

RIVISTA  
TRIMESTRALE  
DI DIRITTO  
DELL'ECONOMIA

RASSEGNA  
DI  
DOTTRINA  
E  
GIURISPRUDENZA

DIREZIONE SCIENTIFICA

G. ALPA - M. ANDENAS - A. ANTONUCCI  
F. CAPRIGLIONE - R. MASERA - R. Mc CORMICK  
F. MERUSI - G. MONTEDORO - C. PAULUS

3 / 2023

ISSN: 2036 - 4873

# RIVISTA TRIMESTRALE DI DIRITTO DELL'ECONOMIA

---

[WWW.RTDE.LUISS.IT](http://WWW.RTDE.LUISS.IT)

La sede della Rivista è presso  
la Fondazione G. Capriglione Onlus,  
Università Luiss G. Carli,  
Viale Romania 32, 00197 Roma.

## *Direzione Scientifica*

G. Alpa - M. Andenas - A. Antonucci - F. Capriglione - R. Masera  
F. Merusi - R. McCormick - G. Montedoro - C. Paulus

## *Direttore Responsabile*

F. Capriglione

## *Comitato Editoriale*

V. Lemma - E. Venturi - D. Rossano - N. Casalino - A. Troisi

I contributi pubblicati in questa Rivista potranno essere  
riprodotti dalla Fondazione G. Capriglione Onlus su altre  
proprie pubblicazioni, in qualunque forma.

*Autorizzazione n. 136/2009, rilasciata dal Tribunale di Roma in data 10 aprile 2009.*

## COMITATO SCIENTIFICO PER LA VALUTAZIONE

L. Ammannati, E. Bani, P. Benigno, R. Bifulco, A. Blandini, C. Brescia Morra, M. Brogi, R. Calderazzi, E. Cardi, A. Cilento, M. Clarich, A. Clarizia, R. Cocozza, G. Colavitti, F. Colombini, G. Conte, P. E. Corrias, C. G. Corvese, L. De Angelis, M. De Benedetto, P. De Carli, C. De Caro, P. de Gioia Carabellese, M. De Poli, G. Desiderio, L. Di Brina, L. Di Donna, G. Di Gaspare, F. Gaspari, F. Guarracino, F. Di Porto, G. Di Taranto, V. Donativi, M. V. Ferroni, L. Foffani, C. Fresa, P. Gaggero, I. Ingravallo, C. Irti, R. Lener, M. Libertini, P. Lucantoni, L. Ludovici, N. Lupo, M. B. Magro, F. Maimeri, A. Mangione, E. Maria Lombardi, G. Martina, S. Martuccelli, M. Maugeri, P. Messina, R. Miccù, F. Moliterni, S. Monticelli, G. Napolitano, G. Niccolini, A. Niutta, M. Passalacqua, M. Pellegrini, M. Proto, M. Rabitti, N. Rangone, P. Reichlin, R. Restuccia, A. Romano, A. Romolini, C. Rossano, G. Ruotolo, C. Russo, A. Sacco Ginevri, I. Sabbatelli, F. Sartori, A. Sciarrone, M. Sepe, G. Sicchiero, D. Siclari, G. Terranova, G. Tinelli, V. Troiano, A. Urbani, P. Valensise, A. Zimatore

## REGOLE DI AUTODISCIPLINA PER LA VALUTAZIONE DEI CONTRIBUTI

I contributi inviati alla Rivista Trimestrale di Diritto dell'Economia sono oggetto di esame da parte del «Comitato scientifico per la valutazione» secondo le presenti regole.

1. Prima della pubblicazione, tutti gli articoli, le varietà, le note e le osservazioni a sentenza inviati alla *Rivista* sono portati all'attenzione di due membri del *Comitato*, scelti in ragione delle loro specifiche competenze ed in relazione all'area tematica affrontata nel singolo contributo.
2. Il contributo è trasmesso dalla *Redazione* in forma anonima, unitamente ad una scheda di valutazione, ai membri del *Comitato*, perché i medesimi – entro un congruo termine – formulino il proprio giudizio.
3. In ciascun fascicolo della *Rivista* sarà indicato, in ordine alfabetico, l'elenco dei membri del *Comitato* che hanno effettuato la valutazione dei contributi pubblicati.
4. In presenza di pareri dissenzienti, la *Direzione* si assume la responsabilità scientifica di procedere alla pubblicazione, previa indicazione del parere contrario dei membri del *Comitato*.
5. Ove dalle valutazioni emerga un giudizio positivo condizionato (a revisione, integrazione o modifica), la *Direzione* promuove la pubblicazione solo a seguito dell'adeguamento del contributo alle indicazioni dei membri del *Comitato*, assumendosi la responsabilità della verifica.

## I CONTRIBUTI DEL PRESENTE FASCICOLO SONO STATI VALUTATI DA:

A. Blandini, L. Di Brina, L. Di Donna, P. Gaggero, M. Guarini, G. Luchena  
R. Motroni, F. Moliterni, M. Romano, I. Sabbatelli, A. Sacco Ginevri, M. Sepe

## **PARTE PRIMA**

### **ARTICOLI**

FRANCESCO CAPRIGLIONE – *Concorrenza e stabilità nel paradigma digitale* (Competition and Stability in the Digital Paradigm) .....281

CLAUDIO COLOMBO – *I servizi di pagamento on line: questioni in tema di identificativo unico e di autenticazione forte* (Online payment services: issues concerning unique identifier (IBAN) and strong customer authentication).....313

MARCO BODELLINI – *Tra principi generali e standards internazionali di soft law: la disciplina europea sulla finanza sostenibile e l’inizio di una nuova stagione per il ‘Brussels effect’?* (Between general principles and international soft law standards: the European legal framework on sustainable finance and the beginning of a new era for the ‘Brussels effect’).....338

MATTEO ARRIGONI – *La disciplina degli incentivi nella prestazione dei servizi di investimento all’interno della strategia per gli investimenti al dettaglio promossa dalla Commissione europea* (The European Commission’s Retail Investment Strategy and the inducements regime in the provision of investment services)..... 369

CARMINE RUGGIERO – *Gli aiuti di Stato in materia tributaria e le emergenze economiche* (State aid in tax matters and economic emergencies).....387

## **PARTE SECONDA**

### **NOTE ED OSSERVAZIONI A SENTENZA**

VALERIO LEMMA – *Amministratori di banca tra rischio d’impresa e responsabilità individuali* (The Bank Directors between Risk Management and Personal Liability), nota ad

ordinanza della Corte di Cassazione del 20 settembre 2023, n. 26867.....61

FRANCESCO AFFINITO – *L’estinzione anticipata dei contratti di credito con i consumatori*  
(Early repayment of financing contracts with consumers), nota ad ordinanza della Corte di  
Cassazione del 6 settembre 2023, n. 25977.....78

## I SERVIZI DI PAGAMENTO *ON LINE*: QUESTIONI IN TEMA DI IDENTIFICATIVO UNICO E DI AUTENTICAZIONE FORTE\*

*(Online payment services: issues concerning unique identifier (IBAN) and strong customer authentication)*

**ABSTRACT:** *The essay analyzes some issues that give rise to many controversies in the application of the regulations regarding online payment services. Having introduced some brief observations regarding the evolution of the concept of payment, as well as regarding the general regulations referred to in the European directives on payment services (the so-called PSD 1 and PSD 2), the essay focuses in particular on the issues of unique identifier (IBAN) and strong customer authentication (SCA), also analyzing the main guidelines of jurisprudence and of the Financial Banking Arbitrator (ABF). Finally, a brief overview of the remedies guaranteed by the law to customers who are victims of scams when using online payment services is provided.*

**SOMMARIO:** 1. Alcune premesse di ordine generale. - 2. Regolazione e applicazione. - 3. Linee generali (per quanto qui interessa) del sistema introdotto con le PSD e con la disciplina interna di recepimento. - 4. Le operazioni dispositive on line. Qualche dato numerico. - 5. Questioni in tema di identificativo unico (IBAN). - 6. La disciplina della S.C.A. - 7. Le frodi.

1. L'evoluzione che ha contraddistinto nel corso del tempo, fino ad arrivare ai giorni nostri, i concetti di moneta<sup>1</sup> e di obbligazione pecuniaria<sup>2</sup> non ha potuto che

---

\* Contributo approvato dai revisori.

L'articolo è tratto dalla relazione svolta nel Convegno "Moneta e pagamento pecuniario nella prospettiva del nascente mercato digitale", tenutosi a Palermo il 16 dicembre 2022, nell'ambito degli incontri dedicati al progetto "Vent'anni di euro: bilanci e prospettive delle politiche monetarie e creditizie in Italia e in Europa", i cui Atti sono in corso di pubblicazione per i tipi di Giappichelli. L'Autore è componente effettivo del Collegio di Milano dell'Arbitro Bancario Finanziario - A.B.F.; le opinioni espresse nel lavoro hanno carattere strettamente personale e non sono in alcun modo riferibili a tale Istituzione.

<sup>1</sup> Su cui vedi, nella prospettiva giuridica, beninteso senza alcuna pretesa di completezza, anzitutto T. ASCARELLI, *La moneta. Considerazioni di diritto privato*, Padova, 1928. Più recentemente, B.

riguardare anche l'atto di pagamento<sup>3</sup>, che nella codificazione del 1942 era sostanzialmente assimilato alle altre ipotesi di adempimento, e cioè alle ipotesi relative alle obbligazioni aventi contenuto diverso da quello pecuniario<sup>4</sup>.

