Pubblicazione Trimestrale
ISSN: 2279-9737

Rivista di Diritto Bancario

dottrina
e giurisprudenza
commentata

Ottobre/Dicembre
2019

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

2019 | 2020

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

NORME PER LA VALUTAZIONE E LA PUBBLICAZIONE

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

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

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

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

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

2019 | 2020

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

SEDE DELLA REDAZIONE

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

2019 | 2020

BRUNELLA RUSSO

I nuovi orientamenti giurisprudenziali sul reato di phishing: "la banca è responsabile se non prova che il cliente ha disposto il pagamento"

SOMMARIO: 1. Profili civilistici e evoluzione normativa. – 2. Il fatto. – 3. Inquadramento della fattispecie alla luce della recente sentenza della Cassazione: la posizione giuridica delle parti nell'ambito dei servizi di *home banking*… – 4. … e gli orientamenti espressi dall'Arbitro Bancario e Finanziario in materia.

1. *Profili civilistici e evoluzione normativa*

La ben nota ordinanza del 2018 della Corte di Cassazione, emessa a seguito del ricorso presentato da due correntisti rimasti vittime di un episodio di *phishing* on line, riprende – soprattutto per le conclusioni alle quali perviene – il dibattito giurisprudenziale sulle questioni legate ai reati informatici[1].

La pronuncia, infatti, nel richiamare le norme civilistiche, nell'intento di individuare la responsabilità della banca per improprio utilizzo di strumenti di pagamento da parte di terzi, si pone nel solco di un filone ampiamente consolidato accogliendo, nelle motivazioni addotte, non solo il criterio di estensione del perimetro applicativo della

[1] Cfr., Cass., ordinanza del 12 aprile 2018, n. 1234, in un caso avente ad oggetto il ricorso presentato da due soggetti contitolari di un conto corrente presso le Poste Italiane, di cui chiedevano la condanna alla restituzione di euro 5.500,00, oltre accessori, pari all'importo bonificato on line a favore di un terzo, il quale aveva utilizzato, senza alcuna autorizzazione da parte dei medesimi, i dati personali dei correntisti. Fa riferimento a tali principi espressi dalla giurisprudenza di legittimità anche Trib. Parma, I sez. civ., sentenza del 6 settembre 2018, n.1268. In merito a quest'ultima pronuncia si lamenta una certa staticità dei giudici su principi formalistici e astratti, senza approfondire gli aspetti correlati all'effettivo e corretto funzionamento dei sistemi informativi, in conformità alle normative bancarie emanate dagli organismi di vigilanza italiani ed europei.
Così, C. TELMON, M.C. DAGA, *La responsabilità della banca sul corretto funzionamento del sistema bancario di home banking*, reperibile all'indirizzo www.pagamentidigitali.it del 28 novembre 2018.

c.d. diligenza tecnica dell'"accorto banchiere" (*ex* art.1176, co.2, c.c.)[2] ma anche un certo orientamento ormai cristallizzato dell'ABF, il quale ribadisce, in più occasioni, l'obbligo di rimborsare le somme sottratte *invito domino* al cliente.

In applicazione a tali principi, il Supremo Collegio prende dunque posizione e riconduce la questione nella cornice disciplinare del D.Lgs. n.218/2017[3] (che modifica il precedente D.Lgs. n.11/2010) addivenendo ad un principio giuridico di massima, ad integrazione di quello normativo già vigente, secondo cui l'eventuale uso dei codici di accesso al sistema, da parte dei terzi, rientra nel c.d. "rischio professionale" del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure tecniche di sicurezza, finalizzate a verificare la riferibilità delle operazioni suddette alla condotta dell'utilizzatore[4].

---

[2] Si veda al riguardo Cass., 24 settembre 2009, n. 20543. In tema di adempimento diligente si rimanda, per la dottrina in argomento, a F. DI CIOMMO, *La responsabilità civile in internet: prove di governo dell'anarchia tecnocratica*, in *La responsabilità civile.,* 2006, VI, 548 ss.; P. TRIMARCHI, *Il contratto: inadempimento e rimedi*, Milano, 2010, 83 ss.; F. GALGANO, *Trattato di diritto civile*, II, Padova, 2009, 39 ss.; P. GALLO, *Il contratto telematico*, in Gallo (a cura di), in *Trattato del contratto*, I, Torino, 2010, 841 ss. Con riferimento alla responsabilità contrattuale ed extracontrattuale on line si consiglia AA.VV., *La responsabilità in internet e nel commercio elettronico*, in Alpa (a cura di), in *Trattato della responsabilità contrattuale*., II, Padova, 2009, 503 ss.; C. IURILLI, *Conto corrente on line e furto di identità. La controversa applicazione dell'art.2050 c.c*., in *La responsabilità civile.,* 2011, I, 54 ss.; S. MARINO, *Nuovi sviluppi in materia di illecito extracontrattuale "on line*", in *Riv. dir. internaz. priv. process..,* 2012, IV, 879-881.

[3] Cfr., D. Lgs. n.218/2017, entrato in vigore il 13 gennaio 2018 di recepimento della direttiva UE 2015/2366 relativa ai servizi di pagamento nel mercato interno (PSD 2 - *Payment Services Directive*), nonché di adeguamento delle disposizioni interne al Regolamento UE n.751/2015 sulle commissioni interbancarie applicate alle operazioni di pagamento basate su carta (IFR – *Interchange Fees Regulation*). Per una rapidissima disamina in tema di PSD 2, cfr., AA.VV., *La Direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno*, in *dirittobancario.it,* del 28 luglio 2016; S.VANINI, *L'attuazione in Italia della seconda Direttiva sui servizi di pagamento nel mercato interno: le innovazioni introdotte da d.lgs. 15 dicembre 2017, n. 218*, in *Le nuove leggi civ. comm.*, 2018, IV, 866 ss.; P. MONTELLA, *La Direttiva PSD 2: obiettivi della revisione e principali tratti di novità*, in *Innovazione e diritto*, 2018, II, 129 ss.; A. ANTONUCCI, *Mercati dei pagamenti: le dimensioni del digitale,* in *Rivista di Diritto Bancario,* 2018, III, 1-8.

