Pubblicazione Trimestrale
ISSN: 2279-9737

Rivista di Diritto Bancario

dottrina
e giurisprudenza
commentata

Gennaio/Marzo

2021

rivista.dirittobancario.it

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

2021 | 2022

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

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

2021 | 2022

LORENZO MUTTINI

Frodi informatiche e responsabilità della banca: i nuovi orientamenti dell'Arbitro Bancario Finanziario

SOMMARIO: 1. Premessa – 2. La vicenda – 3. Le questioni interpretative sottoposte al Collegio di Coordinamento – 4. La normativa di riferimento – 4.1. Gli obiettivi della PSD2: accrescere la fiducia nell'impiego degli strumenti di pagamento e rafforzarne la sicurezza – 4.2. Gli obblighi dell'utente – 4.3. Gli obblighi del prestatore di servizi di pagamento (PSP) – 4.4. Il riparto dell'onere della prova – 5. La nozione di colpa grave nella giurisprudenza dell'ABF in relazione alle truffe informatiche – 6. Critiche all'orientamento maggioritario dell'ABF in tema di "ignoto tecnologico" – 7. Segue: ulteriori profili critici – 8. La Decisione del Collegio di Coordinamento – 9. Segue: l'operatività della franchigia di legge – 10. La successiva giurisprudenza dell'ABF – 11. Conclusioni.

1. *Premessa*

La decisione del Collegio di Coordinamento ABF[1], 10 ottobre 2019, n. 22745, che si annota, resa a seguito dell'ordinanza di rimessione del Collegio di Bari[2], si impone all'attenzione degli interpreti perché

[1] Com'è noto, l'Arbitro Bancario Finanziario è un sistema di risoluzione stragiudiziale delle controversie tra clienti e intermediari in materia di operazioni e servizi bancari e finanziari. Istituito nel 2009, in attuazione dell'art.128-*bis* TUB, esso rappresenta uno strumento di tutela alternativo, più rapido e meno costoso rispetto alla giustizia ordinaria: la procedura dura, infatti, al massimo di 270 giorni e il cliente, per adire l'Arbitro, deve versare un contributo di soli 20 euro per le spese della procedura (rimborsato dall'intermediario in caso di accoglimento, anche solo parziale, del ricorso). *Amplius*, sulle caratteristiche e sul funzionamento dell'ABF, si veda la *Relazione sull'attività dell'Arbitro Bancario Finanziario* anno *2018*, pubblicata sul sito *www.arbitrobancariofinanziario.it*, e, in dottrina, I. A. CAGGIANO, *L'arbitro bancario finanziario, esempio virtuoso di degiurisdizionalizzazione*, in (La) *Nuova giur. comm.*, 2015, 439 ss.; M. MARINARI, *La disciplina dell'onere della prova nel procedimento ABF*, in (Le) *Società*, 2018, 491 ss. e D. DALFINO, *L'Abf e i principi del processo civile: contestazione, "contumacia", onere della prova,* in *Il Processo*, 2019, 27 ss.

[2] Quando ricorrono questioni di particolare importanza o emergono orientamenti contrastanti, ciascuno dei sette Collegi territoriali in cui si articola ABF (Bari, Bologna, Milano, Napoli, Palermo, Roma, Torino), può chiedere l'intervento nomofilattico del Collegio di Coordinamento il quale è deputato a stabilire i principi di diritto da seguire nel decidere le controversie: riferimenti alla nota precedente.

interviene in modo innovativo in materia di responsabilità della banca per utilizzo abusivo degli strumenti di pagamento[3].

Com'è noto, secondo l'orientamento dell'Arbitro consolidato in precedenza, la prova da parte dell'intermediario di aver adottato un sistema di autenticazione a due fattori[4] – basato cioè sull'utilizzo congiunto di credenziali "statiche" (ad esempio il numero della carta e un PIN) e "dinamiche" (come il codice OTP inviato sul cellulare del

[3] In termini generali sulla responsabilità dell'operatore bancario per abusiva utilizzazione degli strumenti di pagamento, senza pretesa di completezza, si vedano F. CIRAOLO, *Prelievi fraudolenti e responsabilità della banca nell'erogazione del servizio Bancomat*, in *Banca borsa tit. cred.*, 2009, II, 29 ss.; ID., *Pagamento fraudolento con carta di credito e ripartizione della responsabilità. Dagli orientamenti attuali alla revisione della PSD,* in *Dir. banc. fin.*, 2017, 150 ss.; M. FRANZONI, *Nota in tema di smarrimento o di furto di strumenti di pagamento elettronici*, in *Giur. it.*, 2008, 319 ss.; R. FRAU, *Sottrazione di credenziali informatiche, bonifici non autorizzati e responsabilità civile della banca da trattamento di dati personali*, in *Resp. civ. prev.*, 2011, 1830 ss.; ID., Home banking*, bonifici non autorizzati e responsabilità della banca*, in *Resp. civ. prev.*, 2013, 1285 ss.; ID., Home banking*, captazione di credenziali di accesso dei clienti tramite* phishing *e responsabilità della banca*, in *Resp. civ. prev.*, 2015, 911 ss.; ID., *Prelevamenti illeciti dal bancomat e responsabilità della banca*, in *Resp. civ. prev.*, 2017, 219 ss.; ID., *Responsabilità civile della banca per operazioni di* home banking *disconosciute dal cliente*, ivi, 853 ss.; *ID.,* Home banking*,* phishing *e responsabilità civile della banca*, in *Resp. civ. prev.*, 2019, 622 ss.; D. SCANO, *Operazioni in conto corrente ed obblighi di monitoraggio della Banca*, in *Giur. Comm*., 2011, 605 ss.; A. SALOMONI, *Responsabilità dell'operatore bancario nei confronti del cliente in caso di addebito non autorizzato su conto corrente* online, in (La) *Nuova giur. comm.*, 2015, 141 ss.; A. PALMIERI, *Vulnerabilità dei servizi di* home banking*: risarcibili i danni da* phishing, in *Il Quotidiano Giuridico*, 21 gennaio 2015; F. A. MARASÀ, *Utilizzo fraudolento di carta bancomat e diligenza professionale della banca*, in *Banca borsa tit. cred.*, 2016, 396 ss.; L. VIGNUDELLI, *Furto della carta di credito, verifica del perdurante possesso e tardiva denuncia della sottrazione*, in *Contratti*, 2016, 870 ss.; S. MARTINELLI, *Sicurezza informatica degli istituti di credito e responsabilità contrattuale*, in *Giur. it.*, 2017, 2069 ss.

[4] Per sistema di autenticazione, in generale, si intende, ai sensi dell'art. 1, comma 1, lett. *q*) del d.lgs. n. 11/2010, la procedura che consente all'intermediario *(rectius* 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.

Si possono distinguere i sistemi di autenticazione a "un solo fattore", basati cioè sull'utilizzo di credenziali di un solo tipo – ad esempio i dati della carta (numero, data di scadenza, CVV) – da quelli a "due fattori", che richiedono, oltre all'inserimento delle predette credenziali, anche la digitazione di una password monouso e di validità temporanea inviata sul dispositivo dell'utente (codice OTP).

cliente) – bastava a fondare una presunzione di responsabilità in capo al cliente per aver custodito le credenziali di accesso allo strumento di pagamento in modo negligente: una deduzione fondata sull'assunto per cui, allo stato attuale delle conoscenze tecnologiche, non è possibile forzare un simile sistema di autenticazione.

La decisione annotata si segnala perché mette in discussione questo argomento, non ritenendolo coerente con la lettera e con la *ratio* della disciplina dettata dal d.lgs. n. 11/2010 in tema di strumenti di pagamento. Quest'ultima è, infatti, informata alla c.d. teoria del rischio di impresa, in base alla quale il "rischio da ignoto tecnologico" (che si ha quando un'operazione fraudolenta si verifica, benché l'intermediario abbia messo a disposizione della propria clientela i presidi di sicurezza più evoluti) non dovrebbe rimanere a carico degli utenti, vittime delle frodi, ma essere allocato in capo agli intermediari, essendo insito nella loro attività professionale e, come tale, facilmente amministrabile dai *Payment Service Provider*[5] a un costo sostenibile.

Da tali considerazioni il Collegio di Coordinamento giunge alla logica conclusione che, ove l'intermediario si sia limitato a presumere la sussistenza di una colpa grave in capo al cliente in ragione della particolare affidabilità del proprio sistema di autenticazione, senza allegare ulteriori elementi di fatto a sostegno del suo assunto, esso dovrà rispondere a titolo di responsabilità oggettiva per rischio di impresa delle perdite subite dal cliente.

---

[5] Conformandoci al lessico adoperato dai Collegi dell'ABF, in questo lavoro si sono utilizzate le coppie di termini clienti/utenti di servizi di pagamento e intermediari/prestatori di servizi di pagamento (per brevità PSP) come intercambiabili.

A voler essere rigorosi, adottando la terminologia legale, bisognerebbe utilizzare i termini "prestatore di servizi di pagamento", da un lato, e "utente" di servizi di pagamento" dall'altro.

Il d.lgs. n. 11/2010 reca all'art. 1, comma 1 una definizione di entrambi i concetti: «g) "prestatore di servizi di pagamento": uno dei seguenti organismi: istituti di moneta elettronica e istituti di pagamento nonché, quando prestano servizi di pagamento, banche, Poste Italiane s.p.a., la Banca centrale europea e le banche centrali nazionali se non agiscono in veste di autorità monetarie, altre autorità pubbliche, le pubbliche amministrazioni statali, regionali e locali se non agiscono in veste di autorità pubbliche; h) "utente di servizi di pagamento" o "utente": il soggetto che utilizza un servizio di pagamento in veste di pagatore o beneficiario o di entrambi».

Come si vedrà meglio in seguito, la soluzione elaborata nella pronuncia annotata, pur in linea con la lettera e lo spirito della normativa, rischia a ben vedere di dare luogo a una serie di inconvenienti applicativi su cui avremo modo di soffermarci nelle battute conclusive di questo commento.

2. *La vicenda*

Il fatto storico da cui origina la decisione in commento è piuttosto semplice: Tizio, titolare di una carta ricaricabile emessa dall'intermediario resistente, scopre un'operazione di pagamento *online* da lui mai autorizzata disposta a favore di un soggetto estero sconosciuto e, dopo aver sporto denuncia alle autorità competenti e presentato inutilmente reclamo all'intermediario, si rivolge all'Arbitro Bancario Finanziario per ottenere il rimborso della somma fraudolentemente sottratta[6].

Il ricorrente affermava di aver sempre custodito con la massima diligenza lo strumento di pagamento e le relative credenziali, mentre l'intermediario, costituitosi in giudizio[7], chiedeva il rigetto del ricorso non essendo emersa alcuna anomalia o irregolarità nell'esecuzione dell'operazione contestata che risultava, al contrario, regolarmente autenticata, registrata e contabilizzata. L'intermediario precisava, del resto, che il servizio di banca telematica messo a disposizione del ricorrente era protetto da un sistema di autenticazione "a due fattori"– che risulta ad oggi, come anticipato, il sistema più sicuro – e produceva sia la trascrizione di tracce informatiche (cc.dd. "log" informatici)

[6] Prima di presentare un ricorso all'Arbitro Bancario Finanziario, i clienti devono cercare di risolvere la controversia inoltrando un reclamo scritto all'intermediario sulla medesima questione. Se l'intermediario non risponde entro 30 giorni o la risposta non è ritenuta soddisfacente, i clienti possono allora rivolgersi all'ABF entro 12 mesi dalla data del reclamo.

[7] Ricevuto il ricorso, la Segreteria tecnica dell'Arbitro Bancario Finanziario lo invia tempestivamente all'intermediario convenuto. Esso ha 45 giorni di tempo dalla ricezione del ricorso per presentare le proprie controdeduzioni, assimilabili ad una memoria difensiva, alle quali il cliente, se crede, può replicare entro i 25 giorni successivi. L'intermediario può, infine, trasmettere le controrepliche nei 20 giorni successivi. Una volta completato il fascicolo, il Collegio dell'ABF si pronuncia sul ricorso entro 60 giorni.

dell'operazione disconosciuta, sia la tracciatura dell'SMS contenente l'OTP inviato al cellulare del ricorrente.

Alla deduzione della banca resistente, per cui in assenza di anomalie registrate da un sistema massimamente sicuro si deve ritenere che il cliente non abbia ottemperato agli obblighi di custodia del PIN, il ricorrente replicava di non aver mai ceduto la carta a terzi, o subìto il furto o lo smarrimento del PIN o rivelatone gli estremi a terzi, e di non aver ricevuto alcun SMS dall'intermediario contenente codici o password.

3. *Le questioni interpretative sottoposte al Collegio di Coordinamento*

Quando, come nel caso illustrato, il cliente disconosce un'operazione di pagamento, ma l'intermediario dimostra di aver adottato un sistema di autenticazione "a due fattori" e produce i "log" dell'operazione contestata, ci si trova dinanzi a una fattispecie di c.d. rischio da ignoto tecnologico, già oggetto di molte decisioni da parte dell'ABF, nel senso che dal quadro probatorio non emergono elementi utili per ricostruire la dinamica dell'illegittima intrusione subita dal cliente, né per valutare se la stessa sia ascrivibile a una condotta colposa o dolosa dello stesso (quali, ad esempio, dichiarazioni confessorie del cliente il quale ammetta di aver "abboccato" a un tentativo di *phishing*).

Come anticipato, in simili casi la giurisprudenza maggioritaria dell'Arbitro[8] era solita dedurre la sussistenza della colpa grave del cliente dalla circostanza che l'intermediario avesse adottato un sistema di autenticazione con OTP, di quasi impossibile forzatura.

[8] Sono numerosissime le decisioni dell'ABF che, nel corso degli anni, si sono mosse nel solco di questo orientamento. Fra le più risalenti cfr. ABF, Coll. Milano, decisione 5 dicembre 2011, n. 2658; ABF, Coll. Milano, decisione 20 giugno 2012, n. 2103; ABF, Coll. Milano, decisione 10 settembre 2015, n. 6967. Più di recente, si vedano invece, ABF, Coll. Napoli, decisione 18 giugno 2019, n. 14809; ABF, Coll. Torino, decisione 27 giugno 2019, n. 15961; ABF, Coll. Milano, decisione 28 giugno 2019, n. 16027; ABF, Coll. Milano, decisione 28 giugno 2019, n. 16028; ABF, Coll. Napoli, decisione 16 luglio 2019, n. 17520; ABF, Coll. Milano, decisione 27 agosto 2019, n. 19961; ABF, Coll. Roma decisione 30 luglio 2019, n. 18923; ABF, Coll. Milano, decisione 04 luglio 2019, n. 16521; ABF, Coll. Milano decisione 28 giugno 2019, n. 16026; ABF, Coll. Torino, decisione 07 marzo 2018, n. 5397. Tutte le decisioni sono accessibili liberamente sul sito dell'Arbitro www.arbitrobancariofinanziario.it.

Il Collegio di Bari, anziché aderire a tale indirizzo interpretativo e respingere il ricorso, ha, però, escluso ogni presunzione di negligenza del cliente ritenendo che, ragionando in quel modo, si giungerebbe nella sostanza a desumere il dolo o la colpa grave del cliente dalla prova della regolarità formale delle operazioni disconosciute, in aperto contrasto con la disciplina dell'onere della prova dettata dal combinato disposto degli artt. 10 e 12 del d.lgs. n. 11/2010.

Queste ultime disposizioni prevedono infatti, nell'ipotesi in cui l'utente neghi di aver autorizzato un'operazione di pagamento, non solo che l'intermediario debba provare che l'operazione contestata sia stata autenticata, registrata e contabilizzata[9] (1° comma dell'art. 10), ma anche che la stessa sia riconducibile sul piano causale ad una condotta dolosa o gravemente colposa dell'utilizzatore (art. 12); con l'importante precisazione, poi, che non è consentito inferire la ricorrenza del secondo elemento – il dolo o la colpa grave dell'utente – dalla sussistenza del primo, ossia dalla c.d. regolarità formale dell'operazione (art. 10, 2° comma)[10].

Poiché nel caso concreto l'intermediario si era limitato a presumere la sussistenza di una condotta negligente in capo al cliente dalla particolare affidabilità dei sistemi di sicurezza adottati, senza tuttavia allegare ulteriori elementi di fatto, il Collegio di Bari ha ritenuto non assolto da parte del PSP l'onere probatorio su di esso incombente.

Consapevole che tali argomentazioni si ponevano in contrasto con l'indirizzo costante seguito dai Collegi ABF e che ciò avrebbe potuto

[9] Il concetto di "autenticazione" implica che l'intermediario debba verificare che l'operazione sia stata disposta dal cliente inserendo le credenziali di accesso personalizzate; "registrazione" significa, in sostanza, che l'operazione deve essere tracciabile, mentre "contabilizzazione" implica che l'operazione deve risultare dalla documentazione di tipo contabile. Sul significato di tali concetti si veda V. SANGIOVANNI, *Bancomat, carte di credito e responsabilità civile nella giurisprudenza dell'ABF*, in *La Responsabilità Civile*, 2012, 697 ss. Il mezzo più semplice a disposizione della banca per assolvere tale onere è la produzione in giudizio dei c.c. log, ossia le evidenze informatiche relative all'operazione contestata (ABF, Coll. Milano, decisione 6 aprile 2018, n. 7559).

