative a uno o piú conti di pagamento accessibili a distanza e carte di pagamento detenuti dall'utente presso altri intermediari». Parafrasando, si tratta di un servizio che attraverso un'interfaccia grafica sintetizza la situazione patrimoniale, finanziaria ed economica dell'utente[20].

Nonostante le condizioni di accesso al mercato per i TPP siano facilitate rispetto a quanto previsto per i prestatori di servizi tradizionali, la direttiva comunque predispone a loro carico una serie di requisiti differenziati sul tipo di business – in parte, quindi, distinti anche tra PISP e AISP (per il principio *a contrario*, "*same business, same risks, same rules*") – che consentano loro di ottenere l'autorizzazione (PISP) o registrazione (AISP) allo svolgimento dell'attività[21]. In particolare, per

consiste nell'uso da parte del *provider* delle credenziali del cliente, dallo stesso fornitegli, per accedere al conto di pagamento ed acquisire le informazioni utili all'operazione richiesta.

20 Le definizioni si trovano rispettivamente all'art. 4, parr. 18 e 19, della direttiva, corrispondenti all'art. 1, co. 1, lett. b-*bis*) e b-*ter*), d.lgs. 11/2010. In realtà, nei TPP rientra anche una terza categoria di soggetti, ossia i prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta, cd. CBPIIs ("*Card Based Payment Instrument Issuers*"), limitatamente allo svolgimento del servizio di conferma della disponibilità di fondi.

21 In generale, sul tema del Third Party Providers e sugli obblighi imposti loro per l'ingresso nel mercato si vedano: Berti De Marinis, G.M.: "La disciplina dei pagamenti", cit., pp. 627 ss.; Marasà', F.: " Servizi di pagamento", cit., pp. 76 ss.; Messore, A.: "La nuova disciplina dei servizi di pagamento digitali prestati dai *Third Party Providers*", *Nuove leggi civ. comm.*, num. 2°, 2020, pp. 511 ss.; Profeta, V.: "I Third Party Provider: profili soggettivi e oggettivi", in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale* (a cura di F. Maimeri e M. Mancini), cit., pp. 47 ss. Esclusivamente sulla figura degli AISP, Catenacci, M. e Fornasaro, C.: "PSD2: i prestatori di servizi d'informazione sui conti (AISP)", *Diritto bancario*, 2018, pp. 1 ss.

quanto qui di interesse, è richiesta la stipula obbligatoria di una "*professional indemnity insurance*" che permetta di far fronte alle eventuali pretese risarcitorie derivanti da responsabilità per i danni causati al prestatore di servizi di pagamento di radicamento del conto o all'utente dei servizi di pagamento a seguito di accessi o usi non autorizzati o fraudolenti del conto. Sopperendo alla minor dotazione di capitale iniziale ad essi richiesto, la polizza, conforme agli Orientamenti dell'EBA (*European Banking Authority*)[22], diviene prerequisito essenziale per l'iscrizione nel registro pubblico centrale dell'EBA e, soprattutto, negli appositi registri presso le Autorità di Vigilanza nazionali competenti. In Italia l'autorizzazione viene rilasciata da Banca di Italia – ricorrendo le condizioni *ex* art. 114 *novies* t.u.b. – la quale assoggetta gli stessi a vigilanza informativa ed ispettiva continua (e, si potrebbe aggiungere, discrezionale)[23], accertandosi preventivamente che nel set informativo predisposto dal TPP sia inserito il documento inerente la *policy* di sicurezza relativa ai rischi che possono scaturire dai servizi offerti (in particolare a seguito di frodi e furto di dati) e ai presidi scelti per il loro monitoraggio e controllo.

È stato evidenziato come la disciplina italiana abbia valorizzato poco le nuove indicazioni fornite dall'art. 5 PSD2 e relative a: *policy* di sicurezza, prevenzione dei rischi, gestione di incidenti e reclami. Tuttavia «il carattere cogente delle disposizioni di dettaglio emanate a tale proposito dall'EBA, alla cui applicazione fanno rinvio anche le norme secondarie messe in consultazione dalla Banca d'Italia, di fatto consente di superare tale lacuna senza pregiudizio per l'uniformità applicativa della direttiva con riguardo ai requisiti di sicurezza informatica»[24].

Proprio in merito al rapporto tra utente e presidio dai nuovi rischi di frodi informatiche, è probabile che in un futuro prossimo l'attenzione normativa (PSD3)

22 Eba: "Final Report on the EBA Guidelines under Directive (EU) 2015/2366 (PSD2) on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers", 11 luglio 2017, disponibile in *eba.europa.eu/eba-publishes-final-guidelines-on-authorisation-and-registration-under-psd2*, provvede a dare attuazione all'art. 5.5 della PSD2, stabilendo un set di obblighi informativi che il TPP deve fornire per ottenere l'autorizzazione ad operare come istituto di pagamento. Si ricordi che il ruolo normativo dell'EBA è stato implementato dalla PSD2 la quale, ad esempio, prevede che sia l'Autorità Europea Bancaria centrale a individuare i criteri per l'importo monetario minimo dell'assicurazione per la responsabilità civile professionale, o di altra comparabile garanzia [Eba: "Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee under Article 5(4) of Directive (EU) 2015/2366", 7 luglio 2017, disponibile in *eba.europa.eu/eba-publishes-final-guidelines-on-professional-indemnity-insurance-under-psd2*] e ad adottare eventuali provvedimenti di sospensione o revoca dell'autorizzazione ad operare dei TPPs, al ricorrere delle condizioni previste dall'art. 13 della PSD2, comminando altresí sanzioni amministrative. Infatti, la direttiva ha conferito all'EBA il compito di sviluppare "*Regulatory Technical Standard*" (RTS) e "*Guidelines*" (GL) riguardanti principalmente tre ambiti: coordinamento tra le autorità competenti "*home*" e "*host*"; armonizzazione dei processi di autorizzazione degli istituti di pagamento; sicurezza dei pagamenti (per approfondire si veda Porta, F.: "Obiettivi e strumenti della PSD2", cit., pp. 34 ss.).

23 L'iscrizione all'albo, invece, è regolata nell'art. 114 *septies* t.u.b. Speciali esenzioni sono previste per coloro che prestano esclusivamente il servizio di informazione sui conti (art. 33, dir. 2015/2366/UE, recepito nell'art. 114 *septiesdecies* t.u.b.). Sui requisiti trasposti in Italia, si veda Minto, A.: "Art. 114-*novies*", in *Commentario al Testo unico delle leggi in materia bancaria e creditizia* (diretto da F. Capriglione), Padova, 2018, pp. 1789 ss.

24 Profeta, V.: "I Third Party Provider", cit., p. 61.

si focalizzerà sugli AISP che, in qualità di aggregatori di dati sensibili, maneggiano il bene giuridico essenziale dell'era dei "*big data*", nonché nuova moneta di scambio[25], con tutte le ricadute fin d'ora immaginabili in tema di *privacy* e furto di dati. Inoltre, come è stato giustamente sottolineato, il loro rilievo si estende all'ausilio che il servizio reso potrebbe avere nella prevenzione al sovraindebitamento. Ciò in quanto consentono all'utente di "tenere sotto controllo" le proprie finanze, fornendogli un quadro completo del proprio stato patrimoniale e anticipando, cosí, movimentazioni, transazioni e investimenti azzardati[26].

Tuttavia, attualmente, sono i PISP a catalizzare l'interesse perché, intervenendo *in medias res* nella procedura di pagamento, allungano la catena di soggetti coinvolti nell'*iter*, rendendo necessario un chiarimento in merito al loro ruolo e, soprattutto, alle loro responsabilità.

IV. I PISP: NATURA E COSTRUZIONE DEL NUOVO RAPPORTO "A TRE FATTORI".

Sebbene il rapporto contrattuale "canonico" tra cliente – titolare del conto di pagamento – e banca – istituto di radicamento del conto – non venga intaccato nella sua struttura "genetica", l'aspetto peculiare della nuova attività di pagamento è la perdita della bilateralità del suddetto rapporto per far spazio ad un terzo fattore, il PISP, in quella che è stata definita una «triangolazione telematica»[27]. Il contratto bancario non muta il suo paradigma ma diviene solo un frammento di una catena di montaggio in cui gli ingranaggi sono quantomeno tre. Resta, dunque, il problema di ricostruire le relazioni giuridiche contrattuali tra questi tre soggetti.