[4] Più complessa è l'opinione della dottrina per la quale la concreta ampiezza della responsabilità attribuibile in capo alla banca è, in ogni caso, rimessa in parte alla

Vale la pena ricordare come la maggiore "connettività" dovuta alle innovazioni dei mercati telematici abbia imposto un'adeguata attenzione dei profili di sicurezza dell'utente on line relativamente ai propri dati personali, sia attraverso regole – si pensi alla "*strong customer authentication*", più comunemente definita autenticazione "a due fattori", ai fini di una più ampia protezione degli account – sia utilizzando delle API, le quali prevedono per la banca maggiori responsabilità nell'investigare e nel rispondere sulle frodi. Per quanto – è bene sottolinearlo sia pure per inciso – la generale tendenza a proteggere il cliente viene in molti casi vanificata dalle stesse tecniche del *phishing* che, per poter funzionare, richiedono la necessaria collaborazione (seppure inconsapevole) dell'utente[5].

Questo cambio di paradigma, nella prestazione di servizi di pagamento elettronici, riconosce pertanto alla banca un livello di colpevolezza esclusivo per il danno patito dal cliente a seguito del mancato adeguamento dei propri sistemi di sicurezza all'evoluzione dei mercati (con restituzione integrale dell'importo eventualmente addebitatogli senza autorizzazione)[6]; a meno che non fornisca la prova del loro corretto funzionamento e, quindi, della riconducibilità dell'operazione al correntista che l'abbia disconosciuti, dimostrando, in tal modo, come il fatto sia da imputare al dolo del titolare "o a

valutazione – in termini di diligenza – dei comportamenti tenuti dai due differenti soggetti. Cfr., a tal proposito, S. MARTINELLI, *Sicurezza informatica degli istituti di credito e responsabilità contrattuale*, in *Giur. It*., 2017, X, 2069-2074.

[5] E' necessario tuttavia ricordare come l'introduzione, ad opera della PSD2, di stringenti standard di sicurezza abbia imposto importanti novità per l'utilizzo dei canali online, richiedendo, da un lato, l'accertamento dell'identità del cliente attraverso due o più strumenti di autenticazione (c.d. *Strong Costumer Authentication*), e dall'altro, l'utilizzo di collegamenti dinamici che certifichino l'unicità della transazione (c.d. *Dinamic Linking*).

[6] Salvo che l'utilizzatore abbia agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi, *ex* art.7, co.2, D. Lgs. n.11/2010 (corretta custodia delle credenziali di autenticazione e comunicazione tempestiva di uso illecito delle stesse), in tutti gli altri casi questi può sopportare, per un importo comunque non superiore a euro 50, la perdita relativa a operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita. Ancora sul bilanciamento degli interessi coinvolti, si veda anche I.A. CAGGIANO, *Pagamenti non autorizzati tra responsabilità e restituzioni. Una rilettura del d.lgs. 11/2010 e lo scenario delle nuove tecnologie*, in *Riv. dir. civ*., 2016, II, 10459.

comportamenti talmente incauti da non poter essere fronteggiati in anticipo".

2. *Il fatto*

La vicenda che si commenta trae origine da un bonifico compiuto mediante piattaforma di *internet banking***,** in favore di individui sconosciuti a due correntisti di Poste Italiane S.p.a. a seguito della ricezione di un'e-mail fraudolenta, tanto da consentire ai truffatori, attraverso la digitazione dei codici personali, di utilizzare le somme oggetto dell'operazione (c.d. reato di *phishing*).

La domanda di risarcimento da parte degli attori veniva tuttavia respinta in prima istanza dalla Corte d'Appello di Palermo che riconduceva (erroneamente) la fattispecie nell'ambito della responsabilità per l'esercizio di attività pericolose, *ex* art.2050 c.c. [7], senza peraltro verificare se l'Ente in questione avesse fornito la prova dell'ascrivibilità dell'azione ai ricorrenti.

Nelle sue motivazioni, infatti, la Corte territoriale giudicava non sussistente un vero e proprio obbligo contrattuale dell'intermediario nel garantire e tutelare i clienti dalle frodi informatiche**,** mentre riconosceva quest'ultimi responsabili di un comportamento definito "imprudente e negligente" nella custodia e nel corretto utilizzo delle credenziali in loro possesso.

Proposto ricorso in Cassazione, i correntisti sottolineavano invece come la Corte d'Appello di Palermo non avesse esaminato opportunamente la circostanza del disconoscimento dell'operazione di addebito sul conto corrente, ai sensi dell'art.10, co.1, d. lgs. n.11/2010

[7] Cfr., App. Palermo, 12 luglio 2016, n. 1348 che ha respinto la domanda, spiegata dai titolari di un conto corrente, volta ad ottenere condanna della convenuta – a titolo di responsabilità contrattuale o extracontrattuale – al pagamento dell'importo bonificato, attraverso una operazione on line, in mancanza di qualunque disposizione da parte degli stessi. Per i precedenti giurisprudenziali sul tema, cfr., Cass., 5 settembre 2014, n. 18812. Quanto alla dottrina in materia, sul presupposto che le banche, disponendo dei dati sensibili dei clienti, sono tenute al risarcimento, ai sensi dell'art.2050 c.c. (allorquando cagionino un danno ad altri per effetto del trattamento dei dati personali), cfr., E. PELLECCHIA, *La responsabilità civile per trattamento dei dati personali*, in *Resp. civ. prev*., 2006, II, 221 ss.; F. AZZARRI, *Responsabilità presunta, responsabilità oggettiva e danno*, *ibidem*, 2008, IV, 1078 e ss.; M. CICORIA, *Quale danno in materia di privacy*?, in *Giust. civ*., 2007, II, 39.

e, di conseguenza, ne avesse fondato le proprie motivazioni su valutazioni presuntive circa la responsabilità dei danneggiati, senza tuttavia provare il reale coinvolgimento degli stessi in attività dolosa o colposa.