[10] E, infatti, la citata norma prevede «[…] l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7 (n.d.r. gli obblighi di conservazione e custodia degli strumenti di pagamento).».

creare incertezza negli operatori del settore, il Collegio di Bari ha deciso di sospendere la decisione del ricorso e porre al Collegio di Coordinamento alcune questioni interpretative, e segnatamente: se il Collegio «possa desumere la sussistenza del dolo o della colpa grave del cliente dalla prova, che l'intermediario abbia fornito, della 'regolarità formale' dell'operazione, nel senso che questa è stata autenticata, correttamente registrata e contabilizzata e […] non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti»; se il Collegio, «valutato il mancato assolvimento dell'onere probatorio posto a carico dell'intermediario, ai sensi dell'art. 10, comma 2, d.lgs. n. 11/2010, debba accogliere il ricorso».

Il rimettente domanda al Collegio di Coordinamento di chiarire, altresì, se il Collegio «possa esaminare e valutare i profili attinenti al dolo o alla colpa grave del cliente anche in assenza di una specifica allegazione dell'intermediario, sulla base delle circostanze risultanti dalla documentazione in atti ovvero dalle dichiarazioni rese dalle parti». Ma si tratta di una questione decisamente meno problematica delle altre due, che verosimilmente non meritava di essere portata all'attenzione del Coordinamento. E ciò per almeno due ragioni.

In primo luogo perché, quantunque nel procedimento ABF valga il principio dispositivo[11] di cui all'art. 112 c.p.c. – sicché l'Arbitro Bancario non può andare alla ricerca della verità, ma deve decidere sulla base dei fatti allegati dalle parti e delle prove fornite per supportarli – risulta altresì applicabile il principio di acquisizione processuale, in virtù del quale le prove prodotte dalla parte che non era tenuta a produrle giovano anche all'altra[12]. Il che comporta, per rimanere nel campo dei servizi di pagamento, che la colpa grave del cliente possa dirsi accertata sulla base dell'affermazione, da questi resa

[11] Come ha chiarito il Collegio di Coordinamento ABF nella decisione 29 giugno 2017, n. 7716.

[12] ABF, Coll. Coord., n. 7716/2017, cit., che così si esprime «Senza alcuna riserva è invece applicabile il principio di acquisizione processuale, in virtù del quale le prove prodotte da una parte (ad es. la banca) che non era tenuta a produrle, servono anche all'altra (il cliente) che aveva l'onere di fornirle (Cass.19.4.2000, n. 5126; Cass. 3.5.1996, n. 4077)». Sulla questione relativa all'applicabilità dei principi e delle disposizioni del diritto processuale civile al procedimento avanti all'ABF, si vedano D. DALFINO, *op. cit.*; M. MARINARI, *op. cit.*; I. A. CAGGIANO, *L'arbitro bancario finanziario, esempio virtuoso di degiurisdizionalizzazione,* cit.

in sede di denuncia e/o nel ricorso, di aver comunicato o inserito su dispositivi o piattaforme informatiche apparentemente riferibili all'intermediario le proprie credenziali personalizzate (c.d. *phishing*), benché si tratti di circostanze non allegate dall'intermediario.

In secondo luogo, occorre ricordare che proprio le dichiarazioni rese dal cliente in sede di ricorso offrono importanti elementi per orientare la decisione dell'ABF, che è dotato di limitati poteri istruttori e deve decidere esclusivamente sulla base della documentazione allegata agli atti, senza poter disporre ulteriori indagini o ricorrere a CT[13].

Alla luce di tali osservazioni si comprende che i Collegi ABF devono poter accertare la colpa grave del ricorrente dal complessivo quadro probatorio risultante dalla documentazione in atti e dalle dichiarazioni rese dalle parti, anche in assenza di una specifica allegazione dell'intermediario.

[13] Al riguardo si vedano ABF, Coll. Milano, decisione 11 luglio 2019, n. 17080; ABF, Coll. Milano, decisione 10 aprile 2019, n. 9898; ABF, Coll. Milano, decisione 15 ottobre 2018, n. 21399; ABF, Coll. Torino, decisione 1° giugno 2018, n. 12151. In tal senso anche I. A. CAGGIANO, *L'arbitro bancario finanziario, esempio virtuoso di degiurisdizionalizzazione*, cit., la quale osserva «La procedura [n.d.r. dinnanzi all'Arbitro Bancario] è snella, grazie ad un sistema probatorio che non prevede escussioni di testi né lo svolgimento di consulenze, ma solo l'ammissione e l'esame della documentazione prodotta dalle parti». Sul tema dei poteri istruttori dell'Arbitro Bancario è intervenuta un'importante decisione del Collegio di Coordinamento, la già menzionata decisione 29 giugno 2017, n. 7716 che ha ritenuto non incompatibile con il procedimento ABF, nonostante l'assenza di specifiche previsioni normative, la possibilità per i Collegi di sospendere il procedimento al fine disporre un'integrazione istruttoria documentale. L'esercizio di tale potere è stato, però, fortemente circoscritto dal Collegio di Coordinamento: l'integrazione dell'istruttoria può essere solo documentale e quindi può avere ad oggetto, unicamente, la richiesta alle parti di fornire chiarimenti scritti o di produrre nuovi documenti; e può essere disposta solo nell'ipotesi in cui la parte abbia perlomeno fornito un principio di prova per iscritto. Chiara è la volontà del Collegio di Coordinamento, nel prevedere siffatti limiti, di evitare che l'esercizio ufficioso del potere di integrazione istruttoria possa tradursi in strumento idoneo a supplire alla inerzia probatoria delle parti. In dottrina una riflessione su questi temi si trova in M. MARINARI*, op. cit.* e D. DALFINO, *op. cit.*

4. *La normativa di riferimento*

4.1. *Gli obiettivi della PSD2: accrescere la fiducia nell'impiego degli strumenti di pagamento e rafforzarne la sicurezza*

Prima di discutere le soluzioni relative alle questioni appena illustrate occorre ricostruire i principi di diritto che disciplinano la materia, dettati essenzialmente dal d.lgs. n. 11/2010[14].

Tale normativa, attuativa della direttiva 2007/64/CE (c.d. PSD1), è stata recentemente novellata con il d.lgs. n. 218/2017, emanato per recepire la nuova direttiva relativa ai servizi di pagamento 2015/2366/UE, in vigore dal 13 gennaio 2018 (c.d. PSD2)[15].

Fra gli obiettivi principali perseguiti dalla PSD2, che si propone di adeguare la normativa in tema di strumenti di pagamento al mutato quadro tecnologico di riferimento, vi è quello di favorire l'utilizzo e la diffusione degli strumenti di pagamento diversi dal contante tramite un sostanziale innalzamento dei livelli di sicurezza delle operazioni.

In questa prospettiva deve essere letto l'inserimento nel d.lgs. n. 11/2010 del nuovo articolo 10-*bis*, introdotto dal d.lgs. n. 218/2017, che impone ai prestatori di servizi di pagamento (PSP), fatte salve poche

[14] In merito alla disciplina di cui al d.lgs. n. 11/2010, cfr. M. MANCINI-M. PERASSI, *Prefazione*, in *Il nuovo quadro normativo comunitario dei servizi di pagamento. Prime riflessioni*, in *Quad. Ric. Giur. della Banca d'Italia* (a cura di M. MANCINI-M. PERASSI), Roma, 2008, 15 ss.; AA.VV., *Armonizzazione europea dei servizi di pagamento e attuazione della direttiva 2007/64/CE*, (a cura di M. RISPOLI FARINA-V. SANTORO-A. SCIARRONE ALIBRANDI-O. TROIANO), Milano, 2009; AA.VV., *La nuova disciplina dei servizi di pagamento. Commentario al d.gls.27 gennaio 2010, n. 11*, (a cura di M. MANCINI-M. RISPOLI FARINA-V. SANTORO-A. SCIARRONE ALIBRANDI-O. TROIANO), Torino, 2011.

[15] Per un commento sulla PSD2 e sulle maggiori novità da essa introdotte in materia di servizi di pagamento v. G. BERTI DE MARINIS, *La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva "PSD2",* in *Dir. banc. fin.,* 2018, 627-655; I. D'AMBROSIO*, La tutela del consumatore nei pagamenti elettronici e la nuova direttiva europea psd2*, in *Notariato*, 2019, 676 ss.; S. VANINI, *L'attuazione in Italia della seconda direttiva sui servizi di pagamento nel mercato interno: le innovazioni introdotte dal d.lgs. 15 dicembre 2017, n. 218*, in (Le) *Nuove leggi civ. comm*., 2018, 839 ss.; AA.VV., *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, in *Quad. Ric. Giur. della Banca d'Italia* (a cura di M. MANCINI-M. PERASSI), Roma, 2019.

eccezioni[16], l'obbligo di applicare sistemi di autenticazione "forte" in caso di accesso da parte del cliente al proprio conto *online*, nel caso di operazioni di pagamento elettronico, nonché, da ultimo, anche di operazioni eseguite tramite un canale a distanza che possa comportare un rischio di frode o di altri abusi.

Per sistema di autenticazione forte[17] si intende una procedura tramite cui il PSP verifica l'identità del pagatore e, conseguentemente, la riferibilità allo stesso dell'operazione di pagamento, in base a una pluralità di "fattori", tra cui: *i*) un fattore che l'utente conosce (es: password/PIN); *ii*) un fattore che l'utente possiede (es. *smart card*, *token*, OTP, SIM cellulare, Firma Digitale); *iii*) un fattore che l'utente è (es. caratteristiche biometriche).

Nel caso sottoposto all'attenzione del Collegio di Bari il sistema di autenticazione adottato dall'intermediario poteva, ad esempio, considerarsi "forte", perché richiedeva l'inserimento tanto di credenziali statiche (numero di carta e PIN) quanto dinamiche (il codice OTP inviato sul cellulare): riconducibili, rispettivamente, a fattori afferenti alla categoria della conoscenza (*i*) e a quella del possesso (*ii*).

[16] Come ha osservato, giustamente, G. BERTI DE MARINIS, *op. cit.*, la previsione di alcune operazioni non necessariamente assoggettabili a sistemi di autenticazione forte risponde alla finalità di preservare la facilità e immediatezza di utilizzo degli strumenti di pagamento che un'estensione indiscriminata e generalizzata delle tecniche di autenticazione forte avrebbe potuto compromettere. Uno degli obiettivi di fondo della PSD2 è, infatti, quello di contemperare l'esigenza di favorire nuove tecnologie, che rendano i pagamenti sempre più semplici, con la necessità di predisporre sistemi di sicurezza sempre più efficaci per mantenere inalterata la fiducia degli utilizzatori. Le ipotesi di esenzione all'autenticazione forte riguardano quelle operazioni considerate a basso rischio quali, ad esempio: le transazioni di modesta entità, transazioni a basso rischio (analizzate tramite programmi di rilevazione delle frodi elaborate dai PSP), pagamenti ricorsivi con valore fisso (abbonamenti) e pagamenti verso beneficiari fidati.

[17] La definizione di autenticazione forte è racchiusa nell'art. 1, comma 1, lett. q-bis) del d.lgs. n. 11/2010: «"autenticazione forte del cliente": un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione». Sul punto, v. S. VANINI, *op. cit.*; G. BERTI DE MARINIS, *op. cit.*

Ciò premesso, tornando a esaminare il d.lgs. n. 11/2010, le disposizioni che rilevano maggiormente ai nostri fini sono gli artt. da 7 a 12, che disciplinano gli obblighi comportamentali posti a carico dell'utente e del prestatore dei servizi di pagamento (artt. 7, 8 e 9), il riparto dell'onere probatorio tra pagatore e intermediario in caso di disconoscimento di una transazione (art. 10), la ripartizione della responsabilità fra utente e banca in caso di utilizzo abusivo dello strumento di pagamento (artt. 11 e 12).

4.2. *Gli obblighi dell'utente*

La normativa appena richiamata pone a carico dell'utente i seguenti obblighi di condotta[18]: mettere in sicurezza, sin dal ricevimento e per tutto il periodo di detenzione, lo strumento di pagamento e i relativi codici di accesso; utilizzare lo strumento secondo quanto previsto dal contratto quadro; comunicare senza indugio – normalmente al numero verde dell'intermediario – il furto, l'appropriazione indebita o l'uso non autorizzato del dispositivo al fine di consentirne il blocco.

Più controversa è la questione se sussista in capo all'utente un obbligo di monitoraggio del conto corrente destinato a recepire le operazioni poste in essere con lo strumento di pagamento, al fine di verificarne il corretto utilizzo. A tale riguardo è dato riscontrare, nelle decisioni dell'ABF e in giurisprudenza[19], un atteggiamento *"consumer*

[18] Per un'analisi degli obblighi di comportamento incombenti sugli utilizzatori degli strumenti di pagamento cfr. F. CIRAOLO, *Prelievi fraudolenti e responsabilità della banca nell'erogazione del servizio Bancomat*, cit.; R. FRAU, *Prelevamenti illeciti dal bancomat e responsabilità della banca*, cit.; S. MARTINELLI, *op. cit.*; I. A. CAGGIANO, *Pagamenti non autorizzati tra responsabilità e restituzioni. una rilettura del d. legisl. 11/2010 e lo scenario delle nuove tecnologie*, in *Riv. dir. civ*., 2016, 459 ss**.**

[19] Trib. Firenze, 19 gennaio 2016, in *Dir. banc. fin.,* 2017, 150 ss., osserva che «Nessuna norma impone la verifica periodica e ravvicinata della disponibilità della carta da parte del suo titolare»; nello stesso senso anche Trib. Verona, 2 ottobre 2012, in *DeJure*, il quale rileva che, seppur il cliente possa monitorare, praticamente in tempo reale, le movimentazioni sul proprio conto corrente tramite il sistema *home banking*, non è, tuttavia, possibile «affermare l'esistenza di un obbligo per il correntista di effettuare il predetto controllo, e conseguentemente nemmeno un concorso di responsabilità dello stesso[…] nel caso in cui non lo eserciti». *Contra* Cass., 7 aprile 2016, n. 6751, in *DeJure,* che ha ritenuto responsabile un soggetto che si era avveduto del furto della carta con (appena) un giorno di ritardo. Quest'ultimo

friendly", nel senso che l'omessa verifica dei conti da parte del cliente tende ad essere punita solo se protratta per periodi piuttosto lunghi (diversi mesi), sulla base della premessa che «il titolare di una carta non può ritenersi tenuto ad un controllo continuativo o periodico delle risultanze del suo conto»[20].

Nel caso in cui violi uno dei suddetti obblighi con dolo o colpa grave, l'utente dei servizi di pagamento sopporterà le perdite derivanti dall'utilizzo abusivo dello strumento per intero[21]; diversamente il cliente avrà diritto al rimborso della somma fraudolentemente sottratta al netto, però, di una franchigia di 50 euro da applicarsi in caso «di operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita»[22]. Sui problemi posti dall'applicazione della franchigia si tornerà nel prosieguo del lavoro.

4.3. *Gli obblighi del prestatore di servizi di pagamento (PSP)*

Il prestatore dei servizi di pagamento è tenuto dalla normativa di settore[23] ad assolvere i seguenti obblighi: adottare le misure più idonee, alla luce dello sviluppo tecnologico, necessarie per impedire l'utilizzo abusivo dello strumento di pagamento; mettere a disposizione dei clienti strumenti gratuiti per permettere il blocco dello strumento; impedire l'utilizzo dello strumento in seguito al blocco.

---

pronunciamento ha attirato le critiche della dottrina, L. VIGNUDELLI, *op. cit.,* che ha considerato l'atteggiamento tenuto dalla Corte nei confronti degli utenti eccessivamente e irragionevolmente severo oltreché idoneo a minare la fiducia del pubblico nell'utilizzo degli strumenti di pagamento. In argomento si vedano anche le considerazioni di F. CIRAOLO, *Pagamento fraudolento con carta di credito e ripartizione della responsabilità. Dagli orientamenti attuali alla revisione della PSD*, cit., il quale rileva che l'obbligo di custodire con diligenza lo strumento di pagamento non implica che possa pretendersi dal titolare l'esercizio di una ininterrotta e costante vigilanza sulla permanenza del documento nella propria sfera personale, dovendosi tenere conto del fatto che le carte di pagamento non sono necessariamente destinate ad un impiego continuativo e quotidiano.

[20] ABF, Coll. Roma, decisione 27 marzo 2015, n. 2371.

[21] V. art. 12 d.lgs. n. 11/2010.

[22] Così dispone l'art. 12, comma 3, d.lgs. n. 11/2010.

[23] V. art. 8, d.lgs. n. 11/2010 «Obblighi a carico del prestatore di servizi di pagamento in relazione agli strumenti di pagamento».

Per opinione consolidata l'obbligo di impedire con misure efficaci che le credenziali di sicurezza dei clienti siano accessibili a terzi si considera assolto dalla banca nel momento in cui essa provi di aver predisposto un sistema di autenticazione forte, ossia, come si è visto, caratterizzato dalla presenza di almeno due fattori di autenticazione[24]. Con la precisazione che tale sistema di autenticazione deve presidiare non solo il momento della transazione – quando il cliente, cioè, dispone l'operazione di pagamento – ma anche qualsiasi attività dell'utente che, comportando l'utilizzo di credenziali personalizzate ovvero l'accesso a dati sensibili, potrebbe implicare il rischio

[24] Si rinvia alle decisioni dell'ABF richiamate alla nt. n. 8.

di frode[25] (ad. es. il cambiamento dei canali di contatto dell'utente, la creazione di strumenti di pagamento virtuale, la modifica del numero di cellulare su cui ricevere il codice OTP) [26].