Si può dire che in un contesto nel quale il pagamento consisteva, per ovvie ragioni, per lo più in una *datio* di banconote o di pezzi monetari, lo stesso finiva inevitabilmente per venire attratto alla dimensione di mero atto materiale (appunto, la *datio*, o la *traditio* del contante). Gli stessi strumenti di pagamento alternativi già all'epoca conosciuti (essenzialmente, gli assegni), come noto venivano riguardati dalla scienza giuridica più nella loro dimensione di titoli di credito, piuttosto che in quella, appunto, di strumenti di pagamento alternativi al denaro contante. Prova ne è anche la ritrosia, con la quale il formante giurisprudenziale ha progressivamente accolto l'idea che certi strumenti di pagamento dovessero essere considerati in tutto e per tutto equipollenti al contante, per l'affidabilità propria dei soggetti emittenti, e che dunque la loro accettazione fosse doverosa per il creditore

---

INZITARI, *Moneta*, in *Digesto disc. priv.*, sez. civ., XI, Torino, 1994, p. 395 ss.; F. CAPRIGLIONE, *Moneta*, in *Enc. dir.*, agg. III, Milano, 1999, p. 747 ss.; G. OLIVIERI, *Compensazione e circolazione della moneta nei sistemi di pagamento*, Milano, 2002; M. SEMERARO, *Pagamento e forme di circolazione della moneta*, Napoli, 2008; E. BARCELLONA, *Ius monetarium. Diritto e moneta alle origini della modernità*, Bologna 2012; G. BOSI, *Considerazioni giuridiche sulla natura della moneta*, in *Giur. comm.*, 2019, I, p. 1061 ss.; V. SANTORO, *Considerazioni sulla moneta*, in *Dir. banc. merc. fin.*, 2022, I, p. 185 ss.

<sup>2</sup> Anche qui, senza pretesa di completezza, cfr. T. ASCARELLI, *Delle obbligazioni pecuniarie*, in *Comm. Scialoja - Branca*, Bologna - Roma, 1959; E. QUADRI, *Le obbligazioni pecuniarie*, in *Tratt. dir. priv.* diretto da P. RESCIGNO, vol. 9, Torino, 1984; A. DI MAJO, *Le obbligazioni pecuniarie*, Torino, 1996; B. INZITARI, *Delle obbligazioni pecuniarie*, in *Comm. Scialoja - Branca*, Bologna - Roma, 2011; T. DALLA MASSARA, *Obbligazioni pecuniarie. Struttura e disciplina dei debiti di valuta*, Padova, 2011; E. CATERINI, *Le obbligazioni pecuniarie nell'ordinamento italo-europeo*, Napoli, 2022.

<sup>3</sup> In tema, pare sufficiente qui rinviare alle voci enciclopediche di R. NICOLO', *Adempimento (diritto civile)*, in *Enc. dir.*, I, Milano, 1958, p. 554 ss.; di M. GIORGIANNI, *Pagamento (diritto civile)*, in *Noviss. Dig. It.*, XII, Torino, 1976, p. 321 ss.; di A. DI MAJO, *Pagamento (dir. priv.)*, in *Enc. dir.*, XXXI, Milano, 1981, p. 548 ss.; e di G. CIAN, *Pagamento*, in *Digesto disc. priv.*, sez. civ., XIII, Torino, 1995, p. 234 ss.

<sup>4</sup> Si veda, a riguardo, anche l'utilizzazione complessivamente fungibile dei due termini (adempimento e pagamento), nell'ambito del Capo II del Libro Quarto del c.c. (*Dell'adempimento delle obbligazioni*), ove ricorre la parola *adempimento* (o suoi derivati) nel testo, o nella rubrica, degli artt. 1176, 1180, 1181, 1182, 1183, 1184, 1187, 1197, 1198, 1208; ricorre, invece, la parola *pagamento* (o suoi derivati), nel testo, o nella rubrica, degli artt. 1185, 1188, 1189, 1190, 1191, 1192, 1193, 1194, 1195, 1196, 1199, 1200, 1201, 1202, 1203, 1205; esiste, poi, anche un caso in cui i termini ricorrono contemporaneamente nell'ambito del medesimo articolo (art. 1206).

pecuniario<sup>5</sup>.

Oggi sappiamo tutti che il contesto, a livello globale, è sostanzialmente rovesciato. Per moltissime ragioni sulle quali non è possibile qui soffermarci approfonditamente<sup>6</sup>, il contante è ormai divenuto l'eccezione (o, quanto meno, sembra decisamente prossimo a diventare tale) e dunque quelli che si sono prima definiti strumenti alternativi<sup>7</sup>, ormai da tempo alternativi non sono più, e questo al di là di recenti provvedimenti normativi in materia di innalzamento del c.d. tetto del contante<sup>8</sup>, che sono destinati ad avere scarso, se non nullo, rilievo, in relazione al discorso che qui stiamo affrontando<sup>9</sup>.

---

<sup>5</sup> Con riferimento al pagamento mediante assegni circolari, è infatti solo nel 2007 che le Sezioni Unite della S.C. ne hanno stabilito l'equipollenza a quello in contanti, peraltro con la limitazione della possibilità di rifiuto, in presenza di un giustificato motivo (da intendersi oggettivamente, alla stregua del canone di buona fede), addotto dal creditore: Cass. SS. UU. 18 dicembre 2007, n. 26617, tra l'altro in *Banca, borsa, tit. credito*, 2008, II, p. 553 ss., con nota di G. LEMME, *La rivoluzione copernicana della cassazione: la moneta legale, dunque, non coincide con la moneta fisica*; in *Corr. giur.*, 2008, p. 500 ss., con nota di A. DI MAJO, *I pagamenti senza denaro nella cashless society*; in *Vita not.*, 2008, p. 727 ss., con nota di C. CARBONE, *Assegni, antiriciclaggio e datio in solutum. L'ultima parola?*

<sup>6</sup> Ragioni riconducibili alla prevenzione dei fenomeni del riciclaggio di danaro di provenienza criminosa, del finanziamento del terrorismo e, indirettamente, dell'evasione fiscale.

<sup>7</sup> Sono ormai acquisiti, a riguardo, i concetti in qualche modo fungibili tra loro, di *moneta scritturale* (cfr. già G.F. CAMPOBASSO, *Bancogiro e moneta scritturale*, Bari, 1979; più di recente, G. LEMME, *Moneta scritturale e moneta elettronica*, Torino, 2003; B. INZITARI, *L'adempimento dell'obbligazione pecuniaria nella società contemporanea: tramonto della carta moneta e attribuzione pecuniaria per trasferimento della moneta scritturale*, in *Banca, borsa, tit. credito*, 2007, I, p. 133 ss.) e di *moneta bancaria* (cfr., per tutti, L. FARENGA, *La moneta bancaria*, Torino, 1997), così come ormai da tempo si discute di *moneta elettronica* (v. già V. SANTORO, *Appunti sulla moneta elettronica*, in *Riv. not.*, 1986, p. 879 ss.), di *pagamento virtuale* (cfr. S. MARTUCCELLI, *Obbligazioni pecuniarie e pagamento virtuale*, Milano, 1998) e, più recentemente, di *pagamenti digitali* (v. G. MARINO, *Dalla traditio pecuniae ai pagamenti digitali*, Torino, 2018) e di *pagamenti elettronici* [cfr. L. MIOTTO – M. SPERANZIN, *I pagamenti elettronici*, in M. CIAN – C. SANDEI (a cura di), *Diritto del Fintech*, Milano – Padova, 2020, p. 163 ss.].

<sup>8</sup> L'art. 49 del d. lgs. 21 novembre 2007, n. 231 (che contiene l'attuale disciplina relativa all'antiriciclaggio, originariamente introdotta con la l. 5 luglio 1991, n. 197) – rubricato “*limitazioni all'uso del contante e dei titoli al portatore*” – dal momento della sua entrata in vigore ha subito numerose modifiche, in aumento o in diminuzione, in poco più di quindici anni, da ultimo ad opera dell'art. 1, comma 384, della l. 29 dicembre 2022, n. 197, e ciò essenzialmente a seconda della composizione della compagine governativa *pro tempore*.

<sup>9</sup> Sintomatico del nuovo assetto è anche il fatto che il Giudice dell'U.E. si è dovuto recentemente pronunciare a proposito della legittimità di provvedimenti normativi che, in una prospettiva diametralmente opposta a quella tradizionale, impongono il divieto di effettuare pagamenti in contanti, in favore delle P.A., anche a prescindere dal relativo importo: cfr. Corte di Giustizia U.E. 26 gennaio 2021, in cause C-422/19 e C-423/19, in *Giur. comm.*, 2022, II, p. 50 ss., con nota di G.L.

Sotto il profilo dell'inquadramento giuridico, la transizione dal denaro contante verso le moderne forme di pagamento ha finito per implicare lo spostamento della questione del pagamento dalla dimensione squisitamente "materiale", o "reale"<sup>10</sup> ad una dimensione che tocca ormai chiaramente i profili dell'autonomia privata (dunque, di indole negoziale), anche nella prospettiva dell'operazione economica<sup>11</sup>, o – se vogliamo – in quella dello stesso collegamento negoziale<sup>12</sup>.

Il pagamento oggi è infatti per lo più la risultante di un reticolo di rapporti, aventi origine in altrettanti contratti, che intercorrono tra diversi soggetti. Pensiamo, ad esempio, ad una semplice operazione di pagamento effettuata con una carta di credito, che coinvolge quattro soggetti diversi (il pagatore / titolare della carta; l'emittente della carta; il creditore / fornitore del bene o del servizio; l'intermediario con il quale il creditore è necessariamente convenzionato per poter accettare pagamenti tramite carte).