3. *Inquadramento della fattispecie. La posizione giuridica delle parti nell'ambito dei servizi di home banking…*

L'intervento chiarificatore operato dai giudici di legittimità, riguardo all'incidenza dei reati in oggetto, ha sicuramente posto un punto fermo su una questione affrontata sovente in modo ondivago nelle aule giudiziarie: responsabile la mancanza di una puntuale regolamentazione relativamente ad alcuni ambiti operativi dei prestatori di servizi, oggi ampiamente superata dalle norme comunitarie in materia. Un difetto che, non di rado, ha generato in passato, differenti posizioni circa l'ampiezza degli obblighi gravanti e sul prestatore e sull'utilizzatore dei servizi elettronici di pagamento, ai fini della ripartizione del carico probatorio in sede contenziosa.

A seguito della puntuale legislazione comunitaria – attraverso l'introduzione delle due importanti direttive PSD sui sistemi di pagamento on line, nonché del tanto atteso Regolamento GDPR (che rivisita il contenuto normativo del precedente Codice Privacy)[8] – si è preso atto del crescente impiego degli strumenti di pagamento elettronico da parte del pubblico degli utilizzatori e del prevedibile espandersi degli attacchi sferrati dalla nuova criminalità nell'ecosistema digitale: la sofisticazione dei metodi di aggressione ha indotto non già a porre in discussione il più generale principio di "ragionevole esigibilità delle contromisure di sicurezza", messe in campo dall'intermediario, quanto ad affermare questo stesso principio secondo metodi di approccio moderni da parametrare ai livelli di offensività dei

[8] Cfr., Regolamento Ue 2016/679, noto come GDPR (*General Data Protection Regulation*), relativo alla protezione delle persone fisiche con riguardo al "trattamento e alla libera circolazione dei dati personali", che a far data dal 25 maggio 2018 è direttamente applicabile in tutti gli Stati membri. Per il vecchio Codice Privacy si rinvia al D.Lgs. 30 giugno 2003 n.196 (Codice in materia di protezione dei dati personali) che prevede la risarcibilità nei casi laddove il trattamento dei dati personali cagioni un danno; equiparando così il suddetto trattamento all'esercizio di un'attività pericolosa (in specie, artt.15 e 31).

fenomeni di *cybercrime* sempre più evoluti. Tanto da ritenere necessari – da parte del regolatore – nuovi e più adeguati sistemi di sicurezza informatica per la protezione delle informazioni riguardanti la clientela, delle quali le banche diventano, da questo momento, responsabili nella loro qualità di titolari del trattamento dei dati personali[9].

Come meglio si dirà, l'introduzione della normativa citata (d. lgs. n.11/2010 che estende anche al nostro ordinamento i principi della PSD del 2007)[10] è stata determinante per la costruzione di un sistema di imputabilità, prima assente, in capo all'intermediario in relazione a specifici obblighi di precauzione, fra tutti quello di garantire l'inaccessibilità dei dispositivi di autenticazione a soggetti non autorizzati, delineando così una responsabilità della banca di tipo oggettivo "aggravata" da cui la stessa, per andare esente da responsabilità, non deve solo dimostrare di aver adottato tutte le misure idonee ad evitare il danno (c.d. "prova liberatoria"), ma è tenuta a

[9] Trattasi nello specifico di meccanismi di autenticazione basati su OTP nei casi di servizio bancario erogato on line. In base a tali meccanismi la banca è obbligata ad adottare misure tecniche quali codici di accesso "statici"; password "dinamica" o "usa e getta" (detta OTP, generata da un dispositivo *Token*). Inoltre è richiesta un'adeguata pubblicità *antiphishing* sul proprio sito Internet, contenente opportune informazioni alla clientela e, da ultimo, un sistema di *Token* mobile associato alla carta di pagamento o al numero di conto, ovvero di un *Token* virtuale presente di solito all'interno dell'app di mobile banking della banca o su un'app apposita. Tecnicamente, tale sistema informatico affianca, ai fini dell'autorizzazione delle operazioni on line, all'inserimento del codice identificativo e della password – noti solo al cliente – un secondo sistema di autenticazione denominato appunto OTP che genera una password monouso ogni sessanta secondi di cui solamente il cliente dev'essere a conoscenza e che va correttamente inserita. La letteratura in argomento è piuttosto vasta. Si veda, *amplius*, per una ricognizione degli interventi legislativi riguardo ai rischi per la clientela e gli operatori, AA.VV., *Il FinTech e l'economia dei dati. Considerazioni su alcuni profili civilisti e penali*, in *Quaderni FinTech* della Consob, n.2/2018, 13-47. Con riguardo al nuovo Regolamento privacy ne discutono, tra gli altri, A. MANTELERO, *Responsabilità e rischio nel Regolamento UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, I, 148 ss; L. GATT, R. MONTANARI, I.A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Politica del diritto*, 2017, II, 57 ss.

[10] Cfr., D. Lgs. n.11 del 20 gennaio 2010, che attua la direttiva 2007/64/Ce del 13 novembre 2007 relativa ai servizi di pagamento nel mercato interno (meglio nota come PSD). Pubblicato in G.U. - Serie Generale n.36 del 13 febbraio 2010 - Suppl. Ord. n. 29.

fornire la prova del sussistere di una causa esterna[11].

Alla luce di quanto argomentato, l'ordinanza epigrafata risulta particolarmente interessante in quanto arricchisce il punto di osservazione giuridica dei fenomeni di *phishing*[12] – reato che oramai occupa saldamente una delle posizioni di primo piano tra le più insidiose minacce del *web* – oltre che dei profili di tutela "tecnica" del cliente, parametrata dal legislatore codicistico alla figura dell'"accorto banchiere", anche di quelli che implicano riflessi diretti e più significativi sul versante della protezione dell'investitore; laddove il *quid iuris* è riconducibile al criterio del c.d. "rischio di impresa" teso a trasferire l'alea contrattuale (derivante dall'utilizzo fraudolento degli strumenti di pagamento) sulla banca, in quanto soggetto più adatto a sopportarlo dal punto di vista giuridico, ma soprattutto economico[13].