Per quanto concerne l'obbligo di offrire un servizio per segnalare tempestivamente la perdita della detenzione o l'abuso dello strumento di pagamento (ad es. un numero verde sempre attivo), esso comporta,

[25] In altre parole, il PSP deve predisporre un sistema di autenticazione forte non solo per autorizzare il compimento delle operazioni di pagamento ma anche per la modifica dei dati personali del cliente, specialmente, dell'utenza telefonica sulla quale ricevere la OTP. A tal riguardo si segnala che una delle frodi che sta prendendo piede negli ultimi anni sfrutta proprio la vulnerabilità dei sistemi previsti dagli intermediari volti a presidiare la modifica dell'utenza telefonica su cui ricevere la OTP. Si fa riferimento alla c.d. "*sim swap fraud*", tipologia di frode che si svolge secondo questo schema ricorrente: il malfattore ottiene, tramite *phishing* o *hacking*, le credenziali di accesso al sistema *home banking* della vittima; attraverso questi dati accede al portale dell'utente e modifica il numero di cellulare associato alla carta dimodochè la password OTP, quando viene inviata dalla banca, arriva sul numero del frodatore anziché su quello della vittima. In questo modo i frodatori riescono ad eludere il sistema di autenticazione a due fattori. Talvolta la manovra fraudolenta appena descritta assume una forma ancor più complessa: dopo aver acquisito i dati della carta e conosciuto il numero di cellulare della vittima, tramite *hacking* o tecniche di ingegneria sociale, i truffatori sostituiscono la SIM telefonica dell'utente presso uno dei punti di assistenza del gestore telefonico (sfruttando la disattenzione o in alcuni casi la compiacenza del personale) mantenendo però invariato il numero di cellulare. Tale operazione comporta un improvviso malfunzionamento dell'utenza telefonica del cliente (dovuta per l'appunto alla disabilitazione della SIM) il quale, però, nella maggior parte delle ipotesi, non riesce a mettere in relazione il non funzionamento del telefono con il rischio di truffa. Ciò consente ai malfattori di ricevere sulla nuova SIM la OTP per disporre le operazioni fraudolente. In quest'ultima ipotesi, anche se l'operazione di modifica dell'utenza telefonica necessitasse a sua volta dell'inserimento della *password* OTP e non solo delle credenziali statiche della carta, i malfattori riuscirebbero ugualmente ad aggirare il sistema di autenticazione a due fattori proprio perché, nel caso di specie, il numero di telefono rimane invariato. Su tale tipologia di frode, v. ABF, Coll. Milano, decisione 5 febbraio 2020, n. 1758; ABF, Coll. Milano, decisione 28 giugno 2019, n. 16009; ABF, Coll. Milano, decisione 14 marzo 2019, n. 7440.

[26] Sull'esigenza che l'autenticazione forte sia posta a presidio dell'operatività via internet e dell'accesso ai dati sensibili relativi ai pagamenti, si veda *ex multis* ABF, Coll. Roma, decisione 16 novembre 2017, n. 14925; ABF, Coll. Palermo, decisione 24 ottobre 2017, n. 13217.

secondo la rigorosa giurisprudenza ABF, anche di fornire gratuitamente un servizio di SMS *alert* o altri assimilabili[27] .

Ed esige non solo che l'intermediario preveda la possibilità per il cliente di accedere a un tale servizio, ma addirittura che lo attivi in modo automatico, a prescindere da un'esplicita richiesta, fatta salva la facoltà del cliente di rifiutarlo espressamente.

Ciò comporta che l'intermediario, in caso di mancata attivazione o mancato funzionamento del servizio di SMS *alert*, risulterà gravemente inadempiente ai propri obblighi di diligenza professionale e sarà chiamato a rispondere delle operazioni di pagamento non autorizzate[28], a meno che non dimostri che il cliente aveva rifiutato l'attivazione del servizio[29] (producendo la dichiarazione liberatoria del cliente), ovvero che l'invio di messaggi di allerta non avrebbe comunque consentito, in concreto, di evitare le operazioni contestate[30].

---

[27] L'esistenza dell'obbligo in capo agli intermediari di attivare il servizio di SMS *alert* è stata affermata dall'Arbitro Bancario sulla base del rilievo che, per consentire ai clienti di denunciare tempestivamente ai PSP l'uso illegittimo dello strumento al fine di richiederne il blocco, essi devono essere posti dagli intermediari nelle condizioni di avvedersi di tale uso improprio: a tale funzione provvede, per l'appunto, il servizio SMS *alert.* Si vedano sul punto le chiare argomentazioni del Collegio di Coordinamento ABF nella decisione 28 marzo 2019, n. 8553 «Sulla base di queste premesse, può affermarsi che nella stessa norma su citata (art. 8, comma 1 lett. "c") sia ravvisabile, in linea di principio, l'obbligo dell'intermediario di predisporre un servizio di avviso tempestivo all'utente delle operazioni compiute utilizzando strumenti di pagamento di cui sia titolare, in quanto solo attraverso un (tempestivo) avviso da parte del gestore del sistema può ritenersi che l'utente sia messo in grado di "eseguire la comunicazione di cui all'art. 7, comma 1, lettera b)", qualificando il pagamento registrato come non autorizzato (nel senso del collegamento con l'obbligo di cui all'art.8 sembra esprimersi anche il Collegio di Roma, nella dec. n. 2262/2018)».

[28] In questo senso cfr. ABF, Coll. Coord., n. 8553/2019, cit. «Può ritenersi, in effetti, che l'attivazione dello strumento di segnalazione 'sms alert' rientri nei su menzionati doveri di adottare misure idonee a garantire la sicurezza del servizio con la dovuta diligenza. In ogni caso, costituisce orientamento consolidato dei Collegi territoriali che l'attivazione del servizio di 'sms-alert' costituisca un onere gravante direttamente sull'intermediario, a prescindere dal fatto che il cliente ne abbia o meno richiesto l'attivazione.».

[29] Così *ex multis*, ABF, Coll. Roma, decisione 18 maggio 2017, n. 5532.

[30] E, infatti, il Collegio di Coordinamento ABF, nella già citata decisione n. 8553/2019, ha stabilito che «Fra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad

Il quadro degli obblighi facenti carico all'intermediario si arricchisce, poi, di ulteriori previsioni: così, il PSP è tenuto, in forza della legge n. 166/2005 e del relativo decreto di attuazione n. 112/2007, a predisporre idonei strumenti per individuare e bloccare quelle transazioni che, presentando profili di anomalia, sono suscettibili di configurare un rischio di frode ai danni dei clienti.

L'art. 8 del d.m. n. 112/2007 ricollega il rischio di frode al raggiungimento di uno dei seguenti parametri: «A) con riferimento ai punti vendita di cui all'articolo 7, lettera b): 1) cinque o più richieste di autorizzazione con carte diverse, rifiutate nelle 24 ore, presso un medesimo punto vendita; 2) tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita; 3) richiesta di autorizzazione, approvata o rifiutata, che superi del 150% l'importo medio delle operazioni effettuate con carte di pagamento, nei tre mesi precedenti, presso il medesimo punto di vendita;

B) riguardo alle carte di pagamento sottoposte a monitoraggio di cui all'articolo 7, lettera c): 1) sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento; 2) una ovvero più richieste di autorizzazione che nelle 24 ore esauriscano l'importo totale del plafond della carta di pagamento 3) due o più richieste di autorizzazione provenienti da Stati diversi, effettuate, con la stessa carta, nell'arco di sessanta minuti».

Nel caso in cui risulti integrato almeno uno dei suddetti indicatori, l'intermediario è tenuto a porre in essere tempestivamente le opportune iniziative a tutela del proprio cliente quali, ad esempio, verificare l'autenticità delle operazioni, ovvero procedere al blocco cautelativo dello strumento di pagamento.

---

avvalersene. Gli effetti della mancata adozione del servizio di alert dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto.». Tale ultima situazione ricorre ad esempio nel caso in cui i malfattori abbiano posto in essere un'unica operazione fraudolenta; ovvero nell'ipotesi in cui le transazioni disconosciute siano avvenute l'una a breve distanza dall'altra, e dunque l'eventuale ricezione dell'SMS *alert* dopo la prima non avrebbe potuto impedire le successive; o ancora nell'ipotesi in cui il cliente abbia perso la detenzione oltre che dello strumento di pagamento anche del cellulare su cui ricevere gli SMS *alert* (per esempio furto della borsa in cui era contenuta la carta di credito e il cellulare.

Laddove l'intermediario rimanga inerte, a fronte del verificarsi di uno degli indici di frode, sarà ritenuto responsabile delle perdite subite dal cliente[31].

Più controverso è se, al di là delle ipotesi previste dal d.m. n. 112/2007 ritenute sempre idonee ad integrare un rischio di frode, sia possibile ravvisare in capo all'intermediario un generale dovere di protezione in favore del cliente avente ad oggetto l'obbligo di rilevare ed, eventualmente, bloccare quelle operazioni che, pur non rientrando nell'elenco *ex* art. 8 del decreto, appaiano "anomale", per frequenza, entità, o a cagione di altri elementi (es. beneficiario estero, operazione disposta da indirizzo IP diverso da quello usualmente utilizzato dal cliente).

[31] In merito alle conseguenze derivanti in capo all'intermediario dalla mancata attivazione in ipotesi che configuravano un rischio di frode tipizzato, è emersa una certa disomogeneità negli orientamenti assunti dai Collegi dell'ABF: in alcune decisioni (ABF, Coll. Milano, decisione 25 ottobre 2017, n. 13267), infatti, il PSP è stato condannato a restituire al cliente solo gli importi delle operazioni successive al verificarsi del rischio di frode. Seguendo questa logica, pertanto, se risultasse integrato a titolo di ipotesi il rischio di frode di cui all'art. 8 del d.m. n. 112/2007, lettera b, numero 1 («sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento») e il cliente disconoscesse nove operazioni di pagamento, gli verrebbero riconosciuti solo gli importi dell' ottava e nona operazione, ma non quelli relativi alle sette precedenti; in altre, invece, (ABF, Coll. Roma, decisione 21 novembre 2014, n. 7797 e ABF, Coll. Napoli, decisione 10 ottobre 2018, n. 21089) al ricorrente è stato rimborsato l'intero importo delle operazioni fraudolente. In altre ancora, infine, (ad es. ABF, Coll. Milano, decisione 29 aprile 2011, n. 888) l'Arbitro ha calcolato l'entità del rimborso in una misura percentuale commisurata alla gravità della colpa dell'intermediario.

Sul punto la giurisprudenza ordinaria, sia di merito[32] che di legittimità[33], così come i Collegi ABF[34] è orientata nel senso di ritenere che l'intermediario, in ragione del proprio *status* di operatore professionale, chiamato ad adempiere le proprie obbligazioni con la

[32] Cfr. Trib. Siracusa, 15 marzo 2012, in *DeJure* che ha ritenuto che costituisse una negligenza inescusabile da parte dell'intermediario eseguire, senza prima verificare l'effettiva provenienza dell'ordine, un'operazione per un importo considerevole proveniente da un indirizzo IP diverso da quello normalmente utilizzato dall'utente. Come ha giustamente osservato P. VALORE, Phishing *sul conto postale e trattamento dei dati personali*, in *Il Corriere del merito*, 2012, 663 ss. non pare che la difformità dell'indirizzo IP, da cui è stata disposta l'operazione disconosciuta, rispetto a quello abitualmente utilizzato dall'utente costituisca, da solo, un indice di anomalia così evidente da giustificare un rimprovero di colpevolezza nei confronti dell'intermediario considerato che una delle caratteristiche proprie del servizio di *home banking* è la sua attivabilità da qualsiasi postazione automatica, anche diversa da quella di proprietà dell'utente.

[33] In questa prospettiva merita di essere segnalata Cass., 31 marzo 2010, n. 7956, in *DeJure* che, pur non vertendo sulla materia degli utilizzi fraudolenti degli strumenti di pagamento, ha svolto delle considerazioni generali che possono attagliarsi anche a tali fattispecie: «Pur non potendosi, ovviamente, pretendere che l'istituto di credito col quale una società abbia rapporti di conto corrente si trasformi nel controllore esterno della regolarità delle operazioni compiute dall'amministratore di detta società, è difficilmente contestabile che rientri nei doveri di esecuzione di buona fede gravanti sul mandatario (e quindi sulla banca alla quale la società abbia affidato i propri depositi stipulando una convenzione di assegno) il rifiuto di operazioni *ictu oculi* anomale, quando esse siano tali da compromettere palesemente l'interesse della correntista». Significativa è, a nostro avviso, l'affermazione della Cassazione secondo la quale rientrerebbe tra i doveri della banca quello di rifiutarsi di eseguire quelle operazioni che appaiano *ictu oculi* anomale e tali da poter compromettere l'interesse del cliente.

[34] Di questo avviso è, ad esempio, ABF, Coll. Milano, decisione 13 aprile 2015, n. 2817 «Ciò chiarito, non può sottacersi un rilevante aspetto di criticità della fattispecie al vaglio di questo Collegio, e cioè che nel giro di qualche giorno sono state compiute svariate operazioni per un rilevante importo complessivo, assolutamente non in linea con un'operatività 'fisiologica'; ciò induce a considerare 'anomale' tali operazioni per frequenza e tipologia. Di ciò avrebbe dovuto avvedersi l'intermediario, non certo monitorando direttamente ogni singola operazione, ma predisponendo sistemi automatici di blocco delle operazioni da postazione remota in presenza di comportamenti decisamente non in linea con l'operatività corrente del proprio cliente. Ciò, nel caso di specie, non è avvenuto e, di conseguenza, l'intermediario che non abbia predisposto idonei strumenti per evidenziare e/o bloccare automaticamente comportamenti che siano evidentemente anomali, non può andare esente da responsabilità». In senso analogo si veda ABF, Coll. Napoli, decisione 14 gennaio 2013, n. 311.

diligenza particolarmente qualificata dell'accorto banchiere, sia tenuto a rilevare l'anomalia delle operazioni effettuate sul conto del cliente a mezzo dello strumento di pagamento e a rifiutarsi di dare corso alle stesse fintantoché non abbia accertato, tramite opportune verifiche, la loro genuinità.

Si tratta di un orientamento, questo, che – va detto per inciso – presta il fianco ad alcune critiche: in primo luogo, perché non si rinviene alcuna espressa disposizione normativa che imponga all'intermediario l'obbligo di costante monitoraggio sulle operazioni di pagamento effettuate dai clienti[35]; e, infatti, il fondamento di un tale obbligo viene individuato o nel dovere generale di comportarsi secondo buona fede, o nel carattere particolarmente qualificato della diligenza cui è tenuta la banca nell'assolvimento dei propri obblighi verso la clientela[36], o, infine, nel dovere di diligenza del mandatario[37].

A prescindere comunque dalle difficoltà nel rinvenire il fondamento giuridico di tale obbligo, ciò che desta maggiori perplessità è se sia esigibile dalla banca, sul piano tecnico ed economico, un monitoraggio così capillare sulle movimentazioni registrate sui conti corrente dei clienti, tenuto conto della miriade di flussi elettronici che affluiscono

[35] Come rileva Trib. Verona, 2 ottobre 2012, cit. «L'attrice, infatti, ha preteso di addossare alla filiale della società convenuta, ove aveva in essere il rapporto di conto corrente per cui è causa, un obbligo di costante monitoraggio sui movimenti dello stesso, perché solo così l'istituto di credito avrebbe potuto avvedersi della loro entità e frequenza. Tale tipo di controllo, però, non ha nessun fondamento normativo o contrattuale ed, anzi, risulta in contrasto con gli obblighi che la convenuta ha normalmente nei confronti dei propri correntisti che operano regolarmente».

[36] È questa la linea interpretativa sostenuta da ABF, Coll. Napoli, decisione 14 gennaio 2013, n. 311; nonché da ABF, Coll. Milano, decisione 29 aprile 2011, n. 888.

[37] La tesi è sostenuta da D. SCANO, *op. cit*., il quale ha rilevato che nei rapporti tra banca e cliente dovrebbero trovare applicazione le norme in tema di mandato, e, fra queste, in particolare, sia quelle che prevedono in capo al mandatario l'obbligo di comunicare al mandante ogni circostanza rilevante ai fini dello svolgimento del rapporto (artt. 1710 , comma 2, c.c., 1712 c.c., 1713, comma 1, c.c., 1718, comma 3, c.c. e 1732, comma 3, c.c.) che quelle le quali consentono al mandatario di discostarsi dalle istruzioni ricevute dal mandante nel caso in cui «circostanze ignote al mandante, e tali che non possano essergli comunicate in tempo, facciano ragionevolmente ritenere che lo stesso avrebbe dato la sua approvazione» (art. 1711, comma 2, c.c.); da tale insieme di norme l'autore ricava l'esistenza in capo all'intermediario sia dell'obbligo di segnalare al cliente la presenza di operazioni, per entità e frequenza, non in linea con la sua operatività storica, sia di rifiutarsi di eseguire le suddette operazioni se non dopo aver compiuto gli opportuni controlli.

ogni giorno ai sistemi informatici delle banche, peraltro anche al di fuori dei normali orari d'ufficio[38].

I Collegi ABF ritengono che un simile controllo sia realizzabile e quindi esigibile dall'intermediario, «non certo monitorando direttamente ogni singola operazione, ma predisponendo sistemi automatici di blocco delle operazioni da postazione remota in presenza di comportamenti decisamente non in linea con l'operatività corrente del proprio cliente»[39].

Il problema, allora, come è evidente, si sposta su un terreno che non è più giuridico, ma tecnico, perché si tratta di stabilire se la tecnologia sia in grado di offrire strumenti, funzionanti tutti i giorni 24 ore su 24, atti ad individuare operazioni sospette sulla base di un confronto con l'operatività abituale del cliente.

Ammesso che tali sistemi siano presenti[40] e che non impongano costi esorbitanti agli intermediari, si porrebbe comunque il problema relativo alla loro affidabilità ed efficacia. Come ha giustamente osservato certa

[38] V., ancora, Trib. Verona, 2 ottobre 2012, cit.