Ecco, uno degli ultimi termini che ho utilizzato – intermediario – è forse quello che più di ogni altro è idoneo a mettere in luce la caratteristica della complessità, che connota la contemporaneità, anche nel diritto. L'agire economico, ma anche giuridico, è sempre più "intermediato" e lo stesso lessico, anche a livello normativo, fa un uso sempre più frequente del concetto di intermediazione.

Dunque – e tornando al nostro argomento – anche il pagamento è oggi una

---

GRECO – V. SANTORO, *Limiti all'uso del contante e regime giuridico del corso legale delle banconote in euro*.

<sup>10</sup> Sul superamento della concezione reale (o materiale) del pagamento, cfr. anche S. MARTUCCELLI, *op. cit.*, p. 38 ss.; T. DALLA MASSARA, *op. cit.*, p. 113 ss.; G. MARINO, *op. cit.*, p. 9 ss.; più recentemente, R. MOTRONI, *I pagamenti non monetari nella finanza digitale europea*, Bari, 2023, p. 17 ss.

<sup>11</sup> Del resto, lo stesso legislatore europeo, allorché è intervenuto nella materia dei pagamenti, con le note Direttive PSD 1 (n. 2007/64/CE) e PSD 2 (n. 2015/2366/UE), ha affrontato la questione nella prospettiva non già del *pagamento* in senso stretto, ma in quella del *servizio* reso dai diversi soggetti (*in primis*, le banche) che lo offrono in favore della propria clientela: sul punto, v. tra gli altri G. MARINO, *op. cit.*, p. 57.

<sup>12</sup> Cfr., esemplificativamente, l'analisi condotta da F. BARTOLINI, *Strutture contrattuali complesse. Problemi della trilateralità nei contratti di finanziamento*, Napoli, 2019, p. 138 ss. e p. 203 ss.

questione nella quale l'intermediazione ha assunto, anche in virtù di provvedimenti normativi cogenti (si pensi alle modalità di pagamento delle imposte, oltre che ai già riferiti limiti all'uso del contante), un ruolo assolutamente preponderante<sup>13</sup>.

Si può dire dunque che la questione del pagamento abbia subito un po' la stessa evoluzione economica e giuridica di quella del finanziamento, dove si è transitati da un modello spesso non intermediato, nel quale era il fornitore del bene a finanziare direttamente l'acquirente, secondo il modello della vendita a rate con riserva di proprietà, ad un modello dove praticamente tutto, o quasi, è caratterizzato dalla presenza degli intermediari<sup>14</sup>.

E siccome intermediazione significa – come ho detto prima – anche complessità (attenzione: complessità che, però, sul piano pratico si traduce in semplificazione; si pensi alla facilità con la quale viene oggi ad esempio effettuato un pagamento *contactless*), l'ordinamento non poteva non occuparsi del tema, al fine ovviamente di tutelare le diverse posizioni coinvolte: anzitutto quelle degli utilizzatori dei servizi di pagamento, ma anche quelle dei prestatori dei servizi di

---

<sup>13</sup> Vedi, a riguardo, G. MARINO, *op. cit.*, p. 53 ss., ove l'illustrazione del paradigma dell'*adempimento necessariamente intermediato*.

<sup>14</sup> È bene peraltro avvertire che – nel vorticoso avvicinarsi di fenomeni antitetici tra loro, anche nel breve volgere di pochi anni – già si profila, proprio nel settore fatto oggetto dell'analisi contenuta in queste brevi riflessioni, un possibile ritorno alla *disintermediazione* (o, quanto meno, ad una forma di intermediazione diversa da quella alla quale siamo abituati), resa possibile soprattutto dall'utilizzo delle tecnologie *blockchain*, da cui originano tra l'altro le c.d. criptovalute: cfr., a riguardo, M. GIULIANO, *L'adempimento delle obbligazioni pecuniarie nell'era digitale. Dalla moneta legale alla moneta scritturale e digitale "legalmente imposta"*, Torino, 2018, p. 151 ss. Sul tema delle criptovalute, anche qui senza pretesa alcuna di completezza, vedi M. CIAN, *La criptovaluta. Alle radici dell'idea giuridica di denaro attraverso la tecnologia*, in *Banca, borsa, tit. credito*, 2019, I, p. 315 ss.; G. RINALDI, *Criptovalute e blockchain*, in *Vita not.*, 2019, p. 453 ss.; F. MAIMERI – M. MANCINI (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, cripto valute e rivoluzione digitale*, in BANCA D'ITALIA, *Quaderni di Ricerca Giuridica della Consulenza Legale*, n. 87, 2019; V. ORSINI, *Della natura giuridica delle criptovalute*, in *Dir. merc. ass. fin.*, 2021, p. 15 ss.; L. PIOVANO, *Criptovalute e NFT. Introduzione*, in *Dir. ec. impr.*, 2022, p. 595 ss.; M. IRRERA – M.S. CATALANO, *Criptovalute e NFT: il quadro normativo di riferimento*, *ivi*, p. 614 ss.

In ordine a queste nuove frontiere, relativamente alle quali ovviamente nella presente sede si può soltanto fare un accenno, si rinvia anche a R. MOTRONI, *op. cit.*, p. 83 ss. (per le questioni relative al c.d. euro digitale, su cui cfr. anche G. MARINO, *Verso l'euro digitale: la moneta legale nell'epoca della digitalizzazione*, in *Jus civile*, 2022, p. 917 ss.), e p. 149 ss. (a proposito del c.d. Regolamento UE n. 1114/23, pubblicato in G.U. dell'Unione Europea del 9 giugno 2023, c.d. Regolamento MiCA, *Markets in Crypto-assets Regulation*).

pagamento, il tutto nella prospettiva della tutela del mercato, intesa ormai come formula per certi versi sovrapponibile a quella un tempo più consueta di interesse generale.

2. Sotto il profilo della produzione e dell'applicazione delle regole, la materia dei servizi di pagamento è caratterizzata, come sempre più sovente accade, dalla partecipazione di una pluralità di attori.

La disciplina interna è, come noto, quella di derivazione eurounitaria, emanata in sede di recepimento delle direttive c.d. PSD 1 e PSD 2 (n. 64/2007 e n. 2366/15), ed è costituita essenzialmente dal d. lgs. 27 gennaio 2010, n. 11, che è stato novellato in modo significativo ad opera del d. lgs 15 dicembre 2017, n. 218 (che ha rappresentato il veicolo per il recepimento della PSD 2), come poi integrato dal d. lgs. 8 aprile 2020, n. 36<sup>15</sup>.

Come si avrà modo di meglio specificare, nella materia che qui stiamo analizzando giocano un ruolo assolutamente non secondario alcune istituzioni che non si collocano in maniera squisitamente formale all'interno del sistema delle fonti,

---

<sup>15</sup> Le Direttive in questione sono state emanate nell'ambito del più ampio progetto «SEPA» (*Single Euro Payments Area*), su cui cfr. per tutti, da ultimo, R. MOTRONI, *op. cit.*, p. 59 ss.

Per quanto concerne i profili generali della PSD 1, cfr. M. RISPOLI FARINA - V. SANTORO - A. SCIARRONE ALIBRANDI - O. TROIANO (a cura di), *Armonizzazione europea dei servizi di pagamento e attuazione della dir. 2007/64/Ce*, Milano, 2009; quanto, invece, alla relativa disciplina di recepimento, vedi M. MANCINI - M. RISPOLI FARINA - V. SANTORO - A. SCIARRONE ALIBRANDI - O. TROIANO (a cura di), *La nuova disciplina dei servizi di pagamento*, Torino, 2011.

Sulla PSD 2 e sulla relativa attuazione, cfr. E. BANI - V. DE STASIO - A. SCIARRONE ALIBRANDI (a cura di), *L'attuazione della seconda direttiva sui servizi di pagamento e "open banking"*, Bergamo, 2021; M.C. PAGLIETTI - M.I. VANGELISTI (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD 2*, Roma, 2020.

In relazione alla specifica materia dei pagamenti con carte, si rinvia anche a (C. COLOMBO) - L. PAOLUCCI, *Bancomat, carte di debito e carte di credito*, in G. CONTE, *Arbitro Bancario e Finanziario* (a cura di L. BALESTRA - R. DI RAIMO - D. MAFFEIS - M. MAGGIOLO - M. MARINARO - R. NATOLI - S. PAGLIANTINI - G. RECINTO), Milano, 2021, p. 603 ss.

la più rilevante delle quali è certamente l'E.B.A. (Autorità Bancaria Europea), costituita nel 2011 quale Agenzia della U.E., avente il compito di creare un sistema bancario e di mercato unico, efficiente, trasparente e stabile per tutti gli Stati membri.

Tra gli strumenti a disposizione dell'E.B.A., si segnala qui quello delle c.d. *Questions and Answers* (Q&As): si tratta di un meccanismo, in virtù del quale gli operatori di mercato presentano domande circa i profili applicativi e/o interpretativi del diritto eurounitario nei settori rientranti nel perimetro di competenza dell'E.B.A., domande che dunque poi danno origine a risposte, il cui contenuto finisce per assurgere ad una sorta di para-fonte normativa (più che di vera e propria *soft law*, si può forse qui parlare di *crypto hard law*), nel senso che le autorità che poi devono applicare le norme – in questo caso, in materia di servizi di pagamento – ai fini della risoluzione delle controversie, tengono conto delle risposte dell'E.B.A., e sostanzialmente conformano (anche) ad esse le proprie decisioni.

