Maria Cecilia Paglietti

Questioni in materia di prova nei casi di pagamenti non autorizzati

Sommario: 1. La regolazione dei servizi di pagamento come sintesi della modernità – 2. Questioni di metodo: interdisciplinarietà e tecnica legislativa – 3. Questioni di merito: l'allocazione del rischio – 4. 1. L'obbligo di autenticazione forte di matrice giurisprudenziale – 4. 2. L'obbligo di autenticazione forte contenuto nella Direttiva – 5. Vincoli di solidarietà tra IP – 6. La ripartizione degli oneri probatori – 7. Fatti generatori di responsabilità dell'intermediario e mezzi di prova – 8. La colpa grave del pagatore.

1. *La regolazione dei servi di pagamento come sintesi della modernità*

L'argomento degli aspetti probatori dei pagamenti non autorizzati è delicato, soprattutto perché, come noto tanto alla dottrina sostanzialista quanto a quella processualistica (quello della prova è uno dei cosiddetti istituti bifronti, come definiti nella Relazione al codice civile[1]), la ripartizione dell'onere della prova è cruciale sull'esito della lite[2].

Per affrontare il tema compiutamente, mi pare opportuno svolgere alcune premesse in ordine all'impianto sistematico della nuova disciplina in materia di servizi di pagamento, alle scelte *policy* ad esso sottese, all'allocazione della responsabilità, e, in ultimo, alle possibili fattispecie concrete.

L'A. è componente supplente del Collegio di Roma dell'Arbitro Bancario Finanziario. Le opinioni espresse nel lavoro hanno carattere personale e non sono in alcun modo riferibili a tale istituzione.

[1] Così definiti in quanto «ponte di passaggio tra il processo e il diritto soggettivo»: Relazione al codice di procedura civile del ministro Guardasigilli Grandi, presentata al Re, Roma, 1940, n. 6, p. 16.

[2] M. R. Damaška, *Evidence Law Adrift*, Yale University Press, New Haven 1997 (del volume esiste anche una versione italiana, dal titolo *Il diritto delle prove alla deriva*, a cura di M. Taruffo. - Trad. di F. Cuomo Ulloa, V. Riva, Il Mulino, Bologna 1991); M. Mekki, *Regard substantiel sur le "risque de preuve" – Essai sur la notion de charge probatoire*, in *La preuve: regards croisés*, a cura di M. Mekki, L. Cadiet e C. Grimaldi, *La preuve, regards croisés*, Thèmes et commentaires, Dalloz, Paris 2015, p. 7.

La necessità di una nuova disciplina e, dunque, della riformulazione della previgente Direttiva (2007/64/CE)[3] si fonda su due grandi architravi concettuali: sicurezza dei sistemi informatici e fiducia degli utenti[4]. I due temi trovano la loro sintesi nella ricerca di un contemperamento tra le istanze della regolazione (maggiore sicurezza dei pagamenti e protezione del soggetto debole del rapporto negoziale) e la promozione della concorrenza (un mercato dei pagamenti efficiente e integrato[5]; miglioramento del *level playing field* per i *providers*; ampliamento del mercato, tramite l'introduzione di nuovi operatori e nuove tecniche[6]: *mobile payments, wallet providers, third party providers, instant payments*), letti nella filigrana della massiccia diffusione di nuovi mezzi pagamento, tecnicamente complessi, implicanti maggiori rischi di sicurezza[7] e relative lacune regolamentari, che a loro volta si svolgono lungo il crinale delle due grandi traiettorie di sviluppo del Fintech: dematerializzazione e disintermediazione[8].

È notorio che il rischio di operazioni fraudolente dipenda tanto dal comportamento delle parti, quanto dal livello di sicurezza del servizio adottato

[3] Direttiva 2007/64/CE del Parlamento europeo e del Consiglio, del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno, su cui cfr. AA.VV., *Il nuovo quadro normativo comunitario dei servizi di pagamento. Prime riflessioni*, a cura di M. Mancini e M. Perassi, Banca d'Italia, in *Quaderni di Ricerca Giuridica della Consulenza Legale*, n. 63, Roma 2008; AA.VV., *La nuova disciplina dei servizi di pagamento*, a cura di M. Mancini, M. Rispoli Farina, A. Santoro, A. Sciarrone Alibrandi e O. Troiano, Giappichelli, Torino 2011, p. 9; D. Mavromati, *The Law of Payment Services in the EU, The EC Directive on Payment Services in the Internal Market,* Kluwer Law International, Alphen aan den Rijn 2007.

[4] Che costituiscono i due grandi temi alla base del progetto di riforma del sistema dei pagamenti: cfr. in argomento Banca d'Italia, *Libro bianco sul sistema dei pagamenti in Italia*, Roma 1987.

[5] Inteso quale presupposto di crescita economica della Unione europea e di realizzazione del massimo vantaggio del mercato interno: v. 5° Considerando, Dir. 2366/2015.

[6] Libro Verde della Commissione Europea dell'11 gennaio 2012 "Verso un mercato europeo integrato dei pagamenti tramite carte, internet e telefono mobile", COM (2011) 941 def.; B. Geva, *The Payment Order of Antiquity and the Middle Ages*, Hart Publishing, Oxford 2011.

[7] 7° Considerando, Dir. 2015/2366.

[8] N. Martial-Braz, *L'apport du numérique au droit bancaire: l'émergence des FinTechs*, in *Revue de Droit bancaire et financier*, 2017, dossier 2; sul tema dell'impatto dell'innovazione digitale sull'industria bancaria cfr. G. Barba Navaretti, G. Calzolari, A. F. Pozzolo, *Banche e fintech. amici o nemici?,* in *Fintech*, a cura di F. Finnamò e G. Falcone, ESI, Napoli 2019, p. 25. In Francia, la normativa di recepimento della Dir. 2015/2566 si sovrappone alla *Loi pour une République numérique* (Loi n° 2016-1321 del 7 ottobre 2016), che, per un verso, ha generalizzato il pagamento tramite sms e, per altro, senza attendere la trasposizione della Direttiva (e andando contro l'avviso del *Conseil d'État*: P. Storrer, *Quand un teste mors sujet entend transposer à contretemps une directive DSP2*, in *Revue Banque*, dossier n° 799) ha creato un'eccezione allo statuto del prestatore di servizio di pagamento per gli operatori di telecomunicazioni.

dall'operatore. Questa osservazione, apparentemente scontata, consente tuttavia di evidenziare l'aspetto dirimente che la tecnologia riveste in materia[9].

Sul piano giuridico, il filo conduttore che anima la Direttiva e le riflessioni in materia è la consapevolezza della necessaria gestione di conflitti tra parti diseguali e, quindi, la ricerca di un *balanced equilibrium* (tanto nel momento della progettazione delle norme, quanto in quello della loro applicazione) tra le istanze di sicurezza (dei sistemi, degli utenti) e quelle dell'innovazione[10].

Il tema delle operazioni non autorizzate (nelle ipotesi di smarrimento, furto o appropriazione indebita), che, cioè, si sono svolte senza il consenso del titolare della carta di pagamento (sia essa di debito che di credito)[11], è, dunque, quello dell'imputabilità.

La tematica può essere scomposta in tre segmenti: i) allocazione del rischio (regime di responsabilità e individuazione del soggetto che deve sopportare le conseguenze dell'evento fraudolento); ii) ripartizione degli oneri probatori; iii) individuazione e portata dei mezzi di prova.

2. *Questioni di metodo: interdisciplinarietà e tecnica legislativa.*

La nuova disciplina pone problemi di metodo e di merito.

Con riguardo all'aspetto metodologico, costituisce un dato di pacifico accoglimento che nel *Fintech* l'oggetto della normazione sia fluido e mutevole; e che l'approccio regolatorio, basato sull'interdisciplinarietà, debba essere caratterizzato da pluralismo e dal necessario dialogo tra saperi

[9] Così già O. Troiano, *I servizi elettronici di pagamento. Addebiti in conto non autorizzati: un'analisi comparata*, Giuffrè, Milano 1996, p. 66. Sull'influenza dell'evoluzione tecnologica sul diritto bancario in generale e sul diritto dei pagamenti in particolare, cfr. già: *Innovation technologique et droit bancaire: Cour de cassation*, Rapport annuel 2005, in *Doc. fr.*, 2006, p. 87; P. Leclercq, *Les titres dématérialisés de paiement et de crédit : Le droit privé français à la fin du XXe siècle*, in *Études offertes à Pierre Catala*, Litec, Paris 2001, p. 785.

[10] Sugli indirizzi dell'UE in materia fintech, S. Chishti, J. Barberis, *The FinTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries Chichester,* John Wiley & Sons., West Sussex 2016; M.T. Paracampo, *Robo-advisor, consulenza finanziaria e profli regolamentari: quale soluzione per un fenomeno in fieri?*, in *Riv. trim. dir. ec.*, Supp. al n. 4, 2016, p. 256; P. Pailler, *Le consommateur de services financiers au coeur des préoccupations du législateur européen*, in *Revue de Droit bancaire et financier*, 2014, p. 8.

[11] Cfr. F. Ciraolo, *Le carte di debito nell'ordinamento italiano. Il servizio bancomat*, Giuffrè, Milano 2008; O. Troiano, *Contratto di pagamento*, in *Enc. dir.*, Annali, V, Giuffrè, Milano 2012, p. 392 ss.

specialisti (che però parlano linguaggi diversi)[12].

Il momento legislativo, quello interpretativo e quello dell'*enforcement* devono incorporare il dato scientifico, basarsi su di esso, a pena di risultare irragionevoli[13]. L'adeguata compenetrazione tra il dato scientifico e il precetto normativo implica che alla base della giuridificazione ci sia una precomprensione del fenomeno tecnico, e che la legge (o la decisione) rappresentino il medio logico attraverso i quali adeguare il diritto alla scienza.

Il tema è quello dell'interscambio tra tecnologia e diritto (a livello sia legislativo sia giurisprudenziale), che obbliga il giurista ad instaurare un dialogo forzoso non più con le aree culturali maggiormente affini (sociologia, economia) ma con le cosiddette "scienze dure".

Se la forma tradizionale di dialogo familiare ai giuristi (soprattutto a chi, come me, è di estrazione comparatista) è quello tra i formanti, che si svolge dunque *all'interno* del medesimo sapere, ora all'interprete si dischiudono nuovi interlocutori, *esterni* e con specificità culturali differenti: questo tipo di dialogo –necessario- che può più facilmente essere raggiunto all'interno del procedimento legislativo, deve permanere anche nei momenti successivi, quelli dell'applicazione del diritto. È solo il perdurare di questo dialogo che può evitare interpretazioni obsolete o irragionevoli e avallarne di rispettose dell'"evento informatico" -così come si è effettivamente svolto- e conferenti all'evoluzione tecnologica (per giungere a quello che Guido Calabresi chiama significativamente il «miglioramento condiviso del diritto»[14]).

Non si tratta, in questa materia, di contrapporre l'economia al diritto, i bisogni del mercato ai valori della giurisdizione, ma cercare di contemperarli e farli convivere senza attriti.

Vorrei riportare un esempio, anticipando un tema che svilupperò nel prosieguo della relazione: il protocollo 3DSecure viene considerato, in alcune decisioni della *Cour di cassation*, come un elemento che, aumentando la sicurezza del sistema informatico, costituisce indice di una condotta diligente dell'intermediario[15]; per contro, la giurisprudenza

[12] N. Irti, *Norme e luoghi. Problemi di geo-diritto*, Laterza, Roma-Bari 2006; nello specifico dell'influenza dell'evoluzione tecnologica sul diritto bancario e, in particolare, sugli strumenti di pagamento: É. Wéry, *Paiements et monnaie électroniques. Droits européen, français et belge,* Larcier , Brusselles 2007.

[13] Su questi temi v J. Habermas, *Fatti e norme*, *Contributi a una teoria discorsiva del diritto e della democrazia,* curato e tradotto da L. Ceppa, Laterza, Roma-Bari 2013*;* S. Penasa, *La legge della scienza: nuovi paradigmi di disciplina dell'attività medico-scientifica. Uno studio comparato in materia di procreazione medicalmente assistita*, Esi, Napoli 2015.

[14] *Il mestiere di giudice. Pensieri di un accademico americano*, Il Mulino, Bologna 2013, p. 85.

[15] Sentenza 31 maggio 2016, in *Dalloz*, 2016, p. 2305, con note di D. R. Martin, H. Synvet; *Sem. Jur., éd. Entr. Aff*., 2016 p. 1450, con nota di J. Lasserre Capdeville.

italiana (segnatamente, l'Arbitro Bancario e Finanziario) considera il sistema 3DSecure non necessariamente sicuro, il che conduce, unitamente alla presenza di altre circostanze contingenti, all'accoglimento delle istanze attoree. Il tema ha necessitato di un specifico intervento chiarificatore da parte dell'EBA. A me pare che questo sia un caso paradigmatico di quanto la differente valutazione di un "fatto informatico" abbia ricadute sul piano giuridico, esitando in decisioni di segno opposto.

Il tema regolatorio si presenta sin dalla scelta della tecnica legislativa: se la disciplina è troppo specifica, rischia di essere "controtempo" [16] e divenire presto, alternativamente, lacunosa od absoleta[17]. In entrambi i casi il rischio è che si apra uno spazio eccessivo tra la norma ed il contesto applicativo. Per contro, se eccessivamente ampia (norme in bianco), rischia di enfatizzare a dismisura il ruolo degli interpreti[18].

Ed in questo ultimo caso, il nodo cruciale della teoria dell'interpretazione intesa come correttivo al silenzio del legislatore è che gli interpreti divengano "legislatori di seconda istanza"[19], riformulando leggi che i postulati positivistici laddove troppo stretti non consentano, o laddove troppo larghi non prevedano. Tuttavia, questa situazione apre, *ça va sans dire*, alle difformità, considerato che l'attività interpretativa ha, notoriamente, una matrice autobiografica, poiché, come ci ricordano i filosofi, risente delle convinzioni e delle posizioni intellettuali di chi la svolge [20].

Appare, dunque, necessaria, da parte di chi fa le leggi, la predisposizione di un programma legislativo aperto, idoneo a coniugare i requisiti di generalità ed astrattezza con la specificità del caso concreto[21]: l'intento del legislatore dovrebbe essere quello di realizzare un sistema regolatorio equamente basato su clausole generali e fattispecie dal perimetro definito.