[39] In questi termini si è espressa ABF, Coll. Milano, decisione 13 aprile 2015, n. 2817.

[40] A tale quesito pare, comunque, doversi dare risposta affermativa. Una conferma di ciò si rinviene in un interessante provvedimento del Garante per la protezione dei dati personali (*Verifica preliminare. Trattamento di dati personali e biometrici basato sull'analisi comportamentale dei clienti di una banca in occasione della loro navigazione nell'area privata del sito web - 9 giugno 2016*, disponibile online sul sito *web* del Garante www.garanteprivacy.it) in cui la predetta Autorità ha autorizzato un intermediario ad utilizzare, al fine proteggere la propria clientela da accessi indebiti, un particolare e sofisticato *software* in grado di registrare i comportamenti tenuti dai clienti durante la loro navigazione nell'area privata del proprio sito *web*, allo scopo di creare per ogni utente (nel corso di più sessioni di utilizzo) un "profilo" comportamentale unico e non riproducibile. Per la creazione di ciascun profilo comportamentale, infatti, il *software* avrebbe utilizzato una serie di dati, in parte riferibili alla persona dell'utente – quali le attività del mouse o del dito; la pressione sullo schermo e/o sui tasti; la velocità di digitazione della tastiera; l'orientamento del *device* – e in parte relativi all'apparecchio utilizzato dallo stesso – la lingua del sistema operativo; taluni parametri del *browser* (versione; *plug-in* installati; *time-zone*; ecc.) – di difficile o quasi impossibile imitazione da parte di terzi. Ad ogni accesso dell'utente alla propria pagina home banking il *software* in oggetto avrebbe confrontato i dati succitati con il comportamento tenuto in concreto dal cliente: nel caso di evidenti scostamenti dal profilo comportamentale storico, il sistema avrebbe inviato una segnalazione all'intermediario per avviare le opportune iniziative di mitigazione del rischio di frode.

dottrina[41], infatti,è ragionevole ipotizzare che anche l'adozione di tali strumenti possa dare luogo a situazioni indesiderate quali, ad esempio, un'operazione fraudolenta non riconosciuta come tale, ovvero, all'opposto, il blocco di una transazione autentica, ma considerata, per errore, anomala dall'algoritmo di controllo[42].

4.4. *Il riparto dell'onere della prova*

Dopo aver esaminato gli obblighi di comportamento del prestatore e dell'utente dei servizi di pagamento, occorre ora affrontare il tema della distribuzione dell'onere probatorio tra le parti nell'ipotesi in cui il secondo disconosca un'operazione di pagamento.

Va subito precisato che è proprio in quest'ambito che la disciplina dei servizi di pagamento esprime il massimo *favor* verso l'utente: questi, infatti, ai sensi dell'art. 10 del d.lgs. n. 11/2010, non deve fare altro che contestare la abusiva utilizzazione dello strumento di pagamento, non essendo tenuto a provare di aver adeguatamente custodito i propri codici di accesso[43]; mentre è sull'intermediario che ricade, *ex* artt. 10 e 12 del citato decreto, l'onere di provare l'inadempimento doloso o gravemente colposo del cliente, con l'importante precisazione che tale prova non può essere ricavata dalla "regolarità formale" delle operazioni (ossia dalla circostanza che nei sistemi informatici dell'intermediario la transazione risulta disposta mediante il corretto utilizzo delle credenziali di accesso)[44].

---

[41] R. FRAU, Home banking, phishing *e responsabilità civile della banca*, cit.

[42] Ivi, par.7, ove viene fatto l'esempio, suscettibile di verificarsi con frequenza nella prassi, dell'operazione posta in essere per la prima volta in favore di un soggetto estero sconosciuto.

[43] Anche i Collegi ABF hanno sottolineato, più volte, la disparità di posizioni che tale regime dell'onere della prova comporta in favore dell'utenza bancaria: «la disciplina in esame istituisce un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta è stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema.». In questi termini si è espresso il Collegio di Coordinamento ABF nella più volte citata decisione n. 8553/2019.

[44] Ciò in virtù del già citato art. 10, comma 2, d.lgs. n. 11/2010: «Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento

A fronte di un onere probatorio così rigoroso, perché avente ad oggetto un fatto, ossia la condotta negligente dell'utente, appartenente alla personale sfera di cognizione e di controllo di quest'ultimo, non sorprende che tanto la giurisprudenza quanto la dottrina si siano sforzate di individuare dei "correttivi" volti ad agevolare la prova, da parte della banca, del dolo o della colpa grave della controparte.

La giurisprudenza, soprattutto dell'ABF[45], ha così riconosciuto agli intermediari la facoltà di provare la colpa grave del cliente per mezzo di presunzioni gravi, precise e concordanti *ex* art. 2729 c.c.[46] e, in particolare, come già si diceva, di limitarsi a provare di aver adottato efficaci misure di sicurezza volte a prevenire illegittime intromissioni da parte di terzi (*i.e*. sistemi di autenticazione "forte").

In dottrina, tra le posizioni più accreditate si segnala anzitutto quelle di chi, come l'ABF, propone di considerare assolto l'onere probatorio da parte dell'intermediario il quale dimostri di aver adottato le misure di sicurezza più idonee, ritenendo altrimenti praticamente impossibile provare la condotta negligente dell'utente[47].

---

eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7. È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente».

[45] Che l'ABF si sia occupato di questa materia molto più spesso dei giudici ordinari non stupisce, se si considera che le controversie concernenti l'uso di strumenti di pagamento hanno generalmente un valore economico modesto tale da non giustificare, per la maggior parte degli utenti, gli oneri e i costi di un giudizio ordinario.

[46] V. ABF, Coll. Coord., decisione 17 ottobre 2013, n. 5304.

[47] A. BISSI, *Responsabilità della banca per indebita esecuzione di operazioni su conto corrente mediante il servizio telematico di home banking*, in *Ridare.it*, 13 giugno 2018, che svolge la seguente rilevante considerazione «In capo alla banca, ad avviso di chi scrive, dovrebbe rimanere l'obbligo di provare di avere adottato idonee misure, anche di natura tecnica, necessarie per impedire l'abusivo accesso ad opera di ignoti; apparendo però manifestamente iniquo addossarle l'onere – praticamente impossibile da soddisfare – di comprovare che l'operazione contestata sia effettivamente stata eseguita dal correntista.». Dello stesso tenore le riflessioni di S. MARTINELLI, *op. cit.:* «Una rigorosa richiesta della prova positiva del comportamento tenuto dal cliente parrebbe in effetti eccessivamente gravosa per l'istituto di credito.

Secondo altra più rigorosa dottrina[48], l'utente non potrebbe invece limitarsi ad affermare di non aver autorizzato l'ordine di pagamento, ma dovrebbe anche provare, seppur tramite presunzioni, tale circostanza[49]: ciò anche al fine di scongiurare disconoscimenti pretestuosi delle operazioni di pagamento o vere e proprie frodi ai danni degli intermediari.

Si tratta di un'impostazione, questa, apprezzabile e innovativa se si tiene presente che, il più delle volte, gli intermediari ritengono pacifico che non sia stato il cliente ad autorizzare l'operazione, contestando piuttosto una condotta negligente dello stesso tale da permettere una frode da parte di terzi.

Per dimostrare la non paternità dell'ordine di pagamento[50], il cliente potrebbe allora invocare il carattere anomalo delle transazioni disconosciute (per frequenza, consistenza degli importi, indirizzo IP di provenienza dell'ordine, beneficiari esteri, etc.), ovvero dimostrare di essere stato nell'impossibilità materiale di autorizzare il pagamento (ad es. perché si trovava in una località diversa da quella dove fu eseguito il prelievo presso uno sportello ATM).

Nonostante i pregi, l'impostazione appena descritta complessivamente non convince. Provare di non aver conferito ordini, in relazione all'operazione contestata, risulterebbe infatti eccessivamente gravoso per l'utente, con l'effetto di dissuaderlo dall'utilizzo degli strumenti di pagamento, in contrasto con l'obiettivo dichiarato della PSD2 di favorire la diffusione di strumenti diversi dal

---

Paradossalmente, proprio nell'ipotesi di comportamenti dolosi da parte del cliente, l'istituto potrebbe essere nell'impossibilità di provare specificamente quanto avvenuto.».

[48] D. MAFFEIS, *Ordini di pagamento e investimenti* on line *nella giurisprudenza di merito e nella fonte persuasiva dinamica dell'ABF, in Riv. dir. civ.,* 2013, 1273 ss.

[49] Coerentemente con questa impostazione, tale dottrina propone, allora, di ricostruire il regime dell'onere della prova in questi termini: 1) il cliente nega di aver autorizzato l'operazione di pagamento; 2) la banca può contestare o non contestare tale circostanza; 3) se l'intermediario non contesta, sarà ritenuto pacifico che l'ordine non proviene dal cliente, e si applicheranno le normali regole in tema di onere della prova e quindi il PSP dovrà provare la regolarità formale dell'operazione e l'inosservanza gravemente colposa dal cliente agli obblighi di custodia; 4) se, invece, la banca contesta quanto asserito dal cliente, spetterà a quest'ultimo provare, anche tramite presunzioni, la non paternità dell'operazione.

[50] D. MAFFEIS, *op. cit.,* par. 5, si limita ad osservare che nella generalità delle ipotesi il cliente proverà che l'ordine non proviene da sé tramite presunzioni.

contante[51]; mentre si ritiene che la prassi degli intermediari di richiedere ai propri clienti di denunciare l'operazione fraudolenta all'autorità giudiziaria prima di presentare la richiesta di rimborso sia già sufficiente per disincentivare, nella maggior parte delle ipotesi, condotte fraudolente degli utenti[52].

In conclusione, appare quindi più condivisibile la soluzione proposta da parte di alcuni Collegi ABF[53] secondo cui «l'adozione da parte dell'intermediario di valide ed efficaci misure di sicurezza di tutela degli interessi dell'utilizzatore (n.d.r. ossia l'utilizzo di un sistema di sicurezza "a due fattori") […] vale sicuramente ad elevare in modo significativo il livello delle allegazioni richieste al cliente, al fine di rendere adeguatamente verosimigliante il carattere fraudolento dell'operazione».

5. *La nozione di colpa grave nella giurisprudenza dell'ABF in relazione alle truffe informatiche*

Dopo aver illustrato gli obblighi di comportamento gravanti sull'utente e sull'intermediario, approfondendo il profilo del riparto dell'onere probatorio tra le parti, si possono ora esaminare gli orientamenti giurisprudenziali precedenti alla decisione del Collegio di Coordinamento che si annota. Per apprezzare la portata innovativa di quest'ultima, occorre infatti ricordare quali comportamenti dell'utente integravano, secondo i Collegi territoriali dell'ABF, gli estremi della colpa grave *ex* art. 12 d.lgs. n. 11/2010, e sulla base di quali allegazioni degli intermediari.

Per condurre questa indagine occorre fin da subito evidenziare che il parametro di colpa grave a cui i Collegi territoriali facevano in passato riferimento è quello, già definito dalla Cassazione[54], di una colpa grave

[51] Per un commento sulla PSD2 si rinvia ai riferimenti bibliografici indicati alla nota 14.

[52] Proprio per proteggersi da possibili comportamenti truffaldini, gli intermediari chiedono ai clienti che vogliano disconoscere un'operazione di pagamento di allegare copia della denuncia (di truffa o furto) presentata alle autorità competenti, confidando nell'effetto deterrente della sanzione penale prevista dall'art. 367 c.p. per la simulazione di reato.

[53] Cfr. *ex multis*, ABF, Coll. Napoli, decisione 27 marzo 2013, n. 1721.

[54] V. Cass., 19 novembre 2001, n. 14456 e Cass., 13 ottobre 2009, n. 21679, entrambe disponibili sulla banca dati Leggi d' Italia.

consistente in una «straordinaria e inescusabile imprudenza, negligenza o imperizia, che si verifica in conseguenza della violazione non solo della diligenza ordinaria del buon padre di famiglia di cui all'art. 1176, 1° comma, c.c.» – vale a dire di una persona di media avvedutezza e accortezza, consapevole dei propri impegni e delle relative responsabilità – ma anche di «quel grado minimo ed elementare di diligenza generalmente osservato da tutti»: non dunque ogni contegno imprudente può far ritenere integrato questo grado di colpa, ma solo quello che appaia abnorme ed inescusabile.[55]

Tale nozione di colpa grave è stata variamente declinata nel contesto delle diverse tipologie di frodi informatiche, dando vita ad almeno tre filoni di decisioni ricorrenti: (*a*) quelle riguardanti i casi riconducibili ai c.d. *phishing attacks*; (*b*) le aggressioni informatiche operate attraverso un *malware*; (*c*) i casi, già richiamati, di cosiddetto ignoto tecnologico, che sono oggetto della decisione annotata.

a) *Phishing attacks*

Sono riconducibili alla prima categoria tutte le frodi poste in essere mediante induzione del titolare dello strumento di pagamento a fornire dati o informazioni personali, come le credenziali per accedere ai servizi bancari *online*, adducendo falsamente l'esistenza di tentativi di accesso abusivo o più in generale l'opportunità di verificare o implementare caratteristiche di sicurezza. Se tradizionalmente il *phishing*[56] comporta l'invio di una *e-mail* "civetta", può presentarsi anche tramite l'invio di SMS (c.d. *SMShing*) o l'effettuazione di chiamate vocali (c.d. *vishing*).

In casi come questi l'orientamento consolidato dei Collegi era quello di respingere la richiesta di rimborso del cliente, considerandolo vittima

[55] Così ABF, Coll. Coord., n. 5304/2013, cit.

[56] Sul *phishing* cfr. R. FRAU, *Sottrazione di credenziali informatiche, bonifici non autorizzati e responsabilità civile della banca da trattamento di dati personali*, cit.; A. SALOMONI, *op. cit*.; G. SATTA, Phishing: *la banca deve rimborsare il correntista truffato*, in *Diritto & Giustizia*, 2018, 13 ss.; 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*, 2015, 61 ss.; B. RUSSO, *I nuovi orientamenti giurisprudenziali sul reato di* phishing: *"La banca è responsabile se non prova che il cliente ha disposto il pagamento"*, in questa *Rivista*, 2019, 71 ss.

di una credulità colpevole e inescusabile, in ragione del fatto che si tratta di tecniche di frode ormai note a tutti[57] e, quindi, facilmente evitabili con un minimo di diligenza e prudenza[58].

La posizione dei Collegi appare sul punto condivisibile, per quanto severa, poiché orientata a ritenere gravemente colposa la condotta del ricorrente a prescindere dalla maggiore o minore verosimiglianza del messaggio ingannatorio[59]. La prova di un episodio di *phishing* è, ad ogni modo, sempre di natura confessoria, ricavandosi dalle dichiarazioni rese dal cliente, in sede di denuncia o nel ricorso, che

[57] Perfino ai meno esperti, anche per la campagna di informazione che i media e gli intermediari hanno da tempo attuato.

[58] Tra le moltissime v. ABF, Coll. Roma, decisione 11 luglio 2019, n. 16954; ABF, Coll. Roma, decisione 12 luglio 2019, n. 17174; ABF, Coll. Palermo, decisione 25 luglio 2019, n. 18449; ABF, Coll. Roma, decisione 5 aprile 2013, n. 1820; ABF, Coll. Bologna, decisione 16 gennaio 2019, n. 1307; per alcuni casi di *SMShing* si vedano ABF, Coll. Palermo, decisione 17 maggio 2019, n. 12655 e ABF, Coll. Bologna, decisione 28 gennaio 2019, n. 2670.

[59] Salvo qualche limitata eccezione: ad esempio ABF, Coll. Milano, decisione 28 giugno 2019, n. 16005 ha ritenuto non inescusabile la condotta di un cliente che aveva comunicato i propri dati rispondendo ad un *email*, poi rivelatasi fraudolenta, proveniente dal medesimo indirizzo utilizzato dall'intermediario; analogamente ABF, Coll. Roma, decisione 27 dicembre 2011, n. 2850 ha ritenuto che non costituisse di per sé fattore di colpa grave il rispondere ad una richiesta di aggiornamento della *password*, apparentemente proveniente dall'intermediario, dal contenuto altamente verosimile e comparsa in occasione della navigazione sul sito *web* della banca. Occorre poi dare conto di un nuovo indirizzo di pensiero che sta formandosi presso la più recente giurisprudenza dell'Arbitro, caldeggiato specialmente dal Collegio di Bari, tendente a riconoscere, nei casi in cui il ricorrente lamenti di aver ricevuto l'SMS ingannevole dallo stesso indirizzo normalmente adoperato dall'intermediario (c.d. Messaggio SMS *"spoofed"*), una corresponsabilità di quest'ultimo per aver utilizzato «un canale di comunicazione con i clienti suscettibile di essere agevolmente contraffatto o, comunque, idoneo a ingenerare un errore, in utenti non particolarmente esperti, in merito alla genuinità del messaggio» (v. ABF, Coll. Bari, decisione 27 marzo 2020, n. 5836; in senso conforme anche ABF, Coll. Bari, decisione 19 marzo 2020, n. 5135 e ABF, Coll. Roma, decisione 29 gennaio 2020, n. 1364).