Pertanto, fermo restando che il rapporto banca-cliente può essere ricondotto a quello tradizionale (banalmente, un "contratto" di conto corrente), occorre in prima istanza, vagliare il secondo segmento che compone l'*iter*: il rapporto contrattuale tra l'utente e il PISP, a sua volta autonomo rispetto a quello tra pagatore e beneficiario della transazione.

Come già accennato, l'utente abilita detto soggetto ad accedere al proprio conto, detenuto presso un istituto bancario, e ordina a quest'ultimo di prelevare

25 L'importanza capitale che stanno assumendo i dati come merce di scambio fa sí che questi vengano definiti molto spesso "*new oil*" se non proprio "*new sun*", perché fonti rinnovabili "di energia" (cosí come affermato dal Professore De Franceschi, A. il 18 ottobre 2022 nel suo intervento a seminario presso l'Università degli Studi del Salento, dal titolo "La tutela della persona nei mercati digitali").

26 Cosí Berti De Marinis, G.M.: "La disciplina dei pagamenti", cit., p. 633; Donnelly, M.: "Payments in the digital market: Evaluating the contribution of Payemnt Services Directive II", *Computer law & security review*, 2016, p. 831.

27 Profeta, V.: "I Third Party Provider", cit., p. 64; Sciarrone Alibrandi, A., Borello, G., Ferretti, R., Lenoci, F., Macchiavello, E., Mattassoglio, F. e Panisi, F.: "Marketplace lending. Verso nuove forme di intermediazione finanziaria?", in *CONSOB*, *Quaderni Fintech*, 5 luglio 2019, p. 245, in cui si parla di «frantumazione della catena di valore».

fondi nella misura in misura congeniale all'operazione da effettuare e trasferirli presso l'istituto di radicamento del conto del beneficiario del pagamento.

Il primo elemento peculiare del suddetto rapporto è l'assenza di disponibilità delle somme di denaro in capo al PISP; quest'ultimo, infatti, non entra mai in possesso dei fondi del pagatore oggetto del trasferimento, i quali verranno sempre detenuti e gestiti dall'istituto in cui è radicato il conto. Ciò comporta che il PISP, a differenza degli istituti tradizionali (per i quali vale la regola della "segregazione dei fondi del cliente" *ex* art. 114 *duodecies*, co. 2, t.u.b.), non sarà gravato dall'onere di separazione delle somme dei clienti da quelle proprie, né gli verrà applicata la disciplina prudenziale sui fondi propri[28]. Di contro, sarà tenuto a rispettare le disposizioni del titolo VI, capo II-*bis*, t.u.b., relative alla trasparenza delle condizioni contrattuali e dei rapporti con i clienti (la cui applicazione agli istituti di pagamento è prevista nell'art. 114 *undecies*, co. 1, t.u.b.). Proprio per questo, parte della dottrina riconduce il rapporto contrattuale tra PISP e utente – la cui natura non viene precisata nella direttiva – nell'alveo di un contratto normativo di prestazione di servizi digitali continuativo, nel quale le condizioni generali sono regolatrici dei futuri atti negoziali con oggetto la trasmissione degli ordini di pagamento, ossia la fase propedeutica in cui si inserisce ed esaurisce il servizio offerto[29]. L'attività a cui è chiamato il PISP, infatti, prende avvio e termina proprio nel momento iniziale della vicenda delegatoria tra banca e cliente (cd. delegazione di pagamento).

Il secondo elemento di rilievo sostanziale è il consenso rilasciato dall'utente, quale unico presupposto che accomuna tutte le modalità di pagamento, nonché imprescindibile requisito tanto per la stipula del contratto quadro che per l'avvio e la regolarità e della singola operazione di pagamento. Consenso che, ai sensi dell'art 64 PSD2 e dell'art. 5, co. 2, d.lgs. 11/2010, può essere ad oggi prestato anche tramite il prestatore di servizi di disposizione di ordine di pagamento e ciò proprio a seguito del differente tipo di consenso, rilasciato in precedenza, con il quale il cliente ha autorizzato il PISP all'uso delle sue credenziali di accesso al conto. In situazioni "ordinarie bilaterali", infatti, il consenso si traduce in un ordine di pagamento impartito al prestatore di servizi. L'ordine di pagamento, dunque, nonostante non sia altro che l'esternazione del consenso, mantiene una sua indipendenza concettuale che sfuma nel momento in cui l'operazione prende

28 Proprio il fatto che il PISP non entra mai in possesso dei fondi del cliente (divieto esplicito disposto dall'art. 66, par. 3, lett. a, dir. 2015/2366/UE), e di conseguenza, non abbia la possibilità di controllarli nella fase delle scritturazioni a debito e a credito, attività che resta di esclusiva competenza della banca del pagatore e del beneficiario, ha spinto alcuni a sostenere che questo soggetto non svolga attività in senso stretto di intermediazione, dovendo essere annoverato, di contro, tra i "*Technical Service Providers*" (Vanini, S.: "L'attuazione in Italia della seconda direttiva", cit., p. 859; Geva, B.: "Payment Transactions", cit., p. 219).

29 Messore, A.: "La nuova disciplina", cit., p. 522; Profeta, V.: "I Third Party Provider", cit., pp. 76 s., fa notare, quindi, che per detto servizio varranno norme speciali su forma e modalità di redazione del contratto, *ius variandi* e informazioni precontrattuali. Marasà', F.: "Servizi di pagamento", cit., p. 85, sostiene invece che l'utente nella prassi non ha un rapporto continuativo con il PISP, il quale è chiamato ad effettuare pagamenti occasionali e di importo tendenzialmente irrisorio.

impulso dal cliente[30]. Tuttavia, una volta che nella procedura si immette il PISP, è quest'ultimo a impartire l'ordine di pagamento previa autorizzazione del cliente: le due fasi dell'operazione si differenziano nuovamente. Detta scissione, funzionale al riparto di responsabilità in caso di operazioni non autorizzate, potrebbe giustificare la tesi di quella parte di dottrina che ricostruisce il rapporto tra cliente e PISP alla stregua di un mandato con rappresentanza in cui il PISP trasmette l'ordine alla banca attraverso l'uso autorizzato delle credenziali di sicurezza dell'utente, cioè spendendo il nome di quest'ultimo (*contemplatio domini*) sul quale ricadono gli effetti (addebito sul conto della somma prelevata) e a cui viene attribuita la paternità dell'operazione. Una ricostruzione che sembra essere supportata da alcuni degli obblighi contrattuali predisposti in capo al PISP dalla normativa, tra i quali spicca l'esecuzione dell'operazione con la diligenza di cui all'art. 1710 c.c. – la tradizionale diligenza "professionale" (*ex* art. 1176, co. 2, c.c.) – che impone rapidità, esattezza e sicurezza nell'adempimento; in una al peculiare obbligo di approntamento di sistemi di sicurezza al fine di custodire le credenziali ed i dati del cliente e garantirne trasmissione e comunicazione sicura ed entro i limiti di quanto necessario per lo svolgimento della propria attività; a tal proposito vige il divieto di conservazione dei «dati sensibili relativi ai pagamenti» dell'utente quali «dati che possono essere usati per commettere frodi, incluse le credenziali di sicurezza personalizzate»[31]. Lo schema del mandato impone al PISP il rispetto dei limiti e delle istruzioni date dal cliente (non può modificare l'importo, il beneficiario o qualsiasi altro dato relativo all'operazione, *ex* art. 5 *ter*, comma 2°, lett. f, d.lgs. n. 11/2010); in caso contrario, risponde per l'esecuzione di atti esorbitanti, salvo eventuale ratifica. In ipotesi di realizzazione di operazioni non autorizzate, truffe ai danni del cliente, furto di dati, la sua è una responsabilità contrattuale da inadempimento.

Pertanto, se la ricostruzione del rapporto PISP-cliente si risolvesse nello schema di mandato (ma parte della dottrina lo nega)[32] l'utente, che subisce il danno

30 De Stasio, V.: "Ordine di pagamento non autorizzato e restituzione della moneta", Giuffrè, Milano, 2016, pp. 103 ss., assimila l'operazione di pagamento ad un procedimento a piú fasi nel quale il consenso assume una funzione non negoziale, bensí procedimentale.