Infatti il prestatore di servizi di pagamento, posto a tutela dell'integrità delle informazioni e dei dati personali, è responsabile dei danni conseguenti per non aver impedito a terzi di introdursi illecitamente nel sistema telematico del cliente mediante la *captatio* dei suoi codici d'accesso, *prevedibile* ed *evitabile* solo predisponendo

[11] Su questo principio si rimanda a M.C. DOLMETTA, Responsabilità dell'intermediario in caso di operazioni fraudolente effettuate a mezzo di strumenti elettronici, in dirittobancario.it del 16 maggio 2018. Per la giurisprudenza di riferimento, cfr., Cass., 23 maggio 2016, n.10638 con nota di R. FRAU, Operazioni di home banking disconosciute dal correntista e responsabilità semioggettiva della banca, in Resp. civ. prev., 2017, III, 855 ss. Precedentemente, Trib. Firenze, 20 maggio 2014, ; Giudice di Pace di Campobasso, 3 maggio 2016, n. 277.

[12] Il Report di ENISA (*European Union Agency for Network and Information Security*) definisce tale reato come « […] the mechanism of crafting messages that use social engineering techniques…», laddove con il termine "*mechanism*" parrebbe intendersi anzitutto un artifizio che si concretizza nella capacità di comporre, attraverso l'impiego delle proprie capacità e della propria "perizia" dei testi mediante i quali si fa uso delle tecniche di ingegneria sociale allo scopo «[…] to persuade potential victims into divulging sensitive information such as credentials, or bank and credit card details».

[13] In tal senso l'ordinanza richiama un principio risalente in giurisprudenza, e di recente ribadito dal Supremo Collegio, secondo il quale è onere della banca fornire la prova della riconducibilità dell'operazione al cliente. La diligenza richiesta alla banca nello svolgimento delle sue attività è una diligenza di natura tecnico-professionale, parametrabile sullo stereotipo del c.d. "accorto banchiere". Tra le tutte, Cass., 3 febbraio 2017, n.2950.

specifiche misure «ritenute adeguate all'evoluzione tecnologica»[14] e destinate a verificare, prima di dare corso all'operazione, la sussistenza di un comportamento negligente o inadempiente dell'utilizzatore, o cause di forza maggiore[15].

Dunque, sul piano applicativo, la correttezza di tale ragionamento mette ancor più in risalto la centralità dell'onere probatorio in capo all'intermediario, solo implicitamente desumibile dalla formulazione del vecchio testo: attualmente, infatti, non solo l'art.10, ult. cpv., del D.Lgs.11/2010, così come modificato dal d. lgs.218/2017 (di recepimento della PSD2), sancisce che è onere del prestatore di servizi di pagamento fornire la prova della frode, del dolo o della colpa grave dell'utente – al fine di far ricadere su quest'ultimo i costi dell'operazione non autorizzata – ma anche il novellato art.11, ad opera del decreto in parola, il quale non si limita più a prevedere genericamente l'obbligo del rimborso bensì impone tempi certi entro i quali esso deve avvenire[16].

Si determina così una sorta di "squilibrio controllato" laddove la posizione della banca appare, rispetto al passato, deteriore se rapportata a quella del cliente, al quale spetta soltanto la prova del danno riferibile al trattamento dei propri dati personali (uno speciale *favor* probatorio a beneficio dell'utilizzatore dei servizi di *internet banking*). Essa (la

[14] Così recita l'art. 31 D.Lgs. n.196/2003. Per la giurisprudenza di merito, Trib. Milano, 4 dicembre 2014, ha osservato come «nel rapporto contrattuale di home banking, la banca ha la veste di contraente qualificato che, non ignaro delle modalità di frode mediante phishing da tempo note nel settore, è tenuto ad adeguarsi all'evoluzione dei nuovi sistemi di sicurezza». Cfr., *ex multis*, Giudice di Pace di Campobasso, 3 maggio 2016, n. 277 e Trib. Firenze, 20 maggio 2014, già richiamate.

[15] In tal senso si era già espressa Cass. 3 febbraio 2017, n.2950/2017, prima citata. E' importante anche richiamare i concetti chiave contenuti nella PSD2 a proposito di "negligenza" e "negligenza fraudolenta", che lasciano adeguato spazio ai legislatori nazionali nella declinazione concreta degli stessi all'interno di ciascun ordinamento. L'unica indicazione fornita dal legislatore europeo è contenuta nel 72° Considerando secondo il quale « […] il concetto di negligenza implica la violazione del dovere di diligenza, mentre per negligenza grave si dovrebbe intendere un comportamento che si spinge oltre la semplice negligenza e implica un grado significativo di mancanza di diligenza; ad esempio, lasciare le credenziali usate per autorizzare un'operazione di pagamento vicino allo strumento di pagamento, in un formato aperto e facilmente individuabile da terzi».

[16] Si parla della medesima giornata in cui si è svolta l'operazione o, al più tardi, entro la giornata operativa successiva. Sul punto, R. FRAU, *op.cit*., 866 ss.

banca) infatti è obbligata alla ripetizione integrale dell'importo addebitatogli senza autorizzazione, tranne nel caso di motivato sospetto di frode e salva la possibilità, per lo stesso intermediario, di dimostrare *ex post* che l'operazione è avvenuta correttamente (cioè, su disposizione del cliente intestatario dei fondi).

Occorre peraltro sottolineare – anticipando quanto dopo si dirà – come la questione riguardante la ripartizione della responsabilità tra i soggetti, a conti fatti, potrebbe prevedere un potenziale spostamento con riferimento, soprattutto ad operazioni fraudolente eseguite mediante sistemi di *internet banking* "a due fattori" (nuova frontiera nella sicurezza on line)[17], riconoscendo al cliente – secondo le indicazioni già espresse dalla Banca d'Italia, poi riprese dal più recente orientamento arbitrale – una ben precisa responsabilità derivante dall'utilizzo, dalla conservazione e dalla protezione di credenziali oramai considerate sicure e difficilmente intercettabili da soggetti esterni[18].

Sempre che tali forme di pirateria informatica siano talmente sofisticate da non poter essere individuate utilizzando il grado di diligenza cui è tenuto il cliente nell'utilizzo dei servizi di pagamento digitalizzati.