Si tratta, però, di una linea di pensiero troppo recente per poter parlare di un *revirement* dell'Arbitro in materia di *phishing*; senza contare poi che essa non incontra il favore di gran parte dei Collegi territoriali (cfr. ABF, Coll. Bologna, decisione 16 aprile 2020, n. 7106; ABF, Coll. Bologna, decisione 16 aprile 2020, n. 7048; ABF, Coll. Roma, decisione 29 gennaio 2020, n. 1390; ABF, Coll. Napoli, decisione 8 gennaio 2020, n. 130; ABF, Coll. Torino, decisione 12 febbraio 2020, n. 2190).

ammette di aver "abboccato" a un messaggio apparentemente riconducibile all'intermediario.

b) *Malware attacks*

Il secondo gruppo di fattispecie, come anticipato, ricomprende quelle tipologie di frodi informatiche che si basano sull'utilizzo di *software* malevoli (c.d. *malware*), in grado di installarsi silenziosamente (senza creare cioè malfunzionamenti o rallentamenti) sulla postazione elettronica dell'utente e di generare, nel momento in cui la vittima si collega al proprio *home banking*, pagine-video perfettamente identiche a quelle dell'intermediario[60], affinché l'utente, credendo di operare sul sito del PSP, sia indotto a comunicare i fattori di autenticazione e il codice OTP[61].

In questi casi i Collegi erano orientati a escludere la sussistenza di un comportamento gravemente colposo del cliente, considerandolo piuttosto una vittima di un raggiro perpetrato con strumenti tecnologici tanto sofisticati da imbrogliare anche il soggetto più accorto[62].

---

[60] Si tratta del fenomeno del *man-in-the-browser*, che si verifica attraverso l'interposizione fraudolenta di ignoti nella fase di dialogo fra il computer impiegato dall'utente e i sistemi di ricevimento della banca.

[61] Sui meccanismi di funzionamento dei codici malevoli, (c.d. *trojan banking*) utilizzati per carpire le credenziali di accesso ai servizi bancari *on line* v. F. CALISAI, *op. cit.*

[62] Lo ha affermato, da principio, il Collegio di Coordinamento ABF nell'importantissima decisione 26 ottobre 2012, n. 3498 del di cui si riportano alcuni passaggi significativi «Non appare ragionevolmente ravvisabile, in siffatto contesto, alcun elemento tale da poter riqualificare siccome colposa, e tanto meno siccome gravemente colposa (ai fini di cui all'art. 12 comma 2° d. lgs. cit.), la condotta dell'utilizzatore del servizio. Per quanto non possa negarsi che il cliente sia caduto nella tagliola ed abbia materialmente permesso l'esecuzione dell'operazione fraudolenta cooperandovi involontariamente, non è chi non veda la profonda differenza strutturale fra i dianzi citati metodi 'tradizionali' di phishing e il descritto fenomeno del man-in-the-browser. […] Nel caso che ci occupa, invece, il subdolo meccanismo di aggressione ha luogo attraverso un sofisticato metodo di intrusione caratterizzato 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, posto che l'unica 'differenza' consta, come si è detto, nell'acronimo del protocollo di trasferimento, individuato come un normale 'http' e non già come un 'https' protetto. Ma va da sé che una simile variazione, che compare solo nella stringa di intestazione della video

Rispetto a tali fattispecie l'indirizzo prevalente dell'ABF appare fin troppo largheggiante, perché tende a non chiedere ai ricorrenti di provare di aver installato efficaci sistemi *antivirus* e *antispam*[63], non prendendo in considerazione la possibilità che il cliente possa aver omesso di proteggersi adeguatamente con appositi *software*. Molti dei programmi malevoli adoperati per queste tipologie di frodi sono, d'altronde, in grado di aggirare i più diffusi sistemi di protezione, sicché la cautela richiesta al cliente sarebbe, oltre che «obiettivamente inesigibile», forse anche «inutile»[64], risultando impossibile una "disinfestazione" di tutte le postazioni informatiche tramite le quali si effettuano operazioni di pagamento *online*[65].

---

schermata mischiata ad almeno cinquanta o sessanta ulteriori caratteri, barre e altri segni di punteggiatura informatica, sfugge normalmente all'attenzione di chiunque si accosti ad una pagina della rete e più che mai sfugge a chi si accosti alla pagina di un sito bancario per compiere un'operazione, dunque in un momento in cui l'attenzione dell'utente è concentrata sul contenuto della schermata e non certo sugli incomprensibili codici che la circondano e che fanno parte del normale apparato di contorno anche delle innocue consultazioni in rete». Sulla scia di questa decisione, i Collegi dell'Arbitro hanno immancabilmente escluso la responsabilità dei clienti nel caso di attacchi condotti tramite *malware:* cfr. tra le molte, ABF, Coll. Milano, decisione 31 gennaio 2019, n. 3119; ABF, Coll. Napoli, decisione 22 settembre 2016, n. 8206; ABF, Coll. Milano, decisione 10 ottobre 2013, n. 5093; ABF, Coll. Milano, decisione 5 marzo 2014, n. 1304; ABF, Coll. Roma, decisione 23 gennaio 2015, n. 511.

[63] Si riscontrano però alcune decisioni controcorrente: ad. es. ABF, Coll. Roma, decisione 12 giugno 2017, n. 6517 ha ritenuto che «La questione della costante e puntuale verifica dell'immunità del proprio sistema da attacchi tramite virus, più o meno insidiosi, non può infatti formare oggetto di identica valutazione, se l'aggressione colpisce il PC di una persona fisica, la quale agisce per scopi estranei alla sua attività, ovvero – come nella specie – un componente del sistema informatico di una società, che alle sue dipendenze annovera financo un tecnico specializzato». Non allineata con l'orientamento maggioritario è anche ABF, Coll. Milano, decisione 18 giugno 2014, n. 3815, la quale ha affermato che è onere del cliente garantire in ogni momento la messa in sicurezza dei mezzi di sua proprietà (computer) adoperati per i collegamenti home banking, pena il riconoscimento a suo carico di un addebito di responsabilità.

[64] ABF, Coll. Coord., n. 3498/2012, cit.

[65] Emblematiche le osservazioni svolte da ABF, Coll. Roma, decisione 11 settembre 2015, n. 6983 in merito alla eventualità di valorizzare, ai fini di valutare la responsabilità del cliente, la circostanza della mancata adozione da parte del medesimo di adeguati sistemi di protezione anti*malware* «Quanto alla presunta mancanza di sistemi antivirus nel computer della ricorrente, si osserva che la messa a

Dal punto di vista probatorio, l'ABF non richiede al ricorrente, in casi come questi, di produrre una perizia di un tecnico informatico che attesti la presenza del *malware* sull'apparecchio utilizzato per effettuare l'operazione contestata[66], né avrebbe la facoltà di disporre una consulenza tecnica d'ufficio a tale scopo. Si fa riferimento, ancora una volta, alle dichiarazioni rese dal cliente nel ricorso valutando se la dinamica dei fatti, per come descritta, risulta compatibile con il *modus operandi* del virus.

Non si può nascondere che un orientamento siffatto sottende il rischio che utenti in mala fede se ne approfittino per lucrare un indebito "rimborso", presentando ricorsi in cui descrivono attacchi informatici, mai verificatisi, in modo tanto accurato da sembrare verosimili. Ma occorre ricordare che l'opportunismo degli utenti trova un argine, sia pure non assoluto, nella responsabilità penale in cui il ricorrente incorrerebbe per aver simulato un reato, dovendo presentare preventivamente una denuncia prima di rivolgersi all'intermediario.

---

disposizione della clientela di strumenti di pagamento on line presuppone che siano gli intermediari proponenti a predisporre idonei presidi di sicurezza al fine di prevenire intrusioni illecite da parte di terzi, come espressamente sancito dall'art.8 del d.l. n.11/2010, non potendosi ritenere che il relativo onere e i correlati rischi gravino sugli utenti, tanto meno nel caso di consumatori».

[66] Appare sorprendente ABF, Coll. Roma, decisione 4 luglio 2019, n. 16186 la quale ha considerato praticamente irrilevante ai fini della decisione la perizia informatica prodotta da una parte che aveva riscontrato la presenza di un programma malevolo in grado di reindirizzare i collegamenti dell'utente. Più condivisibili appaiono invece le argomentazioni sviluppate da ABF, Coll. Roma, decisione 12 giugno 2017, n. 6517 la quale ha ritenuto di non poter porre a fondamento della propria decisione la relazione informatica prodotta dalla società ricorrente, e attestante la presenza di un *malware* sul pc, poiché redatta da un dipendente della società stessa e quindi di dubbia attendibilità. In un'altra decisione (ABF, Coll. Roma, decisione 28 giugno 2012, n. 2264) l'Arbitro ha, invece, escluso la sussistenza di una colpa grave del cliente proprio sulla base della relazione informatica da questi prodotta che attestava la presenza sul proprio computer di un *malware* avente la funzione di registrare e inviare i codici digitati a terze parti. Interessante anche ABF, Coll. Milano, decisione 24 luglio 2013, n. 3953 in cui la richiesta di rimborso avanzata nei confronti dell'intermediario è stata rigettata in conseguenza della condotta contraddittoria del cliente: il quale nel ricorso aveva asserito di essere rimasto vittima di un attacco a mezzo *malware*, salvo poi, però, produrre una perizia di un tecnico informatico che escludeva la presenza sul computer di programmi atti alla trasmissione fraudolenta di informazioni personali.

c) *Ignoto tecnologico*

La terza categoria di frodi informatiche abbraccia quei casi nei quali, pur in presenza di adeguate misure di sicurezza adottate dall'intermediario, come un sistema di autenticazione "a doppio fattore", e in assenza di evidenti profili di colpa dell'utilizzatore (oltreché di elementi che facciano presumere un'aggressione operata tramite *malware*), si verifica ugualmente una illegittima intrusione da parte di terzi nei sistemi informatici dell'utente[67].

Dopo alcune oscillazioni, come detto, l'ABF si era orientato nel senso di ritenere che la pressoché totale invulnerabilità del sistema a "due fattori" fosse tale da fondare la presunzione di una colpa grave in capo al cliente per non aver custodito adeguatamente le credenziali di accesso allo strumento di pagamento[68]. Il che significa, sul piano pratico, che all'intermediario basterebbe dimostrare che l'operazione contestata è stata disposta da soggetto autenticatosi come titolare, inserendo le credenziali di accesso statiche e il codice OTP, per ritenere il cliente negligente e vincere il ricorso.

È appena il caso di osservare che questa linea interpretativa sembra *prima facie* in contrasto con la lettera dell'art. 10, comma 2, del d.lgs. n. 11/2010, per cui «l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata

[67] Si tratta, senza ombra di dubbio, della fattispecie più problematica non solo sul piano della ricostruzione del fatto – poiché non si riesce a comprendere come si sia verificata l'illegittima intrusione da parte di terzi – ma anche sul piano dell'inquadramento giuridico; è ciò ad onta del fatto che si tratti di una tipologia di ricorso già da tempo nota all'Arbitro. Basti pensare che già il Collegio di Coordinamento ABF nella già menzionata decisione 26 ottobre 2012, n. 3498 rilevava «Ma la fattispecie più problematica si colloca nel mezzo dei due estremi ora evocati, realizzandosi là dove l'intermediario abbia messo a disposizione del cliente i predetti strumentari avanzati, il cliente se ne sia avvalso e nondimeno una fraudolenta intrusione ad opera di terzi sia avvenuta o comunque sia stata denunciata.». Anche il formante dottrinale ha preso da tempo coscienza del problema: «il problema della distribuzione del rischio tra fornitore ed utente, che si riscontra quando l'operazione fraudolenta si sia verificata nonostante l'istituto bancario abbia mantenuto un comportamento virtuoso rispetto allo standard di diligenza dalla stessa esigibile, senza tuttavia che il danno sia addebitabile con certezza ad una negligenza dell'utente (c.d. rischio da ignoto tecnologico)». In questi termini si è espresso A. SALOMONI, *op. cit.*

[68] Cfr. nota n. 8.

dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7».

L'Arbitro ha però osservato che il dato testuale non esclude che, al ricorrere di determinate condizioni (come la particolare affidabilità tecnica dello strumento e l'assenza di ulteriori elementi di anomalia dell'ordine), la corretta autenticazione possa essere apprezzata dal giudicante come prova presuntiva della violazione degli obblighi gravanti sul cliente[69].

Verosimilmente, ciò che ha spinto l'ABF a elaborare questo orientamento è l'esigenza pratica di facilitare l'accertamento da parte dei Collegi della colpevolezza del cliente. A tale riguardo è innegabile che la colpa grave dell'utente, salva l'ipotesi in cui sia lo stesso ad ammettere di aver "abboccato" ad un tentativo di *phishing*, confessando la propria inescusabile negligenza, non costituisce una circostanza agevolmente dimostrabile perché, se da un lato l'inadempimento dipende da circostanze ricadenti nella sola sfera di conoscenza del cliente[70], dall'altro, l'ABF non dispone dei poteri necessari per accertare le modalità con cui si è realizzata la frode.

Ciò premesso, occorre precisare che un tale indirizzo, benché prevalente, non ha riscosso presso i Collegi dell'Arbitro solo opinioni favorevoli. Già prima dell'ordinanza di rimessione del Collegio di Bari prima illustrata[71], si erano levate alcune voci di dissenso. In particolare

[69] Tra le tante, ABF, Coll. Milano, decisione 28 giugno 2019, n. 16027; ABF, Coll. Milano, decisione 27 agosto 2019, n. 19961; ABF, Coll. Milano, decisione 4 luglio 2019, n. 16521; ABF, Coll. Milano, decisione 28 giugno 2019, n. 16026.

[70] È del resto anche sulla base di osservazioni di questo genere che le Sezioni Unite della Corte di Cassazione hanno inteso rimeditare, con la ben nota sentenza 30 ottobre 2001, n. 13533, in *DeJure*, il proprio orientamento in tema di prova dell'inadempimento, stabilendo in generale che il creditore può limitarsi ad allegare l'inadempimento del debitore, su cui grava invece l'onere di provare di avere adempiuto.

[71] Il Collegio di Coordinamento nella già citata decisione 26 ottobre 2012, n. 3498 aveva, ad esempio, nitidamente rappresentato il contrasto interpretativo che si stava delineando all'interno dell'Arbitro Bancario «Secondo il Collegio di Milano, la pressoché totale invulnerabilità del sistema a 'due fattori' garantita dai sistemi OTP appare tale da fondare la presunzione di una colpa grave in capo al cliente, precisamente consistente nel non aver custodito con la dovuta diligenza il dispositivo in questione (cfr., fra le moltissime, Collegio Milano, decc. nn. 2103/2012, 2658/2011, 1462/2012). Detto orientamento è stato, in tempi recenti (cfr. dec.

alcuni Collegi[72] avevano osservato che l'impianto normativo delineato dal d.lgs. n. 11/2010, e la *ratio* di tutela degli utenti cui esso si ispirava, impedivano di fondare una presunzione di colpevolezza a carico dell'utente sulla semplice base dell'adozione da parte dell'intermediario di un sistema di autenticazione con password e OTP. Quest'ultima circostanza avrebbe potuto semmai, ad avviso di questo indirizzo minoritario, indurre i Collegi a valutare con maggior rigore la condotta dell'utente, in punto di custodia dei codici dispositivi, fino a pretendere che il ricorrente allegasse specifiche circostanze di fatto tali da far presumere la presenza di meccanismi di aggressione talmente sofisticati da aggirare persino un sistema di autenticazione "a due fattori" (come quelli basati sull'utilizzo di *malware*), ma giammai avrebbe potuto valere in sé come prova dell'inadempimento del cliente.

6. *Critiche all'orientamento maggioritario dell'ABF in tema di "ignoto tecnologico"*

La critica più convincente all'orientamento in parola è però che, a far gravare sugli utenti il rischio della causa ignota dell'addebito non autorizzato, si tradirebbe la *ratio* del d.lgs. n. 11/2010 che è quella,

1583/2012), non pienamente condiviso dal Collegio di Napoli, il quale, pur ammettendo la spiccata capacità protettiva del sistema OTP, ha escluso l'automatismo deduttivo cui si ispira invece il pensiero del Collegio milanese, per concludere che l'impiego dell'OTP non vale di per sé a lasciar irreversibilmente presumere una negligenza comportamentale del cliente, bensì a indurre l'Arbitro ad una valutazione più rigorosa della sua condotta. Il Collegio di Roma ha, a sua volta, ripreso la lettura dell'Arbitro partenopeo ponendo una speciale enfasi sul principio di diritto ricavabile dalle anzidette norme del d. lgs. cit. La ripartizione dell'onere probatorio, per come delineata nell'impianto normativo, non consentirebbe, secondo l'Arbitro romano, di pervenire all'automatismo affermato dal Collegio di Milano, dovendosi al contrario apprezzare, oltre al meccanismo offerto, anche l'intero sistema di controlli approntato dall'intermediario, e potendosi con ciò concludere che la cattura dei codici ad opera di terzi non autorizzati ben possa avvenire in presenza di un pur diligente comportamento da parte del Cliente (Cfr. Collegio Roma, decc. nn. 2264/2012, 2660/2012, 1910/2012).».

[72] ABF, Coll. Napoli, decisione 27 marzo 2013, n. 1721; ABF, Coll. Napoli, decisione 8 aprile 2014, n. 212; ABF, Coll. Roma, decisioni 28 giugno 2012, n. 2264; 30 luglio 2012, n. 2660 e 6 giugno 2012, n. 1910.

ispirata alla c.d. teoria del rischio di impresa[73], di far ricadere i rischi statisticamente prevedibili legati ad attività oggettivamente "pericolose", riguardanti un'ampia moltitudine di consumatori o utenti, sull'impresa che è in grado, determinando i prezzi di beni e servizi, di addossare alla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi[74].