Questo appare tanto più vero nel nostro ordinamento, nel quale, come in tutti gli ordinamenti a diritto codificato, non vige il principio dello *stare decisis*, e dunque il precedente giurisprudenziale non assume un valore vincolante, consentendo ai giudici successivi di discostarsi da quanto in

[16] Dal titolo del libro di S. Rossi, *Controtempo. L'Italia nella crisi globale*, Laterza, Roma-Bari 2009, spec. 173 ss.
[17] G. Timsit, *Les noms de la loi*, PUF, Paris 1991, p. 117.
[18] W. Twining, D. Miers, *How to Do Things with Rules: A Primer of Interpretation*, 5th ed., CUP, Cambridge 2010; sull'indeterminatezza del diritto: *Critical Legal Thought: An American-German Debate*, 1989, a cura di C. Joerges e D. M. Trubeck, Baden-Baden, Nomos 1989.
[19] S. Cassese, *Introduzione allo studio della normazione*, in *Riv. trim. dir. pubbl.*, 1992, p. 311.
[20] C. Atias, *Epistemologie juridique*, Dalloz, Paris 1985, p. 94 ss.
[21] J. Habermas, *Fatti e norme*, cit., spec. p. 521 ss.

precedenza statuito[22].

Il tema della "progettazione di norme"[23] appare quindi contiguo e funzionalmente collegato a quello del creazionismo giurisprudenziale.

La prevedibilità delle decisioni assume, poi, una connotazione del tutto specifica nel quadro della vigilanza bancaria, poiché è nella garanzia di un significativo tasso di uniformità che può giungere a compimento il principio della *regulation by litigation*, attraverso la quale conseguire il fine ultimo dell'effettività della tutela del cliente[24].

Non solo perché la ricerca comparatistica evidenzia, negli ordinamenti di *civil law*, uno scollamento fra la teoria positivista e la realtà operazionale -si pensi alle pronunce della Corte costituzionale e all'esistenza di intere aree del diritto coperte esclusivamente dal diritto giurisprudenziale: da noi il danno biologico-, ma perché al ritardo (fisiologico, in materie ad alto tasso di obsolescenza normativa, stante la fluidità del settore regolato) del formante legale non può che sopperire quello giurisprudenziale.

La connessione fra finanza, tecnica, e diritto non risponde alla logica dell'uniformità, e spetta all'interprete, tramite un complesso lavorìo ricostruttivo, il compito di garantire al complesso assetto istituzionale la coerenza e l'effettività delle norme di cui si compone[25].

[22] Cfr., da ultimo, AA.VV., *Il vincolo giudiziale del passato. I precedenti*, a cura di A. Carleo, Il Mulino, Bologna 2018, *passim*.

[23] R. Pagano, *Introduzione alla legistica. L'arte di preparare le leggi*, Giuffrè, Milano 1999; AA.VV., *Normative europee sulla tecnica legislativa*, a cura di R. Pagano, Camera dei Deputati, 1988. Per un'ampia bibliografia sulla legistica o tecnica legislativa si rimanda a L. Pegoraro, *Linguaggio e certezza della legge nella giurisprudenza della Corte Costituzionale*, Giuffrè, Milano 1988 e soprattutto al volume collettaneo *Corso di studi superiori legislativi 1988-1989*, a cura di M. D'Antonio (e segnatamente al contributo di G. Amato, *Principi di tecnica della Legislazione*) Cedam, Padova 1990, p. 48.

[24] D. Wittman, *Prior Regulation v. Post Liability, the Choice Between Input and Output Monitoring*, 6 *Journal Legal Studies*, 1977, p. 193 ss.; S. Breyer, *Breaking the Vicious Circle: Toward Effective Risk Regulation*, Harv. Univ. Press, Cambridge 1993; H. Jonas, *Le principe du responsabilitè. Une ethique pour la civilisation technologique*, trad. a cura di J. Greisch, Le Cerf, Parigi 2001; AA.VV., *Regulation Through Litigation*, a cura di W. K. Viscusi, Brookings Institution Press, Washington 2002; AA.VV., *Better regulation*, a cura di S. Weatherill, Hart Publishing, Oxford 2007; AA.VV., *Regulation by litigation*, a cura di A. P. Morriss, Yale University Press, New Haven 2009. In un'ottica del tutto specifica, quella della *agencies as litigation rulemakers* (particolarmente conferente alla materia qui trattata) cfr. U. Mittal, *Litigation rulemaking*, 127 *Yale Law Journal*, 4, 2018, 1010.

[25] N. MacCormick, *La congruenza nella giustificazione giuridica*, in AA.VV., *L'analisi del ragionamento giuridico. Materiali ad uso degli studenti*, I, a cura di P. Comanducci e R. Guastini, Giappichelli, Torino 1987, p. 243 ss., spec. 247 ss.; A. Celotto, F. Donati, *Interpretazione conforme a diritto comunitario ed efficienza economica*, in *Interpretazione conforme e tecniche argomentative*, atti del convegno svoltosi a Milano, il 6-7 giugno 2008,

3. *Questioni di merito: l'allocazione del rischio*

È un dato di pacifico accoglimento, e presente al legislatore unionista sin dalla prima formulazione della normativa in materia, che l'allocazione del rischio di pagamenti non autorizzati sia cruciale ai fini dell'effettività della disciplina e, soprattutto, della diffusione dei sistemi di pagamento -promossa in sede comunitaria[26]- la quale dipende dalla fiducia che gli utilizzatori ripongono sull'assetto dei rischi che essi garantiscono rispetto al pagamento in contanti[27].

Le scelte di vertice devono, dunque, essere capaci di garantire un'allocazione del rischio in grado di *prevenire* e *reprimere* gli esiti inefficienti derivanti da comportamenti non rispettosi, sul versante dell'impresa, della predisposizione di sistemi di sicurezza *adeguati* e, sul versante dell'utente, della diligenza nella custodia dello strumento di pagamento e delle relative credenziali.

Il tema del criterio d'imputazione della responsabilità, declinato secondo la retorica dell'individuazione del soggetto su cui più efficientemente far ricadere il danno (colui sul quale, cioè, coesianamente, far gravare il costo degli incidenti), è il cuore delle disposizioni e delle scelte politiche in materia[28], che, nei vari ordinamenti, propongono un'allocazione articolata delle perdite subìte, risentendo della maggiore propensione ad optare per la soluzione della responsabilità oggettiva limitata laddove l'attività bancaria venga ascritta alle attività pericolose[29]. Volendo individuare alcuni

raccolti da M. D'Amico e B. Randazzo, Giappichelli, Torino 2009, p. 478 ss.

[26] Cfr., per tutti, R. De Bonis, M.I. Vangelisti, *Dai buoi di Omero ai Bitcoin*, Il Mulino, Bologna 2019.

[27] Cfr. 95° considerando, Dir. 2366/2015: «La sicurezza dei pagamenti elettronici è fondamentale per garantire la protezione degli utenti e lo sviluppo di un contesto affidabile per il commercio elettronico»; cfr. già il classico studio di J. A. Cousins, W. A. Imparato, B. D. Kelley, *Toward a Less-Check Society*, 47 *Notre Dame Law Rev.*, p. 853 1972; nello specifico della materia che interessa, v. B. Geva, *Bank Collections and Payment Transaction—A Comparative legal Analysis*, Oxford University Press, Oxford 2001; É. Wéry, *Paiements et monnaie électroniques. Droits européen, français et belge*, Larcier, Bruxelles 2007; le ipotesi di furto o smarrimento delle carte di pagamento sono ascrivibili, inoltre, ai costi transattivi della transazione principale: R. D. Cooter, E. L. Rubin, *A Theory of Loss Allocation for Consumer Payments*, 66 *Texas L. Rev.*, 1987, p. 63; cfr. altresì R. Steennot, *Allocation of Liability in Case of Fraudulent Use of an Electronic Payment Instrument: the New Directive on Payment Services in the Internal Market*, 24 *Computer L. Security Rev.*,6, 2008, p. 555.

[28] Cfr. B. Geva, *Payment Transactions Under the EU Payment Services Directive: A U.S. Comparative Perspective*, 27 *Penn State International L. Rev.*, 2009, p. 713.

[29] I. Becker, A. Hutchings, R. Abu-Salma, R.J. Anderson, N. Bohm, S. J. Murdoch, A. Sasse, G. Stringhini, *International Comparison of Bank Fraud Reimbursement: Customer*

punti fermi raggiunti dal dibattito europeo in materia, posta la nota tripartizione del tema nei tre criteri del *loss spreading, loss reduction,* e *loss imposition*[30], in primo luogo appare tratto comune a tutti gli ordinamenti la maggiore propensione alla dimensione causale quale unico fondamento della responsabilità, pur residuando alcune ipotesi eccezionalmente ancorate al principio della responsabilità per colpa. Escluse le soluzioni radicali, ovvero, alternativamente, far sopportare il rischio di utilizzi fraudolenti interamente sul prestatore (modello allocativo che ha il pregio di socializzare il rischio, ma incentiva condotte negligenti dei titolari) o interamente sull'utente (schema che, per un verso, contribuisce a ridurre i danni, inducendolo a tenere uno standard di condotta ottimale ed incentivandolo una custodia vigile dello strumento e delle credenziali, ma per altro verso lo obbliga a sopportare anche i casi di furto o di smarrimento[31]), l'impianto sistematico predisposto dalla Direttiva prevede, dunque, un caricamento del rischio (non solo, come si vedrà, degli utilizzi fraudolenti, ma anche del rischio tecnologico e di quello della prova[32]), quasi esclusivamente sul prestatore[33].

Nello specifico, la nuova formulazione dell'art. 12, D.lgs. 11/2010, prevede un duplice e alternativo regime di responsabilità dell'utente, limitata e illimitata. La prima si configura in relazione ad operazioni poste in essere prima della tempestiva comunicazione di cui all'art. 7, nei limiti della franchigia, ora ridotta a euro 50 (art. 12, comma 3).

L'utente risponde invece a titolo di responsabilità illimitata qualora abbia agito in modo fraudolento, con dolo o colpa grave, venendo meno ai propri

Perceptions and Contractual Terms, 3 *Journal of Cybersecurity*, 2018, p. 109.

[30] Il riferimento è al noto lavoro di R. D. Cooter, E. L. Rubin, *op. cit.*, p. 70 ss.; cfr. anche *The Development Of Liability In Relation To Technological Change*, a cura di M. Martín-casals, Cambridge University Press, Cambridge 2014 (2° ed.), spec. p. 3 ss.

[31] O. Troiano, *op. cit.*, p. 81; cfr. in Francia, le riflessioni di M. Cabrillac, B. Teyssié, *Cartes de paiement ou de crédit. Usurpation*, in *RTD com.*, 1994, p. 538, spec p. 539; F. Ekollo, *La charge des débits d'une carte bancaire volée au domicile de son titulaire avec le code confidentiel, le titulaire ayant formé opposition auprès du Groupement carte bleue et à l'établissement de crédit dès l'ouverture de ce dernier,* in *Dalloz*, 1995, p. 167.

[32] M. Mekki, *Le risque de la preuve: aspects de droit substantiel*», in *La preuve, regards croisés*, a cura di M. Mekki, L.Cadiet e C. Grimald, Dalloz, Paris 2015, p. 7.

[33] Alcuni configurano una presunzione di comportamento incolpevole in capo all'utente: D. Legeais, *Appréciation du manquement par négligence grave d'une victime d'un acte de phishing*, in *Sem. Jur., éd. Entr. Aff.*, 2017, p. 1685. Per un'analitica descrizione della disciplina previgente, cfr. R. Bonhomme, *Instruments de crédit et de paiement*, LGDJ, Paris 2015, 11° ed.; 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, p. 10459 ss; D. Maffeis, *Ordini di pagamento e di investimento online nella giurisprudenza di merito e nella fonte persuasiva dinamica dell'ABF*, in *Riv. dir. civ.*, 2013, p. 11273.

obblighi di custodia delle credenziali e dello strumento di pagamento (art. 7, comma 1, lettera a), e comma 3); ovvero se non abbia dato tempestiva comunicazione dello smarrimento, furto, appropriazione indebita dello stesso (art. 7, comma 1, lettera b).

Nelle ipotesi, però, di mancata adozione del prescritto sistema di autenticazione multi-fattore, la responsabilità dell'utente, esclusa anche nel caso la sua condotta sia caratterizzata da dolo o colpa grave, è configurabile solo in caso di frode dello stesso (la cui prova è a carico del prestatore: art. 12, comma 2-bis). In questa ipotesi la "comminatoria" di responsabilità si ricollega ad un chiaro intento afflittivo più che restitutorio.

In tema di allocazione delle responsabilità, va inoltre tenuta in debita considerazione la prospettiva della probabile evoluzione dei fatti fraudolenti nuovi, ossia fatti generatori di responsabilità riconducibili alle ipotesi di danno da ignoto tecnologico (il danno, cioè, verificatosi a causa di una causa sconosciuta, quali possono essere considerati gli «inconvenienti» menzionati dall'art. 10, comma 1-bis), dei quali viene gravata l'impresa[34].

Il legislatore ha, dunque, optato per un sistema -non monolitico ma graduato[35]- di responsabilità oggettiva limitata -prevista, alternativamente, con una duplicità di funzioni, tanto indennitaria, quanto sanzionatoria[36]- alla quale ha affiancato la previsione di un'inversione dell'onere della prova a

[34] B. Geva, *The Harmonization of Payment Services Law in Europe and Uniform and Federal Funds Transfer Legislation in the USA: Which Is a Better Model for Reform?",* in *European Banking and Financial Law Journal*, 2009, pp. 699-733; e, sul punto, già P. Trimarchi, *Rischio e responsabilità oggettiva*, Giuffré, Milano 1961; R. Costi, *Ignoto tecnologico e rischio d'impresa*, in *Il rischio da ignoto tecnologico*, Giuffrè, Milano 2002, 49; C. Hodges, *Development risk: Unanswered Questions*, 61 *Modern L. Rev.*, 1998, p. 560; nella materia d'interesse: D. Maffeis, *op. ult. loc. cit.*

[35] Il concetto di graduazione è ricorrente negli studi *consumers' behavioural*: Howells, *The Potential and the Limits of Consumer Empowerment by Information*, 32 *Journal Law Soc.*, 2005, p. 349 ss.

[36] Nelle operazioni di pagamento con un terzo non legittimato a ricevere il denaro le ipotesi di sovrapposizione tra rimedi restitutori (volti a riportare «*il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo*» -art. 11, comma 1, D.lgs. 11/2010) e risarcitori (da inadempimento, ravvisabile nell'omissione di un sforzo esigibile) non sono infrequenti, sia per la coincidenza tra l'oggetto del servizio e la misure dell'eventuale risarcimento, sia per la confusione tra i due rimedi in cui è incorsa la normativa (art. 11, comma 2 bis, D.lgs. cit.). Ancorché le soluzioni divergano in dottrina, una base ricostruttiva comune è quella di ravvisare, la compresenza di una pluralità di fattispecie rimediali (sia restitutorie che risarcitorie) nell'àmbito delle operazioni di pagamento, delle quali viene enfatizzata la dimensione procedimentale (V. De Stasio, *Riparto e responsabilità e restituzioni ne pagamenti non autorizzati*, in questo volume; I. A. Caggiano, *Pagamenti non autorizzati tra responsabilità e restituzioni. Una rilettura del d. legisl. 11/2010 e lo scenario delle nuove tecnologie*, cit., p. 10459).

carico del prestatore di servizi di pagamento, denotando una scelta di vertice di forte sensibilità alle esigenze del contraente debole e d'intransigenza per comportamenti sperequativi e pratiche anomale.