Quest'ultima osservazione consente, poi, di estendere la riflessione, appunto, al tema della risoluzione delle controversie. L'esperienza italiana ha visto negli ultimi anni (di fatto coincidenti con l'entrata in vigore del d. lgs. n. 11/2010) l'affermazione di un modello di *A.D.R.*<sup>16</sup>, rappresentato dall'Arbitro Bancario Finanziario (A.B.F.), al quale sono affidate moltissime controversie, quale alternativa più veloce al ricorso alla giurisdizione ordinaria<sup>17</sup>.

In realtà, nel settore che qui stiamo analizzando, le pronunce dell'A.B.F. sono indiscutibilmente in netta preponderanza, rispetto a quelle dei giudici ordinari, e questo non solo per la minore onerosità del procedimento, ma anche per almeno un altro paio di ragioni:

(i) la prima credo che possa essere individuata nel fatto che nel settore dei

---

<sup>16</sup> Acronimo di *Alternative Dispute Resolution*, risoluzione alternativa delle controversie.

<sup>17</sup> Relativamente all'A.B.F., sia con riferimento ai profili di struttura e funzionamento, sia con riferimento ai suoi orientamenti interpretativi, può rinviarsi a G. CONTE, *Arbitro Bancario e Finanziario* (a cura di L. BALESTRA – R. DI RAIMO – D. MAFFEIS – M. MAGGIOLO – M. MARINARO – R. NATOLI – S. PAGLIANTINI – G. RECINTO), cit.

servizi di pagamento le controversie seguono pressoché sempre il paradigma *cliente vs. intermediario*, nel senso cioè che originano da pretese che il cliente avanza nei confronti dell'intermediario, e non viceversa (come accade, invece, in altri settori: si pensi, esemplificativamente, a quello dell'applicazione degli interessi e delle commissioni bancarie, le cui questioni sovente emergono in contenziosi dove è l'intermediario a formulare pretese verso il cliente, e nei quali dunque – in virtù del fatto che l'intermediario è legittimato a rivestire solo la posizione di convenuto, dinanzi all'A.B.F. – la decisione non può che spettare all'A.G.O.);

(ii) la seconda ragione può essere individuata nel fatto che gli intermediari che operano nel settore dei servizi di pagamento sono per lo più soggetti di grandi dimensioni (banche, società emittenti carte di pagamento), le quali – se soccombenti dinanzi all'A.B.F. – tendenzialmente adempiono, come risulta dai relativi rapporti annuali.

A conferma di quanto sopra, si può riportare il dato, per cui nel secondo trimestre del 2022 il 24% dei ricorsi pervenuti all'A.B.F. ha riguardato le carte di pagamento, che come materia è dunque seconda solo a quella dei finanziamenti contro cessione del quinto dello stipendio o della pensione<sup>18</sup>.

3. Ovviamente le direttive eurounitarie e la disciplina interna di recepimento regolano, in maniera tendenzialmente completa, tutta la materia dei pagamenti "intermediati", non solo di quelli *on line*.

Non può essere dunque questa la sede per condurre un'analisi completa del sistema, ma è sufficiente individuare alcuni profili, utili a meglio comprendere le linee di fondo del tema oggetto di queste riflessioni.

I cardini su cui è imperniato il sistema possono a mio avviso essere efficacemente descritti attraverso alcune parole chiave.

---

<sup>18</sup> I rapporti annuali relativi all'attività dell'Arbitro Bancario Finanziario sono consultabili sul sito [www.arbitrobancariofinanziario.it](http://www.arbitrobancariofinanziario.it). Si segnala che il dato ha subito un ulteriore incremento nel primo trimestre del 2023, passando al 28% del totale.

La prima parola chiave è “autenticazione” (art. 10, d. lgs. n. 11/2010), che è la procedura che consente al prestatore di servizi di pagamento di verificare l’identità di un utente di servizi di pagamento o la validità dell’uso di uno specifico strumento di pagamento, incluse le relative credenziali di sicurezza personalizzate fornite dal prestatore. Con la PSD 2, e la relativa disciplina di recepimento (art. 10 *bis*, d. lgs. n. 11/2010), è stata introdotta la necessità di autenticazione c.d. forte (in inglese, *Strong Customer Authentication*, in acronimo S.C.A.) del cliente nei casi di pagamento con accesso dal conto *on line*, di effettuazione di un pagamento elettronico, nonché di effettuazione di qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti, o altri abusi<sup>19</sup>. Su questi aspetti mi soffermerò più diffusamente nel prosieguo<sup>20</sup>.

La seconda parola è “responsabilità” (artt. 7 e 8, d. lgs. n. 11/2010)<sup>21</sup>. Il sistema si basa su di una ripartizione piuttosto precisa delle responsabilità che incombono, rispettivamente, sugli utilizzatori dei servizi di pagamento (USP) e sui prestatori dei servizi di pagamento (PSP), che rilevano soprattutto, anche se non solo, quando – in presenza di un’operazione che l’USP dichiara di non avere autorizzato (e cioè la disconosce) – si tratta di stabilire a carico di chi debba rimanere la perdita derivante dal fatto che è stata effettuata una disposizione non voluta dall’USP.

Qui la legge prevede un regime di sostanziale *favor* a beneficio del cliente, in quanto – in estrema sintesi – fa gravare sul PSP un duplice onere probatorio. Anzitutto, quello di fornire la dimostrazione che l’operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata, e che non ha subito le

---

<sup>19</sup> In tema di autenticazione forte, cfr. da ultimo M.V. ZAMMITTI, *Operazioni di pagamento tramite «wallet» e responsabilità da omessa applicazione della «Strong Customer Authentication» (S.C.A.)*, nota a A.B.F., Coll. Coordinamento, 11 ottobre 2021, n. 21285, in *Banca, borsa, tit. credito*, 2022, II, p. 875 ss.; vedi anche M.C. PAGLIETTI, *Questioni in materia di prova nei casi di pagamenti non autorizzati*, in M.C. PAGLIETTI – M.I. VANGELISTI (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD 2*, cit., p. 43 ss.

<sup>20</sup> Cfr. *infra*, § 6.

<sup>21</sup> Al tema della responsabilità è dedicata la monografia di F. MARASÀ, *Servizi di pagamento e responsabilità degli intermediari*, Milano, 2020.

conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti: se tale prova non viene fornita, secondo il costante orientamento dei Collegi A.B.F., conformemente d'altra parte al testo normativo, non vi è necessità di andare oltre nell'indagine, e la controversia va senz'altro risolta a favore dell'USP<sup>22</sup>.

Sotto questo profilo è bene precisare che la prova in questione è affidata ad un'analisi di tipo informatico, che sconta i limiti probatori che caratterizzano il procedimento dinanzi all'A.B.F. (nel quale, ad esempio, non è possibile disporre la CTU). I Collegi A.B.F., tuttavia, opportunamente hanno introdotto delle semplificazioni probatorie, consentendo agli intermediari di depositare una documentazione equipollente delle tracciate informatiche (in genere, dei fogli *excel*, corredati di una legenda esplicativa)<sup>23</sup>; senza tale semplificazione – che in qualche modo si basa sulla fiducia che quanto gli intermediari attestano nella traduzione “documentale” delle tracciate informatiche non sia falso – il contenzioso in materia di servizi di pagamento sarebbe invero impossibile da delibare, dinanzi all'A.B.F., cosa che invece non si verifica quando il contenzioso viene portato dinanzi all'A.G.O., perché quest'ultima dispone ovviamente di strumenti istruttori per un accertamento più preciso.

Tornando agli oneri probatori gravanti sul PSP, solo una volta assolto a questo primo onere – e cioè quello di dimostrare l'avvenuta corretta autenticazione – scatta il secondo onere, che è quello di dimostrare la frode, il dolo o la colpa grave dell'USP. Va da sé che le ipotesi della frode e del dolo sono complessivamente

---

<sup>22</sup> Le decisioni dell'A.B.F., sul punto, sono numerosissime. A mero titolo esemplificativo, può citarsi anzitutto A.B.F., Coll. Coordinamento, 10 ottobre 2019, n. 22745, nonché – tra le più recenti – A.B.F., Coll. Palermo, 28 aprile 2023, n. 4121; A.B.F., Coll. Milano, 28 aprile 2023, n. 4111; A.B.F., Coll. Napoli, 28 aprile 2023, n. 4028; A.B.F., Coll. Bologna, 17 aprile 2023, n. 3659, tutte consultabili sul sito [www.arbitrobancariofinanziario.it](http://www.arbitrobancariofinanziario.it). Per un recente precedente di merito, cfr. Trib. Verona, 10 gennaio 2022, in *Dir. Internet*, 2022, p. 575 ss., con nota di M. FERRARI, *La responsabilità del gestore di servizi di pagamento elettronici alla luce della graduazione bifasica dell'onere probatorio*.

<sup>23</sup> Anche in ordine a tale profilo, le decisioni dell'A.B.F. sono tantissime. Sempre a mero titolo esemplificativo, cfr. già A.B.F., Coll. Bologna, 19 novembre 2019, n. 25095, in [www.arbitrobancariofinanziario.it](http://www.arbitrobancariofinanziario.it).

residuali e che il contenzioso, a questo punto, finisce per ruotare intorno alla colpa grave del cliente, restando indimostrata la quale, la responsabilità (*rectius*: il peso economico della perdita) rimane a carico del PSP, salva la possibilità da parte di quest'ultimo di invocare, ricorrendone i presupposti<sup>24</sup>, l'applicazione di una piccola franchigia, che è stata ridotta ad un importo poco più che simbolico (50 euro).