31 La tesi del mandato è sostenuta da Messore, A.: "La nuova disciplina", cit., p. 524 ss., la quale fa presente che, pur esistendo una parte della dottrina che suggerisce l'inquadramento del PIPS nella figura del *nuncius* perché semplice incaricato della mera trasmissione della dichiarazione di volontà altrui (del cliente), nella pratica questo non lede alla ricostruzione del rapporto come mandato con rappresentanza, e ciò in quanto la disciplina del mandato comunque spiega il rapporto (interno) che lega il *nuncius* al soggetto che gli affida l'incarico. Né incide sulla scelta ricostruttiva il fatto che rappresentanza e ambasceria generino effetti diversi sulla responsabilità in caso di patologica alterazione della dichiarazione del cliente e ciò proprio grazie alla ricostruzione peculiare che il legislatore europeo fa del riparto di responsabilità tra prestatori di servizi di pagamento. La riprova sono una serie di obblighi in capo al cliente-mandante, quali la somministrazione al mandatario dei mezzi per eseguire l'attività, il rimborso di eventuali spese ed il risarcimento danni subiti a causa dell'incarico. In realtà, questa ricostruzione potrebbe non essere propriamente adeguata rispetto al regime di spese e costi addebitabili dal PISP al cliente e desta non pochi punti interrogativi.

32 Troiano, O.: "Contratti di pagamento e disciplina privatistica comunitaria (proposte ricostruttive con particolare riferimento al linguaggio ed alle generalizzazioni legislative)", *Banca borsa tit. cred.*, num. 5°, 2009, pp. 535 ss., ritiene che nell'ambito dei servizi di pagamento, l'uso di schemi tradizionali come il mandato (ma anche la delegazione) sia frutto di una generalizzazione nella disciplina di settore. «L'agency relationship si basa sul customer's mandate e comporta un duty to exercise reasonable care and skill a carico del

ad opera di terzi, potrebbe rivolgere le proprie pretese risarcitorie direttamente al Third Party Provider, imputandogli, ad esempio, la violazione dell'obbligo di diligenza previsto da contratto.

La questione, però, è piú complessa, proprio perché la procedura non si esaurisce nel rapporto bilaterale cliente-PISP e cliente-banca. Affinché l'operazione venga effettivamente eseguita diviene indispensabile l'intervento dell'istituto di radicamento del conto il quale "apparecchia" il sistema trasformando i conti di pagamento – finora rapporti contrattuali esclusivi e bilaterali – in ciò che alcuni, seguendo la logica del diritto *antitrust*, definiscono "*essential facility*", ossia «in un'infrastruttura funzionale allo sviluppo di un ecosistema aperto per i pagamenti *retail*»[33].

Ed è proprio nella terza relazione tra PISP e banca, la piú innovativa e "controversa", che si ravvisa la peculiarità maggiore prevista dalla direttiva nonché la maggiore anomalia rispetto alle regole del diritto comune: l'assenza dell'obbligo – forse auspicabile? – di istaurare un rapporto contrattuale tra i due prestatori di servizi il cui legame, invece, è previsto ed imposto *ex lege* (Considerando n. 30, dir. 2015/2366/UE). La PSD2, orientata al principio di liberà concorrenza e non discriminazione, ha sottratto all'autonomia contrattuale privata dei prestatori di servizio di radicamento del conto la scelta di dialogare con i nuovi operatori, al fine di evitare che accordi contrattuali stipulati con solo alcuni di essi potessero minare il principio di neutralità tecnologica[34], consentendo agli istituti di credito

mandatario (agent). Le problematiche si articolano nel senso che non sarà legittimato ad addebitare il conto del cliente quel fornitore che agisce outside the mandate, ovvero che paga sulla base di un forged or unauthorised mandate. In realtà questi tratti comuni - pur quando adattati alle odierne innovazioni - spiegano poco. Il recente ampio ricorso a servizi elettronici di pagamento ha reso impossibile riconoscere se esiste un impiego autorizzato o no dei codici di accesso dell'utente; le innovazioni tecniche hanno reso la disciplina sí specifica ed articolata che le norme generali sul mandato (...) non si rivelano risolutive per molti problemi concreti» Talvolta, anzi, questa disciplina generale diverge dalle soluzioni ormai accolte anche sul piano legislativo (come nel caso della responsabilità del fornitore per inadempimento - estesa anche all'operato dell'intermediario -, regolata sul piano comunitario in base alla *strict liability* e non già al criterio della colpa)». Cosí anche Santoro, V.: "Servizi di pagamento", in *Contratti bancari* (a cura di E. Capobianco), Wolters Kluwer, Milano, 2021, p. 2157, il quale sottolinea che l'allontanamento dal modello del mandato si spiega per via dell'abbandono di forme contrattuali basate su un rapporto fiduciario, sostituite da contratti di massa che oggettivizzano la diligenza del prestatore del servizio (che diviene una valutazione di adeguatezza della banca rispetto alle procedure *standard* richieste dalla legge).

33 Gammaldi, D, e Iacomini, C.: "Mutamenti del mercato dopo la PSD2", in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale* (a cura di F. Maimeri e M. Mancini), in *Quaderni di ricerca Giuridica della Consulenza Legale della Banca d'Italia*, num. 87°, 2019, p. 139; sulla stessa linea, pare, Mezzacapo, S.: "L'inquadramento normativo della PSD2, tra 'dark side' del nuovo framework regolamentare UE dei servizi di pagamento e 'singolarità' dei pagamenti delle Pubbliche Amministrazioni", in *Innovazione e regole nei pagamenti digitali il bilanciamento degli interessi nella PSD2* (a cura di M.C. Paglietti e M.I. Vangelisti), Romatre-Press, Roma, 2020, p. 114, che paragona, anche giuridicamente, i PSP di radicamento del conto a «*facilities necessarie* per l'operatività nei connessi mercati *downstream* che su questi si basano»; *contra* Santoro, V.: "Servizi di pagamento", cit., pp. 2169 s., il quale nega tale ricostruzione derivata dal diritto *antitrust*, in primo luogo perché «sarebbe surreale» considerare tale una singola relazione tra banca e cliente; in secondo luogo, perché non sarebbe tale neanche l'insieme dei rapporti banca-clienti, eccetto il caso in cui si provi che la banca sia colpevole di abuso di posizione dominante oppure abbia concluso con altri operatori un accordo anticoncorrenziale per limitare l'ingresso nel mercato dei nuovi *players*.

34 Secondo il quale «… per la stessa attività devono valere le medesime regole a prescindere dal soggetto che le pone in essere (...) e indipendentemente dalle soluzioni tecniche oggettivamente prescelte» (La Sala,

di decidere arbitrariamente con chi dialogare e a quali condizioni e a chi, invece, negare accesso al mercato. La libertà – se non propriamente un eventuale obbligo – di contrarre viene sostituita da un obbligo legale di cooperazione e trasparenza posto in capo alla banca[35]. Per tale ragione, il cliente non ha l'onere preventivo di avvisare la stessa del fatto che usufruisce dei servizi di un qualsiasi PISP. Di conseguenza, una volta che la banca riceve un ordine di pagamento dall'operatore terzo – il quale ovviamente *in primis* deve identificarsi come tale – ha l'obbligo di aprire il conto del cliente e fornire le informazioni richieste sull'ordine di pagamento e sulla relativa esecuzione (tra le quali la conferma immediata della disponibilità economica per operare), assicurando il medesimo trattamento ad ordini che provengono dal cliente o dal PISP[36], salvo giustificate e comprovate situazioni di sospetta frode che le impongono di bloccare l'operazione, dandone immediata notizia all'utente. Il prestatore di radicamento del conto, quindi, è esonerato dall'indagare la relazione contrattuale tra il cliente e l'operatore terzo dovendo, di contro, presumere, per effetto dell'autenticazione e dell'utilizzo delle credenziali di accesso al conto, che quest'ultimo agisca sulla base del consenso esplicito rilasciato in precedenza dal cliente stesso[37]. Un siffatto controllo, infatti,

G.P.: "Intermediazione, disintermediazione, nuova intermediazione: i problemi regolatori", in *Diritto del Fintech* (a cura di M. Cian e C. Sandei), Cedam, Padova, 2020, p. 6).