Va, tuttavia, sin da subito segnalato che, nonostante le scelte politiche ispirate a unitarietà e sintesi, i commentatori sono concordi nell'individuare il nodo maggiormente problematico dell'intera disciplina nell'applicazione diversificata del concetto di colpa grave (*faute lourde*), stante l'inevitabile localismo dell'*enforcement*[37]: la Direttiva lo definisce quale «comportamento che implica un grado significativo di mancanza di diligenza»[38]; in Italia è ravvisabile in una condotta connotata da straordinaria e inescusabile imprudenza, negligenza o imperizia, la quale presuppone che sia stata violata non solo la diligenza ordinaria del buon padre di famiglia di cui all'art. 1176 c. 1 c.c., ma anche «quel grado minimo ed elementare di diligenza generalmente osservato da tutti»[39]; in Francia viene definito come «*un comportement qui s'écarte largement du comportement qu'aurait eu dans les mêmes circonstances le bon père de famille*»[40].

4.1 *L'obbligo di autenticazione forte di matrice giurisprudenziale*

In materia di rimedi adottabili contro pagamenti non genuini si segnala una duplice linea di tendenza, tanto quella il cui baricentro riposa sulla tutela preventiva e volta ad evitare il danno (la *Strong Customer Authentication*, tipizzata dall'art. 4, comma 30, Dir. 2015/2366[41]), quanto quella successiva e volta a contenerlo (*ex post* rispetto al primo pagamento contestato: Sms o e-mail Alert; sistemi di monitoraggio antifrode).

[37] *Study on the Impact of Directive 2007/64/Ec on Payment Services in the Internal Market and on the Application of Regulation (Ec) No 924/2009 On Cross-Border Payments in the Community*, pp. 81-2 e 151.
[38] 72° considerando, Dir. 2366/2015.
[39] Cass., 19 novembre 2001 n. 14456, in *I Contratti*, 2002, p. 804.
[40] G. Cornu, *Vocabulaire juridique*, PUF, Paris 2007, 7ª éd., p. 387. Sul tema specifico cfr. S. Torck, *L'exécution et la contestation des opérations de paiement*, in *Sem. Jur., éd. Gén.*, 2010, p. 1033 ; N. Kilgus, *L'évolution des procédures de contestation des paiements*, in *Revue de Droit bancaire et financiere*, 2018, Dossier 11; A. Boujeka, *La charge du risque d'utilisation illicite d'une carte bancaire*, in *Dalloz*, 2008, p. 454.
[41] Testualmente «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»: così art. 1, comma 1, lett q-bis, d.lgs. 11/10.

Con riguardo ai sistemi di sicurezza di natura preventiva, uno degli slogan associati alla PSD2 è che essa realizza la transizione da un sistema di autenticazione monofattore a quello doppio/multi fattore[42], richiedendo la predisposizione, da parte dell'intermediario, di un sistema che combina più paradigmi di autenticazione, venendo all'utente richiesto qualcosa che solo egli conosce, qualcosa che solo egli possiede e/o qualcosa che solo egli è[43].

Nel nostro sistema, tuttavia, l'obbligo di predisposizione di sistemi siffatti era già previsto, dapprima per via giurisprudenziale (tramite il ricorso alle regole del diritto generale delle obbligazioni e a quelle della responsabilità per attività pericolosa), e successivamente in virtù della legislazione subprimaria e speciale, dando avvio un generale processo di definizione e tipizzazione giurisprudenziale del corretto comportamento del prestatore di servizi[44].

Dalla *law in action* dell'ABF, che è la giurisprudenza più copiosa sul punto (e qui emerge vistosamente la rilevanza del creazionismo giurisprudenziale e la circostanza che la materia dei servizi di pagamento rappresenti un laboratorio particolarmente prolifico in cui verificare i rapporti tra "giurisdizione" e legislazione), emerge che entrambi gli approcci (tanto quello che muove dalla disciplina generale, quanto quello che si rifà alla disciplina subprimaria) assumono quale punto focale dell'analisi l'esigenza di garantire *l'adeguatezza* dei presidi di sicurezza informatica allo scopo e agli standard consentiti dallo sviluppo della tecnologia e aggiornato all'evoluzione del fenomeno criminale[45]. È questo (l'adeguatezza) lo stilema di giudizio assunto dalla giurisprudenza pratica, la quale giunge all'enunciazione di un obbligo di autenticazione forte, muovendo dal presupposto che la diligenza dell'accorto banchiere implichi, sul piano del diritto generale dei contratti, l'obbligo di adozione di un modello organizzativo adeguato alla tipologia di operazioni posta in essere: appurato che banca debba sottostare al canone dell'art. 1176, comma 2, c.c. (noto essendo che l'attività bancaria è attività

[42] A partire dal 14 settembre 2019: cfr. art. 38, comma 2, Regolamento delegato (UE) 2018/389 della Commissione del 27 novembre 2017 che integra la Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri.

[43] Artt. 1, comma 1, lett. q-bis; 10 bis, comma 1, d.lgs. 11/10 aggiornato.

[44] La previsione è, invece, di assoluta novità per il sistema francese: per un primo commento cfr. P. Storrer, *Derrière la DSP 2: le règlement Authentification forte et Communication sécurisée*, in *Revue Banque*, 2018, p. 86; J. Lasserre Capdeville, J. Bernardin, *Une évolution notable des services de paiement: l'exigence d'authentification forte*, in *Banque et Droit*, 2019, p. 13.

[45] Coll. coord., Dec. n. 3498/2012.

riservata[46] e ascritta alla categoria delle attività pericolose, art. 2050 c.c.), lo sforzo tecnico protettivo richiesto doveva essere idoneo a prevenire possibili eventi pregiudizievoli[47]. Si è statuita, dunque, in relazione ad una controversia relativa a fatti accaduti nel 2009, l'inidoneità della sola *password* statica a tutelare il cliente stante l'esistenza, già all'epoca, di «mezzi più efficienti per fronteggiare il fenomeno della pirateria informatica ... ragione sufficiente per indurre a concludere che un sistema di protezione ad un solo fattore … non può essere considerato misura sufficiente a proteggere adeguatamente il cliente»[48].

Quantunque il dato letterale taccia sul punto, il silenzio della normativa non può ragionevolmente precludere di ritenere che «la mancata adozione delle misure idonee di sicurezza dei codici debba integrare anch'essa un comportamento doloso o gravemente colposo»[49].

La ricostruzione poggia le proprie basi dogmatiche sul principio del rischio d'impresa, sul presupposto, cioè, che sia «razionale far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente "pericolose", che interessano un'ampia moltitudine di consumatori o utenti, sull'impresa, in quanto quest'ultima è in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ribaltare sulla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi»[50].

Sul piano subprimario, la prima menzione della necessità di un sistema multi-fattore è stata anticipata dal 16° aggiornamento della Circolare n. 285/2013 della Banca d'Italia[51], la quale, nel recepire gli "*Orientamenti finali sulla sicurezza dei pagamenti via Internet*" emanati da EBA il 19 dicembre 2014[52], ha introdotto una specifica Sezione volta a disciplinare gli obblighi imposti alle banche che prestano servizi di pagamento tramite canale internet.

[46] Coll. Milano, Dec. n. 1241/2010.
[47] Coll. coord., Dec. n. 3498/12. Ancora in questi termini si esprime la Corte di cassazione, da ultimo nella sentenza 9158 del 12 aprile 2018 su www.dirittobancario.it.
[48] Coll. Milano, Dec. n. 1506/2010.
[49] Coll. coord., Dec. nn. 6166 e 6168, del 2013.
[50] ABF, Dec. n. 1111/2010.
[51] Circolare n. 285/2013 del 17 maggio 2016 "*Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica*" introduce la nuova Sezione VII "*Principi organizzativi relativi a specifiche attività o profili di rischio*".
[52] ABE/GL/2014/12_Rev1, del 19 dicembre 2014; ma il tema era già stato anticipato nelle *Recommendations For The Security Of Internet Payments*, del dicembre 2013.

4.2. *L'obbligo di autenticazione forte contenuto nella Direttiva*

Il tema della sicurezza, uno dei pilastri tanto della prima quanto della seconda versione della normativa che occupa, viene svolto sulla base dell'assunto che, in materia, è impossibile raggiungere la totale invulnerabilità di un sistema per un periodo prolungato; posto dunque che un margine di rischio è ineliminabile, accorgimenti vengono imposti allo scopo di «mitigare» il rischio, non eliminarlo[53].

Col passaggio dalla PSD1 alla PSD2 si ritiene comunemente normata la transizione dalle regole di autenticazione monofattore a quelle multifattore.

Se è vero, come ricordato, che l'obbligatoria predisposizione di un sistema multifattore non ha carattere di novità nel nostro sistema, il regolatore europeo è intervenuto, sia in sede di legislazione primaria, sia nei *Regulatory technical standards*[54], ad imporre requisiti di sicurezza aggiuntivi e rigorosi, richiedendosi che le misure di sicurezza che presidiano all'autenticazione del pagamento non siano solo plurime (multifattore), ma anche indipendenti e collegate ai parametri della transazione.

Direttiva e decreto di recepimento (rispettivamente, artt. 4, comma 1, n. 30; e 1, comma 1, lett. q-bis) impongono il requisito dell'indipendenza delle misure di sicurezza tra loro, tipizzando dunque la relazione che deve improntarne il rapporto, tale, cioè, che la violazione di una non comprometta l'affidabilità delle altre.

L'assunto è che la piena operatività del sistema di autenticazione multifattore si fondi sull'indipendenza tra le singole misure di sicurezza. L'esistenza di una relazione funzionale tra di esse consentirebbe di eludere il doppio controllo delle credenziali, e rendere, nei fatti, il sistema di autenticazione (non più forte ma) debole.

La necessaria presenza di suddetto requisito era tuttavia già prevista nel nostro ordinamento. La giurisprudenza dell'ABF ha, a più riprese, riconosciuto la portata dirimente allo stesso, ravvisando in capo all'intermediario gli estremi della condotta negligente, non rispettosa della diligenza ad esso richiesta nell'esecuzione delle proprie obbligazioni, nella predisposizione misure di sicurezza tra loro in rapporto di reciproca dipendenza, consentendo che la violazione delle credenziali relative alla

[53] EBA, *Final Report Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)*, 12 dicembre 2017.

[54] Regolamento delegato (UE) 2018/389 della Commissione del 27 novembre 2017, che integra la Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri.

conoscenza comprometta anche le credenziali relative al possesso, in luogo, per converso, della necessaria segregazione logica tra il canale dispositivo della transazione e il canale dispositivo verso il pagatore[55].

Sul piano tecnico, la novità più profonda della PSD2 è, tuttavia, quella relativa all'imposizione di un sistema di autenticazione forte in cui l'elemento dinamico sia collegato ai parametri della transazione (all'importo e al beneficiario specificati dal pagatore al momento di disporre l'operazione)[56].

Di particolare interesse, anche in tema di riparto probatorio, è la sanzione per la mancata predisposizione del sistema di autenticazione forte nel senso normativamente richiesto, che viene prevista -come già ricordato- nell'imputazione a titolo di responsabilità oggettiva per il prestatore, salva la prova della frode dell'utente (art. 12, comma 2-bis, D.lgs. 11/2010). Il legislatore, nel ricorrere al modello di responsabilità oggettiva più severo, appare utilizzare la "comminatoria" di responsabilità quale sanzione, riconoscendole una funzione compensativa dell'ingresso dei nuovi soggetti (terze parti). La previsione dell'unica esimente della frode (che, *a contrario*, esclude la rilevanza alle ipotesi di dolo e colpa grave dell'utente) dota la sanzione di un elevato grado di afflittività, considerato che il prestatore sarà responsabile anche nelle ipotesi di dolo o colpa grave della condotta dell'utente.

Il *proportionality check* circa l'adeguatezza della sanzione appare tuttavia soddisfatto, considerato che l'importanza della norma di diritto sostanziale

[55] Coll. Roma, Dec. n. 14925/2017. L'ABF ha osservato che dalla sequenza dell'attacco informatico -articolato in quattro fasi: 1) l'utilizzo del canale telematico (ricezione da parte degli autori del *phishing* delle credenziali inviate dalla ricorrente); 2) l'uso di codici dispositivi (accesso al portale titolari e modifica del numero di utenza cui inviare il codice alfanumerico); 3) l'effettuazione degli acquisti *online*; 4) la ricezione della *password* dinamica sull'utenza sostituita e conferma della genuinità dell'operazione- era emerso come nel servizio bancario oggetto di contestazione l'efficacia del meccanismo di autenticazione fosse inscindibilmente legata all'utenza telefonica, e che, dunque, la modifica del numero avrebbe dovuto generare una notifica (anche attraverso il medesimo canale telefonico), tale da allertare il titolare nel caso in cui la modifica non sia stata da lui effettuata (nello stesso senso cfr. anche Coll. Roma, Dec. n. 15027/2017; Coll. Bologna, Dec. n. 6987/2017.

[56] L'art. 5, comma 1, lett a, Regolamento Delegato (Ue) 2018/389, cit.: richiede che «a) l'elemento dinamico sia collegato ai parametri della transazione il pagatore è informato dell'importo dell'operazione di pagamento e del beneficiario; b) il codice di autenticazione generato è specifico per l'importo dell'operazione di pagamento e il beneficiario concordato dal pagatore al momento di disporre l'operazione; c) il codice di autenticazione accettato dal prestatore di servizi di pagamento corrisponde all'importo specifico originario dell'operazione di pagamento e all'identità del beneficiario approvato dal pagatore; d) qualsiasi modifica dell'importo o del beneficiario comporta l'invalidamento del codice di autenticazione generato»; cfr. anche art. 97, par. 2, Dir. 2366/2015.

che si assume violata[57], con particolare riferimento alla *ratio* e agli interessi tutelati, appare giustificare il grado di afflittività della previsione, funzionale alla sua effettività e dissuasività[58].

Tornando alle caratteristiche del sistema di sicurezza, oggetto della valutazione è, dunque, principalmente l'adeguatezza dello stesso a prevenire l'uso fraudolento degli strumenti di pagamento ed elevare al massimo livello attualmente possibile il grado di protezione del cliente[59]. L'Arbitro bancario e finanziario ha, al riguardo, una posizione che a me pare molto ragionevole (intendendo *ragionevole* nel senso visto in apertura, ossia di aderenza alla realtà concreta) giacché ritiene che la pur elevata capacità protettiva dell'autenticazione a due fattori (la quale garantisce una probabilità molto bassa che entrambi i canali siano compromessi), non valga di per sé a far automaticamente presumere un negligente comportamento del cliente, dovendosi considerare, oltre al meccanismo offerto, anche l'intero sistema di controlli predisposto dall'intermediario[60]. Questa impostazione ricostruttiva presuppone il dato, aderente alla realtà, che per quanto la forzatura di un sistema a due fattori sia improbabile, non è possibile predicare la totale invulnerabilità per alcun sistema (considerata la continua evoluzione dei metodi di aggressione informatica).