La terza ed ultima parola chiave, che peraltro non rileva in tutti i casi di pagamento disciplinati dalla normativa qui in esame, ma essenzialmente nei pagamenti effettuati tramite bonifico, è "identificativo unico" (o IBAN, acronimo di *International Bank Account Number*). Qui – come avremo modo di vedere<sup>25</sup> – per come la disciplina normativa è stata interpretata, ormai anche a livello di Corte di Giustizia U.E., si determina invece un regime di *favor* a beneficio degli intermediari, i quali – ma lo si dirà meglio in seguito – sono esonerati da ogni responsabilità quando danno esecuzione alla disposizione conformemente all'IBAN (del beneficiario) comunicato (dal pagatore), anche se nella specie vi siano alcune evidenze idonee a comprovare la non corrispondenza tra IBAN e soggetto effettivamente beneficiario della disposizione.

La combinazione di questi due diversi regimi – l'uno orientato a favore del cliente, l'altro orientato a favore dell'intermediario – converge nel senso di tentare di istituire un sistema efficiente e rapido (in quanto sostanzialmente sottratto al fattore umano, dal lato dei PSP: di entrambi i PSP), dove al regime di responsabilità aggravata del PSP nei casi di utilizzi fraudolenti (regime che si giustifica anche in un'ottica, che nel lessico dell'analisi economica del diritto è traducibile nella formula del *superior risk bearer*, il quale peraltro può stipulare idonee coperture assicurative del rischio in questione), si giustappone, a mo' di contraltare, un regime che autoresponsabilizza fortemente il cliente, durante la fase del conferimento

---

<sup>24</sup> L'applicazione della franchigia è infatti limitata alle sole ipotesi di smarrimento, furto o sottrazione dello strumento di pagamento, e non anche a quelle riconducibili alle diverse ipotesi di *phishing* (su cui, cfr. quanto si dirà *infra*, § 7).

<sup>25</sup> *Infra*, § 5.

dell'ordine di pagamento<sup>26</sup>.

4. Prima di entrare nello specifico degli argomenti oggetto di queste brevi riflessioni, ritengo opportuno fornire qualche dato numerico, tratto da alcuni studi di istituzioni pubbliche e private, per avere maggiore contezza delle dimensioni del fenomeno.

In Italia si stima che, anche ma non solo a causa della pandemia, tra il 2020 e il 2025 vi sarà un incremento delle transazioni *on line* pari al 76%, transazioni che nel 2025 dovrebbero “cubare” grosso modo 63 miliardi di dollari, per circa 40 milioni di utenti - acquirenti *on line*<sup>27</sup>.

Un altro dato che merita di essere evidenziato è quello relativo alla ripartizione, tra i vari strumenti di pagamento, delle transazioni *on line*.

Lo strumento maggiormente utilizzato in Italia è rappresentato dalle carte di pagamento, che, stando ad uno studio della B.C.E. pubblicato a dicembre 2020<sup>28</sup>, assorbiva circa il 54% del totale.

Una notevole quota, pari al 28%, era poi rappresentata dai c.d. *e-payments*, tra cui si segnalano in particolare i *digital wallets* (di attori globali, come *Apple Pay*, *Amazon Pay*, *Google Pay*, o anche *Satispay*, per restare alla dimensione interna), ma in realtà questo è un dato forse già vecchio, perché alcuni studi più recenti hanno già constatato un forte aumento dell'uso di questi strumenti.

I bonifici *on line*, dunque, sia quelli disposti direttamente attraverso i canali degli intermediari bancari tradizionali, sia quelli di alcune piattaforme operative anche in Italia (*Mybank*, ad esempio), costituiscono una parte complessivamente minoritaria, anche se non marginale, del fenomeno complessivo, stimandosene l'entità nel 9% del totale. Va da sé, però, che – visti i limiti di utilizzo delle carte di pagamento – questa percentuale è certamente maggiore, se il dato da prendere in

---

<sup>26</sup> In generale, sulla tematica degli ordini di pagamento non autorizzati, vedi V. DE STASIO, *Ordine di pagamento non autorizzato e restituzione della moneta*, Milano, 2016.

<sup>27</sup> *Statista.com, Digital Market Outlook*, 2021.

<sup>28</sup> B.C.E., *Study on the Payment Attitudes of Consumers in the Euro Area (SPACE)*.

considerazione non è il numero complessivo delle operazioni, ma quello relativo al valore economico delle stesse.

5. Come si è già avuto occasione di accennare, nel settore delle disposizioni effettuate tramite bonifico la scelta del legislatore è stata quella di responsabilizzare gli utenti, con conseguente allentamento dei doveri di diligenza dei PSP.

L'art. 24 del d. lgs. 11/2010 ha infatti cura di stabilire, a più riprese, che l'unico elemento che rileva è l'IBAN, anche quando – la precisazione è contenuta nell'ultimo comma – l'USP fornisce ulteriori elementi, idonei ad individuare il beneficiario (per lo più, nome e cognome, o ragione sociale).

Per la verità non erano mancate, nell'ambito delle prime applicazioni della norma, alcune tesi inclini a ritenere applicabili i principi di cui all'art. 24 al solo PSP del pagatore<sup>29</sup>, il quale ovviamente non può effettuare alcuna operazione di confronto tra IBAN e nominativo del beneficiario (a meno che non sia nel contempo, come può accadere, PSP di entrambi), cosa che invece potrebbe fare il PSP del beneficiario.

Il contrasto tra i Collegi territoriali (in particolare tra quello di Milano, che è sempre stato fermo nel ritenere applicabile la norma anche al PSP del beneficiario<sup>30</sup>, e – come detto – quello di Roma) sarebbe stato risolto dal Collegio di

---

<sup>29</sup> Cfr. A.B.F., Coll. Roma, 3 luglio 2014, n. 4172, in *Riv. dir. merc. fin.*, 2016, p. 199 ss., con nota di G.B. BARILLÀ, *Responsabilità della banca del beneficiario per errata esecuzione di ordine di bonifico impartito tramite home banking: configurazione di un obbligo di protezione in favore di terzo?*; nello stesso senso, A.B.F., Coll. Roma, 25 marzo 2016, n. 2841, nonché A.B.F., Coll. Roma, 8 aprile 2016, n. 3278, entrambe in *Nuova giur. civ. comm.*, 2016, p. 1261 ss., con nota di G. MARINO, *Iban «sbagliato» e responsabilità delle banche nell'esecuzione dell'operazione di bonifico*.

Per un precedente in termini analoghi della giurisprudenza ordinaria (ma riferibile ad una fattispecie anteriore all'entrata in vigore della disciplina di recepimento della PSD 1), vedi Trib. Como, 7 agosto 2013, con nota di E. DEPETRIS, *La responsabilità della banca per pagamento illegittimo di bonifico bancario*, in *Banca, borsa, tit. credito*, 2015, II, p. 192 ss.

<sup>30</sup> Si veda, per la decisione più risalente in ordine temporale, A.B.F., Coll. Milano, 5 luglio 2016, n. 6149, in [www.arbitrobancariofinanziario.it](http://www.arbitrobancariofinanziario.it). Per un precedente dell'A.G.O. in tal senso, cfr. Trib. Firenze 9 luglio 2015, in *Riv. dir. merc. fin.*, 2016, p. 199 ss., con nota di G.B. BARILLÀ, cit.

Coordinamento, nel senso dell'applicabilità della disciplina ad entrambi i PSP<sup>31</sup>.

Le argomentazioni del Collegio di Coordinamento si fondano sulle già rilevate esigenze di sottrarre al fattore umano le operazioni di pagamento in questione (così di fatto agevolando, sotto l'aspetto organizzativo, i PSP, ed in particolare quello del beneficiario), oltre che sulle discipline di recepimento dei principali Stati membri, su alcuni profili desumibili dalla stessa PSD 2 (ci si riferisce, in particolare, al considerando n. 88), nonché infine sulle stesse indicazioni operative fornite dalla Banca d'Italia.

In ultimo, e a definitiva conferma del fatto che questa debba essere ineludibilmente la corretta interpretazione della norma (alla luce di quanto dispone l'art. 267 T.F.U.E.), si segnala che è intervenuta anche la Corte di Giustizia dell'U.E., la quale con la sentenza 21 marzo 2019, in causa C-245/18 (cui ha dato origine un'ordinanza di rinvio pregiudiziale di una Corte italiana, il Tribunale di Udine), ha stabilito espressamente che il c.d. *safe harbour*, costituito dall'IBAN, quale unico ed esclusivo elemento al quale fare riferimento nell'esecuzione dell'operazione, si applica ad entrambi i PSP<sup>32</sup>.

Il consolidamento dell'indirizzo giurisprudenziale sul punto implica dunque la necessità – e questo è un aspetto che in concreto si determina proprio nel caso dei bonifici *on line*, che il pagatore dispone in via autonoma – che chi inserisce nel sistema la disposizione faccia molta attenzione alla compilazione del campo relativo all'IBAN: ogni errore, infatti, è destinato a rimanere a suo carico, salvo quanto si dirà tra breve a proposito degli obblighi di *recall* dei PSP.