35 Di "anomalia" parla De Stasio, V.: " Riparto di responsabilità e restituzioni nei pagamenti non autorizzati", in *Innovazione* e *regole nei pagamenti digitali il bilanciamento degli interessi nella PSD2* (a cura di M.C. Paglietti e M.I. Vangelisti), RomaTre-Press, Roma, 2020, p. 28 e Id.: "Ordine di pagamento non autorizzato", cit., pp. 237 s., il quale fa presente che proprio questa innovazione è stata accolta dai giuristi tedeschi come una «crisi del paradigma interpretativo dei servizi di pagamento, sempre piú vicino a una configurazione di "*Netzvertrag*" inteso come strumento idoneo al superamento dei limiti della *privity of contract*». L'A., però, sostiene che ormai, nel settore dei pagamenti, sia in crisi proprio l'istituto del contratto, sostituito da una logica procedimentale e di impresa. Si potrebbe affermare che ciò che sostiene l'A., non sia altro che la riconferma del difficile adattamento degli istituti tradizionali (mandato, delega ecc.) alle nuove formule tecnologiche. *Contra*, Messore, A.: "La nuova disciplina", cit., p. 525, nota 40, che sostiene che, essendo tutta l'operazione costruita come una fattispecie trilaterale a struttura delegatoria, con tre rapporti negoziali distinti ma collegati [utente (delegante)-TPP (delegato); TPP (delegato)-PSP(delegatario), utente (delegante)-PSP (delegatario)], la mancanza di un rapporto contrattuale diretto tra PIPS e prestatore di servizio di pagamento nega la presenza di una delegazione obbligatoria, bensí "pura", con la conseguenza della possibile applicabilità o meno delle eccezioni *ex* art. 1271 c.c. (per l'A. resta comunque «l'opponibilità della c.d. "nullità della doppia causa": ossia, in caso di invalidità, revoca o inefficacia sopravvenuta dello i*ussum* [*solvendi*)]».

36 I comportamenti imposti dall'obbligo di collaborazione della banca verso il PISP sono riportati all'art. 66 dir. 2015/2366/UE, e in Italia, all'art. 5 *ter*, d.lgs. 11/2010.

37 Diversa, ma non di minor rilievo, la questione della revoca del consenso ai servizi del PISP da parte del cliente, la cui disciplina non viene definita dalla normativa europea. L'aspetto non è di secondario rilievo in quanto interviene nel bilanciamento tra due esigenze contrapposte: stimolare l'utilizzo da parte dell'utente di questi nuovi servizi (evitando che le banche possano imporre clausole limitative in tal senso) e garantire a quest'ultimo una tutela tale da consentirgli di comunicare la revoca del consenso direttamente all'operatore che gestisce il conto corrente. A tal proposito, è stato fatto notare come, da un lato, influisce il principio generale dell'ordinamento che prevede di portare a conoscenza della revoca del consenso direttamente il soggetto cui il consenso era stato originariamente prestato (PISP); dall'altro, però, un'applicazione eccessivamente rigorosa di tale principio, volto a escludere la possibilità per l'utente di revocare il consenso all'accesso ai conti anche presso la banca, ridurrebbe il livello di tutela garantita. Come conseguenza, si potrebbe generare una incertezza giuridica nel caso in cui la banca, a seguito dell'eventuale ricezione della revoca del consenso dell'utente all'utilizzo di un determinato TPP, dovesse procedere a bloccarne l'accesso al conto senza che il PISP ne sia a conoscenza (Gammaldi, D. e Iacomini, C.: "Mutamenti del mercato dopo la PSD2", cit., p. 129 s.). Su questo aspetto, il legislatore nazionale si è mosso nelle pieghe dell'armonizzazione "meno che massima" della disciplina, favorendo un'ottica di accrescimento delle tutele dell'utente; in prima battuta, ha precisato che una volta rilasciato il consenso alla singola operazione, questo diviene irrevocabile, salvo accordo tra l'utente e tutti i prestatori coinvolti nell'operazione (art. 17,

richiederebbe tempi non compatibili con l'immediatezza che caratterizza i nuovi servizi digitali, finendo per disincentivarne l'uso ed invalidarne l'efficacia.

Allo stesso tempo, il rifiuto ingiustificato da parte della banca di ammettere l'accesso al conto da parte del PISP o di accettare l'ordine proveniente da quest'ultimo, violerebbe il dovere di leale collaborazione imposto dalla direttiva, generando in capo alla stessa una responsabilità contrattuale nei confronti del cliente. Inoltre, tale atteggiamento configurerebbe una possibile condotta ostruzionistica, violativa della libertà di concorrenza ed aprirebbe a nuovi scenari di illeciti di competenza dell'*Antitrust*. Ciò, quantomeno, nella circostanza in cui l'atteggiamento di chiusura arbitraria della singola banca rifletta comportamenti concordati fra operatori tradizionali (cd. divieto di intese restrittive della concorrenza)[38].

Alla impossibilità della banca di controllare le modalità di relazione con i PISP sotto "minaccia" di responsabilità contrattuali, la direttiva aggiunge in capo alla stessa ragguardevoli costi di sviluppo, programmazione e manutenzione delle piattaforme, necessarie a garantire un canale di accesso e trasmissione sicuro per lo scambio di informazioni con i terzi operatori, tutelando al contempo la riservatezza e la sicurezza dei dati del cliente (si pensi solo all'API, "*Application Programming Interface*")[39]. Come giustamente è stato affermato, la conseguenza immediata del sistema creato dalla PSD2 è l'immagine di una banca che si fa carico di investimenti ingenti al fine di soddisfare un obbligo normativo.

commi 2 e 5, d.lgs. 11/2010); quanto, invece, alla revoca del consenso alla prestazione dei servizi da parte dei PISP, si consente la ricezione della stessa anche dalla banca che gestisce il conto di pagamento (art. 6 *bis*, comma 3, d.lgs. n. 11/2010) la quale, a sua volta, è tenuta ad informarne senza ritardo il terzo *provider*.

38 Sul tema Meli, V.: "Opportunità e sfide per la concorrenza nella disciplina dei servizi di pagamento", in *Innovazione e regole nei pagamenti digitali il bilanciamento degli interessi nella PSD2* (a cura di M.C. Paglietti e M.I. Vangelisti), Romatre-Press, Roma, 2020, p. 135 ss., il quale si confessa piú scettico nel caso in cui gli ostacoli posti ai nuovi operatori siano frutto di politiche dettate dalla singola banca, la quale potrebbe venire sottoposta all'attenzione dell'Antitrust solo se fosse considerata soggetto in posizione dominante, situazione non ravvisabile, attualmente, in Italia. D'altronde, non può sfuggire come, molto spesso, la situazione "di dominanza" appartiene non all'istituto bancario, bensí ai soggetti terzi, i quali forniscono anche i nuovi servizi di pagamento oltre ad altri che hanno permesso loro di emergere in differenti mercati. Basti solo pensare a Google, Amazon, Facebook e altri colossi della stessa caratura.

39 Le sue funzioni sono elencate nel regolamento delegato 2018/389/UE, art. 30 par. 2 e 3. Uno studio completo sul tema è stato compiuto da Borgogno, O. e Colangelo, G.: "Data Sharing and Interoperability Trough APIs: Insights from European Regulatory Strategy", *European Union Law Working Paper*, Stanford -Vienna Transatlantic Technology Law Forum, 2018. In merito ai problemi irrisolti relativi all'utilizzo di tale piattaforma si veda, ad esempio, Sciarrone Alibrandi, A.: "Impostazione sistematica della Direttiva PSD2", cit., pp. 20 ss., che ipotizza una sostituzione della stessa con la tecnologia "*blockchain*". Ciò in quanto, come si accennerà in seguito, mancano *standard* normativi (nazionali o internazionali) unici di comunicazione banca-TPP, che faciliterebbero la intercomunicabilità tra sistemi. Sul punto, anche il parere di Insurance Europe del 2 agosto 2022 (disponibile al sito *ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules*), che lamenta la gravosità, onerosità e problematicità del processo di approvazione dell'API da parte delle varie autorità nazionali, alcune delle quali autorizzano determinate piattaforme e non altre che, invece, sono legali in differenti Stati. Ciò sempre a causa della totale assenza di *standards* univoci.

V. LA STRUTTURA DEL RIPARTO DI RESPONSABILITÀ TRA PISP E PSP IN CASO DI OPERAZIONI FRAUDOLENTE.

L'incremento del numero di soggetti coinvolti nelle già complesse procedure di pagamento digitale, corrisponde ad un numero superiore di passaggi intermedi che portano ad esitare l'operazione finale. Questa struttura aumenta vertiginosamente le probabilità di falle o punti deboli nei sistemi che, nonostante le nuove tecnologie, restano imperfetti perché, in ogni caso, frutto dell'elaborazione umana e, di conseguenza, vulnerabili ad attacchi esterni fraudolenti. Basti solo pensare alla quantità ingente di dati personali sensibili dell'utente che ogni giorno migrano da una piattaforma di dialogo ad un altra. Nonostante i costi, oltretutto a titolo gratuito, che le banche sono chiamate a sostenere *ex lege* per rendere sicuro il dialogo con i *players* terzi – che, si ricorda, sono anche suoi potenziali concorrenti – il numero di decisioni dell'ABF e dei Tribunali, chiamati a difendere l'utente da frodi informatiche ed operazioni non autorizzate, non accenna a calare. Riassumendo in una sola frase: vecchi pericoli, nuovi rischi[40].