L'impiego dell'OTP non può, dunque, dare origine ad un automatismo deduttivo in virtù del quale ad esso corrisponda una presunzione assoluta di negligenza dell'utente, ma può condurre ad una valutazione più rigorosa della condotta dello stesso.

Il tema è sviluppato nei medesimi termini in Francia, dove la *Cour de cassation* ha escluso la configurabilità di una presunzione di colpa grave dell'utente solo in ragione della presenza di un sistema di autenticazione forte (quantunque non considerando obbligatoria la sua predisposizione)[61].

Il sillogismo, proposto in sede difensiva dagli intermediari, che la predisposizione di un sistema multi-fattore implichi necessariamente un'autorizzazione o la colpa grave del pagatore viene dunque escluso negli

[57] Ricorrendo al principio, elaborato in sede comunitaria, della necessaria proporzionalità tra sanzione e violazione: CGUE, sentenza del 9 novembre 2016, *Home Credit Slovakia a.s. contro Klára Bíróová*, C-42/15, § 63.

[58] CGUE, sentenza del 27 marzo 2014, *LCL Le Crédit Lyonnais SA contro Fesih Kalhan*, C-565/12, § 47.

[59] Ex *multis* Coll. Roma, Dec. n. 6606/16.

[60] Coll. Roma, Dec. n. 2660/2012.

[61] *Cour cass.* 18 gennaio 2017 in *Sem. Jur., éd. Entr.*, 2017, p. 1122, con nota di K. Rodriguez; in *Banque et Droit*, 2017, p. 32, con nota di G. Helleringer e Th. Bonneau; in *Dalloz*, 2017, p. 156 e *idibem*, 2018, p. 259, con osservazioni di A. Aynès; in *RTD com.*, 2017, p. 154, con nota di D. Legeais.

ordinamenti interni, evitando così che il generalizzato innalzamento del livello di sicurezza dei pagamenti possa sortire un paradossale effetto nocivo per gli utenti[62].

Questo è un dato su cui soffermarsi: la valutazione della condotta della banca dovrà essere oggetto di differenti criteri di giudizio, a seconda che abbia adottato o meno un sistema di autenticazione multi-fattore.

Dell'obbligatoria adozione di (almeno) due delle categorie tra quelle della conoscenza, del possesso e dell'inerenza, il Reg (EU) No 1093/2010 e la *Eba opinion*, indicano, a livello esemplificativo[63], che prova della prima possono essere considerati *password*, pin, risposte a domande di sicurezza, frasi di accesso; non, invece, i dettagli della carta o il relativo codice di sicurezza[64]. Prova della seconda, che può avere ad oggetto un bene anche non materiale, quale un'app[65], può essere costituita da un dispositivo (posto che la generazione o la ricezione di un elemento dinamico sul dispositivo costituisce un «*reliable means to confirm possession*»[66]), dalla prova della generazione di una OTP da parte di un software o di un hardware (come token, sms, e-mail), ed, ancora, dalla firma digitale, dalle carte nelle quali sia presente il QR Code; al contrario, il numero di carta ed il codice di sicurezza non sono prova di elementi del possesso[67]. La categoria dell'inerenza, la più innovativa ed in evoluzione delle tre, riferendosi ad elementi intrinseci relativi a caratteristiche biologiche e comportamentali, a loro volta inerenti a proprietà fisiche del corpo e a caratteristiche fisiologiche, comprende la scansione della retina e dell'iride, delle impronte digitali, delle vene, del viso, il riconoscimento vocale, le dinamiche di digitazione (identificando l'utente dal modo in cui digita i tasti al computer), e la verifica di tali elementi determina «*very low probability of an unauthorised party being authenticated as the payer*»[68].

[62] L. C. Henry Marie, L. Guinamant, *L'utilisation frauduleuse de la carte bancaire après hameçonnage: la recherche d'un équilibre*, in *Dalloz*, 2018 p. 2316.
[63] Art. 1, comma 1, lett q-bis, d.lgs. 11/2010.
[64] *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* (EBA-Op-2019-06, 21 giugno 2019), p. 6.
[65] *EBA-Op-2019-06*, cit. *supra*, p. 6.
[66] *EBA Opinion on the implementation of the RTS*, pubblicata nel giugno del 2018 (EBA-Op-2018-04), disponibile sul sito https://eba.europa.eu/-/eba-publishes-opinion-on-the-implementation-of-the-rts-on-strong-customer- authentication-and-common-and-secure-communication (ultimo accesso 28 dicembre 2019).
[67] *EBA-Op-2019-06*, cit. *supra*, p. 6.
[68] Art. 8, par. 1, Commission Delegated Regulation (EU) 2018/839 of 27 November 2017 supplementing Directive (EU) 2015/2366 of European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and

5. *Vincoli di solidarietà tra IP*

I menzionati aspetti *Tech* hanno un rilevante punto di caduta anche giuridico, risultando determinanti in caso di controversie sulla ripartizione della responsabilità tra i diversi IP coinvolti in una stessa operazione di pagamento e sull'ammissibilità (e consistenza) di alcuni mezzi di prova.

Il concetto di responsabilità, ed, in particolare, la ripartizione della responsabilità tra i diversi soggetti coinvolti rappresenta una tematica cruciale in quanto strettamente connessa ad una delle maggiori novità introdotte dalla PSD2, ossia l'estensione dell'ambito di applicazione della nuova Direttiva anche ai PISP (*Payment Initiation Service Provider*: servizio con cui si dispone un ordine di pagamento su richiesta dell'utente e rispetto a un conto di pagamento detenuto da altro intermediario[69]) ed AISP (*Account Information Service Provider*: servizio *online* per raccogliere informazioni da conti di pagamento detenuti dall'utente presso altri intermediari[70]).

Nello specifico, come già accennato, la PSD2 non fa dipendere la prestazione di servizi di disposizione di ordini (ovvero di informazione sui conti) dall'esistenza di un rapporto contrattuale tra il PISP/ AISP ed il prestatore di servizi di pagamento di radicamento del conto (ASPSP: *Account Servicing Payment Service Provider*[71]).

L'art. 11, D.lgs. 11/10, stabilisce che, nel caso di operazione di pagamento non autorizzato, incomba sull'ASPSP l'obbligo di rimborso dell'operazione (immediatamente o entro la giornata operativa successiva), a prescindere dall'eventuale coinvolgimento di un PISP. Nel caso, però, l'ordine dell'operazione di pagamento non autorizzata sia disposto mediante Pisp, quest'ultimo è gravato dell'obbligo di rimborso all'ASPSP, che ne faccia richiesta, degli importi già rimborsati al pagatore (comma 2-bis). Entrambi possono sempre dimostrare che l'operazione era stata autenticata e ottenere la restituzione delle somme rimborsate (l'ASPSP dall'utente e il PISP dall'AISP: comma 3).

Il meccanismo restitutorio previsto dal legislatore, volto al fine di regolare il diritto al rimborso dell'utente e ripartire le responsabilità tra i corresponsabili, prevede, dunque, che nel caso in cui sia stata disposta un'operazione di pagamento non autorizzata mediante un PISP, l'ASPSP sia chiamato a rimborsare immediatamente *prima facie* il pagatore dell'importo

common and secure open standards of communication.
[69] Art. 4, par. 1, n. 19, Dir. 2366/2015.
[70] Art. 4, par. 1, n. 18, Dir. 2366/2015.
[71] Art. 4, par. 1, n. 17, Dir. 2366/2015.

corrispondente all'operazione di pagamento non autorizzata, ponendo una delicata questione di ripartizione di responsabilità tra prestatori di servizi di pagamento. È pur vero che la medesima disposizione introduce un diritto di regresso in capo all'ASPSP nei confronti del PISP; qualora, tuttavia, quest'ultimo sia responsabile dell'operazione di pagamento non autorizzata[72], l'eventuale assenza di un rapporto contrattuale potrebbe rendere meno agevole l'applicazione di tale norma.

Il tema si sposta dunque sulla necessità di stabilire se il rapporto richiamato si atteggi nei termini della solidarietà o meno.

Si tratta di valutare se, posta l'astratta configurabilità pratica del concorso di colpa –ossia che in un'operazione contestata, sia l'ASPS che il PISP possano essere responsabili, nel segmento di operazione di loro competenza, di disfunzioni nel sistema di sicurezza- dal tenore della norma e dall'impianto sistematico della Direttiva possa ravvisarsi un vincolo di solidarietà tra i corresponsabili; verificare, cioè, se, posto il principio generale di solidarietà nei rapporti obbligatori con una pluralità di debitori, la fattispecie contemplata dall'art. 10, sia ascrivibile, normativamente, alle ipotesi di cui all'art. 2055, comma 1, c.c. e, in materia qui affine, all'art. 120 *quater*, 7 comma, d. lgs. 1° settembre 1993, n. 385, Testo Unico delle leggi in materia bancaria e creditizia (d'ora in avanti T.U.B.), i quali sono calibrati sulle esigenze di tutela della vittima.

È pacifico che la previsione di un vincolo di solidarietà, ampliando la schiera dei soggetti legittimati ai quali può rivolgersi, sia disposta nell'interesse del debitore; così come incontroverso è il *favor* del diritto europeo per la pluralità dei debitori, in luogo dell'unicità[73].

È altresì pacifico che l'imperativo metodologico europeo (e, quindi, anche interno) richieda la centralità dell'approccio rimediale nei termini dell'effettività della tutela e il superamento culturale della mera ricostruzione dogmatica delle fattispecie normative[74].

La lettura nei termini della solidarietà presenta, da questa angolatura, dei limiti, in primo luogo politici. La necessaria adozione di un angolo prospettico che trascenda la dogmatica concettuale in ragione delle teorie funzionaliste che elevano il piano della tutela a momento centrale della garanzia dei diritti, ha reso il canone dell'effettività il perno concettuale

[72] Sul punto cfr. anche quanto previsto dall'art. 92, par. 1, Dir. 2366/2015.

[73] Cfr., per un'impostazione anche europea, *Le nuove obbligazioni solidali*, a cura di U. Breccia e F. D. Busnelli, in *Quaderni della Rivisita di diritto civile*, Cedam, Padova 2016.

[74] Il richiamo all'effettività è presente anche nella struttura motivazionale dei giudici di legittimità: cfr. per tutte Cass., S.U., sentenza del 12 dicembre 2 14, n. 26242, in *Foro it.*, 2015, I, p. 862.

che deve informare di sé le scelte dell'interprete[75]. Nel caso dell'ABF, e degli *Ombudsmen* in àmbito finanziario, poi, -che sono i decisori maggiormente coinvolti in liti di questo tipo- questo punto di osservazione di arricchisce di un elemento ulteriore. In Italia, alla luce dell'evoluzione della natura dell'attività bancaria, comprensiva, oggi, oltre che dei tradizionali obiettivi della vigilanza prudenziale propriamente detta (racchiusi nella *grundnorm* dell'art. 5 T.U.B.) anche della tutela del cliente (art. 127 T.U.B.)[76], all'ABF viene riconosciuta una duplice funzione: immediata -di risoluzione delle controversie private[77]- e mediata -di regolazione del mercato, producendo le pronunce un effetto conformativo sulla condotta degli intermediari[78]. Il portato, dunque, della funzione regolatoria svolta dall'ABF, è la necessaria considerazione dell'effetto conformativo delle sue pronunce[79]. L'interpretazione e l'applicazione consequenzialista delle norme

[75] L'effettività, divenuta parola chiave delle moderne riflessioni sul diritto, più che un concetto dotato di una propria autonomia e rilevanza normative, costituisce una formula riassuntiva di un indirizzo di politica del diritto (F. Snyder, *New Directions in European Community Law*, Weidenfeld and Nicholson, London 1990, p. 3). Per un inquadramento in ottica moderna e trasversale del principio d'effettività Ad. di Majo, *La tutela dei diritti*, 4° ed., Giuffrè, Milano 2003, pp. 1-2.

[76] Non ancillare rispetto alle finalità dell'art. 5 ma autonoma, equivalente sul piano valoriale, dotata di valenza di interesse pubblico generale, strumentale ai valori obiettivo della vigilanza prudenziale: cfr. I. Visco, *Considerazioni finali del Governatore della Banca d'Italia*, 2010, p. 8.

[77] Art. 127 T.U.B..

[78] Art. 5 T.U.B.; cfr. M. Perassi, *Il ruolo dell'ABF nell'ordinamento bancario: prime riflessioni*, in *Analisi Giuridica dell'Economia*, 2011, pp. 154 ss.; A. Zoppini, *Appunti in tema di rapporti tra tutele civilistiche e disciplina della vigilanza bancaria*, in *Banca, borsa, tit. cred.*, 2012, pp. 26 ss.; P. Sirena, *Il ruolo dell'Arbitro Bancario Finanziario nella regolazione del mercato creditizio*, in *Oss. dir. civ. comm.*, 2017, p. 3 ss. e in *Principi, regole, interpretazione. Contratti e obbligazioni, famiglie e successioni: Scritti in onore di Giovanni Furgiuele*, a cura di G. Conte e S. Landini, Universitas Studiorum, Mantova 2017, p. 511.

[79] Il tema dell'efficacia conformativa dei sistemi ADR - *Alternative Dispute Resolution*- è tipico dei settori regolati (dove gli organismi di risoluzione vengono generalmente incardinati presso i regolatori, dando origine a delle figure ibride, nelle quali coesistono elementi privatistici e pubblicistici: D. Marrani, Y. Farah, *ADR in the Administrative Law: a Perspective from the United Kingdom*, in *Alternative Dispute Resolution in European Administrative Law*, a cura di D. C. Dragos e B. Neamtu, Springer, Berlin-Heidelberg 2014, 259 ss.; in Italia aveva già individuato la tendenza all'espansione dei "moduli misti" L. Torchia, *Il controllo pubblico della finanza privata*, Cedam, Padova 1992, p. 10; A.A. Dolmetta e U. Malvagna, Sul nuovo "*ADR Consob*", in *Banca borsa, tit. cred.*, 2016, p. 251; M. Stella, *Lineamenti degli arbitri bancari e finanziari*, Cedam, Padova 2016, p. 98; M. Remàč, *Coordinating Ombudsmen and the Judiciary: A Comparative View on the Relations Between Ombudsmen and the Judiciary in the Netherlands, England and the European Union*, Intersentia, Cambridge 2014, p. 7; C. Gill, J. Williams, C. Brennan e N. O'Brien, *The Future of Ombudsman Schemes: Drivers for Change*

assume dunque una connotazione del tutto specifica, poiché, collocata nel quadro più complesso della vigilanza bancaria, rappresenta il punto di congiuntura tra l'attività decisoria e la regolazione del mercato svolta dagli organismi di risoluzione[80]. In quest'ottica, l'analisi deve essere svolta con approccio critico che non si appiattisca sulla retorica del contraente debole, nella consapevolezza che gli interventi "a supporto" della parte debole, pur giustificati nella loro impostazione di base, devono tuttavia essere contenuti per evitare comportamenti opportunistici dei consumatori. Le letture enfaticamente pro-consumeriste rischiano, cioè, un paradossale effetto *boomerang*, finendo col danneggiare il soggetto che si intende proteggere.