In siffatto contesto, però, c'è da porsi una domanda, correlata alle prassi dei sistemi informatici di *home banking* degli intermediari. Normalmente, quando si

---

<sup>31</sup> A.B.F., Coll. Coordinamento, 12 gennaio 2017, n. 162, in [www.arbitrobancariofinanziario.it](http://www.arbitrobancariofinanziario.it).

<sup>32</sup> Vedila in *Banca, borsa, tit. credito*, 2019, II, p. 653 ss., con nota di F. MARASÀ, *Riflessioni su Iban errato e responsabilità degli intermediari*. Va da sé che, a seguito della pronuncia della Corte di Giustizia, la giurisprudenza ordinaria si sarebbe poi ad essa totalmente uniformata: cfr., ad esempio, App. Milano, 16 luglio 2020, in *Giur. comm.*, 2021, II, p. 1107 ss., con nota di F. MARASÀ, *Sulla distribuzione del rischio di errore nell'individuazione del beneficiario del pagamento per Iban inesatto*.

inserisce una disposizione di bonifico *on line*, i portali dei diversi PSP richiedono, obbligatoriamente, l'indicazione del nominativo, o della ragione sociale, del beneficiario. L'ipotesi, dunque, delle "informazioni ulteriori rispetto all'identificativo unico", menzionate nel terzo comma dell'art. 24, non è mai, o quasi mai, il frutto di un'iniziativa dell'utente, ma la conseguenza delle modalità di funzionamento del sistema informatico del suo PSP.

Ebbene, a nostro avviso non è da escludere che la pretesa di indicazione del nominativo del beneficiario, in aggiunta all'IBAN, potrebbe – specie negli utenti meno avveduti – ingenerare il convincimento che l'eventuale discrasia tra IBAN e nominativo avrebbe come conseguenza il non perfezionamento dell'operazione di pagamento, e invece si è visto che così non è. E allora, una soluzione in chiave di disciplina di trasparenza potrebbe essere quella di obbligare i PSP ad evidenziare in maniera quanto più chiara possibile, prima che l'utente finalizzi l'operazione, che l'eventuale discrasia tra IBAN e nominativo, o ragione sociale, non impedisce il perfezionamento dell'operazione; oppure si potrebbe prevedere la mera facoltatività dell'indicazione del nome del beneficiario, perché in tal modo l'utente, del tutto verosimilmente, finirebbe per prestare più attenzione nella digitazione dei caratteri alfanumerici che compongono l'IBAN.

Ciò premesso – e come già si è anticipato – il possibile rimedio all'errore dell'utente è affidato alle procedure di richiamo (o *recall*), rispetto alle quali la legge pone uno specifico obbligo a carico dei PSP.

Quanto al PSP del pagatore, l'obbligo è generalmente ritenuto assolto quando questi, una volta ricevuta la denuncia dell'errore da parte dell'utente, invia la richiesta di storno al PSP del beneficiario, e dunque qui si tratta essenzialmente di valutarne la condotta sotto il profilo della tempestività con cui esso si attiva.

Più articolati sono, invece, gli obblighi a carico del PSP del beneficiario, il quale – ove il conto su cui è erroneamente affluito il bonifico fosse ancora capiente – dovrà assumere iniziative più consistenti (come l'apposizione, ad esempio, di un

blocco cautelativo temporaneo sul conto di destinazione del bonifico), fermo restando però che, per ottenere la restituzione delle somme, sarà sempre necessario il consenso del beneficiario, ovvero un provvedimento dell'A.G.O.<sup>33</sup>.

In ogni caso, il PSP in questione è tenuto a fornire ogni informazione utile ad individuare il soggetto beneficiario, onde agevolare il recupero dell'indebitato per le vie ordinarie nei confronti del titolare del conto di accredito del bonifico, senza poter frapporre eccezioni legate alla tutela della *privacy*, come invece alcuni intermediari hanno sovente fatto; ma, sul punto, occorre dire che l'indirizzo dell'A.B.F., dopo alcune incertezze, si è consolidato nel senso qui sostenuto<sup>34</sup>.

6. La necessità della c.d. autenticazione forte, per le operazioni più a rischio, rappresenta una delle maggiori novità tra quelle introdotte dalla PSD 2 (sul punto integrata, per le specifiche di natura tecnica, dal Regolamento delegato U.E. n. 2018/389), con decorrenza dal 14 settembre 2019 (termine poi prorogato dall'E.B.A., per i pagamenti *on line* effettuati tramite carte, al 31 dicembre 2020).

La norma di riferimento, nell'ambito della disciplina interna, è l'art. 10 *bis*, d. lgs. 11/2010, la quale, come si è già accennato in precedenza, prevede che la S.C.A. debba essere richiesta in caso di accesso al conto di pagamento *on line* (*login*), in caso di effettuazione di disposizioni di pagamento elettronico ed in caso di effettuazione di qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi (ad esempio, l'abbinamento di una nuova utenza telefonica per l'operatività *on line*, l'*enrollment* di un'*App* su un dispositivo, la digitalizzazione di carte su *wallet*). La norma poi, precisa la necessità che l'autenticazione forte includa elementi che colleghino in maniera dinamica l'operazione a uno specifico importo e a un beneficiario specifico: a riguardo, sono ormai entrati anche nell'uso comune acronimi come OTP, *One time password*, OTS,

---

<sup>33</sup> Sul punto, vedi A.B.F., Coll. Milano, 29 dicembre 2022, n. 16506, in [www.arbitrobancariofinanziario.it](http://www.arbitrobancariofinanziario.it).

<sup>34</sup> Cfr. A.B.F., Coll. Coordinamento, 3 maggio 2022, n. 6886, in [www.arbitrobancariofinanziario.it](http://www.arbitrobancariofinanziario.it).

*One time SMS, OTC, One time QR Code*, che configurano altrettante ipotesi di elementi dinamici, a differenza ad esempio delle vecchie *password* statiche.

La legge fornisce la definizione di autenticazione forte (art. 1, lett. *q-bis*, del d. lgs. 11/2010). Si tratta di un'autenticazione:

(i) basata sull'uso di almeno due elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce, come una *password*, o un PIN), del possesso (qualcosa che solo l'utente possiede, come una chiavetta, o *token*, o più frequentemente oggi uno *smartphone*) e dell'inerenza (qualcosa che caratterizza l'utente, come l'impronta digitale o il riconoscimento facciale), i quali devono essere indipendenti tra loro, in quanto la violazione di uno non compromette l'affidabilità degli altri;

(ii) concepita in modo tale da tutelare la riservatezza dei dati di autenticazione.

Come anticipato, nella materia che qui interessa giocano senz'altro un ruolo molto importante le c.d. *Q&As* dell'E.B.A.: sul relativo sito si contano, in tema, oltre 130 risposte fornite dall'Autorità ai quesiti che le vengono sottoposti dai vari soggetti abilitati a formularli.

Per avere un'idea dell'importanza delle *Q&As* dell'E.B.A., basti leggere l'ultima decisione del Collegio di Coordinamento dell'A.B.F. in tema<sup>35</sup>. Il caso riguardava una truffa particolarmente articolata, nella quale con un'unica OTP inviata tramite SMS ad un soggetto che, in proprio e quale legale rappresentante di tre società aveva a disposizione quattro carte di credito, era stato effettuato l'abbinamento di tutte e quattro le carte ad una nuova utenza telefonica in uso ai frodatori, tramite la quale poi sarebbero state effettuate le successive operazioni dispositive. Il Collegio di Milano aveva dubitato che tale meccanismo fosse *compliant* con la disciplina in materia di autenticazione forte e, vista la questione di particolare importanza, aveva rimesso la stessa al Collegio di Coordinamento.

---

<sup>35</sup> A.B.F., Collegio Coordinamento, 18 ottobre 2022, n. 13398, in [www.arbitrobancariofinanziario.it](http://www.arbitrobancariofinanziario.it).

Ebbene, al di là della soluzione fornita dal Collegio di Coordinamento – che è stata nel senso della natura *compliant* della procedura nella specie seguita dall'intermediario – è interessante osservare come la decisione si basi, e citi a supporto della propria motivazione, ben tre *Answers* dell'E.B.A.:

- la n. 4141 del 2018, in cui si afferma che il primo dei fattori della S.C.A. (ad esempio, quello usato per il *login*) può essere riutilizzato per le operazioni dispositive (purché ovviamente a queste sia abbinato un ulteriore fattore, che deve essere unico per ogni singola disposizione);

- la n. 4039 del 2018, dove si legge che l'OTP inviato via SMS è un fattore di possesso, nella misura in cui viene ricevuto su un dispositivo che il titolare della carta detiene e che risulta essere stato in precedenza associato in modo sicuro alla carta;

- la n. 4560 del 2019, in cui sostanzialmente si dice l'abbinamento va riferito all'USP, e non alle carte.

Le medesime osservazioni possono formularsi relativamente ad un'altra decisione del Collegio di Coordinamento dell'A.B.F., nella quale si citano sempre alcune *Answers* dell'E.B.A., a supporto del principio di diritto affermato, secondo cui, in caso di pagamenti effettuati con carta tramite *wallet*, non basta l'autenticazione forte in fase di *tokenizzazione*, ma la stessa va effettuata anche relativamente alle singole disposizioni<sup>36</sup>.