4. *... e gli orientamenti espressi dall'Arbitro Bancario e Finanziario in materia*

Al concetto d'imputabilità della condotta all'operatore finanziario, sancito dall'ordinanza in commento – la quale riprende, in buona

[17] I requisiti della *Strong Customer Authentication* (*SCA*) sono contenuti nella *PSD2 (Payment Services Directive 2*) e sono già operativi dal 14 settembre 2019. I requisiti di tali fattori di autenticazione e le relative esenzioni sono quelli previsti nel Regolamento Delegato della Commissione (UE) 2018/389 sulle "Norme tecniche di regolamentazione per l'autenticazione forte del cliente" (RTS).

[18] Tale principio dell'autenticazione "a due fattori" è ritenuto coerente alle disposizioni della Banca d'Italia, finalizzate a fare in modo che «[…] le banche si attrezzino adeguatamente per identificare, valutare, misurare, monitorare e mitigare le minacce di natura tecnologica […]». Cfr., Circolare della Banca d'Italia n.285/2013 avente ad oggetto l'adozione di soluzioni atte ad accertare l'identità del cliente per le operazioni di pagamento.

sostanza, quanto già affermato in precedenti giudizi[19] – va rapportata la consolidata giurisprudenza dell'ABF chiamata con sempre maggiore frequenza a dirimere fenomeni di indebita appropriazione di credenziali nell'utilizzo di servizi on line.

Invero, l'attenzione dei vari Collegi arbitrali si è concentrata di volta in volta, facendo proprio il substrato normativo di riferimento, ora sulla sussistenza di colpa grave in capo al cliente (che deve comunque custodire con la dovuta diligenza le proprie credenziali al fine di non renderle facilmente accessibili a soggetti esterni), ora puntando la lente sul "contegno" dell'intermediario (*rectius* "diligenza professionale", *ex* art.1176, co.2, c.c.) sulla base di un concetto già ampiamente condiviso dai giudici di legittimità – e in questa sede richiamato – in virtù del quale il parametro di valutazione dell'"accorto banchiere" è destinato a valere anche con specifico riferimento ai servizi di *home banking*[20].

Per quanto l'orientamento dominante sia sempre stato tendenzialmente volto a tutelare il correntista e ad ascrivere la responsabilità alla banca – sul presupposto, come prima sottolineato, secondo il quale viene richiesta una diligenza professionale elevata ed una specifica capacità di prevedere operazioni fraudolente da parte di terzi – le decisioni pronunciate in ambiente extragiudiziale non sempre hanno assunto un atteggiamento di sostegno a favore del cliente, soffermandosi piuttosto sulla cura loro richiesta nel custodire le credenziali e nell'informarsi dei possibili rischi legati all'incauto utilizzo dei dati personali[21].

---

[19] L'onere della banca di dimostrare di aver predisposto un sistema adeguato a protezione dei dati del cliente trova riscontro nell'importante sentenza della Cass., 23 maggio 2016, n.10638, prima citata, in un caso in cui una titolare di conto corrente presso Poste Italiane aveva subito il furto delle proprie credenziali di accesso on line al conto (codice identificativo, nome utente e password) mediante l'invio di una mail, a seguito della quale era stata effettuata un'operazione di postagiro non autorizzata dalla correntista. Si veda anche Cass., 19 gennaio 2016, n. 806 e Cass., 12 giugno 2017, n.13777 nel ribadire l'obbligo per la banca di porre in essere strumenti idonei a garantire gli impianti da manomissione, rispondendo in mancanza dei relativi rischi.

[20] In particolare sul punto, Cass., 31 marzo 2010, n.7956. Cfr., *ex plurimis*, ABF, Coll. Roma, 6 dicembre 2010, n. 1440 e Coll. Milano, 9 novembre 2010, n. 1241 e 4 ottobre 2010, n. 1030.

[21] Come si è avuto già modo di evidenziare, nella maggior parte delle decisioni arbitrali si tendeva ad utilizzare una più accentuata severità nei confronti del cliente allorquando la frode, perpetrata ai suoi danni, fosse stata ricondotta a tecniche di *phishing* piuttosto note e ricorrenti «tanto che qualunque utente dotato di quella

Va premesso, tuttavia, come tale indirizzo interpretativo – a parte qualche percorso motivazionale poco convincente di alcuni Collegi[22] – sia stato frutto del clima normativo antecedente al recepimento della direttiva comunitaria 2007/64/CE, in materia di utilizzo fraudolento di strumenti elettronici di pagamento, e pertanto, *ratione temporis*, dev'essere valutato alla luce delle disposizioni prima vigenti.

Queste ultime, nello specifico, attraverso una prescrizione dal tenore più rigido, rispetto a quella comunitaria, imponevano contestualmente all'utilizzatore un obbligo negoziale (custodia) e uno prescrittivo (adozione di misure di sicurezza, declinabile nelle azioni di conservazione e memorizzazione del codice identificativo) la cui reciproca connessione – pur nella loro autonoma rilevanza – costituiva la condizione richiesta per il corretto utilizzo degli strumenti di pagamento[23]. Ne è scaturito – ai fini della risoluzione delle controversie in sede arbitrale – il riconoscimento di un regime di responsabilità del solo cliente, graduato sulla base del comportamento dello stesso, indicante sia ipotesi di dolo (oltre che di fraudolenza) che, e più in

normale avvedutezza e prudenza che si richiede a chi utilizzi servizi di home banking dovrebbe essere in grado di sottrarsi all'inganno». La "colpevole credulità" del cliente valeva pertanto a fondare una presunzione di colpa grave con esclusione di responsabilità in tutto o in parte in capo all'intermediario, nell'ipotesi di mancata predisposizione di uno strumentario avanzato di sicurezza. Così, ABF, Coll. di Coordinamento, 26 ottobre 2012, n. 3498, citato; Coll. Roma, 16 maggio 2014, n. 3262 e, più di recente, Coll. Milano, 4 maggio 2017, n. 4785.

[22] Cfr., ABF, Coll. Roma, n.2338/2014 e n.9262/2015. In argomento, *contra*, Cass, 3 febbraio 2017, n. 2950, citata. I giudici confermano un'interpretazione oramai costante escludendo espressamente che si possano addossare responsabilità al correntista «sulla stregua del mero possesso degli apparati e dell'ipotetica sottrazione dei codici, vieppiù alla stregua di operazioni di tipo presuntivo». Ritenendo invece più opportunamente come «la sottrazione dei codici del correntista, attraverso tecniche fraudolente, rientra nell'area del rischio di impresa, destinato ad essere fronteggiato attraverso l'adozione di misure che consentano di verificare, prima di dare corso all'operazione, se essa sia effettivamente attribuibile al cliente».