Secondo questa impostazione, sarebbe equo oltreché economicamente efficiente, anche al fine di promuovere negli utenti la fiducia nell'utilizzo degli strumenti di pagamento elettronici, ricondurre nell'area del rischio professionale del PSP i casi di utilizzo fraudolento degli strumenti di pagamento non riconducibili al dolo o alla colpa del titolare, né a un grave carenza dei presidi di sicurezza predisposti dall'intermediario (il c.d. rischio da ignoto tecnologico, cioè

[73] La tesi del rischio di impresa, elaborata in Italia da P. TRIMARCHI, *Rischio e responsabilità oggettiva*, Milano, 1961, *passim*, per fondare una responsabilità oggettiva extracontrattuale, è stata in seguito applicata anche per imputare una responsabilità oggettiva contrattuale in capo all'imprenditore non negligente, il cui inadempimento sia dovuto al realizzarsi di un rischio associabile alla sua attività di impresa: così L. MENGONI, voce *Responsabilità contrattuale (dir. priv.)*, in *Enc. dir.*, XXXIX, Milano, 1988, 1072 ss., a partire dalle ipotesi *ex* artt. 1693, 1787, 1785, 1839 c.c. in cui l'inadempimento dei contratti tipici non dipende dal grado di diligenza dell'imprenditore, ma da un giudizio sull'inerenza o meno dell'evento causativo dell'inadempimento alla sfera di rischio dell'attività svolta dal debitore, fino al limite del caso fortuito. Più di recente, ha condivisibilmente applicato la teoria del rischio di impresa alla materia dei servizi di pagamento U. MALVAGNA, *Clausola di "riaddebito" e servizi di pagamento. Una ricerca sul rischio d'impresa*, Milano, 2018, su cui si veda *infra* nota 78. In senso critico, per tutti, A. LUMINOSO, *Sulla responsabilità contrattuale ed extracontrattuale dell'impresa*, in *Contr. Impr.*, 2007, 917 ss., considerando non immune da forzature «una generalizzazione delle norme speciali sopra ricordate per indurne l'esistenza di un principio di responsabilità oggettiva valido per l'intero campo delle prestazioni d'impresa». In tema si veda, altresì, F. DEGL'INNOCENTI, *Rischio di impresa e responsabilità civile. La tutela dell'ambiente tra prevenzione e riparazione dei danni*, Firenze, 2013, 27 ss.

[74] Cfr. ABF, Coll. Roma, decisione 2 luglio 2010, n. 665 «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 facilitare e perciò a moltiplicare le transazioni commerciali, nell'interesse delle imprese, degli stessi utenti/consumatori, nonché, ovviamente, delle banche».

l'addebito disconosciuto dal cliente di cui non sia individuabile la causa)[75].

Gli intermediari, insomma, traendo profitto dalla diffusione degli strumenti di pagamento elettronici in termini di «significativi ed evidenti risparmi rispetto ad una tradizionale operatività di sportello»[76], devono sopportare altresì i rischi e i costi che l'utilizzo di tali strumenti inevitabilmente comporta per la collettività[77] (*i.e.* le perdite derivanti dalle operazioni fraudolente)[78].

Tale opzione sarebbe, del resto, razionale ed efficiente anche dal punto di vista giuridico: l'intermediario, infatti, data la sua qualità di operatore professionale dotato di elevate conoscenze tecniche e ampie possibilità economiche, è in grado, molto più che il singolo utente, di valutare la dimensione del rischio al fine non solo di adottare i presidi di sicurezza più evoluti ed efficaci per contenerlo, ma anche per tradurlo in un costo economicamente sostenibile[79] (stipulando ad esempio

[75] Su questa posizione sembra essersi attestato anche il giudice di legittimità: cfr. Cass., 3 febbraio 2017, n. 2950 in *DeJure*.

[76] Lo ha rilevato ABF, Coll. Coord., n. 3498/2012, cit.

[77] Questa idea trova il proprio fondamento nel principio espresso dall'antico brocardo c*uius commoda eius et incommoda,* secondo il quale chi trae profitto da una certa attività o bene deve assumere su di sé anche i relativi oneri. Si veda in argomento F. DEGL'INNOCENTI, *op. cit.*, 29. Ulteriore punto di riferimento teorico di questa prospettazione, è la teoria del rischio-profitto che considera la responsabilità come contropartita del profitto conseguito.

[78] Sembra esprimersi in senso favorevole all'orientamento che pone in capo all'intermediario il rischio dell'addebito non autorizzato dovuto a causa ignota F. CIRAOLO, *Pagamento fraudolento con carta di credito e ripartizione della responsabilità. Dagli orientamenti attuali alla revisione della PSD,* cit. che afferma «[…] l'intermediario deve sopportare le conseguenze negative dell'attività da cui trae utilità economica […]». Chiaramente favorevole all'interpretazione in parola è D. MAFFEIS, *op. cit.*, «[…] il problema dell'ignoto tecnologico, che è, per definizione, a carico dell'impresa».

[79] Analogamente, *mutatis mutandis*, U. MALVAGNA, *Clausola di "riaddebito" e servizi di pagamento. Una ricerca sul rischio d'impresa*, cit., arrivando a dedurre l'invalidità delle pattuizioni con cui i prestatori dei servizi di pagamento si (auto)attribuiscono il diritto di stornare le somme accreditate sui conti correnti degli esercenti convenzionati che abbiano ricevuto il pagamento (ad es. il negoziante presso cui il cliente ha acquistato un bene), in caso di utilizzo fraudolento della carta di credito, di debito o prepagata. Significativo, ai fini del nostro discorso, il passaggio (v. p. 106) in cui l'A. rileva che «il rischio dell'adulterazione del latte inerisce all'impresa casearia, quello della contaminazione del sangue a quella ospedaliera, e

contratti di assicurazione o accantonando le somme necessarie a rimborsare i clienti[80]); senza considerare, peraltro, che tali costi non graverebbero sui prestatori dei servizi di pagamento che potrebbero facilmente trasferirli sul pubblico degli utenti attraverso l'aumento dei

quello dello sciopero dei mezzi di trasporto al vettore», così il rischio di frode inerisce all'attività dell'impresa fornitrice dei servizi di pagamento, che può prevedere e gestire in modo economicamente efficiente un tale rischio (riducendolo,"a monte", mediante un innalzamento dei livelli di sicurezza degli strumenti di pagamento, ovvero attenuando, "a valle", le conseguenze economiche delle frodi sul proprio patrimonio: «direttamente esternalizzando le perdite di cui al fattore di rischio sulla clientela mediante apposite clausole; ovvero distribuendo e "spalmando" il relativo costo nel prezzo del prodotto, se del caso previa assicurazione dal rischio medesimo», cfr. p. 107). Del tutto condivisibile è, dunque, la conclusione per cui il pregiudizio economico della frode incolpevole, cioè il rischio da ignoto tecnologico, dovrebbe gravare, nei rapporti di convenzionamento, sull'intermediario e non già sull'esercente convenzionato: conclusione da noi condivisa relativamente al rapporto bilaterale tra prestatore del servizio e titolare dello strumento di pagamento. Lo stesso P. TRIMARCHI, *Il contratto: inadempimento e rimedi*, Milano, 2010, 7 ss. e 16, aveva affrontato in tempi piuttosto recenti il problema dell'efficiente allocazione dei danni dovuti a cause non ben accertate o accertabili tra i contraenti, ritenendo che, al fine di individuare il soggetto tenuto a sopportare il costo economico del danno "incolpevole", diventa rilevante la valutazione comparativa delle possibilità per le parti di assorbire economicamente il rischio, «la quale dipende in larga, dalla possibilità di prevederlo».

[80] P. TRIMARCHI, *Rischio e responsabilità oggettiva*, cit., *passim.*

prezzi[81] ovvero, nell'ambito dei servizi di pagamento a circuito, tramite apposite clausole contrattuali di esternalizzazione del rischio[82].

Lo scenario che si presenterebbe se si seguisse questo indirizzo interpretativo sarebbe, ad avviso di tali Collegi, decisamente preferibile sul piano economico e sociale, rispetto a quello che si viene a delineare in applicazione dell'orientamento maggioritario. Adottare infatti il rischio di impresa come criterio di imputazione della responsabilità farebbe, infatti, sì che la perdita conseguente all'utilizzo fraudolento venga ridistribuita nel pubblico degli utilizzatori degli strumenti di pagamento, con sacrificio irrilevante per i singoli membri di esso, e che al singolo pagatore, vittima della frode, venga garantito il rimborso degli importi illegittimamente sottratti[83]. Viceversa, consentire all'intermediario di esonerarsi dalla responsabilità sol che soddisfi l'onere di aver adottato un sistema di autenticazione a doppio fattore comporta che la perdita derivante dall'utilizzo fraudolento rimane interamente a carico della sfortuna vittima della frode ingenerando nella totalità della clientela bancaria un senso di sfiducia rispetto all'utilizzo degli strumenti di pagamento.

---

[81] Si vedano in questo senso le osservazioni di R. FRAU, *Home banking, captazione di credenziali di accesso dei clienti tramite* phishing *e responsabilità della banca*, cit. «Per inciso, detta ultima configurazione si rivelerebbe, sul piano economico, non del tutto neutra per la generalità dell'utenza bancaria, sulla quale verrebbe poi a ripartirsi l'onere finale derivante dall'aumento delle tariffe del servizio (al fine di consentire la copertura, anche assicurativa, dei sinistri).». Concorde nel ritenere che gli intermediari frazioneranno i costi sostenuti per fronteggiare il rischio di impresa sulla totalità dei propri clienti attraverso un aumento generalizzato dei prezzi dei propri servizi è I. A. CAGGIANO, *Pagamenti non autorizzati tra responsabilità e restituzioni. una rilettura del d. legisl. 11/2010 e lo scenario delle nuove tecnologie*, cit. «Resta inteso che questo pur agevole criterio di ripartizione delle conseguenze economiche degli utilizzi da parte di terzi, che pure ricade quasi interamente sul gestore dell'infrastruttura, non significa altro che una socializzazione del danno sull'intera collettività degli utenti su scala generale, giacché i prevedibili costi a carico dell'intermediario vengono fatti gravare sulla totalità della clientela bancaria, attraverso il calcolo attuariale e l'inclusione della percentuale così definita nel " prezzo " dei servizi bancari e finanziari".».

[82] Il riferimento corre alle clausole di riaddebito su cui si veda nota 78.

[83] Venendo, peraltro, realizzata in tale maniera una delle funzioni principali che viene tipicamente attribuita alle regole di responsabilità civile ossia quella di garantire una tutela effettiva a chi sia stato ingiustamente danneggiato.

Sulle diverse funzioni di cui è generalmente investita la responsabilità aquiliana cfr. F. DEGL'INNOCENTI, *op. cit.*, 38-39.

Inoltre, si è aggiunto, un regime di responsabilità oggettiva costituirebbe una costante e benefica pressione economica sugli intermediari a ricercare misure sempre più efficaci per limitare la frequenza delle operazioni fraudolente generando, così, un circolo virtuoso in cui la necessità per l'impresa di razionalizzare l'attività, diminuendo i costi, alimenterebbe il progresso tecnologico[84] (sotto forma, in questo caso, di un'implementazione dei presidi di sicurezza degli strumenti di pagamento)[85].

Tali considerazioni, peraltro sostenute da autorevole dottrina, non hanno però, fino a tempi a noi recenti, fatto breccia nella giurisprudenza dell'Arbitro che, al di là di alcuni richiami dal valore più teorico che pratico alla teoria del rischio di impresa, si è attestata nel ritenere che il "rischio da ignoto tecnologico"debba gravare sull'utente.

7. *Segue: ulteriori profili critici*

Ad un'attenta analisi, l'orientamento dell'ABF – fino all'intervento del Coordinamento, maggioritario – che deduce l'esistenza di una condotta colposa del cliente dalla spiccata capacità protettiva del

[84] Viceversa, come osserva U. MALVAGNA, *Clausola di "riaddebito" e servizi di pagamento. Una ricerca sul rischio d'impresa*, cit., 192 « […] l'esonero dell'intermediario dal costo economico derivante dalla frode opera alla stregua di un rilevante controincentivo agli investimenti volti all'acquisizione di mezzi tecnici di sicurezza più avanzati di quelli esistenti. In effetti, esternalizzato il rischio inerente al prodotto sul cliente, ogni logica di migliore efficienza, *sub specie* del generale incremento della qualità del servizio, risulta contraddetta e negata.».

[85] P. TRIMARCHI, *Rischio e responsabilità oggettiva*, cit., 36 «[…] la attribuzione all'imprenditore del rischio di impresa che costituisce una pressione economica perché sia razionalizzata (dal punto di vista sociale) la produzione; il che potrà avvenire, secondo i casi, mediante l'adozione di misure supplementari di sicurezza, mediante la sostituzione del metodo di produzione e, nei casi estremi, mediante l'abolizione di un settore marginale di impresa o con la chiusura dell'impresa stessa.». Quest'ultima circostanza condurrebbe, poi, ad un' ulteriore conseguenza positiva a livello di efficienza del mercato, ossia all'eliminazione dallo stesso degli operatori meno capaci: vuoi perché non in grado di garantire ai propri utenti le misure di sicurezza più evolute (e quindi estromessi dalle preferenze della clientela bancaria perché considerati operatori poco sicuri) vuoi perché non in grado di gestire in modo economicamente razionale i costi sostenuti per adottare le misure di contenimento del rischio di impresa (e quindi eliminati dal mercato perché incapaci di tradurre correttamente tale rischio in un costo e di ripartirlo poi sulla propria clientela).

sistema di autenticazione a "due fattori" presta il fianco ad ulteriori critiche.

In primo luogo, si ravvisa un'incoerenza interna alla giurisprudenza dell'Arbitro che, in settori diversi da quello delle truffe telematiche, ammette presunzioni in modo molto più limitato: così nel caso di furto di carte dotate di *microchip*, che pure garantiscono un elevato standard di sicurezza. Secondo l'opinione consolidata dell'Arbitro, non sarebbe, infatti, possibile desumere che l'utente conservasse il PIN insieme alla carta di pagamento, se non nel caso in cui sia trascorso un ridottissimo lasso temporale tra il furto della carta e il verificarsi dell'operazione fraudolenta[86] (per il Collegio di Milano di appena 15 minuti)[87]; e ciò ad onta del fatto che autorevoli studi scientifici abbiano dimostrato che non sia possibile estrarre il PIN dalle carte dotate di *chip* se non in tempi molto lunghi (in media diverse ore) e con l'ausilio di apparecchiature sofisticate e costose[88]. A nostro giudizio, allo stato attuale della tecnica,

[86] La giurisprudenza dell'Arbitro sull'argomento è vastissima: tra le tantissime v. ABF, Coll. Bologna, decisione 20 agosto 2019, n. 19638; ABF, Coll. Roma, decisione 11 luglio 2019, n. 17037; ABF, Coll. Milano, decisione 4 luglio 2019, n. 16533; ABF, Coll. Milano, decisione 4 luglio 2019, n. 16422; ABF, Coll. Palermo, decisione 24 giugno 2019, n. 15483; ABF, Coll. Napoli, decisione 7 ottobre 2013, n. 5072.

[87] Secondo il Collegio di Milano, infatti, se l'operazione contestata risulta essere effettuata in un intervallo di tempo minore di 15 minuti rispetto all'orario del furto indicato dal cliente nella denuncia, allora si può presumere che il PIN della carta fosse conservato insieme a quest'ultima; viceversa nel caso in cui tale arco di tempo superi i 15 minuti la suddetta presunzione non potrebbe operare. Tra le più recenti v. ABF, Coll. Milano, decisione 6 febbraio 2020, n. 1820.

[88] Ci riferiamo al noto studio scientifico condotto nel 2013 dal Politecnico di Torino per analizzare da un punto di vista scientifico la sicurezza logica e fisica della carte dei circuiti BANCOMAT e PagoBANCOMAT, disponibile online all'indirizzo https://bancomat.it/sites/default/files/Lioy_consulenza_BM_20131025.pdf . Il predetto istituto di ricerca è pervenuto alle seguenti conclusioni: (1) «la clonazione di un chip non è possibile con procedure software mentre e possibile con un processo hardware ma esso richiede tempi e costi molto elevati, rendendo ` l'attacco più teorico che pratico: a meno che il titolare non si accorga del furto della carta, sicuramente la denuncia del furto (e quindi il blocco della carta) avverrà prima che gli attaccanti abbiano ` potuto duplicarne il chip»;

(2) «l'uso di una carta Bancomat a chip senza conoscerne il PIN non e` possibile», né è possibile estrarre il PIN dal chip della carta tramite software;

(3) «nonostante sia facile copiare e duplicare la banda magnetica di una carta ` – non e possibile in alcun modo estrarre dalla banda stessa il PIN, perché ` e esso non ´ e presente tra i ` dati registrati nella banda magnetica»;

sarebbe ragionevole e in linea con l'indirizzo adottato in tema di frodi informatiche escludere un comportamento malaccorto del cliente, consistente nell'aver conservato il PIN insieme alla carta, soltanto quando siano trascorse diverse ore tra il furto della carta e l'utilizzo indebito della stessa[89].

In secondo luogo, più in generale, non convincono più di tanto i raffinati tentativi dell'Arbitro di argomentare la compatibilità tra il proprio orientamento dominante e la lettera dell'art. 10, comma 2, del d.lgs. n. 11/2010[90]. In applicazione dello stesso, agli intermediari viene

4) gli attacchi di *power analysis* e *Null PIN* (su cui vedi pp. 11-14 della Relazione) non pongono alcun pericolo all'operatività delle carte Bancomat;

5) è possibile, invece, intercettare il PIN mentre viene trasmesso al verificatore per controllarne la correttezza o tramite sovra-tastiere applicate sul terminale manomesso; o tramite micro-telecamere appositamente posizionate per osservare il PIN introdotto; o manomettendo il POS introducendo al suo interno una sottile lamina (detta "*shim"*) che permette di leggere il PIN. Peraltro, l'acquisizione del PIN tramite una delle predette modalità deve necessariamente essere seguita dal furto della carta altrimenti la conoscenza del codice risulta inutile. Inoltre, esaminando i log delle transazioni (presso il relativo Centro Servizi) è possibile sapere su quali terminali o POS è stata usata la carta e quindi esaminarli per verificarne l'integrità o la manomissione.