Eppure, nelle consultazioni svolte per riformare la PSD2 è unanime il parere di operatori e clienti *retail* che sostengono l'utilità delle misure di sicurezza apportate dalla direttiva nel ridurre alcuni tipi di frode (le piú comuni e già in precedenza richiamate). Di fatto, si assiste ad «*fraud migration process*»[41], laddove le forme di intrusione illecita nei conti si aggiornano, scavalcando gli ormai "obsoleti" sistemi di tutele della direttiva.

Orbene, fatte queste premesse, va da sé che nell'ipotesi di operazioni fraudolente ai danni dei clienti, la pluralità dei soggetti coinvolti nell'operazione di pagamento dal lato debitore, per effetto dell'intervento del prestatore del servizio di disposizione di ordine di pagamento, intorbidisce le acque dell'allocazione di responsabilità. Se, normalmente, in un rapporto bilaterale cliente-banca, il problema è fino a che punto si possa collocare la responsabilità in capo alla seconda, salvaguardando l'esistenza dell'eventuale negligenza grave del primo – ormai molto mitigata[42] –, nel rapporto "a tre fattori" la questione diviene verificare

40 Beck, U.: "Vivere nella società del rischio globale", *Ars Interpretandi*, 2007, num. 12°, p. 125.

41 L'impresa ADigital: "Payment Services – EU rules", nel parere rilasciato sul sito della Commissione Europea (rinvenibile in *ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules_en*), ribadisce l'evidenza di come le frodi siano diminuite in alcune aree (piú tradizionali) e aumentate in altre. Tra le nuove forme di intrusione illecita emerge, ad esempio, la "*Request-to-Pay feature* (*person-to-person or second hand purchases*)": «*This type of fraud is more developed and complex and entails a certain defenselessness for the consumer since it is usually associated with means of payment where there is no dispute process (or chargebacks) which can be used*».

42 Tuttora, però, non mancano ipotesi in cui l'ABF pone in evidenza un comportamento gravemente negligente dell'utilizzatore che può portare ad un riparto di responsabilità, secondo il concorso di colpa ai sensi dell'art. 1227 c.c. (es: Marseglia, C.: "Responsabilità civile - «Furto della tessera di bancomat e concorso di colpa tra l'utilizzatore e l'intermediario», *Nuova giur. civ. comm.*, num. 3°, 2020, pp. 561 ss.; in giurisprudenza, si veda, per esempio ABF, Coll. Napoli, 20 luglio 2020, n. 12845, in *arbitrobancariofinanziario.it*) o ad un rigetto del ricorso per riconosciuta colpa grave del cliente ricorrente come, ad esempio, in ABF, Coll. Bologna, 16 marzo 2022, n. 4453, in *arbitrobancariofinanziario.it*.

in che momento e sotto la responsabilità di chi sia avvenuto l'accesso illecito ma, soprattutto, su chi conviene far ricadere "la colpa".

A tal proposito, la *policy* della PSD2 (in Italia, del d.lgs. 11/2010) adotta un regime di responsabilità favorevole agli utenti dei servizi ed a supporto dei nuovi meccanismi di pagamento, tutelandone, altresí , l'efficienza. In un sistema con piú operatori, ciascuna fase dell'*iter* diviene invisibile ad un occhio esterno al punto che, talvolta, è difficoltoso persino per l'intermediario stesso individuare il momento esatto in cui si è verificata la disfunzione. La struttura di responsabilità elaborata dalla direttiva, nel rapporto banca-cliente, risponde ai cd. "principio di vicinanza della prova"[43] e "di prossimità" per i quali il secondo si interfaccia solo con la prima di cui conosce "il volto", i servizi e le responsabilità, ed unica a conoscenza del funzionamento (o malfunzionamento) dei sistemi di gestione dei pagamenti. Nel rapporto PISP-banca, invece, la direttiva opta per una ripartizione della responsabilità che imponga a ciascuno di rispondere della parte di operazione sottoposta al proprio controllo.

In verità, la procedura prevista dalla normativa ricalca la stessa struttura dell'allocazione di responsabilità tradizionale cliente-banca, sia in relazione al principio di presunzione di responsabilità del prestatore del servizio di pagamento, che all'inversione dell'onere della prova a tutela dell'utente[44].

Ciò implica che, in un rapporto in cui è coinvolto anche un terzo *player*, l'utente che contesta la mancata autorizzazione di un'operazione di pagamento eseguita a suo carico «non sarà onerato di dimostrare quale tra i prestatori coinvolti sia stato in concreto responsabile dell'esecuzione di tale pagamento, al fine di proporre correttamente nei suoi confronti domanda di rimborso o di risarcimento»[45], bensí farà valere tale diritto solo nei confronti del prestatore di radicamento del conto. Quest'ultimo è tenuto non solo a pagare, ma ad eseguire l'immediata restituzione di quanto perso indebitamente dall'utente al piú entro il giorno successivo alla richiesta, senza formalità ed a prescindere da sue reali responsabilità (cd. tutela immediata ma non definitiva)[46]. A sua volta, quest'ultimo, sarà tenuto indenne dal

43 Sul principio *de quo*, Dolmetta, A.A. e Malvagna, U.: "Vicinanza della prova e prodotti d'impresa del comparto finanziario", *Banca borsa tit. cred*., fasc. 6°, 2014, pp. 659 ss.

44 Sul tema dell'inversione dell'onere della prova, che sappiamo gravare principalmente sul prestatore del servizio, si veda Paglietti, M.C.: "Questioni in materia di prova", cit., pp. 43 ss. e in particolare p. 50, nota come il nodo critico risieda nel concetto di colpa grave (*faute lourde*) a causa del localismo nazionale che colora il concetto di sfumature differenti.

45 Profeta, V.: "I Third Party Provider", cit., p. 73.

46 Nella prassi, a seguito dell'inoltro della domanda di rimborso alla banca, l'utente non riceve alcun ristoro, attendendo l'intermediario che questi adisca il giudice. Per questo, le decisioni ABF sul punto sono innumerevoli. In genere, l'utente si limita a richiedere il rimborso di quanto perso; non è, tuttavia, escluso che possa richiedere altresí il risarcimento del danno ulteriore. Sul tema né la PSD2 né il decreto 11/2010 prendono posizione, facendo spesso confusione il secondo tra i termini "risarcimento" e "restituzione" (come spiegato ampliamente da De Stasio, V.: "Riparto di responsabilità", cit. pp. 25 ss.) e demandando al contratto stipulato (e solo in questo caso, secondo De Stasio) ed alle regole di diritto comune sulla

PISP con la stessa immediatezza, senza alcuna formalità, in una catena che ricalca precisamente il rapporto tra il cliente ed il primo intermediario. Si presume *ab origine*, sebbene in via relativa, una responsabilità in capo al prestatore del servizio di disposizione dell'ordine di pagamento e un conseguente diritto di regresso della banca verso quest'ultimo. La stessa ha, altresí, diritto, a semplice richiesta e senza messa in mora, al risarcimento delle perdite subite e al ristoro di un eventuale danno ulteriore nel caso in cui l'operazione illegittima risultasse definitivamente imputabile al PISP[47]. Questi, a sua volta, se non vuole accollarsi la perdita, ha l'onere di fornire prova liberatoria, dimostrando che «nell'ambito delle proprie competenze, l'operazione è stata autenticata, correttamente registrata e non ha subito le conseguenze di guasti tecnici o di altri inconvenienti» (art. 11, co. 2 *bis*, d.lgs. n. 11/2010), provando allo stesso tempo che, ad esempio, i sistemi di sicurezza della banca si sono dimostrati inadeguati o irrispettosi degli *standard* europei o, ancora, che la banca abbia precluso l'accesso ai servizi SCA o, peggio, non abbia adottato tale tecnologia. Parte della dottrina, inoltre, asserisce che il PISP, in qualità di soggetto su cui ricade la presunzione di responsabilità, sia legittimato ad agire per dimostrare la frode, il dolo o la colpa grave del cliente[48] rispetto, ad esempio all'uso corretto degli strumenti di pagamento, di cautela nella conservazione delle proprie credenziali e di tempestiva denuncia di utilizzo fraudolento degli stessi. In sintesi, una volta che il cliente ottiene la tutela predisposta in suo favore, si apre una fase eventuale, regolata *in toto* dalla normativa, nella quale i due attori protagonisti, l'operatore tradizionale ed il PISP, delineano i confini delle reciproche responsabilità in quello che alcuni definiscono «vincolo di solidarietà tra IP»[49].