Nel caso specifico, peraltro, si trattava di operazioni effettuate in modalità *contactless*, la quale rappresenta una delle ipotesi in cui è possibile derogare rispetto alla disciplina cogente della S.C.A., relativamente ad alcune operazioni, tra cui quelle di piccolo ammontare (individuato, nell'ambito del Regolamento delegato U.E. n. 2018/389, nell'importo di € 50,00)<sup>37</sup>. È bene tuttavia segnalare che l'utilizzo

---

<sup>36</sup> A.B.F., Collegio Coordinamento, 11 ottobre 2021, n. 21285, in *Banca, borsa, tit. credito*, 2022, II, p. 861 ss., con nota di M.V. ZAMMITTI, cit.

<sup>37</sup> Sui pagamenti *contactless*, cfr. G. MARINO, *Carte di pagamento con funzione contactless, uso non autorizzato e responsabilità dei prestatori di servizi di pagamento*, in *Oss. dir. civ. comm.*, 2021, p. 137 ss.; R. GRISAFI, *L'autonomia negoziale alla prova dei nuovi sistemi di pagamento*

della deroga prevista dalla disciplina eurounitaria rappresenta una scelta del PSP, e dunque non esonera quest'ultimo dal rischio (d'impresa) riconducibile ad eventuali utilizzi fraudolenti<sup>38</sup>.

7. Il requisito dell'autenticazione forte si ricollega essenzialmente al fatto che le operazioni *on line* sono senz'altro tra quelle caratterizzate dai maggiori rischi di frode.

La totale dematerializzazione, che caratterizza i pagamenti effettuati *on line*, consente infatti la commissione di truffe di tipo informatico, slegate dunque da ogni forma di sottrazione del supporto fisico, e dunque da un'attività che va ad attingere – come dire? – in senso materiale il titolare dello strumento di pagamento.

Le truffe informatiche hanno ovviamente un grado di sofisticazione più o meno elevato: già la decisione del Collegio di Coordinamento A.B.F. 26 ottobre 2012, n. 3498<sup>39</sup> aveva evidenziato la maggiore insidiosità, ad esempio, della truffa del c.d. *man in the middle*, specificamente nella variante del c.d. *man in the browser*<sup>40</sup>, rispetto ai classici casi di *phishing* commessi tramite *email*<sup>41</sup>.

---

- *Le c.d. «carte contactless»*, in *Vita not.*, 2021, p. 493 ss.; F. MARASÀ, *I pagamenti contactless nel sistema della PSD2*, nota a Corte di Giustizia U.E. 11 novembre 2020, in causa C-287/19, in *Banca, borsa, tit. credito*, 2022, II, p. 149 ss.

<sup>38</sup> A.B.F., Coll. Roma, 8 gennaio 2021, n. 431; A.B.F., Coll. Bologna, 23 settembre 2021, n. 20392; A.B.F., Coll. Milano, 26 aprile 2023, n. 3921, tutte consultabili in [www.arbitrobancariofinanziario.it](http://www.arbitrobancariofinanziario.it).

<sup>39</sup> Consultabile in [www.arbitrobancariofinanziario.it](http://www.arbitrobancariofinanziario.it).

<sup>40</sup> Tale tecnica consiste nella dolosa installazione di un *malware* nel *computer* dell'inconsapevole utente, «che una volta annidatosi in un certo numero di *computer*, genera quella che in gergo suole definirsi una *botnet*, ossia per l'appunto una rete di macchine egualmente infettate dallo stesso *virus*. Il *malware* – riconducibile alla più ampia categoria dei cc.dd. *trojan* (“cavalli di Troia”) e dotato di sofisticate capacità di elusione dei migliori *antivirus* – si annida in modo silenzioso nel *computer* della vittima senza creare alcun malfunzionamento o alterazione del sistema tali da attrarre l'attenzione dell'utente. Il *malware* resta completamente “in sonno”, attivandosi solo nel momento in cui l'utente si colleghi ad un sito finanziario compreso fra quelli che il programma abbia posto nel mirino (*targeted banks*). In quel preciso istante il *malware* “si risveglia” ed entra in azione captando il collegamento dell'utente e propinandogli una pagina-video esattamente identica a quella che l'utente è abituato a riconoscere in sede di accesso regolare al sito del proprio intermediario»: così è descritta la truffa in questione nella menzionata decisione A.B.F., Coll. Coordinamento, 26 ottobre 2012, n. 3498.

Sulla fattispecie del *man in the browser*, tuttavia, vedi la recente Trib. Roma, 9 aprile 2023, in *Dir. risp.*, [www.dirittodelrisparmio.it](http://www.dirittodelrisparmio.it), 2023, con nota di S. RESCIGNO, *La colpa grave del cliente in*

Il punto attiene qui alla valutazione della condotta dell'utente, nel senso che, tanto più è insidioso il mezzo, tanto meno sono le probabilità che venga ritenuta la sussistenza della colpa grave in capo all'USP, anche in presenza di ammissioni – da parte di costui – in ordine ad esempio alla dichiarata comunicazione delle credenziali a soggetti poi rilevatosi truffatori, o all'inserimento delle stesse in *internet*.

A riguardo occorre infatti puntualizzare una cosa: il meccanismo di ripartizione dell'onere della prova – che, come abbiamo visto, onera l'intermediario di dimostrare la colpa grave dell'utente – finisce quasi sempre, nell'esperienza concreta, per far sì che la prova possa essere acquisita o a seguito di dichiarazioni confessorie dell'USP, o come conseguenza di un ragionamento di tipo presuntivo (e questo peraltro non concerne solo gli utilizzi fraudolenti commessi a mezzo di truffe informatiche, ma anche quelli di tipo tradizionale, che si ricollegano alla sottrazione materiale dello strumento di pagamento).

Diverso è, rispetto a quello della ripartizione dell'onere della prova sulla colpa, il tema della ripartizione degli oneri di allegazione e prova sui fatti: l'utente, infatti, è pur sempre gravato dell'onere di allegare (e conseguentemente di provare) i fatti che, a suo giudizio, hanno consentito la commissione della truffa ai suoi danni. Solo una volta acquisita l'allegazione e la prova di detti fatti, invero, è possibile affrontare il diverso e conseguente problema della prova della colpa grave, l'onere

---

*ordine alle operazioni fraudolente di phishing*, nella quale è stata riconosciuta la sussistenza di colpa grave a carico del cliente, con conseguente rigetto della domanda restitutoria.

<sup>41</sup> Per alcune prime analisi sulle diverse forme di *phishing*, cfr. A.G. IMBESI, *Phishing and pharming on the net*, in *Nuovo dir.*, 2006, p. 797 ss.; M. EROLI, *Carte di pagamento tipo "bancomat" e servizi bancari on line: la responsabilità per le operazioni contestate*, in *www.diritto.it*, 2010; R. FRAU, *Home Banking, bonifici non autorizzati e responsabilità della banca*, in *Resp. civ. e prev.*, 2013, 1284 ss., ID., *Home Banking, sottrazione di credenziali informatiche, bonifici non autorizzati e responsabilità civile della banca da trattamento di dati personali*, *ivi*, 2013, 1830 ss.; ID., *Responsabilità civile della banca per operazioni di home banking disconosciute dal cliente*, nota a Cass. 23 maggio 2016, n. 10638, *ivi*, 2017, p. 853 ss.; ID., *Home banking, phishing e responsabilità civile della banca*, nota a Cass. 12 aprile 2018, n. 9158, *ivi*, 2019, p. 622 ss.; F. CALISAI, *Il Phishing: profili civilistici ed evoluzione delle forme di tutela alla luce delle decisioni dell'Arbitro Bancario Finanziario*, in *Dir. merc. e tecnologia*, 7 luglio 2015, consultabile sul sito *www.dimt.it*.

della cui dimostrazione grava, come detto, sul PSP.

Tornando alle varie ipotesi di frodi, al *phishing* classico (il cui veicolo è una *email*), si affiancano lo *smishing* (il cui veicolo è un SMS) ed il *vishing* (il cui veicolo è una telefonata, e dunque una voce umana interattiva). C'è poi il *pharming*, che consiste nel camuffamento di un sito *web*, che replica quello di un intermediario, sicché l'utente crede di interfacciarsi con il proprio intermediario, ed invece interfaccia con dei truffatori, ai quali dunque inconsapevolmente comunica le proprie credenziali.

Va detto che l'autenticazione forte ha ridotto di molto l'incidenza delle truffe di tipo classico, ma – come sempre – i frodatori sono molto rapidi nell'inventarsi nuovi strumenti.

Il tipo di frode che maggiormente oggi interessa l'attività dell'A.B.F. è lo *spoofing* (che spesso si presenta in forma mista a *vishing*, nel qual caso si parla anche di *ID caller spoofing*).

Il termine deriva da un neologismo inglese risalente a circa un secolo fa (*spoof*, imbroglio, ma anche beffa), ed è ciò che fa un *cybercriminale* quando finge di essere una fonte affidabile (si camuffa, potrebbe dirsi) per ottenere accesso a informazioni importanti.

In concreto, i truffatori riescono – ad esempio – ad inserirsi nel *thread* o nella *chat* dei messaggi SMS tra il PSP e l'USP, in modo da determinare nell'utente il convincimento che un dato messaggio sia genuino e proveniente appunto dal proprio PSP. A volte poi, come detto, la dinamica della frode si articola anche con una fase di *vishing*, nella quale il truffatore riesce a far apparire una telefonata come intercorsa con un soggetto riferibile al PSP.

L'orientamento dei Collegi A.B.F. è nel senso di considerare tendenzialmente lo *spoofing* un sistema particolarmente insidioso, la cui utilizzazione da parte dei truffatori dovrebbe escludere in linea di principio la colpa grave dell'utente, con conseguente addossamento del peso economico della frode a carico

dell'intermediario<sup>42</sup>.