Stando quindi al succitato lavoro del Politecnico di Torino una volta che il ladro sia entrato in possesso di una carta a chip, per poterla poi utilizzare dovrebbe disporre di un laboratorio molto sofisticato (chimico ed elettronico) oltreché costoso, e di tempi molto lunghi (parecchie ore o giorni) per poter estrarre il PIN dallo strumento di pagamento*;* lo stesso tipo di laboratorio (e quindi gli stessi tempi e costi) sarebbe necessario nel caso si cercasse di clonare una carta a chip.

[89] A meno che sussistano circostanze tali da far supporre l'esistenza di una differente modalità di captazione dei codici, quali ad esempio manomissioni o malfunzionamenti dei terminali da cui risultano essere stati effettuati i prelievi fraudolenti.

[90] Come rileva, tra gli interpreti, anche A. SALOMONI, *op. cit.,* «A tal proposito, va osservato che il d. legis. n. 11/2010 sceglie di allocare il rischio della causa ignota dell'addebito non autorizzato in capo al fornitore. ». Anche *S. Toscano, Abuso dei mezzi di pagamento: questioni irrisolte,* disponibile online sul sito https://fchub.it/abuso-dei-mezzi-di-pagamento-questioni-irrisolte/ osserva che la presunzione stabilita dal'Arbitro fra uso, da parte dell'intermediario, di sistemi di autenticazione a due fattori e prova della colpa grave del cliente «appare in distonia rispetto quanto meno alla *ratio*, ma forse anche alla lettera, dalla normativa speciale che regola le fattispecie indagate. Ed infatti, la normazione in parola appare chiaramente volta ad imputare in misura maggiore al prestatore il rischio connesso allo svolgimento di attività fraudolente in danno dell'utilizzatore, e ciò al fine precipuo di promuovere la fiducia degli utenti nell'utilizzo dei mezzi di pagamento

infatti consentito di provare la colpa grave del ricorrente semplicemente producendo i "log" dell'operazione contestata da cui risulta l'avvenuta autenticazione a due fattori, mentre la legge richiederebbe, come sopra si è evidenziato, non solo di allegare le evidenze informatiche della transazione, ma anche ulteriori elementi di fatto idonei ad integrare la colpa grave dell'utilizzatore.

8. *La Decisione del Collegio di Coordinamento*

Una volta rappresentato il quadro giurisprudenziale preesistente e le ragioni che hanno indotto il Collegio di Bari a richiedere l'intervento chiarificatore del Coordinamento, si può procedere ora ad esaminare i principi di diritto espressi da quest'ultimo nella decisione n. 22745 del 10 ottobre 2019.

Come anticipato, la questione di natura processuale posta al Coordinamento – consistente nello stabilire se compete ai Collegi ABF accertare il dolo o la colpa grave del cliente «anche in assenza di una specifica allegazione dell'intermediario, sulla base delle circostanze risultanti dalla documentazione in atti ovvero dalle dichiarazioni rese dalle parti» – non solleva particolari problemi. E, infatti, è stata risolta nel modo più ovvio, vale a dire mediante il riconoscimento di un tale potere di accertamento[91]: ne esce così intatta, come era auspicabile, la capacità decisionale dell'ABF, che una risposta di segno diverso avrebbe, invece, potuto compromettere.

La questione più problematica che il Collegio di Coordinamento si trova ad affrontare è quella di chiarire se il Collegio possa desumere la

elettronici, politica questa ritenuta strategica per lo sviluppo dell'economia nonché per il controllo del flusso dei pagamenti».

[91] Con delle limitate eccezioni: secondo il Coordinamento, infatti, i Collegi ABF non potrebbero rilevare d'ufficio la colpa grave del cliente – benché palesemente emergente dal complessivo materiale probatorio – sia nel caso di mancata costituzione dell'intermediario in giudizio che in quello in cui quest'ultimo, pur costituendosi, non abbia prodotto i log dell'operazione contestata. Secondo questa impostazione, pertanto, un cliente che dichiarasse nel ricorso di essere rimasto vittima di *phishing*, ammettendo così di aver tenuto un comportamento gravemente negligente, potrebbe ugualmente vedere accolta la propria istanza di rimborso sia nell'ipotesi di mancata costituzione in giudizio dell'intermediario che in quella di assenza delle evidenze informatiche.

sussistenza del dolo o della colpa grave del cliente dalla prova, fornita dall'intermediario, della mera "regolarità formale" dell'operazione di pagamento, nei termini visti. Ed proprio nel risolvere tale questione che il Coordinamento attira la nostra attenzione, perché enuncia un innovativo principio di diritto, che sconfessa l'orientamento dominante, riconoscendo finalmente che il più volte citato art. 10, comma 2, del d.lgs. n. 11/2010 «va interpretato nel senso che la produzione documentale volta a provare l'"autenticazione" e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente».

Alla luce di questi rilievi il giudicante risolve in senso positivo anche la terza ed ultima questione interpretativa postagli dall'ordinanza di rimessione, vale a dire se i Collegi ABF, a fronte di un intermediario che si sia limitato a dimostrare la regolarità formale dell'operazione contestata traendo da ciò la prova della colpa grave dell'utente, senza tuttavia fornire ulteriori elementi di prova, debbano ritenere non assolto l'onere probatorio di cui all'art. 10, comma 2 d.lgs. n. 11/2010 e conseguentemente accogliere l'istanza di rimborso del ricorrente.

Si supera così l'idea, che prima avevamo criticato, di una colpa grave in *re ipsa*, imputabile all'utente per difettosa custodia dei dispositivi di accesso in ragione del solo fatto che l'operazione contestata risulta regolarmente disposta mediante un sistema di autorizzazione a "due fattori", mentre resta impregiudicata l'eventualità che le credenziali dell'utente «siano state apposte da un hacker o effettivamente dal cliente».

Aderendo alle argomentazioni svolte nell'ordinanza di rimessione, il Coordinamento critica l'indirizzo in passato prevalente tra i Collegi territoriali ritenendolo non in linea con il regime dell'onere della prova stabilito dall'art. 10, comma 2 del d.lgs. n. 11/2010, che tende a limitare, come si è visto, l'efficacia probante della regolare autenticazione delle operazioni. Si esclude, insomma, che dalla prova della regolare autenticazione si possa desumere automaticamente la sussistenza della colpa grave. Il che, sottolinea il Coordinamento, è del resto incoerente con la *ratio* di fondo della disciplina dei servizi di pagamento, che è quella di istituire un «regime di speciale protezione e

di altrettanto speciale *favor* probatorio a beneficio degli utilizzatori». Si coglie così, tra le righe, il richiamo alla teoria del rischio di impresa a cui prima facevamo riferimento, e dunque alla necessità di allocare in capo all'intermediario, anziché in capo all'utente, il rischio del danno "da ignoto tecnologico".

A livello teorico le argomentazioni del Coordinamento sono senz'altro condivisibili e coincidono con la ricostruzione anche qui accolta. Dal punto di vista applicativo, non si possono d'altra parte obliterare del tutto le oggettive difficoltà che gli intermediari e i Collegi ABF incontrano quando si tratta di provare ovvero accertare la negligenza dell'utente dei servizi di pagamento.

In tal senso, è apprezzabile lo sforzo che il Collegio di Coordinamento fa, in maniera forse troppo succinta, di indicare tre possibili elementi di fatto che gli intermediari potrebbero allegare per assolvere il proprio onere probatorio: «l'assenza di tentativi falliti di digitazione del PIN», «la ricezione della password dinamica tramite cellulare o altro dispositivo del cliente, in assenza di deviazioni o intrusioni nel *device*», «l'accertata assenza di *malware*».

Il primo elemento non è del tutto inedito nel panorama delle decisioni dell'Arbitro, essendo spesso valorizzato dai Collegi per presumere il possesso congiunto del PIN e della carta da parte del cliente in caso di furto della seconda. Ciò in quanto, come si è avuto modo di osservare, la mancanza di tentativi falliti di digitazione del PIN induce a ritenere che il codice era facilmente associabile alla carta. Non è per la verità chiaro se una tale circostanza possa assumere rilievo anche nel caso delle truffe informatiche; ma, considerato anche il contesto in cui la pronuncia si colloca (*i.e.* i pagamenti fraudolenti *online*), la risposta affermativa sembra preferibile.

Il secondo elemento probatorio che il Coordinamento indica – vale a dire la ricezione della password dinamica tramite cellulare o altro dispositivo del cliente – sembra destinato a diventare, stando alla giurisprudenza successiva, la vera e propria "prova regina" in mano agli intermediari per dimostrare la colpa grave del cliente[92]. Con la precisazione che il Coordinamento non si accontenta della semplice prova dell'avvenuto invio, da parte dell'intermediario, del messaggio contenente la OTP al dispositivo del cliente, ma richiede anche la prova

[92] V. *infra* par. 10.

dell'avvenuta ricezione del predetto messaggio; ma fa pure sempre salva la possibilità che il cliente neghi, come nel caso oggetto della pronuncia annotata, di aver ricevuto l'SMS contenente la password dinamica: allegazione, questa, che prevarrebbe sulla documentazione prodotta dall'intermediario da cui risulti l'invio – ma non anche la ricezione – della OTP al dispositivo del ricorrente.

Se gli intermediari non fossero in grado di provare, tramite i propri sistemi informatici, l'avvenuta ricezione del messaggio da parte del ricorrente, non resterebbe allora che ottenere una tale informazione dal gestore dell'utenza telefonica dell'utente, tenendo presente che l'ABF non dispone dei poteri di ordinarne l'esibizione in giudizio.

Il terzo elemento atto a provare la colpa grave del ricorrente non è di immediata intelligibilità, poiché non si comprende, da un lato, se "l'accertata assenza di *malware*" sia da riferirsi all'apparecchio elettronico utilizzato dall'utente o ai sistemi informatici dell'intermediario, dall'altro, se l'onere di provare tale circostanza ricada sul PSP o sul cliente.

Per quanto riguarda la prima questione, è verosimile ritenere, anche basandosi sui precedenti in materia dell'ABF, che la presenza o assenza di un attacco di pirateria informatica sia da riferire al computer dell'utente. In merito invece al secondo aspetto non si può fare a meno di evidenziare che entrambe le soluzioni darebbero luogo ad alcuni inconvenienti: per un verso, porre a carico dell'intermediario l'onere di provare l'assenza di *malware* sulla postazione informatica dell'utente significherebbe richiedere una prova inesigibile poiché l'intermediario non ha, evidentemente, modo di verificare lo stato di sicurezza dei *pc* della propria clientela; d'altro canto, esigere che sia il cliente a dimostrare la presenza (e non già l'assenza) di un *malware* sul proprio computer implicherebbe di chiarire, come si diceva, le modalità per assolvere tale onere: se sia cioè sufficiente la descrizione dell'accaduto operata dal cliente in sede di denuncia e/o ricorso, con il rischio però di agevolare comportamenti fraudolenti, o se invece sia necessario produrre la perizia di un tecnico informatico, con conseguente aggravamento dell'onere a carico dei clienti e rallentamento della procedura (oltre a possibili problemi circa l'attendibilità delle dichiarazioni rese dal tecnico consultato dal cliente).

9. *Segue: l'operatività della franchigia di legge*

Una ulteriore riflessione merita la decisione del Collegio di Coordinamento che si annota, là dove rileva infine che «non può essere accolta la richiesta, formulata dall'intermediario in via subordinata, di applicazione della c.d. "franchigia", in quanto la stessa è prevista in ipotesi di 'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita' (art. 12, co. 3 d.lgs. n. 11/2010)».

Per chiarire la portata di tale affermazione, che suscita a nostro avviso alcune perplessità, occorre richiamare brevemente l'art. 12, comma 1, del d.lgs. n. 11/2010 che, fatta salva l'ipotesi in cui il cliente abbia agito in modo fraudolento, pone ad esclusivo carico dell'intermediario le perdite derivanti dall'utilizzo indebito dello strumento di pagamento intervenuto dopo la comunicazione di smarrimento, furto od uso non autorizzato effettuata dal cliente *ex* art. 7, comma 1, lett. b.

Per quanto riguarda, invece, le perdite derivanti dalle operazioni fraudolente compiute prima della suddetta comunicazione, la normativa distingue: se sussiste dolo o colpa grave del cliente, quest'ultimo sopporta integralmente le perdite; diversamente, l'utente ha diritto a ricevere dall'intermediario il rimborso delle somme sottratte fraudolentemente, al netto però di una franchigia, dell'importo massimo di € 50,00, da applicarsi ove l'utilizzo indebito dello strumento di pagamento sia conseguente al suo furto, smarrimento o appropriazione indebita.

La previsione di una franchigia, che resta a carico del cliente anche in mancanza di un comportamento colposo, risponde al fine – come si legge nel considerando n. 71 della Direttiva (UE) 2015/2366 sui servizi di pagamento – di incentivare l'utente di tali servizi a notificare senza indugio al prestatore «l'eventuale furto o perdita di uno strumento di pagamento e di ridurre pertanto il rischio di operazioni non autorizzate»[93]. Se il PSP viene messo in condizioni di poter bloccare

[93] Lo ha evidenziato anche il Collegio di Coordinamento ABF nella decisione 29 novembre 2013, n. 6168. Sulla funzione della franchigia si veda anche I. A. CAGGIANO, *Pagamenti non autorizzati tra responsabilità e restituzioni. una rilettura del d. legisl. 11/2010 e lo scenario delle nuove tecnologie*, cit. «Il primo correttivo, rappresentato dalla previsione di responsabilità concorrente dell'utilizzatore titolare,

rapidamente lo strumento e di impedirne l'utilizzo da parte di terzi, ciò comporta del resto vantaggi sia per il cliente, che non subisce alcun addebito, sia per l'intermediario, che non sarà chiamato in futuro a rimborsare le somme sottratte.

Ciò premesso, è difficile stabilire se le ragioni che hanno indotto il legislatore a prevedere una franchigia a carico del cliente nei casi indicati, sussistano anche nell'ipotesi di frodi informatiche. A giudicare dalle modalità con cui tali truffe vengono realizzate, la risposta sembra invero dover essere negativa: nel caso di operazioni fraudolente *online*, non vi è infatti uno iato temporale tra sottrazione dello strumento e utilizzo fraudolento, perché alla "cattura" dei codici segue istantaneamente l'operazione di pagamento. Non sussiste, cioè, quell'intervallo temporale tra evento prodromico all'utilizzo indebito, come può essere il furto, e l'operazione fraudolenta in cui il cliente avrebbe potuto attivarsi tempestivamente per richiedere il blocco della carta.

L'applicazione della franchigia anche in caso di operazioni *online* potrebbe, dunque, apparire irragionevole proprio perché essa, in tale diverso contesto, non potrebbe svolgere la funzione, alla quale è deputata, di sollecitare i clienti ad adottare tempestivamente le misure più idonee ad impedire il realizzarsi delle operazioni fraudolente.

Ciononostante, la soluzione del Coordinamento non sopisce ogni dubbio: potrebbe, ad esempio, sembrare iniquo che l'utente incolpevole ottenga il riaccredito integrale della somma sottratta, quando è rimasto vittima di una truffa informatica, mentre in caso un furto materiale veda il rimborso decurtato della franchigia. E, allora, anziché limitarsi a richiamare la lettera della norma (che non prevede l'operatività della franchigia in caso di frodi informatiche), lasciando in ombra la ragione della mancata applicazione della franchigia, il Coordinamento avrebbe potuto soffermarsi sulla funzione della franchigia e spiegare perché essa trova applicazione in caso di furto, smarrimento o appropriazione indebita dello strumento, e non di pagamenti *online*.

---

fino a un massimo di 150 euro, per le operazioni avvenute prima della comunicazione al prestatore, è volto ad accelerare l'adozione delle misure di salvaguardia previste a carico degli utilizzatori, per ridurre il verificarsi dei danni».

Per inciso, viene peraltro da chiedersi se non sarebbe preferibile, *de iure condendo*, eliminare la previsione della franchigia[94], atteso che lo scopo della stessa è già raggiunto dalla previsione di una responsabilità dell'utente per violazione dell'obbligo di cui all'art. 7, comma 1, lett. *b*), del d.lgs. n. 11/2010, ossia quello di comunicare senza indugio al prestatore di servizi di pagamento lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza. Sembrerebbe, in effetti, più ragionevole consentire ai Collegi ABF di valutare di volta in volta se la suddetta comunicazione sia stata o meno tempestiva, modulando di conseguenza l'entità del rimborso da corrispondere al cliente, piuttosto che far ricadere sugli utenti incolpevoli una quota fissa delle perdite dovute a operazioni fraudolente eseguite prima della loro comunicazione.