[23] Cfr., art.7, co.2, D. Lgs. n.11/2010. Conforme, ABF, Coll. Napoli, 10 settembre 2015, n.6846 secondo il quale sia l'obbligo di custodia (in conformità alle prescrizioni contrattuali) sia l'adozione, *ex lege*, di misure idonee atte a garantire la sicurezza (di quei dispositivi che consentono il regolare utilizzo dello strumento) incombono sull'utilizzatore sin dal ricevimento dello strumento; al tempo stesso, però, pur nel silenzio della norma, deve ritenersi che essi permangono sin tanto che l'utilizzatore resti in possesso dello strumento di pagamento, posto che detti impegni garantiscono il suo regolare utilizzo.

particolare, riconducibile a casi di colpa grave «dell'agente che, senza volontà di arrecare danno agli altri, operi con straordinaria e inescusabile imprudenza o negligenza, omettendo di osservare non solo la diligenza media del buon padre di famiglia, ma anche quel grado minimo ed elementare di diligenza generalmente osservato da tutti»[24]. Integrando, per tale via, una violazione (gravemente colpevole) degli obblighi, di custodia dei dati identificativi e dispositivi del proprio conto, nascenti dal contratto[25].

Di conseguenza – a prescindere da una certa linea di pensiero basata sul concorso di colpa[26] – l'atteggiamento via via consolidatosi è stato

[24] Si rinvia agli arresti del Coll. Roma, decisione n.1440/2010 e Coll. Milano, decisioni n.1241/2010 e n.103/2010 già citate e poi successivamente riprese dal Coll. Milano, decisione n.40/2012; n.2310/2011; n.4317/2013; Coll. Roma, decisione n.2157/2011; n.712/2010; Coll. Napoli, decisione n.961/2013 e n.6846/ 2015, tutti sostanzialmente reputando provata la colpa grave della parte ricorrente (cliente) e pertanto dichiarando imputabile alla medesima la comunicazione dei codici segreti di accesso. Così anche Cass., 19 novembre 2001, n. 14456, secondo la quale «ad integrare gli estremi della colpa grave del cliente è necessario che il suo comportamento sia connotato da straordinaria ed inescusabile imprudenza o negligenza, idonea a far ritenere che chi ha agito ha omesso di osservare, non soltanto la diligenza del buon padre di famiglia, ma anche quel grado minimo di elementare diligenza generalmente osservato da tutti».

[25] Così, in particolare, Coll. Napoli, decisione n.6846/2015 già citata. In una simile prospettiva anche Coll. Milano, decisione n.2310/2011 e n.40/2012; Coll. Roma, decisione n.712/2010 e n.2157/2011, qui più volte ricordate. Per una ricostruzione del panorama dottrinale in materia di responsabilità contrattuale e adempimento diligente, si rimanda ancora alle opere di F. DI CIOMMO*, op.cit.,* 545 ss.; P. GALLO, *op.cit.,* 839 ss. Con riferimento ai temi generali della responsabilità contrattuale ed extracontrattuale on line, cfr. S. SICA, N. BRUTTI, *La responsabilità in internet e nel commercio elettronico*, in Alpa (a cura di), *Trattato della responsabilità contrattuale*, II, Padova, 2009, 503 ss.; C. IURILLI, *op.cit.* 54; S. MARINO, *op. cit.*, 879.

[26] Le motivazioni avanzate dall'ABF in più occasioni vertono su una responsabilità concorrente con l'intermediario, derivante dalla mancata adozione di strumenti tecnici di protezione evoluti, soprattutto se già disponibili e fruibili. Cfr., *ex plurimis,* Coll. Milano, 9 luglio 2010, n. 719, nel ribadire come « […] da un lato si può verosimilmente ravvisare una responsabilità del cliente in relazione alla mancata diligente custodia dei codici di accesso per il servizio di home banking, dall'altro lato, non si può negare una concorrente responsabilità dell'intermediario che non ha predisposto adeguati sistemi per proteggere più efficacemente i propri clienti con riferimento al rischio di truffe perpetrate in via telematica. Questo Collegio, valutata la gravità delle rispettive colpe in relazione ai fatti illustrati e documentati, ritiene,

quello di riconoscere un comportamento gravemente colposo del cliente, soprattutto qualora egli stesso comunichi le proprie credenziali in risposta a messaggi chiaramente ingannevoli, salvo i casi ove la responsabilità del soggetto «che ha materialmente consentito l'esecuzione dell'operazione fraudolenta cooperandovi seppur involontariamente» risulti colpevole «in quanto egli è portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario […] laddove si consideri che tali forme di "accalappiamento" possono dirsi ormai note al pur non espertissimo navigatore di Internet»[27].

A partire dall'impianto regolamentare introdotto dal D. Lgs. n.11/2010 cambia la prospettiva entro la quale sono stati ricondotti, in seno alle decisioni arbitrali, i reati di *phishing*. Si viene a determinare pertanto una nuova ricomposizione degli obblighi ricadenti sulle parti contrattuali[28] attraverso un meccanismo di "traslazione" del rischio in capo all'intermediario sul quale graverà un vincolo di rimborso delle perdite subite in conseguenza di operazioni non autorizzate e/o fraudolente[29].

---

dunque, di doverle ripartire nella misura del 50% in capo al cliente e del 50% in capo al resistente». Ma ancora in argomento, Coll. Roma,10 febbraio 2010, n. 33.

[27] Cfr., Coll. Roma, 25 ottobre 2016, n. 9538, sostanzialmente riconoscendo colposa la condotta del cliente che inserisca le proprie credenziali, qualora l'e-mail "truffaldina" sia redatta con errori marchiani e lessico inadeguato, rendendo evidente lo scopo fraudolento o qualora cada reiteratamente in errore, continuando ad inserire i propri dati di accesso in risposta a e-mail palesemente "false". Ancora in argomento Coll. Roma, decisione n.3076/2015, n.4991/2016 e n.8487/16; Coll. Milano, decisione n.8841/2016; Coll. Napoli, decisione n.1965/2017; Coll. Bologna, decisione n.4785 del 4 maggio 2017.