Tuttavia va precisato, e qui mi ricollego a quanto detto in precedenza circa il riparto degli oneri di allegazione e prova, che l'utente il quale assuma di essere stato vittima di *spoofing*, e il quale dunque, ad esempio, abbia ammesso di aver comunicato le proprie credenziali ad un interlocutore, ma nel convincimento che lo stesso fosse un operatore del proprio PSP, è gravato dell'onere di provare il proprio assunto, producendo documentazione idonea a dimostrarlo (ad esempio, il c.d. messaggio civetta, e cioè l'SMS fraudolento, oppure lo *screenshot* della rubrica delle telefonate ricevute sul proprio cellulare)<sup>43</sup>.

Tornando al tema della colpa, va rilevato che l'adozione da parte dei PSP di strumenti informativi particolarmente efficaci (mi riferisco qui, ad esempio, ai c.d. SMS parlanti, che sono dei messaggi che contengono delle indicazioni particolarmente specifiche relativamente all'operazione, dispositiva o anche non dispositiva, che si sta autorizzando), ove vi sia certezza che questi siano stati ricevuti dall'USP (e non dai truffatori), potrebbero invece condurre all'accertamento della colpa grave<sup>44</sup>, e dunque al rigetto della domanda, o al limite alla declaratoria di un concorso di responsabilità<sup>45</sup>. Va infatti sottolineato che la disciplina speciale non contiene alcun riferimento al concorso di responsabilità, ma nella giurisprudenza dell'A.B.F. (e sul punto non sembra che vi siano smentite da parte della

---

<sup>42</sup> Vedi, ad esempio, A.B.F., Coll. Roma, 1° settembre 2022, n. 12005; A.B.F., Coll. Milano, 27 ottobre 2021, n. 22277; A.B.F., Coll. Bari, 19 ottobre 2021, n. 21791, tutte consultabili in [www.arbitrobancariofinanziario.it](http://www.arbitrobancariofinanziario.it).

<sup>43</sup> I c.d. disconoscimenti non circostanziati, infatti, finiscono per determinare il rigetto della pretesa restitutoria del cliente, in applicazione del principio per cui in tali casi viene ad esserne presunta la colpa grave: per un'applicazione recente di questo principio da parte della giurisprudenza ordinaria, cfr. Trib. Ancona, 23 maggio 2023, in *Dir. risp.*, [www.dirittodelrisparmio.it](http://www.dirittodelrisparmio.it), 2023, con nota di V. TROIANELLI, *Esclusione della responsabilità della banca per pagamento disconosciuto dal cliente*.

<sup>44</sup> Per un'affermazione della sussistenza della colpa grave del cliente, sia pure con riferimento ad una fattispecie non ricadente sotto la disciplina delle PSD, cfr. Cass. 13 marzo 2023, n. 7214, in [www.smartlex24.ilsole24ore.com](http://www.smartlex24.ilsole24ore.com). Vedi anche, sempre recentemente, Trib. Genova, 20 aprile 2023, in *Dir. risp.*, [www.dirittodelrisparmio.it](http://www.dirittodelrisparmio.it), 2023, con nota di V. TROIANELLI, *Truffa telematica e mancato risarcimento danni (ex art. 1227, comma 2, c.c.)*, in relazione ad una ipotesi di *smishing*.

<sup>45</sup> Vedi, sul punto, esemplificativamente, A.B.F., Coll. Milano, 15 novembre 2021, n. 23385, in [www.arbitrobancariofinanziario.it](http://www.arbitrobancariofinanziario.it).

giurisprudenza ordinaria) viene spesso fatto uso del concetto di concorso.

L'accertamento in capo all'USP della colpa grave, infatti, non si traduce sempre e comunque nel rigetto integrale della domanda, ma – in presenza ad esempio della prova, comunque acquisita, di un malfunzionamento dei presidi di sicurezza del PSP – può esservi un accoglimento della domanda solo parziale, dovendosi a quel punto poi effettuare una gradazione delle colpe, ai sensi dell'art. 1227 c.c. Questo principio vale sia quando la frode abbia riguardato una singola operazione, sia – e forse con maggiore frequenza – quando la stessa abbia riguardato una pluralità di operazioni.

In quest'ultima ipotesi, ad esempio, si valorizza spesso il mancato invio del c.d. SMS *alert*, il cui ricevimento avrebbe consentito all'utente di bloccare lo strumento di pagamento, anteriormente alle disposizioni truffaldine successive alla prima (o alle prime, se queste si sono svolte in un arco temporale molto ristretto); oppure il fatto che il PSP non abbia tenuto conto degli indici di frode, desumibili dall'art. 8 del d.m. n. 112/2007, che sono:

- sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento;
- tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita;
- due o più richieste di autorizzazione provenienti da Stati diversi, effettuate, con la stessa carta, nell'arco di sessanta minuti<sup>46</sup>.

Oltre alle frodi genericamente inquadrabili nelle forme più o meno sofisticate di *phishing*, la casistica annovera altre fattispecie, rispetto alle quali gli orientamenti dell'A.B.F. sono costanti, rispettivamente, nel senso del rigetto e nel senso dell'accoglimento delle richieste di rimborso proposte dagli USP.

---

<sup>46</sup> Cfr., su questi profili, A.B.F., Coll. Coordinamento, 6 novembre 2019, n. 24366, in [www.arbitrobancariofinanziario.it](http://www.arbitrobancariofinanziario.it). Va tuttavia segnalato che, secondo Trib. Milano, 28 febbraio 2023, in *Dir. risp.*, [www.dirittodelrisparmio.it](http://www.dirittodelrisparmio.it), 2023, con nota di V. TROIANELLI, *Servizi di pagamento: bilanciamento di responsabilità tra PSP e utenti*, i menzionati indici di frode, desumibili dal d.m. n. 112/2007, non potrebbero assumere alcun rilievo nella ripartizione della responsabilità tra cliente ed intermediario.

La prima frode prende il nome di *business email compromise*, o *invoice fraud*, e si realizza allorché i truffatori riescono ad alterare, entrando abusivamente nella posta elettronica dell'utente, i dati relativi all'IBAN indicato per il pagamento di una fattura commerciale, con conseguente accredito della somma su un conto diverso da quello genuinamente segnalato dal fornitore/creditore: in questo caso l'orientamento è univocamente nel senso di ritenere non responsabile il PSP, trattandosi di frode che fuoriesce totalmente dalla sua sfera di controllo, non attenendo essa al momento dell'operazione dispositiva, ma ad un momento precedente, rispetto al quale gli intermediari risultano essere totalmente estranei<sup>47</sup>.

La seconda tipologia di frode, invece, esita normalmente nell'accoglimento (quanto meno parziale) delle domande degli USP, e viene normalmente individuata come *SIM swap fraud*: si tratta di una frode in cui risulta involontariamente (quanto colpevolmente) coinvolta anche la compagnia telefonica dell'USP, che consente al truffatore di sostituire la SIM della vittima con un duplicato, così permettendogli a quel punto di carpire le credenziali di accesso agli strumenti di pagamento e di effettuare operazioni dispositive fraudolente in autonomia. Come anticipato, i Collegi A.B.F. tendono ad inquadrare la fattispecie in termini di frode particolarmente sofisticata, equiparandola a volte alla mancanza di autenticazione, e rilevando inoltre che l'affidamento parziale a terzi soggetti – le compagnie telefoniche – della procedura di autenticazione delle operazioni di pagamento attraverso l'invio dell'OTP con SMS su cellulare, giustifica l'attribuzione della responsabilità a carico del PSP, in chiave di rischio d'impresa<sup>48</sup>.

Occorre tuttavia rilevare che, presso la giurisprudenza di merito, pare invece prevalere un orientamento incline a considerare responsabile, eventualmente in via

---

<sup>47</sup> Per un caso di questo tipo, cfr. A.B.F., Coll. Napoli, 10 novembre 2022, n. 14452, in *Dir. risp.*, [www.dirittodelrisparmio.it](http://www.dirittodelrisparmio.it), 2023, con nota di V. TROIANELLI, "Truffa della fattura" (c.d. "invoice fraud") e sostituzione delle coordinate bancarie.

<sup>48</sup> Vedi, ad esempio, A.B.F., Coll. Bari, 25 maggio 2021, n. 13285; A.B.F., Coll. Milano, 12 marzo 2021, n. 6758; A.B.F., Coll. Milano, 23 giugno 2022, n. 9749, tutte in [www.arbitro bancariofinanziario.it](http://www.arbitro bancariofinanziario.it).

concorrente con l'USP, la compagnia telefonica<sup>49</sup>: va da sé che la differenza di posizioni tra A.B.F. e giurisprudenza ordinaria può anche essere la risultante dell'impossibilità di convenire in giudizio, dinanzi all'organo arbitrale, soggetti diversi dagli intermediari finanziari, sicché – in un'ottica di tutela dell'utente del servizio di pagamento – appare giustificato l'addossamento della responsabilità a carico del PSP, il quale ovviamente poi avrà la possibilità di rivalersi nei confronti del gestore telefonico, che colpevolmente ha consentito il perpetrarsi della truffa.

**Claudio Colombo**

*Ordinario di Diritto privato*

*nell'Università degli Studi di Sassari*

---

<sup>49</sup> Cfr. Trib. Milano 13 aprile 2022, in *Dejure*.