responsabilità contrattuale la possibilità di prevedere questa richiesta aggiuntiva. Come spiega Marasa', F.: "Servizi di pagamento", cit. pp. 163 ss., la scelta del silenzio da parte di entrambi i legislatori, europeo e nazionale, è in linea con la *ratio* della direttiva che richiede tempi rapidi di risposta alle esigenze dell'utente; di contro, l'accertamento dell'*an* e del *quantum* del risarcimento allungherebbe i tempi delle tutele del ripristino della situazione *quo ante*; ciò non toglie che l'A. apra alla possibilità di risarcimento di un danno ulteriore (previsto d'altronde all'art. 26, d.lgs. 11/2010) *ex* artt. 1218, 1223, 2697 c.c., purché non sia mera duplicazione del rimborso. D'altronde, proprio la prassi bancaria di non corrispondere subito il rimborso, cosí come viene previsto dalla direttiva, porta alla maturazione degli interessi almeno fino all'effettiva corresponsione del rimborso. Il lucro cessante, invece, secondo l'A., si potrebbe qualificare come danno da perdita di *chance* per mancata disponibilità del denaro, se non proprio per l'utilizzo illecito dei dati personali sottratti all'utente. In quest'ultimo caso, la banca ne risponde come titolare del trattamento degli stessi [la questione del rapporto tra PSD2 e GDPR (regolamento 2016/679/UE) è molto complessa e parzialmente irrisolta. Si veda, Marasa', F.: "Servizi di pagamento", cit., pp. 169 ss.; Burchi, A., Mezzacapo, S., Musile Tanzi, P. e Troiano, V.: "Financial Data Aggregation e Account Information Services. Questioni regolamentari e profili di business", in *CONSOB, Quaderni Fintech*, num. 4°, marzo 2019].

47 De Stasio, V.: "Riparto di responsabilità", cit., pp. 44 s., fa notare come il termine "rimborso" del PISP verso PSP appaia solo nel d.lgs. 11/2010, all'art. 11, par. 2 *bis*. Di contro, la direttiva, all'art. 73, par. 2, parla direttamente di "risarcimento". Una discrasia che l'A. porta sul piano pratico, sostenendo che il rimborso a carico della banca generi un rischio di *overcompensation* rispetto allo scopo da raggiungere, tenendo conto dell'eventualità «di un recupero parziale dei fondi trasferiti e non conteggiabili all'utente nel rapporto di conto di pagamento».

48 Cosí Profeta, V.: "I Third Party Provider", cit., p. 74.

49 Paglietti, M.C.:" Questioni in materia di prova", p. 59; in verità, si parla di "solidarietà" in senso lato legale (imposta) in quanto, alla chiusura della eventuale fase patologica giudiziaria tra prestatori di servizi, solo uno dei due assorbirà il danno patito dal cliente. Proprio in relazione alla solidarietà, Santoro, V.: "Servizi di pagamento", cit., pp. 2159 s., con riferimento alla scelta del legislatore di ancorare la responsabilità esclusiva del prestatore alla parte del procedimento sottoposta al suo controllo, propone scelte alternative tra le quali la risposta in solido degli intermediari coinvolti, secondo la regola del trasporto cumulativo di

In verità, l'impalcatura di responsabilità eretta dalla direttiva, già *in nuce* nella PSD1, in ambito giurisprudenziale sembra, almeno per il momento, trovare riscontro effettivo solo con riferimento alla parte relativa al "rimborso" del cliente. Né le decisioni dell'ABF, né le sentenze dei tribunali ordinari paiono occuparsi della seguente fase di allocazione di responsabilità tra i due prestatori di servizi. Non è ancora chiaro se la motivazione sia da rinvenire, come si sostiene, nella radicata preferenza della clientela – specialmente italiana – a preservare il contatto umano, affidandosi per le operazioni quotidiane ai funzionari di banca ed a renderla naturalmente diffidente rispetto ad app. o a servizi di pagamento *online* (il cui carattere "virtuale" trasmette l'idea di un'attività che sfugge alla propria sfera di controllo); o se invece (orientamento a cui si aderisce) le banche ritengano poco conveniente intentare azioni contro i TPP – che, come già accennato, molto spesso sono colossi della tecnologia con sede legale in Paesi esteri – o se, ancora, prediligano transazioni stragiudiziali, data la generale irrisorietà delle cifre da rimborsare (ciò in quanto, molto spesso, sono i piccoli clienti *retail* a cadere vittima di truffe informatiche). Il risultato comunque non cambia: il panorama giurisprudenziale è costellato di decisioni ABF che si occupano solo di valutare la natura e la portata della responsabilità bancaria nei confronti del cliente, in particolare con riferimento all'eventuale violazione da parte della prima del sistema di sicurezza SCA ma che non vedono alcun confronto tra intermediari.

Nell'ultimo periodo, tuttavia, si sta assistendo ad un incremento del contenzioso che vede come protagoniste le banche in contrapposizione ad un altro nuovo *player* del mercato digitale, l'*e-wallet provider*, depositario e gestore di un portafoglio elettronico (*e-wallet*). Sebbene quest'ultimo non sia classificabile come Third Party Provider secondo la direttiva in vigore, il crescente ruolo che va assumendo nella catena del pagamento come ausilio dell'attività bancaria ha dato adito, nella recente consultazione, ad una proposta di inclusione tra i servizi di pagamento e regolamentazione nel contesto normativo europeo[50]. Esso, infatti, a differenza dei PISP, la cui relazione con la banca è imposta per legge, instaura un vero e proprio rapporto contrattuale con la stessa, coadiuvandola nella fase esecutiva del pagamento (e non, come il PISP nella fase preparatoria). La banca, infatti, può esternalizzare (cd. *outsourcing*) a terzi alcune fasi della propria attività come, ad esempio, in qualità di emittente di strumenti di pagamento la gestione tecnologica degli stessi. Nel caso degli *e-wallet*, la registrazione del singolo strumento (come una carta) nel portafoglio (in genere, un *mobile wallet* scaricato sul telefonino) necessita dell'autenticazione forte (ai sensi dell'art. 97, par. 1, PSD2)

cose *ex* art. 1700 c.c. (paragonando, dunque, la catena virtuale del pagamento al trasporto per tappe di una bene materiale) o, come si accennava già nel testo, consentire al cliente di rivolgersi direttamente agli intermediari terzi seguendo le regole del mandato.

50 Solo a titolo esemplificativo si rinvia ai pareri rilasciati da Abi: "ABI position paper", cit., p. 3 e Intesa San paolo: "Call for evidence Review of the Second Payment Services Directive (PSD2)", luglio 2022, p. 1, disponibile su *ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/feedback_en*.

la cui tipologia e caratteristica sono lasciate in decisione alla banca stessa e ciò a causa dell'alto rischio frode a cui questa operazione va incontro[51]. Nell'esecuzione del pagamento a mezzo di e-*wallet provider* l'operatività dello strumento, compresa la SCA, viene gestita da questi che cura, altresí, la protezione delle credenziali di accesso dell'utente. L'EBA, tuttavia, ha precisato come la procedura SCA sia una procedura di verifica dell'identità che può essere eseguita ma non gestita dal terzo operatore. Da questa precisazione, consegue l'orientamento finora unanime della giurisprudenza ABF[52] la quale sostiene che, nell'ipotesi in cui si verifichi lo scenario peggiore, ossia che attraverso questo sistema il frodatore abbia carpito le credenziali di accesso all'*home banking* sottraendo fondi all'utente, il prestatore del servizio di radicamento del conto non è sollevato dalle proprie responsabilità, gravando sullo stesso l'onere di fornire la prova dell'avvenuta autenticazione forte sia in fase di "*tokenizzazione*" della carta nel *wallet*, che nella fase esecutiva delle singole operazioni. Resta, tuttavia, aperta la questione di una eventuale responsabilità del *provider* a cui si appoggia la banca. Il mancato riconoscimento dello stesso ad opera della PSD2 tra i servizi di pagamento genera una lacuna normativa che inficia l'eventuale riparto di responsabilità. In attesa di un intervento *ad hoc* da parte del legislatore europeo, che potrebbe giungere auspicabilmente con la riforma della PSD3, si potrebbe giustificare l'orientamento dell'ABF secondo il medesimo principio di prossimità e vicinanza della prova, utilizzato per l'allocazione di responsabilità tra PISP e PSP, in una all'obbligo della banca di garantire la sicurezza dei propri sistemi informatici. Si potrebbe, inoltre, fare un passo aggiuntivo ed ipotizzare che, nel caso in cui la frode sia stata causata da un errore o negligenza di qualche tipo dell'e-*wallet provider* – essendo lo stesso ausiliario della banca e potendo stipulare un contratto con la medesima – la banca possa rispondere in via indiretta del danno subito dal cliente proprio in forza del suddetto legame, seguendo la logica della *culpa in vigilando* o *culpa in eligendo* che le imporrebbe di scegliere ausiliari competenti e controllarne l'operato[53].