Nel caso che interessa, considerato che «la prestazione di servizi di disposizione di ordine di pagamento non è subordinata all'esistenza di un rapporto contrattuale»[81], sembra che la regola maggiormente protettiva per l'utente e appagante in termini di effettività economica del sistema, venga integrata dall'azione diretta verso la parte contrattuale più vicina (alla quale viene normativamente attribuita una posizione sostanzialmente di garanzia)[82]: l'adozione di un tale congegno ipersemplificato consolida la fiducia del pagatore (uno degli obiettivi della PSD2, insieme alla sicurezza dei pagamenti e all'integrità del mercato dei sistemi pagamento) e agevola il conseguimento del risarcimento del danno risparmiandogli l'onere di dimostrare l'effettiva distribuzione della responsabilità tra i soggetti coinvolti[83].

and Strategic Responses, Queen Margaret University, Edinburgh 2013, p. 10; S.F. Ali, *Consumer Financial Dispute Resolution in a Comparative Context: Principles, Systems and Practice*, New York, Cambridge University Press 2013, p. 57; I. Benöhr, *Alternative Dispute Resolution for Consumers in the European Union*, in *Consumer ADR in Europe: Civil Justice Systems*, a cura di C. Hodges, I. Benöhr e N.Creutzfeldt-Banda, Hart Publishing Ltd, Oxford 2012, p. 1; I. Ramsay, *Consumer Redress and Access to Justice*, in *International Perspectives on Consumer's Access to Justice*, a cura di C.E. Rickett, T. G. W. Telfer, CUP, Cambridge 2003, p. 167 ss.

80 Esempio più significativo nel nostro ordinamento è la previsione degli artt. 13 e 23 Cod. com. el., il cui combinato disposto correla la soluzione delle controversie agli obiettivi generali del settore e, specificamente, quelli della regolazione.

81 Art. 66, par. 5, Dir. 2015/2366.

82 Così V. De Stasio, *Riparto di responsabilità e restituzioni nei pagamenti non autorizzati*, in questo Volume.

83 Per una critica a quest'impostazione v. A. Gourio, M. Gillouard, *La nouvelle directive sur les services de paiement (DSP 2),* in *Revue de Droit bancaire et financier*, 2016, comm. 91, i quali rilevano che quella introdotta è una la forma di responsabilità del terzo «*pour autrui sans existence d'un lien juridique quelconque entre les personnes concernées apparaît totalement exorbitant du droit commun des États membres et des principes du droit de la responsabilite, animé seulement par l'objectif d'une indemnisation facilitée du payeur*».

6. *La ripartizione degli oneri probatori*

Pacifica la configurabilità di un concorso colposo del pagatore[84], l'onere di provarne la negligenza (o la colpa grave o la frode) incombe, come ricordato, sull'intermediario.

Nell'apprestare la disciplina (e rinnovarla) il legislatore adotta un modello di tutela consolidato nella legislazione diseguale (non solo consumeristica, ma che di essa riproduca gli antagonismi di asimmetria), lavorando con particolare attenzione alla ripartizione degli oneri probatori (art. 10, comma 7, d.lgs. 11/2010)[85].

È pacifico che si sia in presenza di un'inversione dell'onere della prova, non derogabile dall'autonomia privata (la norma è imperativa)[86].

Il tema è un classico della contrattazione diseguale: è un dato acquisito nel dibattito giuridico, infatti, che la tutela del della parte debole del rapporto negoziale si svolga anche attraverso una speciale ripartizione degli oneri probatori, posto che il principio dispositivo (comune a tutti gli ordinamenti, e da noi racchiuso nell'art. 2697 c.c.)[87], è, nella sua formulazione pura, inadeguato alle liti disuguali, rischiando di danneggiare la parte debole.

Comune è, dunque, la tendenza dei sistemi europei a spostare l'assolvimento dell'onere della prova sul professionista, intanto per motivi politici (quale strumento di riequilibrio delle posizioni asimmetriche) e, poi, anche processuali (facilitare l'accertamento dei fatti assegnando l'onere della prova al soggetto che si trova nella posizione migliore per soddisfarlo)[88].

Vorrei però sottolineare che il tema della riferibilità o vicinanza della prova appare, contrariamente ad una convinzione ampiamente diffusa in dottrina, residuale rispetto alle scelte politiche e sistematiche.

Pacifica, dunque, la deroga realizzata per via normativa al principio dell'*actori incumbit probatio*, va verificato, prima, come l'inversione degli oneri probatori si raccordi con la possibilità di fornire la prova liberatoria, riconosciuta in capo all'ASPS, e, poi, quali siano i mezzi di prova idonei ad

[84] Cfr., da ultimo, Coll. Bari, Dec. n. 16875/2018.

[85] Sul problematico rapporto tra l'evoluzione tecnologica e il diritto delle prove: P. Leclercq, *Les titres dématérialisés de paiement et de crédit,* in *Le droit privé français à la fin du XXe siècle. Études offertes à Pierre Catala*, Litec, Paris 2001, p. 785; B. Geva, *Bank Collections and Payment Transaction—A Comparative legal Analysis*, OUP, Oxford 2001; spec. 580.

[86] 72° Considerando, Dir. 2366/2015.

[87] *International Encyclopedia of Comparative Law,* vol. *XI,* «Torts», diretta da A. Tunc, I, Tübingen, The Hague 1983, p. 149-150.

[88] Da Ultimo, N. Hoffshir, *La charge de la preuve en droit civil*, Dalloz, Paris 2014.

esonerare l'ASPS dalla propria responsabilità.

Considerato il problematico ottenimento delle evidenze necessarie per dimostrare la fondatezza della propria posizione, all'intermediario -che non ha accesso ad informazioni relative all'organizzazione dei propri clienti ed alle modalità di custodia dei dispositivi, ulteriori rispetto a quelle dichiarate dai clienti stessi in sede di denuncia e, eventualmente, di giudizio- viene riconosciuta l'ammissibilità del ricorso a prove di natura presuntiva[89]. Tali presunzioni -giudiziali, *ante-judiciaire*[90]- sono state tipizzate, con riferimento alle ipotesi maggiormente diffuse, dalla giurisprudenza, e, nel caso dell' *internet banking*, sono ravvisabili nella decettività del messaggio di abboccamento e nel livello di sofisticazione della frode informatica perpetrata; nel caso di utilizzi fraudolenti, sono individuabili nella dotazione del microchip; nel lasso temporale intercorrente tra il furto e il primo prelievo contestato; nell'alternanza tra operazioni legittime e illegittime; nella tempestività/tardività della richiesta di blocco e della verifica del conto corrente[91].

Nonostante l'apparente chiarezza normativa, il tema della ripartizione dell'onere della prova, crinale lungo il quale si misura l'effettività della tutela, ha dato luogo a decisioni controverse negli ordinamenti interni.

In Francia, ad esempio, la *Cour de cassation*, dopo una sentenza iniziale estremamente criticata, ha dovuto pronunciarsi a più riprese -e talora in modo contraddittorio[92]- elaborando criteri ermeneutici che non privilegiassero unidirezionalmente le interpretazioni in senso preferenziale per il consumatore.

La Corte, infatti, aveva inizialmente statuito -in materia di *internet banking*- che, pur in presenza di un sistema di sicurezza molto elevata (con sistema di autenticazione a due fattori[93]), la prova dell'utilizzo dei dati personali (nella specie: *user id*, *password*, credenziali personali e OTP dinamica inviata sull'utenza telefonica) non fosse sufficiente ad esonerare l'ASPS, affermando la necessità della prova dell'avvenuta divulgazione da parte dell'utente, la quale «*ne peut se déduire du seul fait que l'instrument*

[89] Coll. Napoli, Dec. n. 11189/2016.

[90] A. Danis-Fatôme, *Paiement à distance et preuve de la négligence grave de l'utilisateur d'un service de paiement : une nouvelle probatio diabolica?* in *Revue des contrats*, 2017, p. 274.

[91] Il ritardo nella denuncia è stato, invece, ritenuto irrilevante quando non concorrente a determinare l'entità del danno: cfr. Coll. Roma, Dec. n. 598/2014.

[92] D. Legeais, *Hameçonnage*, in *RTD com.*, 2018, p. 436.

[93] L'intermediario eccepiva la negligenza grave, ai sensi dell'articolo L. 133-19, IV, *Cod. mon. fin.*, sul presupposto che il carattere altamente sicuro del dispositivo implicasse che l'utente avesse «*sinon divulgué ses données personnelles à un tiers, à tout le moins laissé celles-ci à disposition du tiers ayant frauduleusement effectué les débits litigieux*».

de paiement ou les données personnelles qui lui sont liées ont été effectivement utilisés»[94].

L'impostazione difensiva dell'intermediario, che inferiva dall'utilizzo dei dati personali la divulgazione degli stessi a terzi e la conseguente negligenza nella custodia, obbligando l'utente a dare, a sua volta, prova contraria della presunzione, non è stata condivisa dalla Corte, la quale, muovendo dal dato normativo (la lettura congiunta degli artt. L. 133-18, IV, e L. 133-23, *Cod. mon. fin.*), ha dedotto la previsione di un'inversione dell'onere della prova, addossando al prestatore di servizi di pagamento l'onere di dimostrare la negligenza dell'utilizzatore.

Le ragioni del rifiuto della *Cour* di alleggerire il carico probatorio incombente sull'ASPS apparivano di natura politica e giurisprudenziale, inscrivendosi la sentenza essa nel solco delle decisioni precedenti marcatamente *consumer oriented*[95]. Quantunque, infatti, si rinvenissero precedenti di legittimità di segno opposto (che, non ravvisando alcuna inversione dell'onere della prova, applicavano le regole di diritto comune)[96], l'indirizzo maggioritario della giurisprudenza era caratterizzato da un marcato *favor* verso il pagatore (coinciso, sul piano temporale, con l'adozione della legge n° 2001-1062 del 15 novembre 2001 sulla *sécurité quotidienne*)[97], tale da configurare una «*présomption de comportement non*

[94] *Cour cass.*, 18 genn. 2017, in *Dalloz, 2017,* con nota di X. Delpech; in *Sem. Jur., éd. G.*, 2017, p. 117, con nota di K. Rogriguez, *Contestation des opérations de paiement sur Internet: le fardeau de la preuve pour le banquier*; in *Sem. Jur., éd. G.*, 2017, p. 241, con nota di J. Lasserre Capdeville, *Précisions sur la question de la preuve en cas de fraude au paiement sur internet*. Nel caso di specie, l'intermediario lamenta, al contrario, la "negligenza grave", ai sensi dell'articolo L. 133-19, IV, del *Cod. mon. Fin.*, e ricorre in Cassazione sul presupposto che il carattere altamente sicuro del dispositivo implicasse «*nécessairement que [son client] avait, sinon divulgué ses données personnelles à un tiers, à tout le moins laissé celles-ci à disposition du tiers ayant frauduleusement effectué les débits litigieux*».
Che, per la dottrina maggioritaria, è e rimane una questione sostanziale.

[95] Cfr. A. Hontebeyrie, *Perte ou vol d'une carte bancaire: quel régime probatoire? Réflexion sur la nature juridique du dispositif prévu à l'article L. 132-3 du Code monétaire et financier*, in *Dalloz* 2009, p. 1492.

[96] *Cour cass*. 31 maggio 2016, n° 14-29.906, in *Dalloz*, 2016, p. 2305, osservazioni di D. R. Martin e H. Synvet; in *Sem. Jur., éd. Gén.*, 2016, p. 1450.

[97] La prima applicazione della nuova disciplina è solo con la sentenza della *Cour cass.*, 2 ottobre 2007, in *Sem. Jur., éd. G*, 2008, II, p. 10014, con nota di É. Bazin; in *Dalloz*, 2007, p. 2765, con nota di L. Belaval; in *Dalloz*, 2008, p. 454, con nota di A. Boujeka; alla quale seguirono decisioni omogenee: *Cour cass.*, 21 settembre 2010, n° 09-16.534, in *Sem. Jur., éd. Entr. Aff.*, 2010, 2008, co nota di J. Stoufflet; in *Revue de Droit bancaire et fin.*, 2011, comm. 40, con nota di F.-J. Crédot, T. Samin; nonché *Cour cass.*, 28 marzo 2008, in *Sem. Jur., éd. Entr. Aff.*, 1735, con nota di P. Bouteiller; in *Dalloz*, p. 1136, con nota di V. Avena-Robardet; in *RTD com.*, 2008, p. 607, con nota di D. Legeais.

fautif» dell'utente[98], posto che, non solo l'utilizzazione dello strumento veniva considerata insufficiente a provare la colpa del pagatore, ma anche quella dei relativi dati riservati[99].

Tale impostazione ha però suscitato una serie di interrogativi.

Intanto, sul piano procedimentale, le decisioni non indicavano come si sarebbe dovuta provare la negligenza grave, e la prova liberatoria per l'ASPS appariva una prova impossibile[100], configurando una «*quasi-immunité*» dell'utente[101].

Sul piano sistematico, e di conseguenza, tale lettura finiva con lo svuotare di precettività la previsione del rilievo della colpa grave dell'utente; in terzo luogo, sul piano degli esiti politici, tale lettura implicava il rischio di una totale deresponsabilizzazione dell'utente (sui cui effetti v. *retro*, par. 5)[102].

La *Cour* appare quindi aver aderito, nella varietà delle possibili letture, al criterio ermeneutico dell'interpretazione più favorevole per il consumatore, il quale, invece, se non maneggiato con accortezza, rischia di creare un eccesso di frammentazione (eterogenesi dei fini rispetto all'attuale linea di *policy*), facendo incorrere le decisioni in una deriva eccessivamente garantista e producendo il paventato effetto *boomerang* di cui si è già discorso.

Nel tentativo di fornire ricostruzioni, per un verso, maggiormente aderenti alle indicazioni europee, e, per altro verso, di maggior equilibrio tra le istanze contrapposte dell'utilizzatore e dell'ASPS, la *Cour* è tornata a più

[98] D. Legeais, *Appréciation du manquement par négligence grave d'une victime d'un acte de phishing,* in *Sem. Jur., éd. Entr. Aff.*, 2017, p. 1687.

[99] L'impostazione si basava su di una lettura particolarmente rigorosa e filoconsumerista dai dati normativi: la formulazione dell'art. L. 133-19, comma 2, Cod. fin. mon., infatti, non esclude che l'utilizzazione dello strumento e dei relativi dati riservati possa essere sufficiente a provare la colpa del pagatore, ma semplicemente costituisce un invito a tener conto delle circostanze concrete e contingenti e non conferire rilevanza risolutiva all'utilizzo (K. Rodriguez, *Contestation des opérations de paiement sur Internet: le fardeau de la preuve pour le banquier*, in *Sem. Jur., éd. Entr. Aff.*, 2017, p. 1122).