[28] Nello specifico, artt.7-8 del citato D. Lgs. n.11/2010.

[29] Si riporta in commento una pronuncia del Coll. Roma, 2 luglio 2010, n. 665, che recita: «[…] si tratta di una disciplina evidentemente ispirata al principio del rischio d'impresa, e cioè all'idea secondo la quale è razionale far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente pericolose, che interessano un'ampia moltitudine di consumatori o utenti, sull'impresa, in quanto quest'ultima è in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ribaltare sulla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi. Si tende, in altri termini, a spalmare sulla moltitudine degli utilizzatori il rischio dell'impiego fraudolento di carte di credito e strumenti di pagamento, sì da evitare che esso gravi esclusivamente e direttamente sul singolo pagatore, in funzione dell'obiettivo di incrementare la fiducia del pubblico riguardo ai suddetti strumenti e di incentivarne l'uso e la diffusione, in quanto strumenti atti a

Si passa – come si desume chiaramente – da una banca "irresponsabile" e "insensibile" di fronte alle pretese del cliente a una banca "potenzialmente responsabile" – tenuta, in determinate ipotesi, a rimborsare quest'ultimo e indennizzarlo delle perdite subite[30] – nel solco del "progressivo spostamento del metro valutativo nella direzione di una più ampia ed efficace protezione del cliente". Pertanto, ai fini dell'esimente da responsabilità, sarà onere del prestatore dei servizi di pagamento provare, da un lato, la legittimità dell'operazione on line non autorizzata e, dall'altro, di avere posto in essere tutte le necessarie precauzioni valutate anche con riferimento all'attuale sviluppo tecnologico, imputando al cliente un comportamento gravemente colposo e negligente in quanto, nell'aprire la mail sospetta, questi è portato comunque a digitare i propri codici d'accesso on line al conto consentendo, in tal modo, il furto dei relativi dati.

Tuttavia, secondo l'approdo arbitrale più recente (dunque a far data dall'introduzione della PSD 2) l'adozione di tutte le misure di sicurezza previste dalle leggi in materia e "*ritenute adeguate all'evoluzione tecnologica*" non libera comunque l'utilizzatore – da un'eventuale imputazione di responsabilità. Anzi "invertendo la rotta" l'Arbitro finisce con il considerare l'"invulnerabilità" del sistema a "due fattori" addirittura idonea a riconoscere una presunzione di colpa grave in capo al cliente, al quale automaticamente – in caso di violazione del sistema

facilitare e perciò moltiplicare le transazioni commerciali, nell'interesse delle imprese, degli stessi utenti/consumatori, nonché, ovviamente, delle banche». Ed ancora, Coll. Roma, 14 gennaio 2011, n. 105, delineando un'efficace tutela per il cliente, con diritto di rimborso delle perdite subite in conseguenza di operazioni non autorizzate e/o fraudolente da parte dello stesso.

[30] Tale passaggio è stato ampiamente trattato da F. CALISAI, Il Phishing: profili civilistici ed evoluzione delle forme di tutela alla luce delle decisioni dell'Arbitro Bancario Finanziario, in Rivista di Diritto Mercato Tecnologia del 7 luglio 2015, reperibile in www.dimt.it . Secondo l'autore, l'introduzione di importanti innovazioni normative, già a partire dalla prima PSD, unitamente alla particolare interpretazione orientata di alcune specie di clausole inserite nei contratti tra intermediario e cliente, hanno consentito di aggirare alcuni limiti ontologici e di approntare una tutela più incisiva, arrivando a configurare, in determinati casi, una responsabilità dell'intermediario nei confronti del cliente vittima di *phishing attack*.

– viene contestata l'omessa diligente custodia delle credenziali di accesso[31].

Le ragioni di tale cambio risiedono nella stretta interazione tra "evoluzione dei metodi di aggressione informatica" utilizzati dai *phishers* e sistemi di sicurezza maggiormente incisivi per i clienti (leggasi "sistemi di autenticazione forte" o "SCA")[32]. Pertanto, la predisposizione di sistemi di *best practice* – in grado di assicurare gli obiettivi di confidenzialità, integrità, disponibilità dei sistemi informativi e dei dati ad essi associati – pone la banca fuori dal rischio di eventuale intrusione fraudolenta: una volta che il sistema OTP sia stato chiaramente offerto al cliente, e questi se ne sia avvalso, l'utilizzo indebito da parte di un terzo soggetto non può che ricadere nella pur ristretta area di rischio che la legge pone a carico dell'utente.

Parimenti – sviluppando considerazioni già accennate ed avvalorate dalle disposizioni della stessa Banca d'Italia a riguardo – proprio in ragione dell'accertata aggressione informatica operata attraverso l'utilizzo di *malware* particolarmente sofisticati, alcune pronunce arbitrali hanno invece ritenuto di dover assumere una posizione diversa rispetto alla precedente negando la sussistenza di un comportamento negligente del cliente sul presupposto che tale software sia «capace di sorprendere la buona fede anche di un pur normalmente attento fruitore del servizio» così da risultare «difficilmente individuabile e neutralizzabile anche dai più evoluti ed efficienti sistemi antivirus»[33].

A supportare siffatta opinione la circostanza secondo cui il sistema di sicurezza "a due fattori", pur essendo caratterizzato da una spiccata capacità protettiva non risulta idoneo «a fondare una irreversibile presunzione di negligenza in capo al cliente in caso di violazioni e

[31] Cfr., Coll. Roma, 25 novembre 2011, n. 2568 e Coll. Milano, 9 ottobre 2012, n. 1462. Si veda anche ABF, Coll. Milano, 20 giugno 2012, n. 2103, laddove riconosce la responsabilità del cliente che «non avesse viceversa compiutamente custodito i dispositivi personali necessari per l'utilizzo del sistema di pagamento, con negligenza che si presenta rilevante».