51 Eba: "Q&A 2019_4910. Strong customer authentication and common and secure communication (incl. access)", 25 settembre 2020, disponibile in *eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4910*, ha confermato che «*Adding a payment card to a digital wallet is an action which may imply a risk of fraud or other abuses and thus would require the application of SCA. This means that … the payer would need to apply SCA for accessing its payment account via its mobile application and apply a second SCA when adding the payment card to a digital wallet*».

52 A partire da ABF, Coll. Coord., 11 ottobre 2021, n. 21285, a tema "*phising*"; sulla stessa scia, *ex multis*, si veda, ABF, Coll. Roma, 3 giugno 2022, n. 8706; ABF, Coll. Napoli, 20 giugno 2022, n. 9516; ABF, Coll. Roma, 4 agosto 2022, n. 11703, tutte disponibili in *arbitrobancarioefinanziario.it*.

53 Marasa', F.: "Servizio di pagamento", cit., pp. 143 ss.; si veda art. 12, co. 2 *ter*, d.lgs. 11/2010: «il pagatore non sopporta alcuna perdita […] se la perdita è stata causata da atti o omissioni di dipendenti, agenti o succursali del prestatore di servizi di pagamento o dell'ente cui sono state esternalizzate le attività» e, nel codice civile italiano, combinato disposto degli artt. 1228-2049. In generale, la banca risponde secondo detta normativa se: il danno esiste; tra l'ausiliario e la banca sussiste un rapporto che si possa definire "di preposizione"; si provi il nesso causale tra danno e fatto dell'ausiliario. Si ricordi inoltre che l'art. 27 d.lgs. 11/2010, in caso di responsabilità *ex* art. 11 (cioè per operazioni non autorizzate), fa salva la possibilità per il prestatore del servizio di pagamento di azionare il regresso nei confronti di «qualsiasi altro soggetto interposto nell'esecuzione dell'operazione», regola quest'ultima ad oggi applicabile a tutti quegli operatori che costituiscono l'infrastruttura tecnica del servizio di pagamento, ma che potrebbe estendersi anche agli e-*wallet providers* una volta entrati a far parte della categoria dei servizi di pagamento. Facoltà, tuttavia,

Una ricostruzione quest'ultima, forse banale, che si limita ad applicare gli istituti del diritto civile ad un settore, quello dei servizi di pagamento, multiforme e complesso la cui natura impone la costruzione di una disciplina completa e uniforme, che sappia mantenere il passo o, quantomeno, limitare i ritardi rispetto al dinamismo evolutivo che lo connota. Il nuovo rapporto tra banca e e*-wallet provider* (soggetto terzo presente nel mercato ma ancora in cerca di collocazione nel diritto), che sta catalizzando l'attenzione dell'ABF nell'ambito dei ricorsi per operazioni fraudolente, è la prova che la PSD2 necessita di alcuni ritocchi sistematici che puntino a "disciplinare l'indisciplinato", alla ricerca del delicato equilibrio nell'allocazione dei rischi e delle perdite conseguenti all'avverarsi degli stessi.

VI. BREVI RIFLESSIONI CONCLUSIVE.

Negli ultimi anni si sta assistendo ad un paradosso. L'emersione sul mercato di nuovi operatori, difficili da ricondurre nell'alveo delle definizioni tradizionali e portatori di proprie regole e discipline – costruite, spesso, per facilitare il loro ingresso nel mercato – in prima battuta, genera un fenomeno di disintermediazione nel quale le banche perdono l'esclusività del rapporto con la clientela e sono costrette *ex lege* a dialogare con i nuovi *players*, inserendoli nelle dinamiche delle operazioni di pagamento; allo stesso tempo, però, si assiste al fenomeno contrario del rafforzamento dell'intermediazione stessa: senza la banca o l'istituto di credito che permette l'apertura di conti correnti, predispone le piattaforme digitali di dialogo, effettua concretamente i trasferimenti di fondi, i nuovi operatori semplicemente non operano. Il capitale del cliente resta in mano agli operatori tradizionali, *cosí* come la sua fiducia. Per tali ragioni, ad una apparente disintermediazione non corrisponde una conseguente deresponsabilizzazione della banca bensí , al contrario, una allocazione del rischio tendenzialmente sbilanciato a carico dell'istituto di radicamento del conto. Non sorprende, pertanto, scoprire dalla consultazione pubblica che le banche ritengono che, allo stato attuale, responsabilità, rischi e costi non siano equamente distribuiti tra loro ed i TPPs, lamentando altresí una evidente asimmetria normativa – che si tramuta in uno squilibrio competitivo – di cui beneficiano i fornitori dei nuovi servizi. E ciò si manifesta palesemente nel fatto che i PISP si appoggiano alle procedure di autenticazione fornite dalla banca all'utente, facendo nella prassi ricadere l'onere della prova principalmente su quest'ultima. Lo squilibrio viene avvertito anche nell'obbligo della banca di immediata restituzione delle somme di denaro al cliente, il cui rientro, in caso di responsabilità del PISP, dipende interamente dalla solvibilità e disponibilità di quest'ultimo. Resta aperta, altresí, la questione, spinosa, relativa

che per ora è ben riconosciuta già nei principi generali dell'ordinamento civile italiano e, quindi, ad essi applicabile nella prassi.

alla gratuità dei servizi e delle piattaforme messi a disposizione dall'istituto di credito non solo dei clienti ma dei PISP. Una gratuità, ovviamente, momentanea e apparente in quanto il costo del complesso apparato richiesto dalla direttiva per il dialogo con i TPPs si tramuta in un "costo sociale" che la banca riversa in percentuale sulla platea di clienti.

Quanto al tema delle frodi informatiche, è sentire comune la necessità di elaborare procedure di *recovery funds* che siano piú semplici, veloci ed intuitive. La presenza di un nutrito numero di soggetti che intervengono nella medesima operazione di pagamento, come detto, ha aumentato i punti deboli della procedura, vulnerata dalla origine "umana" dei sistemi algoritmici alla base, permettendo a esterni di insinuarsi illecitamente. Emergono, ad esempio, nuovi modelli di hacking che sfruttano tecniche di "*social engeneering*". Da tali rilievi, il suggerimento di modificare la nozione di frode in base al tipo di manipolazione subita dal pagatore, distinguendo «*between phenomenology with a technical component and phenomenology based exclusively on social engineering attacks*»[54].

In verità, dalle prime indiscrezioni emerse sulla riforma della PSD2, non sembra che il legislatore voglia intaccare la struttura della fase patologica dell'allocazione di responsabilità tra prestatori di servizi statuita dalla direttiva, quanto migliorare il rapporto fisiologico tra banca e TPPs. Ad esempio, proponendo *standard* condivisi per le piattaforme di dialogo, migliorando la qualità dei dati che le banche forniscono ai terzi (aggiungendo descrizioni e specificando le causali delle operazioni) e soprattutto, implementando i sistemi di interoperabilità[55] a sfavore della frammentazione attuale.

Con tutta probabilità, la riforma dovrà occuparsi dei nuovi soggetti emergenti, tra i quali *technical service provider* e *payments wallet provider*, definendoli e definendone il rapporto con gli altri operatori.

L'importanza massiva che i dati – ed il loro scambio – assumono nella società attuale, potrebbe dare risalto agli altri TPPs, ossia gli AISP, la cui attività si incentra proprio nella aggregazione di informazioni e loro gestione e trasmissione. Non può sottacersi come l'attività che questi particolari operatori svolgono è caratterizzata da profili di rischio peculiari che impongono la ricerca di un giusto equilibrio tra

54 Parere Intesa San Paolo, cit.

55 «Spesso le banche scelgono una *sandbox* unica e bloccano gli accessi a *provider* diversi da quelli che hanno scelto. Dal punto di vista dei consumatori, la PSD2 ha introdotto opportunità in ambito sicurezza del dato e accesso a partner di terze parti ma hanno ridotto la *customer experience* .Perché una volta che ho fatto l'accesso alla banca con tre codici poi devo avere anche un'autenticazione rafforzata per l'accesso a un conto corrente che mi ha già approvato?», queste le riflessioni in merito alla riforma del Senior Advisor Innovation & Fintech Partnership di Supernovae Labs, Pasotti, R.: "Lo stato dell'arte della PSD2, l'evoluzione in PSD3 e l'impatto sullo sviluppo di nuovi strumenti di pagamento" durante un intervento all'iniziativa "Payments 2022" del 16 febbraio 2022 (agenda disponibile in *ikn.it/evento/11446/payments-2022/agenda*).

la condivisione dei dati e la retorica della loro protezione secondo il GDPR (al cui rispetto sono già vincolati), con particolare riferimento ai limiti di utilizzo degli stessi. Peculiare, allora, potrebbe essere anche il profilo di responsabilità da inadempimento degli AISP nel caso di sottrazione fraudolenta di dati e codici di accesso per predisposizione di mezzi inadatti a garantire gli standard di sicurezza. In questa ipotesi, essendo il suddetto rischio intrinseco all'attività svolta dall'operatore, potrebbe non risultare peregrina la possibilità di far rispondere direttamente ed immediatamente quest'ultimo del danno causato all'utente secondo il ben noto principio del "rischio di impresa"[56].