[100] P. Storrer, *Utilisation frauduleuse d'un instrument de paiement: la probatio diabolica?,* in *Revue Banque*, 2017, p. 72; A. Danis-Fatôme, *Paiement à distance et preuve de la négligence grave de l'utilisateur d'un service de paiement: une nouvelle probatio diabolica?,* in *Revue des contrats*, 2017, p. 270.

[101] K. Rodriguez, *Hameçonnage et preuve de la négligence grave du client du banquier*, in *Sem. Jur., éd. Entr. Aff.*, 2018, p. 1272.

[102] S. Piédelièvre, *L'ordonnance du 15 juillet 2009 relative aux conditions régissant la fourniture de services et de paiement,* in *Gaz. Pal.*, 2009, p. 2820; più in generale J. Lasserre Capdeville, *La contestation des opérations de paiement non autorisées*, in *Revue de Droit bancaire et financier*, 2011, dossier 6; S. Torck, *L'exécution et la contestation des opérations de paiement*, cit., p. 1033; M. Roussille, *Contestation et opposition du paiement par carte bancaire*, in *Gaz. Pal.,* 2012, p. 7.

riprese sul punto, tentando di affinare i propri canoni ermeneutici.

Intanto, ha, dapprima, valorizzato l'analisi delle «*circonstances de l'espèce*»[103], introducendo il correttivo della riconoscibilità della natura fraudolenta del messaggio ricevuto dall'utente, e stabilendo che nel caso di non riconoscibilità della c.d. mail civetta, la comunicazione dei dati personali, quantunque intenzionale, è incolpevole[104]. Per converso, il cliente consapevole della natura fraudolenta del messaggio è responsabile, ma l'apprezzamento di tale consapevolezza non deve avvenire in concreto (costringendo l'intermediario anche in questo caso alla prova impossibile dello stato soggettivo dell'utente)[105], ma in astratto, alla stregua del parametro dell'uomo normalmente attento[106]. L'ASPS, dunque, deve dimostrare che l'utente, con un grado di attenzione nella norma, avrebbe dovuto nutrire dei dubbi sulla provenienza della missiva, dubbi che possono essere suscitati da indici quali: errori di ortografia; difformità degli indirizzi; difformità del logo riportato; imprecisioni sul numero di contratto menzionato, inesattezze sull'ammontare reclamato (introducendo la teoria del *faisceau d'indices*)[107].

Una riflessione sull'individuazione di ulteriori indizi dai quali dedurre la negligenza del prestatore dei servizi di pagamento, ha riguardato l'attitudine dell'indirizzo IP (*Internet Protocol*) a costituire prova della circostanza che l'ordine di pagamento sia stato impartito dal computer dell'utente[108] . Una

[103] In linea con quanto previsto anche dal 72° considerando, Dir. 2366/2015.

[104] Cass. com., 25 ottobre 2017, in *Sem. Jur., éd. Entr. Aff.*, 2017, p. 1685, con nota di D. Legeais; in *Revue de Droit bancaire et fin.*, 2017, p. 37, con nota di Th. Samin e S. Torck; in *Dalloz*, 2017, p. 2465, con nota di F. Mélin, *Utilisation frauduleuse des données personnalisées: être victime d'un hameçonnage n'exclut pas la négligence grave*, in *Dr. et proc.*, 2017, p. 262, note É. Bazin.

[105] Come dapprima statuito con la decisione della *Cour de cassation*, 25 ottobre 2017, sopra richiamata.

[106] È alla stregua di questo parametro che la *Cour* valuta gl'indizi contenuti nella mail civetta: Cass., 28 marzo 2018, in *Sem. Jur., éd. Entr. Aff.*, 2008, p. 1735, con nota di P. Bouteiller; e a p. 1496, con nota di M. Roussille; in *Revue de Droit bancaire et fin.*, 2008, con commento di A. Caprioli; in *Sem. Jur., éd. G*, 2008, II, p. 10109, con nota di É. Bazin; in *Dalloz*, 2008, p. 1136, con nota di V. Avena-Robardet; in *RTD com.*, 2008, p. 607, con nota di D. Legeais.

[107] Così come elencati nella decisione della *Cour de cassation* del 6 giugno 2018, che può essere letta in *Comm. Com.*, 2018, p. 43 con il commento di E. Caprioli, *Responsabilité du particulier en cas d'hameçonnage*, e in *Dalloz IP/IT*, 2018, p.643, con osservazioni di J. Lasserre Capdeville, *Confirmation de solutions jurisprudentielles en matière de phishing*; cfr., inoltre, *Cour cass.* 31 maggio 2016, in *Dalloz*, 2016, p. 2305, osservazioni di D. R. Martin e H. Synvet; *Sem. Jur., éd. Entr. Aff.*., 2016, p. 1450.

[108] Sul *tema* cfr. la decisione di Metz, 8 dicembre 2010, n° 08/01529, in *L'essentiel droit bancaire*, 2011, p. 6, con osservazioni di J. Lasserre Capdeville, *Précisions sur la notion d'utilisation frauduleuse d'une carte bancaire*.

critica a questa ricostruzione contesta, tuttavia, l'affidabilità degli indirizzi IP (ovvero «sequenze numeriche assegnate a computer collegati a Internet al fine di consentire la comunicazione tra i medesimi attraverso tale rete», così come definiti dalla Corte di giustizia [109]) facendo leva su considerazioni di carattere tecnico (ecco che ritorna il tema della precomprensione del fatto informatico), potendosi, infatti, ben verificare l'ipotesi che, con un furto di identità, il malfattore si appropri anche dell'indirizzo IP della vittima[110]. L'indirizzo IP, dunque, non ha l'idoneità a costituire piena prova della riferibilità dell'ordine di pagamento al computer dell'utente [111].

7. *Fatti generatori di responsabilità dell'intermediario e mezzi di prova*

Quanto sopra è sufficiente per far emergere la tendenza all'adozione di una prospettiva intesa a valorizzare le circostanze del caso concreto, incluso lo stato soggettivo del pagatore, il quale influisce sulla valutazione dell'organo giudicante[112]. Dal costante scandagliare, da parte della giurisprudenza, il contegno delle parti, può dedursi, sul piano dell'elaborazione generale, la configurazione di un obbligo di diligenza informatica in capo all'utente[113], intesa quale obbligo di consapevolezza «della delicatezza del mezzo telematico e della possibilità che attraverso quel mezzo siano perpetrate frodi, tanto più insidiose quanto meno facilmente riconoscibili»[114], e, simmetricamente, di

[109] CGUE, sentenza del 19 ottobre 2016, *Breyer*, C-582/14.
[110] «*Si des faussaires ont pu se procurer toutes les données qui leur permettent d'usurper l'identité des époux X., il est logique d'imaginer qu'ils ont également eu connaissance de l'adresse IP de l'ordinateur qu'ils utilisaient pour consulter leur compte bancaire*»: Tribunal de commerce de Cannes, 27 luglio 2017, *Dalloz IP/IT*, 2017, p. 661.
[111] J. Lasserre Capdeville, *Problèmes liés à l'adresse IP en matière bancaire*, in *Dalloz IP/IT*, 2017, p. 219.
[112] Il tema, nel caso il pagatore sia un consumatore, s'interseca con quello frammentazione della categoria dei consumatori in base al loro grado di avvedutezza (criterio che ha fatto il suo ingresso anche in àmbito normativo con la Direttiva 2005/29/CE, con l'introduzione della figura del consumatore medio cioè «normalmente informato e ragionevolmente attento ed avveduto»), ovvero *vulnerable, average, smart, responsible*: costruzioni debitrici agli studi americani di analisi economica del diritto, che ricollegandosi a parametri di carattere personale sul presupposto che lo stato di debolezza contrattuale -così come la simmetria e la sperequazione di poteri- possa dipendere anche da circostanze contingenti, prevedono differenti criteri di valutazione delle condotte; cfr. sul tema specifico K. Rodriguez, *ult. op. loc. cit.*
[113] A. Antonucci, *I contratti bancari online,* in *I contratti bancari*, a cura di E. Capobianco, Utet, Torino 2016, p. 422.
[114] Coll. Roma, Dec. n. 33/2010.

un obbligo di predisposizione di un'adeguata organizzazione tecnica idonea a garantire la sicurezza dello svolgimento di incarichi di pagamento in via informatica (la condotta dei prestatori deve essere scrutinata sotto il profilo della conformità ai canoni di correttezza e diligenza del *bonus argentarius* che ne devono informare l'operato). Tale organizzazione deve caratterizzarsi, in particolare, per l'adozione di strumenti in linea con l'evoluzione scientifica e tecnologica del settore[115].

Elemento cruciale (tanto in linea teorica, di ripartizione del rischio, quanto pratica, di frequenza della sua rilevanza) incidente sull'allocazione della responsabilità, è la presenza del servizio di Sms-Alert, presidio di sicurezza *ex post* (attivandosi una volta effettuato un prelievo) volto ad evitare il compimento di ulteriori -rispetto a quello notificato- prelievi. Il sistema prevede che venga notificata all'utente, tramite messaggi di testo sull'utenza cellulare o mail sulla casella di posta elettronica, ogni operazione realizzata, per consentirgli di procedere alla richiesta del blocco della carta nel caso riscontri la presenza di un utilizzo fraudolento. La giurisprudenza, ritenendo tale misura di sicurezza un servizio ormai normalmente esigibile, configura la sua mancata predisposizione come un'ipotesi di responsabilità da inadeguata organizzazione, imputabile all'intermediario (dovendosi escludere che il relativo costo possa essere sopportato dal cliente), il quale dovrebbe adottarla in modo generalizzato in virtù dell'obbligo di diligenza professionale[116]. Ovviamente è da escludere che la mancata predisposizione del presidio sia fatto generatore di responsabilità nell'ipotesi di assenza del nesso causale tra l'occorrenza del danno e l'assenza della messaggistica di Alert. Se l'intermediario, infatti, offre la prova che, alla luce dello svolgimento dei fatti, l'adozione di tale sistema di avvertimento non avrebbe consentito di limitare il pregiudizio sofferto (ad esempio, che la presenza dell'Sms-Alert non avrebbe, verosimilmente, impedito la realizzazione dei prelievi successivi al primo, stante l'arco temporale estremamente ridotto in cui si sono svolte le operazioni contestate[117]), la sua responsabilità sarà esclusa.

Pacifico che la messa a disposizione di strumenti accessori al rafforzamento della sicurezza non valga a tramutare in colpa grave la circostanza che il cliente non se ne sia avvalso[118], è, invece, controverso se l'adozione del sistema di notifica debba avvenire automaticamente o se l'obbligo di diligenza del prestatore sia soddisfatto tramite la mera sollecitazione

[115] Coll. Napoli, dec.n. 985/2011.
[116] Coll. Roma, cfr. Dec. nn. 5543/13 e 2319/2014.
[117] Coll. Roma, Dec. n. 11457/2016; Coll. Napoli, Dec. n. 1372/2016.
[118] Coll. coord., Dec. n. 3498/2012.

all'adozione dello stesso[119]. Sul piano contrattuale, l'alternativa si pone tra un modello di adesione c.d. *opt-out* (basato sul principio dell'autoesclusione: il servizio è attivato per tutti i clienti, ad eccezione di chi comunica di volersene sottrarre) ovvero *opt-in* (l'adesione al servizio avviene solo su base volontaria, previo consenso del cliente).

Se si accoglie l'idea, maggiormente diffusa, che l'imputazione della responsabilità all'ASPSP avvenga su base colposa, la stessa si dovrà escludere nell'ipotesi in cui il cliente, debitamente informato della disponibilità di siffatto strumentario di sicurezza, ometta di avvalersene. Si è, dunque, ritenuto che il meccanismo contrattuale che subordina la ricezione dell'Sms-Alert alla preventiva manifestazione del consenso del cliente (laddove l'offerta, se pure non personalizzata, sia rispettosa dei requisiti di trasparenza e adeguata evidenza) sia sufficiente ad integrare il livello di diligenza protettivo richiesto al fine di prevenire possibili eventi pregiudizievoli[120]. Il prestatore di servizi di pagamento potrà, dunque, essere esente da responsabilità se, producendo il contratto, dimostrerà che esso conteneva un'offerta sufficientemente stimolante all'uso del servizio (non una semplice e indistinta menzione nell'àmbito del contratto) e una descrizione sufficientemente chiara dello stesso, considerato che l'utilità dei presidi di avvertimento viene ormai considerata nota anche al pur non avveduto utente di strumenti di pagamento.

L'inerzia dell'intermediario nell'attivazione d'idonei strumenti di sicurezza può riguardare non solo la mancata predisposizione del servizio di Sms-Alert, ma anche di un sistema di monitoraggio della carta (ai fini del possibile blocco) in relazione ad operazioni anomale per frequenza e tipologia: attesa la pericolosità della clonazione/utilizzo fraudolento delle carte di pagamento, la strategia di contrasto è stata identificata nella velocità d'individuazione delle transazioni suscettibili di configurare un rischio di frode oggettivo, imminente e rilevabile, attraverso l'analisi delle informazioni riguardanti le transazioni "sospette"[121]. A fronte di un rischio

[119] Cass. 24 settembre 2009, n. 20543.

[120] Nello specifico, affinché alla clausola di offerta del servizio di allerta possa essere riconosciuta portata esimente, è necessario che questa presenti una formulazione idonea a consentire una scelta consapevole del consumatore sia in relazione al canone della trasparenza sia in relazione alla sua rappresentazione grafica, dovendo essere indicata con caratteri di adeguata evidenza (così i parametri enunciati dal Collegio di coordinamento, nella citata Dec. n. 3498/2012).

[121] L'art. 8, comma 1, lett. 2, D.M. 30 aprile 2007, n. 112, Regolamento di attuazione della L. 17 agosto 2005, n. 166, recante «Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento» individua specifici indici di anomalia: "Si configura il rischio di frode di cui all'articolo 3, comma 1 della legge, quando viene raggiunto uno dei seguenti parametri:

di frode così normativamente tipizzato (nonchè in considerazione delle norme in materia di ripartizione del rischio dettate dal D. Lgs. 11/ 2010 e di quelle in materia di concorso colposo del creditore nella causazione dell'evento -art. 1227-, e dell'art 1176 c.c.) si ritiene che l'intermediario diligente sia tenuto ad attivarsi e predisporre il blocco automatico della carta a séguito di operazioni anomale per frequenza e tipologia[122]. All'ASPSP non si richiede il monitoraggio di ogni singola operazione, ma la predisposizione di sistemi automatici di blocco di operazioni caratterizzate da un rapido succedersi, e non in linea con la normale operatività del titolare del conto[123].