A ben vedere, ragionando in questo modo, gli utenti resterebbero incentivati a comunicare senza indugio la perdita o il furto dello strumento di pagamento. E ciò in quanto essi saranno interessati, da un lato, a ottenere il blocco tempestivo dello strumento (al fine di evitare ogni utilizzo indebito dello stesso, e potendo contare sul rimborso delle transazioni eseguite dopo la comunicazione di perdita) e, dall'altro, a non incorrere nella responsabilità per violazione dell'obbligo previsto

[94] Certa dottrina (I. A. CAGGIANO, *Pagamenti non autorizzati tra responsabilità e restituzioni. una rilettura del d. legisl. 11/2010 e lo scenario delle nuove tecnologie*, cit.) propone, invece, di riconoscere ai Collegi dell'ABF la facoltà di modulare l'importo della franchigia, fino al massimale di euro 150, sulla base dei seguenti criteri: «proporzione con l'entità della somma fraudolentemente sottratta (i.e.: su una somma esigua, di poche centinaia di euro, la franchigia da dedurre non potrà comunque attingere la soglia massima di euro 150); maggiore o minore lievità della compartecipazione colposa del cliente nella produzione del fatto illecito (il o i prelievi fraudolenti); grado di negligenza dell'intermediario». Al riguardo, occorre segnalare che il Collegio di Coordinamento ABF, nella decisione 29 novembre 2013, n. 6170 ha escluso espressamente che l'Arbitro Bancario abbia il potere di graduare l'importo della franchigia sulla scorta dei criteri anzidetti: «Invero, la norma, pur utilizzando la espressione 'può', tuttavia non indica criteri per una eventuale graduazione della franchigia. Ne discende che se essi debbono essere individuati dall'interprete questi deve però attenersi a criteri non di carattere soggettivo, ma oggettivo e quindi a criteri che siano omogenei e non discriminatori. Tuttavia la struttura del procedimento avanti l'ABF non fa emergere tutte le sfaccettature delle circostanze di fatto che consentano una graduazione della franchigia secondo criteri oggettivi. Di qui la necessità più che l'opportunità di attenersi ad un importo fisso, eguale per tutti i ricorrenti, importo che non può non coincidere con quello indicato dispositivamente ex lege».

dal già citato art. 7, comma 1, lett. *b*). Con il risultato, a nostro avviso più equo, di non far gravare la franchigia sugli utenti non responsabili.

10. *La successiva giurisprudenza dell'ABF*

Dopo aver analizzato i principi di diritto enunciati dalla decisione del Collegio di Coordinamento che si annota, occorre ora considerare l'impatto di quest'ultima sulla successiva giurisprudenza dell'ABF e, in particolare, sulle decisioni dei Collegi territoriali che si sono occupate di frodi *online* affrontando il profilo della prova della colpa grave del cliente.

L'impressione che si ricava a questo proposito è quella di un assetto giurisprudenziale ancora in fase di assestamento: se infatti, può dirsi fortemente ridotto il ricorso al ragionamento deduttivo censurato dal Coordinamento, in base al quale la colpa grave del cliente può dirsi provata ove la banca abbia adottato efficaci misure di sicurezza (*i.e.* il sistema di autenticazione a "due fattori"), si rinvengono ancora diverse pronunce che continuano ad adoperare quell'argomento[95]: così, ad

[95] Si veda, ad esempio, ABF, Coll. Milano, decisione 13 febbraio 2020, n. 2386 la quale rileva «[…] l'adozione di un sistema a "due fattori" induce a ritenere, in assenza di ulteriori indici di anomalia dell'operazione, da un lato, che la banca abbia assolto all'onere di provare l'adempimento degli obblighi su di essa gravanti ai sensi dell'art. 8 del D.lgs. n. 11/2010 e, dall'altro lato, che il cliente si sia reso gravemente inadempiente all'obbligo di custodia degli strumenti e dei codici di accesso che consentono l'utilizzo del servizio *online*». La medesima osservazione si rinviene anche in ABF, Coll. Milano, decisione 13 febbraio 2020, n. 2389 ove, però, la richiesta di rimborso del cliente viene respinta più che sulla base della prova resa dell'intermediario di aver predisposto un sistema di autenticazione multifattoriale, in ragione del fatto che il ricorrente era incorso in un fenomeno c.d. di *phishing*. Anche ABF, Coll. Roma, decisione 29 gennaio 2020, n. 1394 sembra fondare la propria decisione sul precedente orientamento adottato dall'Arbitro in materia di frodi informatiche benché lo stesso, come si è visto, sia stato sconfessato dal Coordinamento: «[…] il ricorso ad un sistema di autenticazione a doppio fattore, in assenza di malfunzionamento del sistema, consente di ritenere che l'intermediario abbia assolto all'onere della prova che la legge gli impone in caso di disconoscimento di una operazione di pagamento». Sostanzialmente allineate all'orientamento "pre-Coordinamento" sono anche ABF, Coll. Bologna, decisione 3 gennaio 2020, n. 13; ABF, Coll. Napoli, decisione 8 gennaio 2020, n. 137; ABF, Coll. Bologna, decisione 3 gennaio 2020, n. 24.

esempio, un nutrito filone di decisioni[96] che, in sostanziale continuità con l'indirizzo tradizionale, considera raggiunta la prova della grave negligenza del cliente ove il PSP dimostri che le operazioni contestate sono state effettuate mediante un sistema di autenticazione multifattoriale, e il cliente non sia stato in grado di fornire elementi utili a individuare le modalità della truffa informatica, allocando così il rischio da ignoto tecnologico in capo a quest'ultimo, anziché agli intermediari come vorrebbe la *ratio* del d.lgs. n. 11/2010.

Nell'ambito delle pronunce che più correttamente gravano gli intermediari dell'onere di provare la colpa grave dell'utente, si riscontrano poi incertezze e contraddizioni circa l'oggetto dell'onere probatorio.

Degli elementi indicati a questo proposito dal Coordinamento – l'assenza di tentativi falliti di digitazione del PIN, l'accertata assenza di *malware*, la ricezione della password dinamica tramite cellulare o altro dispositivo del cliente in assenza di deviazioni o intrusioni nel *device* – è l'ultimo a essere maggiormente valorizzato dai Collegi, mentre gli altri due elementi hanno, invece, avuto minore "fortuna". Per il secondo, potrebbe invero esserci spazio in futuro, dal momento che verosimilmente esso non è stato richiamato dalle pronunce considerate, perché riguardavano casi in cui i clienti non affermavano di essere stati vittime di *malware*[97]. Il primo elemento – l'inserimento delle credenziali corrette al primo tentativo – sembra, al contrario, destinato a rilevare in un ambito diverso da quello delle transazioni *online*, per presumere che il PIN fosse conservato insieme alla carta in caso di furto degli strumenti di pagamento. In questo quadro, permane dunque una notevole incertezza circa il riparto dell'onere della prova tra PSP e utilizzatore in caso di aggressioni informatiche tramite *virus*.

[96] In questo senso, si veda soprattutto Collegio ABF di Bologna, decisioni 22 gennaio 2020, nn. 1064, 1070, 1078, 1129; ma sembra propendere per questo indirizzo anche il Collegio di Roma, nelle decisioni 22 gennaio 2020, nn. 846 e 856, nonché 29 gennaio 2020, n. 1386.

[97] E del resto, dal momento che il procedimento davanti all'ABF, come già ricordato, si conforma al principio dispositivo (cfr. ABF, Coll. Coord., decisione n. 7716/2017, cit.), il Collegio non è tenuto a indagare, in assenza di una specifica deduzione della parte, se l'operazione fraudolenta è dipesa dalla presenza di un *malware* nel sistema del ricorrente.

Ulteriori incertezze riguardano l'elemento che più spesso i Collegi territoriali hanno valorizzato, come si diceva, per presumere la colpevolezza del cliente: l'avvenuta ricezione della password dinamica tramite cellulare o altro dispositivo del cliente in assenza di deviazioni o intrusioni nel *device*.

Così, in alcune decisioni,[98] più fedeli a quanto stabilito dal Coordinamento, l'Arbitro ha considerato raggiunta la prova della colpa del cliente ove l'intermediario aveva documentato tanto l'invio, quanto l'avvenuta ricezione da parte del ricorrente del messaggio contente l'OTP per autorizzare l'operazione; in altre[99], è stata invece ritenuta sufficiente la prova del solo invio dell'OTP sul cellulare dell'utente.

---

[98] ABF, Coll. Milano,decisione 5 febbraio 2020, n. 1813 ha accolto il ricorso presentato dal cliente sulla base del rilievo che «l'evidenza prodotta [n.d.r. dall'intermediario] dà conto dell'invio del predetto sms, ma non della sua ricezione. Questo elemento risulta indirettamente confermato dal fatto che la parte ricorrente non menziona detto messaggio, anzi, si è accorta dell'operazione soltanto successivamente alla stessa grazie alla verifica dei movimenti del conto.». Nello stesso senso anche ABF, Coll. Milano, decisione 5 febbraio 2020, n. 1756 «La prova (presuntiva) della colpa grave è stata assolta, avendo l'intermediario fornito la prova dell'invio e della recezione dell'sms con l'OTP all'utenza telefonica del ricorrente». Conformi anche ABF, Coll. Milano, decisione 13 febbraio 2020, n. 2397 – che ha deciso il ricorso in senso favorevole all'intermediario valorizzando la circostanza che l'utente si era regolarmente autenticato e aveva ricevuto l'*sms* con la *password* dinamica – nonché ABF, Coll. Napoli, decisione 8 gennaio 2020, n. 180.

[99]ABF, Coll. Milano, decisione 5 febbraio 2020, n. 1757 rileva «Un elemento di fatto utile a trarre la prova, presuntiva, della colpa grave della cliente, è la prova fornita l'intermediario dell'invio delle password OTP sul numero di cellulare (certificato) del cliente»; anche ABF, Coll. Milano, decisione 5 febbraio 2020, n. 1759 fa riferimento al solo invio e non già alla ricezione del messaggio:«Tali prove sono state date per le prime due operazioni disconosciute (e peraltro oggetto di parziale restituzione delle somme sottratte), avendo l'intermediario fornito evidenza dell'invio delle password OTP sul numero di cellulare (certificato) del cliente.»; conforme anche ABF, Coll. Napoli, decisione 8 gennaio 2020, n. 159: «Si tratta, quindi, di valorizzare le singole e specifiche circostanze relative alle fattispecie di volta in volta sottoposte da entrambe le parti all'esame dell'Arbitro Bancario Finanziario, in ordine alle quali è necessario verificare se – alla luce degli elementi costituitivi della fattispecie – sia possibile desumere in capo all'utilizzatore un comportamento gravemente colposo. Nel caso di specie, la prova in questione può considerarsi raggiunta. L'intermediario ha fornito prova della corretta autenticazione, registrazione e contabilizzazione delle operazioni contestate, nonché dell'invio, immediatamente precedente le due operazioni in esame, degli sms di autorizzazione sul numero di cellulare "certificato" dall'utente». Riconducibili a tale indirizzo sono anche ABF, Coll. Bologna, decisione

La comprovata trasmissione della password OTP al cellulare del cliente è stata ritenuta da un diverso indirizzo[100] una circostanza idonea a dimostrare soltanto la regolarità sostanziale dell'operazione contestata, piuttosto che la colpa grave dell'utente.

Un profilo che meriterebbe di essere chiarito dalla giurisprudenza dell'Arbitro, su cui il Coordinamento non si è pronunciato, riguarda infine il caso in cui l'intermediario abbia dimostrato che l'operazione di pagamento è stata disposta mediante un sistema di autorizzazione a "due fattori" e che la password monouso è stata correttamente inviata dal cliente, ma non anche ricevuta, senza che quest'ultimo abbia sollevato contestazioni.

Una tale fattispecie potrebbe essere risolta sulla scorta del principio di non contestazione *ex* art. 115 c.p.c.,[101] ritenendo pacifica, perché non contestata, la ricezione del messaggio da parte del cliente[102]. Si tratterebbe, però, di una soluzione eccessivamente rigorosa e penalizzante per la platea degli utilizzatori degli strumenti di pagamento che, non dovendo farsi assistere da un difensore per adire l'ABF, ben potrebbero ignorare l'onere di contestazione. In questo senso, ci si deve allora domandare se, in un caso come questo, l'Arbitro non sia tenuto a rilevare d'ufficio la mancata prova dell'avvenuta ricezione della password OTP sul dispositivo del cliente.

Oltre all'accertamento della colpa grave del cliente, vi sono però anche altri aspetti trattati dalla decisione annotata che esigono maggiore

22 gennaio 2020, n. 1066; ABF, Coll. Bologna, decisione 3 gennaio 2020, n. 35; ABF, Coll. Napoli, decisione 8 gennaio 2020, n. 184; ABF, Coll. Roma, decisione 13 gennaio 2020, n. 464 che ha ipotizzato la negligente custodia dello strumento di pagamento e dei codici di accesso da parte del ricorrente sulla base del fatto che l'intermediario aveva prodotto le tracciature degli SMS inviati, ma non anche ricevuti, all'utente.

[100] ABF, Coll. Milano, decisione 22 gennaio 2020, n. 1057; ABF, Coll. Palermo, decisione 30 marzo 2020, n. 5889; ABF, Coll. Bari, decisione 27 marzo 2020, n. 5833; ABF, Coll. Roma, decisione 22 gennaio 2020, n. 1037; ABF, Coll. Palermo, decisione 3 febbraio 2020, n. 1575.

[101] È pacifico che il procedimento avanti all'Arbitro Bancario è regolato dalle norme e dai principi generali del processo civile, tra cui anche il principio di non contestazione, cfr. ABF, Coll. Coord., n. 7716/2017, cit. In dottrina si veda D. DALFINO, *op. cit.*

[102] È questa la soluzione interpretativa adottata da una recente decisione dell'Arbitro (ABF, Coll. Bologna, decisione 3 gennaio 2020, n. 27) che ha considerato dirimente la circostanza che il ricorrente non avesse negato la ricezione dell'OTP.

chiarezza, come ad esempio quello dell'applicazione della franchigia di cui all'art. 12, co. 3, d.lgs. n. 11/2010. Si è visto che il Coordinamento ha inteso limitare l'operatività della franchigia alle sole ipotesi testualmente previste nel citato art. 12 (furto, smarrimento o appropriazione indebita dello strumento di pagamento), escludendone l'applicazione in fattispecie di utilizzo illecito diverse, tra cui quella della frode informatica. Si rinvengono nondimeno decisioni successive[103] che parrebbero applicare la franchigia proprio al caso in cui i clienti contestano l'addebito sul proprio conto corrente di pagamenti *online* non autorizzati. Si tratta invero di ipotesi isolate; ma vi è comunque il sospetto che esse denotino una certa insofferenza dei Collegi ABF verso la soluzione del Coordinamento che rischia di trattare in modo – forse irragionevolmente – diverso il cliente-vittima di furto della carta e il cliente-vittima di frode informatica.

11. *Conclusioni*

Il tema della responsabilità dell'intermediario per utilizzo abusivo degli strumenti di pagamento implica, come si è visto, un delicato bilanciamento tra gli interessi contrapposti degli utenti e prestatori del servizio. Stabilire il riparto dell'onere probatorio tra le parti e allocare il rischio dell'operazione dovuta a causa ignota pongono, del resto, problemi complessi che non si prestano a soluzioni semplicistiche.

Alcune considerazioni finali possono tuttavia essere svolte. Si è detto che tra gli obiettivi del legislatore nazionale e comunitario c'è quello di incrementare la fiducia del pubblico negli strumenti di pagamento diversi dal contante, per incentivarne la diffusione e allo scopo ultimo di aiutare la crescita economica[104]. Si comprende, dunque, l'esigenza di garantire la sicurezza dei pagamenti elettronici[105] e, al contempo, di agevolare le procedure di rimborso agli utenti in caso di

[103] Ad es. ABF, Coll. Milano, decisione 5 febbraio 2020, n. 1813 e ABF, Coll. Roma, decisione 29 gennaio 2020, n. 1364.

[104] Sull'importanza che riveste la diffusione degli strumenti di pagamento elettronici per la crescita economica di un paese si veda I. D'AMBROSIO, *op. cit.*, a cui si rinvia per ulteriori riferimenti bibliografici.

[105] In questa direzione si muove la previsione dell'obbligo, per i prestatori dei servizi di pagamento, di applicare sistemi di autenticazione "forte" *ex* art. 10-*bis*, d.lgs. n. 11/2010.

operazione fraudolenta. Alla luce di tali obiettivi, attribuire agli intermediari una responsabilità oggettiva per rischio d'impresa, come fa la pronuncia annotata, sembra in effetti la soluzione preferibile, perché massimizza la tutela della clientela bancaria soprattutto nei casi, e sono numerosi, in cui l'Arbitro non riesce ad accertare la causa dell'operazione fraudolenta.

D'altra parte, occorre però tutelare anche l'interesse dei *Payment Service Provider* a non rimborsare gli utenti resisi gravemente inadempienti agli obblighi di conservazione e custodia degli strumenti di pagamento o che, addirittura, hanno agito in mala fede per conseguire un ingiusto arricchimento. In questa prospettiva, la configurazione di una responsabilità oggettiva in capo ai prestatori dei servizi di pagamento si rivela, a ben vedere, più problematica.

E viene da chiedersi se, a fronte di orientamenti dell'ABF troppo rigorosi nell'esigere la prova della colpa grave del cliente, non vi sia forse il rischio che gli intermediari decidano di non prestare più adesione alle decisioni rese dall'Autorità[106], costringendo così la clientela a rivolgersi alla ben più onerosa e lenta giustizia ordinaria, magari per recuperare importi di poche centinaia di euro.

[106] Com'è noto, le decisioni dell'Arbitro Bancario non hanno efficacia di giudicato (tant'è che le parti, anche dopo la decisione, conservano la facoltà di ricorrere all'autorità giudiziaria), mentre l'unica sanzione prevista a carico dell'intermediario che si rifiuti di eseguire la decisone è rappresentata dalla pubblicità dell'inadempimento sul sito dell'ABF e in due quotidiani ad ampia diffusione nazionale. Sulla valenza giuridica delle decisioni assunte dall'Arbitro Bancario Finanziario, si veda I. A. CAGGIANO, *L'arbitro bancario finanziario, esempio virtuoso di degiurisdizionalizzazione*, cit.