56 Teoria avanzata già da Messore, A.: "La nuova disciplina dei servizi di pagamento", cit. pp. 549 s.

BIBLIOGRAFIA

Antonucci, A.: "I contratti bancari on line", in *Contratti bancari* (a cura di E. Capobianco), Wolters Kluwer, Milano, 2021, pp. 585 ss.

Beck, U.: "Vivere nella società del rischio globale", *Ars Interpretandi*, 2007, num. 12°, pp. 123 ss.

Berti De Marinis, G.M.: "La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD2", *Dir. banc. merc. fin.*, num. 4°, 2018, pp. 627 ss.

Borgogno, O. e Colangelo, G.: "Data Sharing and Interoperability Trough APIs: Insights from European Regulatory Strategy", *European Union Law Working Paper*, Stanford-Vienna Transatlantic Technology Law Forum, 2018.

Burchi, A., Mezzacapo, S., Musile Tanzi, P., Troiano, V.: "Financial Data Aggregation e Account Information Services. Questioni regolamentari e profili di business", in *CONSOB, Quaderni Fintech*, num. 4°, marzo 2019.

Caggiano, A.: "Pagamenti non autorizzati tra responsabilità e restituzioni. una rilettura del d. legisl. 11/2010 e lo scenario delle nuove tecnologie", *Riv. dir. civ.*, num. 2°, 2016, pp. 10459 ss.

Capuano, S. e Sala, T.: "La PSD2 sotto la lente di ingrandimento del Comitato europeo per la protezione dei dati: le Linee Guida 06/2020", in *Privacy &*, num. 1°, 2021, pp. 25 ss.

Catenacci, M. e Fornasaro, C.: "PSD2: i prestatori di servizi d'informazione sui conti (AISP)", *Diritto bancario*, 2018, pp. 1 ss.

Cian, M. e Sandei, C.: "Diritto del Fintech", Cedam-Wolters Kluwer, Padova, 2020.

De Stasio, V.: "Ordine di pagamento non autorizzato e restituzione della moneta", Giuffrè, Milano, 2016.

Dolmetta, A.A. e Malvagna, U.: "Vicinanza della prova e prodotti d'impresa del comparto finanziario", *Banca borsa tit. cred.*, fasc. 6°, 2014, pp. 659 ss.

Donnelly, M.: "Payments in the digital market: Evaluating the contribution of Payment Services Directive II", *Computer law & security review*, 2016, pp. 826 ss.

Falcone, G.: "Contratti bancari e fintech", in *Contratti bancari* (a cura di E. Capobianco), Wolters Kluwer, Milano, 2021, pp. 613 ss.

Frau, R.: "Home banking, phishing e responsabilità civile della banca", *Resp. civ. prev.*, num. 2°, 2019, pp. 622 ss.

Gammaldi, D. e Iacomini, C.: "Mutamenti nel mercato dopo la PSD2", in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale* (a cura di F. Maimeri e M. Mancini), in *Quaderni di ricerca Giuridica della Consulenza Legale della Banca d'Italia*, num. 87°, 2019, pp. 123 ss.

Geva, B.: "Payment Transactions under the E.U. Second Payment Services Directive - An Outsider's View", *54 Texas International Law Journal*, 2019, pp. 211 ss.

La Sala, G.P.: "Intermediazione, disintermediazione, nuova intermediazione: i problemi regolatori", in *Diritto del Fintech* (a cura di M. Cian e C. Sandei), Cedam, Padova, 2020, pp. 3 ss.

Maffeis, D.: "Ordini di pagamento e di investimento on line nella giurisprudenza di merito e nella fonte persuasiva dinamica dell'ABF", *Riv. dir. civ.*, num. 5°, 2013, pp. 1273 ss.

Marasa', F.: "Servizi di pagamento e responsabilità degli intermediari", Giuffrè, Milano, 2020.

Marseglia, C.: "Responsabilità civile - «Furto della tessera di bancomat e concorso di colpa tra l'utilizzatore e l'intermediario», *Nuova giur. civ. comm.*, num. 3°, 2020, pp. 561 ss.

Meli, V.: "Opportunità e sfide per la concorrenza nella disciplina dei servizi di pagamento", in *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella* PSD2 (a cura di M.C. Paglietti e M.I. Vangelisti), Romatre-Press, Roma, 2020, pp. 170 ss.

Messore, A.: "La nuova disciplina dei servizi di pagamento digitali prestati dai *Third Party Providers*", *Nuove leggi civ. comm.*, num. 2°, 2020, pp. 511 ss.

Mezzacapo, S.: "L'inquadramento normativo della PSD2, tra 'dark side' del nuovo framework regolamentare UE dei servizi di pagamento e 'singolarità' dei pagamenti delle Pubbliche Amministrazioni", in *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2* (a cura di M.C. Paglietti e M.I. Vangelisti), Romatre-Press, Roma, 2020, pp. 105 ss.

Minto, A.: "Art. 114-*novies*", in *Commentario al Testo unico delle leggi in materia bancaria e creditizia* (diretto da F. Capriglione), Padova, 2018, pp. 1789 ss.

Paracampo, M. (a cura di): "Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari", ed. 2°, Giappichelli, Torino, 2017.

Porta, F.: "Obiettivi e strumenti della PSD2", in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale* (a cura di F. Maimeri e M. Mancini), in *Quaderni di Ricerca Giuridica della Consulenza Legale della Banca di Italia*, num. 87°, settembre 2019, pp. 21 ss.

Profeta, V.: "I Third Party Provider: profili soggettivi e oggettivi", in *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale* (a cura di F. Maimeri e M. Mancini), in *Quaderni di Ricerca Giuridica della Consulenza Legale della Banca di Italia*, num. 87°, 2019, pp. 47 ss.

Rispoli Farina, M.: "La *Strong Customer Authentication* e la responsabilità dei prestatori dei servizi di pagamento", *I-Lex*, num. 12°, 2019, pp. 105 ss.

Santoro, V.: "Servizi di pagamento", in *Contratti bancari* (a cura di E. Capobianco), Wolters Kluwer, Milano, 2021, pp. 2131 ss.

Sciarrone Alibrandi, A.: "Impostazione sistematica della Direttiva PSD2", in *Innovazione e regole nei pagamenti digitali il bilanciamento degli interessi nella PSD2* (a cura di M.C. Paglietti e M.I. Vangelisti), RomaTre-Press, Roma, 2020, pp. 13 ss.

Sciarrone Alibrandi, A., Borello, G., Ferretti, R., Lenoci, F., Macchiavello, E., Mattassoglio, F. e Panisi, F.: "Marketplace lending Verso nuove forme di intermediazione finanziaria?", in *CONSOB*, *Quaderni Fintech*, 5 luglio 2019.

Sica, S. e Sabatino, M.B.: "Disintermediazione finanziaria e tutela del cliente e dell'utilizzatore", *Dir. inf.*, num. 1°, pp. 1 ss.

Troiano, O.: "Contratti di pagamento e disciplina privatistica comunitaria (proposte ricostruttive con particolare riferimento al linguaggio ed alle generalizzazioni legislative)", *Banca borsa tit. cred.*, num. 5°, 2009, pp. 520 ss.

Vanini, S.: "L'attuazione in Italia della seconda direttiva sui servizi di pagamento nel mercato interno: le innovazioni introdotte dal d.lgs. 15 dicembre 2017, n. 218", *Nuove leggi civ. comm.*, num. 4°, 2018, pp. 839 ss.

Zammitti, M.V.: "Appunti per una ricerca sui servizi di disposizione di ordini di pagamento", *Banca borsa tit. cred.*, num. 3°, 2021, pp. 399 ss.