Con riguardo all'*internet banking*, posto che il fenomeno maggiormente diffuso è quello del *phishing*[124], l'intermediario deve provvedere a fornire evidenza tanto del grado di accortezza (non) tenuto dall'utente quanto della presenza dei necessari sistemi di sicurezza prescritti.

Il principio che orienta la valutazione della condotta dell'utente è quello per cui la divulgazione dei dati identificativi riservati che abilitano all'utilizzo del proprio conto vale a configurare una condotta gravemente colposa[125], ritenendosi il fenomeno del *phishing* ormai noto al pur non esperto navigatore di Internet[126]. In sostanza, si ritiene che la consapevolezza del rischio di attacchi informatici e della circostanza che gli istituti di credito non richiedano informazioni personali via mail, siano divenuti ormai parte del bagaglio culturale di ogni consociato, assurgendo dunque

(…) lettera a): 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 (…); lettera b): 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"; per le decisioni cfr., tra le molte, quelle del Coll. Milano, Dec. n. 20897/2018; Coll. Coord., Dec. n. 3947/2016; Coll. Milano, Dec. n. 2817/2015.

[122] Coll. Coord., Dec. n. 27252/2018; Coll. Milano, Dec. n. 5255/2015.

[123] Coll. Napoli, Dec. n. 1220/2016.

[124] Il *phishing* consiste in "una truffa informatica realizzata inviando un'email con il logo contraffatto di un istituto di credito o una società di commercio elettronico, in cui si invita il destinatario a fornire i dati riservati quali numero di carta di credito, *password* di accesso al servizio di *home banking*, ecc., motivando tale richiesta con ragioni di ordine tecnico." (Cass. pen. 10060/2017).

[125] Coll. Coord., Dec. n. 3498/2012.

[126] Nello specifico, il comportamento del titolare del conto assume i caratteri della «colpevole credulità», tanto per aver comunicato «le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario», tanto più colpevole se si considera che la notorietà del fenomeno del *phishing*: Coll. coord., Dec. n. 1820/13.

al rango di fatto notorio[127]. Valutata in questa prospettiva la condotta delle parti coinvolte, si comprende la distinzione, elaborata dalla giurisprudenza, tra differenti tipi di truffe informatiche perpetrate -ai quali si accordano distinti metri di valutazione della condotta dell'utente[128]- quale il *phishing* tradizionale (considerato inescusabile, in quanto evitabile da qualunque utente dotato di normale avvedutezza e prudenza[129]) o quello c.d. di seconda generazione (quali, ad esempio, il *real time phishing*[130]), il quale, avvenendo la *captatio* attraverso meccanismi più sofisticati e subdoli, impercettibili anche al più scrupoloso utente, esclude automaticamente la ricorrenza di una colpa grave (e finanche di una colpa lieve) in capo all'utente che pure, inconsapevolmente, abbia cooperato alla realizzazione della frode[131].

Pacifica, in quanto non controversa, sarà la colpa grave dell'utente che ammetta di aver fornito riscontro all'email o all'sms civetta[132], mentre nel caso di negazione dell'abboccamento, la colpa grave (coincidente, sovente, con un grado di avvedutezza inferiore a quella dell'utente medio) andrà provata dall'intermediario, sia tramite la prova del grado di sofisticazione con cui la truffa sarebbe stata perpetrata, sia evidenziando la manifesta decettività del messaggio o l'anomalia ed inusualità della richiesta.

In Francia, invece, il discrimine per distinguere una *naiveté coupable* da una scusabile è individuato nella consapevolezza dell'utente circa la natura fraudolenta della missiva. Valutazione che, a sua volta, deve svolgersi alla luce del parametro della riconoscibilità del carattere fraudolento stesso: la non riconoscibilità (come, ad esempio, la ricezione di una mail recante la perfetta riproduzione del logo dell'intermediario)[133] esclude la negligenza, per cui l'abboccamento, quantunque intenzionale, viene considerato incolpevole. L'apprezzamento del grado di decettività presente nelle *e-mail* (o sms) civetta deve svolgersi *in abstracto*, avendo la *Cour* indicato una serie di elementi che consentono ad un utente "*normalement attentif*" di dubitare

[127] Per una definizione del fatto notorio in chiave contemporanea, cfr. D. Weinberger, *Too Big to Know. Rethinking Knowledge Now That the Facts Aren't the Facts, Experts Are Everywhere, and the Smartest Person in the Room is the Room*, Basic Books, New York 2011 (di cui è disponibile una traduzione italiana a cura di N. Mataldi: *La stanza intelligente. La conoscenza come proprietà della rete*, Codice edizioni, Torino 2012).
[128] Coll. Coord., Dec. n. 3498/2012.
[129] Coll. Coord., Dec. n. 1820/13.
[130] Coll. Milano, Dec. n. 9661/2017.
[131] Coll. Bologna, Dec. n. 14695/2018; Coll. Roma, Dec. n. 1507/2017.
[132] Coll. Bologna, Dec. n. 6323/2018; Coll. Napoli, Dec. n. 9322/2016; *Cour cass.*, 25 ottobre 2017, cit.
[133] *Cour cass.*, 28 marzo 2018, n° 16-20.018, cit.

della sua provenienza[134].

Una recente variante del fenomeno del *phishing* è quella in cui l'acquisizione fraudolenta dei dati rilevanti avviene mediante l'impiego di mezzi di comunicazione apparentemente istituzionali dell'ASPSP. La peculiarità della fattispecie consiste, dunque, nell'ammessa comunicazione, da parte dell'utente, delle *password* dinamiche, giustificata, tuttavia, dal legittimo affidamento che questi eccepisce di aver riposto sulla riconducibilità dell'interlocutore all'intermediario, escludendo di poter incorrere in colpa grave per aver confidato nell'autenticità dell'identità dell'operatore che appariva nella *chat box* con i propri dati anagrafici e il logo dell'intermediario con annessa "spunta blu"[135] (a garanzia dell'autenticità).

In questo caso, a prescindere dal grado di sofisticazione -pur elevato- dell'"ambiente informatico" creato dal frodatore, si è ritenuto che la comunicazione via *chat* delle *password* dinamiche configuri *ex se* una condotta gravemente negligente, essendo ormai noto che gli intermediari non richiedono tramite mail né *chat* dati riservati e *password* dinamiche[136].

Con riguardo alla condotta dell'intermediario, nelle prime decisioni in materia veniva attribuita una (limitata) rilevanza all'eventuale adozione di una politica aziendale volta a prevenire i rischi di frodi informatiche, ammonendo gli utenti a non fornire a terzi i propri dati di identificazione e di accesso ai servizi, ed in particolare rendendo disponibile, con accesso dal proprio sito web istituzionale, una sezione specificamente dedicata al *phishing* con informazioni utili per utilizzare il canale *online* in condizioni di sicurezza[137]. Tale condotta ha progressivamente perso rilevanza sul presupposto che del fenomeno del *phishing* abbia ormai conoscenza anche «il pur non esperto internauta»[138] e che, dunque, «*peu important qu'il soit, ou non, avisé des risques d'hameçonnage*»[139].

---

[134] *Cour cass*., 28 marzo 2018, in *Rev. banque*, 2018, p. 75, con nota di Ph. Storrer; in *Banque et droit*, 2017, p. 32, con nota di Helleringer e Bonneau, in *Contrats, conc., consom.*, 2018, comm. 83, con osservazioni di L. Leveneur.

[135] La frode prende avvio quanto il titolare utilizza la piattaforma *social* ufficiale dell'intermediario (generalmente *chat box* tramite messaggio pubblico visibile a tutti gli utenti) per una richiesta di supporto; dopo la segnalazione viene contattato (di norma sull'utenza telefonica) da un sedicente operatore il quale, a garanzia della propria autenticità, si presenta coi propri dati anagrafici e l'apposizione di una "spunta blu", ossia di un *badge* di verifica all'interno dell'immagine del profilo della piattaforma, richiedendo, ai fini del ripristino delle funzionalità di cui si lamentava il disservizio, i dati sensibili dello strumento di pagamento.

[136] Coll. Milano, Dec. n. 3312/2019; Coll. Bari, Dec. n. 27318/2018.

[137] Difesa ripetutamente sottolineata dalla banche convenute: *Cour cass*., 25 ottobre 2017, cit.

[138] Coll. coord., Dec. n. 3892/2013.

[139] *Cour cassation*, 25 ottobre 2017, cit.

8. *La colpa grave del pagatore*

Escluso che il corretto utilizzo delle credenziali personali possa assumere carattere dirimente nel ravvisare una colpa grave del cliente - stante la contraria previsione normativa dell'art. 10, comma 2, del d.lgs. n. 11/2010 e, in Francia, degli artt. L. 133-16 e L. 133-23 *Cod. mon. fin.*- il tema della colpa grave è quello su cui si sono maggiormente concentrati gli sforzi ricostruttivi della giurisprudenza e della dottrina, le quali hanno tentato una tipizzazione delle ipotesi di colpa grave del pagatore nell'adempimento degli obblighi di custodia, valutandola alla luce di una molteplicità di profili, attinenti sia alle modalità con le quali si è verificata la sottrazione dello strumento di pagamento, sia al comportamento del cliente successivo al furto e/o allo smarrimento.

Con riguardo alle carte di pagamento, la norma che ne detta la disciplina (art. 69, Dir. 2366/2015; art.7, d.lgs. 11/2010, artt. L. 133-16, *Cod. mon. fin.*) viene riformulata sin dalla rubrica (ora intitolata agli "*Obblighi a carico dell'utente dei servizi di pagamento in relazione agli strumenti di pagamento e alle credenziali di sicurezza personalizzate*"), introducendo, dunque, una duplicazione degli obblighi di custodia, tanto dello strumento di pagamento (comma 1)[140], quanto delle credenziali (comma 2) [141].

Anche in questo caso, si tratta di una riformulazione dallo scarso impatto in termini di innovatività, poiché segna il recepimento normativo di un principio (quello che la valutazione dell'adempimento degli obblighi di custodia debba riguardare tanto lo strumento di pagamento quanto le credenziali) pacificamente accolto dalla giurisprudenza.

Posta la reciproca connessione degli obblighi indicati in quanto configurano, unitariamente considerati, il corretto utilizzo degli strumenti di pagamento, le due disposizioni vanno lette congiuntamente, di tal che è sufficiente l'omesso rispetto di uno dei due obblighi legali per la configurazione della responsabilità dell'utente.

Variamente qualificata negli ordinamenti interni è la verifica della permanente disponibilità dello strumento, la cui omissione, in Italia, è stata ascritta alle ipotesi d'incuria nell'utilizzo complessivo dello strumento di pagamento -omissiva di «quel grado minimo di diligenza osservato da

[140] Ossia un «dispositivo personalizzato e/o insieme di procedure concordate tra l'utente e il prestatore di servizi di pagamento e di cui l'utente di servizi di pagamento si avvale per impartire un ordine di pagamento», così come dalla definizione dell'art. 4, par. 1, n. 14, Dir. 2366/2015.

[141] Definite dall'art. 4, par. 1, n. 31, Dir. 2366/2015, come «funzionalità personalizzate fornite a un utente di servizi di pagamento dal prestatore di servizi di pagamento a fini di autenticazione».

tutti»[142], mentre in Francia viene rapportata alle «*habitudes d'utilisation de la carte*»[143], di talchè è stata considerata diligente la condotta dell'utente che abbia tempestivamente proceduto al blocco della carta solo una volta rientrato dalla crociera[144].

Il caso di negligente custodia dello strumento di pagamento, la quale viene valutata in prima battuta con riguardo alla conformità ai termini contrattuali, è tipicamente quello in cui esso venga lasciato incustodito in luoghi pubblici o privati[145].

Nell'ipotesi delle credenziali, invece, il principio generale è che esse debbano essere protette tramite misure ragionevolmente idonee[146]: le

[142] «Il possesso di strumenti per i pagamenti elettronici, intrinsecamente pericolosi perché esposti a rischi di frode e di utilizzi non autorizzati, comporta che gli obblighi di diligente custodia degli stessi comprendano anche un monitoraggio dei conti destinati a recepire le operazioni effettuate a loro mezzo, onde appunto verificarne il corretto impiego. Ora, seppure non può pretendersi che tale monitoraggio venga effettuato in continuo, appare certamente anomala la condotta della ricorrente che per lungo tempo ha omesso ogni riscontro delle operazioni registrate nel conto»: Coll. Napoli, Dec.n. 6472/2014. *Contra* v. però la giurisprudenza di merito per la quale nessuna norma impone verifiche periodiche ravvicinate della disponibilità della carta di credito da parte del suo titolare: Tribunale di Firenze, 19 gennaio 2016 *De Iure*.

[143] Trib. Parigi, 12 dicembre 2002, n° 2002/05702 sentenza citata da J. Lasserre Capdeville, in *Dalloz*, 2013, p. 407, nt 11, cit. alla nt. seguente

[144] *Cour cass.*, 16 ottobre 2012, in *Sem. Jur., éd. Entr. Aff.*, 2012, p. 1680, con nota di S. Piedelièvre; e in *Dalloz*, 2013, p. 407, con nota di J. Lasserre Capdeville; in *Sem. Jur., éd. G*, 2012, p. 1202, con osservazioni di K. Rodriguez.

[145] Luoghi di lavoro, palestre, ospedali: Milano, Dec. n. 377/2014; Coll. Napoli, Dec. n. 6798/2014; Coll. coord., Dec. n. 6168/2013; o automobili posteggiate nella pubblica via (benchè lo strumento di pagamento sia stato nascosto nel vaso portaoggetti): *Cour ass.*, 16 ottobre 2012, cit. nella nota *supra*. Un discorso differente riguarda la custodia in luoghi privati, specialmente in àmbito domestico: il principio che regola la ripartizione delle responsabilità è che «ciascuno è responsabile della propria sfera domestica e non può pretendere di addossare a terzi estranei, nel caso che ci occupa l'intermediario resistente, le conseguenze dannose di comportamenti lesivi posti in essere da chi sia stato ammesso in tale sfera personalissima» (Coll. Milano, Dec. n. 969/2015); parimenti responsabile è colui che, pur vittima di raggiro, consenta a delle persone estranee di introdursi nella propria abitazione senza adottare una maggiore diligenza nella custodia e vigilanza dei propri beni e valori (Coll. Napoli, Dec. n. 2166/2016). In alcune ipotesi di furto presso la propria abitazione, si è, tuttavia, ritenuto che la natura di tale evento, eccezionale e non prevedibile, possa escludere, in assenza di evidenze, da parte dell'intermediario, di adeguata prova della colpa grave dell'utente nella custodia dello strumento di pagamento, la responsabilità dell'utente stesso (Coll. Roma, Dec. n. 590/2014).
Tali distinzioni non sono invece recepite in Francia, dove la circostanza che il furto si avvenuto presso l'abitazione dell'utente è stata considerata irrilevante: *Cour cass.*, 1° marzo 1994, in *RTD com.*, 1995, p. 458, con nota di R. Cabrillac.