[32] Vedasi, nello specifico, ABF, Coll. di Coordinamento, 26 ottobre 2012, n. 3498, che indica il principio operativo di tale meccanismo di intrusione con l'espressione "*man-in-the-browser*" a significare l'interposizione che questo genere di *malware* è in grado di operare fra il sistema centrale dell'intermediario e il singolo utente.

[33] Cfr., ancora ABF, Coll. di Coordinamento, 26 ottobre 2012, n. 3498 escludendo ogni colpa a carico del cliente. *Contra*, Coll. Milano, decisione n.11126/2016 e, pur partendo da diverse motivazioni, anche Coll. Roma,9 febbraio 2017, n. 1181

intrusioni in detto sistema, bensì (solamente) a indurre una valutazione più rigorosa del contegno del cliente stesso»[34].

Conclusione questa che ribalta, ancora una volta, il sistema di bilanciamento di responsabilità tra le parti con conseguente (ri)allocazione del rischio in capo all'intermediario derivante da frodi e intrusioni illecite nel sistema dei pagamenti, ma con una sostanziale differenza, sotto l'aspetto motivazionale, rispetto alla precedente formulazione.

I più sofisticati metodi di intrusione odierni «caratterizzati da un effetto-sorpresa, capace di spiazzare l'utilizzatore, grazie alla perfetta inserzione nell'ambiente informatico originale e nella correlata simulazione di un messaggio che a chiunque non potrebbe apparire che genuino»[35] – il riferimento va ovviamente al *malware* (ma non il solo nella scala dei reati informatici particolarmente insidiosi) che determina il confine tra vecchie e nuove tecniche di *phishing*[36] – non sono provocati da autorizzazioni e/o da comportamenti negligenti addebitabili al cliente, giacché «costituisce ormai un dato di comune esperienza che i codici personali di accesso ai sistemi di home banking possono essere catturati da terzi non autorizzati anche in assenza di comportamenti negligenti da parte del cliente che quei codici è tenuto diligentemente a custodire». Ma, secondo l'arresto della più recente giurisprudenza dell'ABF prima accennata, più verosimilmente

[34] ABF, Coll. Napoli, 8 ottobre 2012, n. 3192 e Coll. Roma, 6 giugno 2012, n. 1910 riaffermando un principio, già peraltro espresso in altre pronunce, per il quale «costituisce ormai un dato di comune esperienza che i codici personali di accesso ai sistemi di home banking possono essere catturati da terzi non autorizzati anche in assenza di comportamenti negligenti da parte del cliente che quei codici è tenuto diligentemente a custodire… […]». Ed ancora Coll. Roma, 28 giugno 2012, n. 2264 e Napoli, decisione n.1583/2012 i quali hanno contestato l'automatismo deduttivo dal quale si fa dipendere l'irreversibile presunzione di responsabilità in capo al cliente, dipendente dalla sola adozione del sistema OTP da parte dell'intermediario.

[35] In tal senso ABF, Coll. di Coordinamento, 26 ottobre 2012, n. 3498, già citata.

[36] Riconducibile alle tecniche di *phishing* più evolute è anche il c.d. "*farming*", una nuova modalità che non si basa più sull'invio di "messaggi-esca" fraudolenti, ma sulla creazione di siti web falsi, verso i quali l'utente viene reindirizzato nonostante abbia digitato correttamente l'indirizzo web della banca e/o del portale su cui compiere le operazioni. Cfr., ABF, Coll. Milano, 11 dicembre 2014, n. 8364, secondo il quale «si tratta di una forma assai subdola di truffa on-line che implica una sorta di duplicazione della pagina web, la quale si presenta perciò identica all'ignaro utente on line».

innescati da un insufficiente grado di protezione del sistema informatico e del servizio offerto dall'intermediario: spetta a questi infatti, pur non disconoscendo la capacità di protezione del sistema OTP, predisporre opportuni e mirati accorgimenti volti a scongiurare violazioni e operazioni fraudolente da parte di terzi, anche – se del caso – mediante blocco tempestivo della carta, da comunicare immediatamente al cliente[37].

Si ritorna in tal modo a quel principio giuridicamente condiviso, e fatto proprio nel corso di questi ultimi anni da vari Collegi arbitrali, del c.d. "rischio di impresa" volto, alla luce della più generale regola di salvaguardia del contraente più debole, a porre la responsabilità derivante da frodi informatiche, sempre più sofisticate ed ingannevoli – e pertanto difficili da individuare prontamente poiché oggettivamente "pericolose" – in capo all'intermediario «in quanto soggetto più adatto a sopportarla e ad assorbirne le conseguenze dannose»[38].

Infatti, la sua attitudine a trasporre sulla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi (attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio) consente di distribuire sulla moltitudine degli utilizzatori il rischio dell'impiego fraudolento di carte di credito e strumenti di pagamento «sì da evitare che esso gravi esclusivamente e direttamente sul singolo pagatore»[39].

---

[37] Detta misura "cautelare" del blocco della carta – anche in assenza di previsioni contrattuali *ad hoc* – può essere letta alla luce del più generale principio di buona fede, *ex* art.1176 c.c., che implica un preciso obbligo di protezione nei confronti del cliente. Cfr., ABF, Coll. Roma, 10 novembre 2010, n. 1312, nel ritenere che «allorché la misura non sia stata comunicata tempestivamente alla ricorrente, con indicazione dei motivi giustificatici e dei contenuti della misura deve ritenersi che il comportamento della banca non risponda ai canoni della trasparenza e della buona fede che è tenuta ad osservare […]».

[38] In questo senso, *ex plurimis*, è chiarissima la decisione del Coll. di Coordinamento più volte richiamata.

[39] Conforme all'orientamento espresso in argomento dal Coll. di Coordinamento, anche la precedentemente pronuncia del Coll. Roma n.1111/2010 e Coll. Milano, 13 luglio 2016, n. 6376 il quale ha ritenuto che «in ipotesi di mancato assolvimento di detto onere probatorio gravante sull'intermediario, la richiamata disciplina prevede che l'intermediario sopporti la relativa perdita, atteso il fatto che quest'ultimo si è assunto il rischio d'impresa connesso con l'esercizio dell'attività ed è in grado di ribaltare tale rischio sulla massa degli utenti attraverso la determinazione dei prezzi per la fornitura del servizio».