[146] Art. 7, comma 2, D.lgs. 11/10.

circostanze relative alla (omessa) custodia delle credenziali vengono considerate avere rilevanza assorbente nella concreta concatenazione degli eventi[147], ferma restando la non configurabilità di un obbligo di memorizzazione, purchè le credenziali non siano immediatamente associabili alla carta[148], posto, al contrario, che l'ipotesi di conservazione congiunta dello strumento e del PIN, configura una totale trascuratezza verso i minimi accorgimenti utilizzati dai consociati al fine di evitare un accadimento dannoso[149]. Il tema viene sviluppato negli stessi termini anche in Francia, dove la conservazione congiunta viene considerata *faute lorde*[150].

La prova -presuntiva- della conservazione del PIN unitamente alla carta viene generalmente rinvenuta sulla base di un criterio temporale, ossia il breve lasso che intercorre tra il momento del furto il primo utilizzo fraudolento[151]. La circostanza che gli utilizzi fraudolenti avvengano con successo nell'àmbito di un ristretto arco temporale viene ritenuta incompatibile con l'eventualità della decrittazione del PIN tramite reiterati tentativi di digitazione, rivelando, al contrario, la necessaria conoscenza dello stesso da parte dei malfattori. In sede di giudizio, l'intermediario ricorre alla produzione dei Log (trascrizione di tracce informatiche) delle operazioni disconosciute che consentono, all'un tempo, di dimostrare la breve sequenza temporale (idonea a fondare la presunzione della sussistenza della colpa grave in capo all'utente) e la corretta e regolare autenticazione delle transazioni (idonea ad

[147] Coll. coord., Dec. n. 991/2014.

[148] La necessaria adozione di tecniche di annotazione opportunamente criptate era già stata evidenziata da X. Favre-Bulle, *Le droit communautaire du paiement électronique*, Schultess éditeur, Zurigo 1992, p. 31. È stato, dunque, considerato scusabile il comportamento di colui il quale conserva il codice nel luogo in cui è tenuta la carta, purché non sia immediatamente associabile alla carta stessa: Coll. Milano, Dec. n. 5540/2014; Coll. coord., Dec. n. 6170/2013.

[149] Per quanto la Direttiva non li recepisca, si rinvengono dei precedenti di soft-law in materia, che raccomandavano espressamente all'utente «di non trascrivere sullo strumento di pagamento l›eventuale numero personale di identificazione o il codice, e di non registrare tali dati su qualsiasi altro documento che egli abitualmente detiene o porta con lo strumento di pagamento, in particolare se tale documento può essere perso o rubato o riprodotto»: cfr. artt. 4.1, lett. c, Racc. 88/590/CEE (Raccomandazione della Commissione del 17 novembre 1988 concernente i sistemi di pagamento, in particolare il rapporto tra il proprietario della carta e l'emittente della carta); 5.1, lett. c, Racc. 97/489/CE (Raccomandazione della Commissione del 30 luglio 1997 relativa alle operazioni mediante strumenti di pagamento elettronici, con particolare riferimento alle relazioni tra gli emittenti ed i titolari di tali strumenti).

[150] V. già *Cour cass.*,10 gennaio, 1995, in *Sem. Jur., éd. Gén.*, 1995, p. 591, la quale avvallava la violazione, da parte del titolare della carta, dell'«*obligation de prudence, et plus particulièrement celle de préserver la confidentialité du numéro de code*»; cfr. anche *Cour cass*., 16 ottobre 2012, cit. *retro*, e *Cour cass.*, 17 maggio 2017, in *Contrats conc. consom.,* 2017, comm. 77, con osservazioni di E. A. Caprioli.

[151] Coll. Torino, Dec. n. 16444/2018; Coll. Palermo, Dec. n. 14353/2017.

assolvere l'onere probatorio relativo alla funzionalità del sistema)[152].

Altri indici di grave negligenza vengono ravvisati nella (in)tempestività del blocco richiesto dell'utente una volta presa coscienza del furto o dello smarrimento (ovvero la verifica, in base alla documentazione versata in atti, che un blocco tempestivo avrebbe consentito di prevenire in toto i prelievi non autorizzati)[153], nonché nella circostanza che la carta sia dotata di microchip (il che rende l'ipotesi di una clonazione così complessa sul piano tecnico e statistico, da considerarla, se non di impossibile evenienza, almeno altamente improbabile): essa, tuttavia, non è sufficiente, da sola, a configurare una responsabilità in capo all'intermediario, se questi offre evidenza della sussistenza, *a latere* dell'adozione della tecnologia a microchip, di ulteriori indici idonei ad escludere l'eventualità dell'utilizzo fraudolento[154].

In considerazione di ulteriori elementi circostanziati sulla dinamica della vicenda, anche l'alternanza tra operazioni fraudolente e operazioni genuine (ossia l'utilizzo dello strumento da parte del legittimo titolare durante il periodo dei prelievi successivamente disconosciuti) viene considerata indice di colpa grave[155], così come la prossimità degli sportelli ATM presso i quali sono stati effettuati i prelievi disconosciuti rispetto a quelli abitualmente utilizzati dall'utente (anche in questo caso la circostanza potrà essere suffragata dai tabulati dei singoli ATM[156]), l'utilizzo di più carte da parte dei terzi non autorizzati[157]; infine, l'affidamento dello strumento ad un

[152] Cfr. Collegio Milano, Dec. n. 605/2015; Coll. Coordinamento, Dec. n. 5304/2013. Per converso, la circostanza che le operazioni disconosciute siano state effettuate in un arco temporale non ravvicinato -ed in giorni fra loro non consecutivi-, è stato considerato indice idoneo ad escludere l'ipotesi di una sottrazione fraudolenta, in quanto incompatibile con l'*id quod plerumque accidit,* in cui l'utilizzo fraudolento delle carte sarebbe caratterizzato da prelievi in rapida successione fino ad esaurimento della disponibilità, nell'intento di trarre il massimo vantaggio dalle operazioni prima che il soggetto derubato si accorga dell'abuso e provveda al blocco della carta (Coll. Roma, Dec. nn. 308 e 4163 del 2015 e 4884/2014).

[153] Coll. Roma, Dec. nn. 2498/2014 e 33/2015; Coll. Coord., Dec. n. 5304/2013.

[154] Coll. Roma, Dec. nn. 1415 e 308 del 2015; Coll. coord., Dec. n. 3947/2014.

[155] Giacché «porta inevitabilmente a concludere che per tutte le operazioni deve necessariamente essere stata utilizzata la medesima carta, ossia quella originale» (Coll. Roma, Dec. n. 4163/2015).

[156] Se le operazioni contestate sono avvenute in un'area circoscritta e prossima al domicilio dell'utente e presso sportelli abitualmente utilizzati dal medesimo, si ritiene che la dinamica dei prelievi non presenti gli elementi tipici comuni agli episodi di clonazione che normalmente avvengono in luoghi diversi e lontani dal domicilio del titolare della carta (Coll. coord., Dec. nn. 897 e 3479 del 2014).

[157] La contestuale sottrazione di altri strumenti di pagamento, cui è seguito – nello stesso ristretto lasso di tempo – il loro fraudolento utilizzo rende ancor più evidente l'impossibilità

familiare del titolare non costituisce *ex se* colpa grave se temporaneo (cioè circoscritto all'effettuazione di un specifica operazione)[158]. Prova della genuinità dell'operazione viene, invece, considerato il carattere abituale -per ammontare e frequenza- delle operazioni contestate (ad esempio, l'acquisto ogni anno il 31 dicembre del medesimo bene presso il medesimo sito)[159].

In ogni caso, come già rilevato, non esistono indici di presunzioni assolute di negligenza dell'utente, ai fini della configurazione della quale deve svolgersi una valutazione complessiva tutte le circostanze del caso concreto[160].

Nel caso in cui le operazioni disconosciute siano state effettuate in un esteso arco temporale, si ravvisa giudizialmente una presunzione di omesso monitoraggio del proprio conto, indice di grave negligenza. L'ABF, infatti, ritiene che dovrebbe essere ormai noto a tutti gli utilizzatori di strumenti elettronici di pagamento il rischio di incorrere in utilizzi fraudolenti da parte di terzi e ciò dovrebbe indurre ad una vigilanza più frequente, idonea, quanto meno, ad evitare che detti utilizzi risultino ripetuti nel tempo[161].

Con riguardo, infine, al presidio tecnico del 3D Secure, al quale avevo accennato in apertura, il percorso della giurisprudenza francese (la quale l'ha utilizzato quale grimaldello per consentire agli intermediari di fornire la prova della colpa grave dell'utilizzatore, altrimenti considerata impossibile), che ne ha enfatizzato la funzione di elevare la sicurezza di un sistema di autenticazione[162], al quale si contrappone quello della giurisprudenza italiana che, allo stato attuale, lo considera un mero protocollo di trasmissione dei dati (inidoneo a qualificare il sistema di sicurezza di una banca), trovano la loro sintesi nell'intervento chiarificatore dell'EBA che, specificandone la natura di strumento di supporto all'autenticazione forte[163], introduce

per i malviventi di effettuare in tempi così brevi un rilevante numero di tentativi finalizzati all'ottenimento dei PIN di diverse carte (Coll. Roma, Dec. n. 8345/2016).

158 Non può, infatti, ritenersi che l'affidamento temporaneo ad un familiare possa essere invocato a supporto del riconoscimento di una colpa grave dell'utente «potendosi ritenere non infrequente, né irragionevole, che nell'ambito del nucleo familiare uno stretto congiunto sia delegato a procedere ad un determinato utilizzo della carta nell'interesse comune»: Coll. Roma, Dec. n. 2339/2013; per contro, è fonte di responsabilità illimitata dell'utente l'affidamento che abbia i caratteri della stabilità: Coll. Roma, Dec. n. 8383/2014; in materia cfr. G. Liberati Buccianti, *L'affidamento a un familiare della carta di pagamento e l'obbligo di diligente custodia*, in *Nuova giur. civ. comm.*, 2013, I, p. 849 ss.

159 *Cour cass.*, 4 luglio 2018, n° 17-10.158.

160 Così, espressamente, il 72° considerando, Dir. 2366/2015.

161 Coll. Roma, Dec. n. 4444/2016.

162 Cfr. le citate decisioni della *Cour* del 18 gennaio 25 ottobre 2017 e del 28 marzo 2018.

163 Escluso che, allo stato attuale, costituisca un elemento di inerenza (posto che nessuno dei dati scambiati include informazioni relative ad elementi biometrici), ciò non preclude che lo possa divenire in futuro, laddove in grado di trasmettere elementi di inerenza

un'importante distinguo tra la versione 2.0 -e successive- e le versioni precedenti -1.0-, specificando che solo la prima soddisfa i requisiti richiesti dall'autenticazione forte[164].

Conclusivamente, possono rilevarsi alcune traiettorie ricostruttive nella valutazione della condotta dell'utente: intanto la tendenza -comune con la Corte di giustizia e le riflessioni europee in materia di politiche di *decisionmaking* nelle controversie[165]- ad adottare una prospettiva intesa a giustificare e valorizzare soluzioni "contestualizzate", ossia incentrate sulla rilevanza di «*autres éléments extrinsèques*»[166].

Tali elementi sono stati tipizzati dalla giurisprudenza, che, individuando gl'indici sui quali svolgere le proprie valutazioni, ha dunque specificato che il proprio sindacato sul comportamento dell'utente vada effettuato *in abstracto*[167], secondo il modello del "*reasonably circumspected consumer*"[168], criterio che ha fatto il suo ingresso anche in àmbito normativo con la Direttiva 2005/29/CE con l'introduzione della figura del consumatore medio cioè «normalmente informato e ragionevolmente attento ed avveduto»[169]. Il richiamo, tuttavia, alle circostanze contingenti, pone indirettamente l'interrogativo se l'oggetto di valutazione possa essere anche il profilo soggettivo del danneggiato (o asseritamente tale) ed in particolare se e quale rilevanza debba essere riconosciuta alle sue caratteristiche intrinseche. In altri termini, se il sindacato sulla colpa grave del pagatore implichi una distinzione tra vittima accorta e non accorta e, dunque, quale sia la frontiera tra la "colpevole credulità" ("*naivieté exusable*") e la colpa grave ("*negligence coupable*"): la risposta è dirimente, giacché se si accede alla risposta positiva, la circostanza che l'utente sia una persona vulnerabile per ragioni, ad esempio, anagrafiche (caratterizzazione che nel diritto delle nuove tecnologie è tra le più ricorrenti) condurrà a ritenere la sua credulità giustificabile e, dunque, ad escluderne la colpa grave. Viceversa, se si ritengono irrilevanti le caratteristiche soggettive dell'utente nella valutazione della credulità si dovrà escludere rilevanza ad una serie di elementi relativi

(*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 -EBA-Op-2019-06*, 21 giugno 2019, punto 21).

[164] *Opinion of the European Banking Authority*, cit. nt. *supra*, punto 23.

[165] Sin dalla sentenza *Océano*, CGCE, 27 giugno 2000, cause riunite C-240/98 a C-244/98.

[166] *Cour cass.*, 21 settembre 2010, cit.

[167] D. Legeais, *Hameçonnage*, cit.

[168] Figura la cui prima menzione in giurisprudenza risale alla sentenza della Corte di Giustizia del 16 luglio 1998, *Gut Springenheide GmbH*, § 31 e 37, C-210/96.

[169] 18° considerando, Direttiva del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno.

alla sua qualità di *vulnerable, average, smart,* o *responsible* [170].

Abstract
Nelle controversie in materia di pagamenti non autorizzati, uno degli àmbiti più rilevanti è quello probatorio. È noto, infatti, che la ripartizione dell'onere della prova sia cruciale sull'esito della decisione.
La PSD2, in cui l'imputazione della responsabilità avviene a titolo colpa (ad eccezione di alcune isolate ipotesi in cui l'imputazione avviene a titolo di responsabilità oggettiva per il prestatore di servizi di pagamento), vengono accolte le principali linee di tendenza comuni ai vari ordinamenti interni: lo spostamento dell'assolvimento dell'onere della prova sul professionista -per facilitare l'accertamento dei fatti assegnando l'onere della prova al soggetto che si trova nella posizione migliore per soddisfarlo-; e, al contempo, il rifiuto di una deroga permanente al principio dell'*actori incumbit probatio*.

Parole Chiave: Onere della prova; pagamenti non autorizzati; frode informatica.

Abstract
An issue that concerns the "case-law" on digital payements is that of the burden of proof.
Since the allocation of the burden of proof is key to the outcome of the decision, this represents, as the watershed along which the effective- ness of the protection is measured.
The PSD2 recepies the main tendencies of the domestic legal systems: to shift the burden of proof onto the business, seen as the party that is in the best position tobearit; but, at the same time, a permanent derogation from the principle of the *actori incumbit probatio*, is rejected.

Keywords: Burden of proof; unauthorized payment; phishing.

[170] N. Cayrol, *La Cour de cassation et les faits de société*, in *RTD civ.*, 2018, p. 485.