

La tutela dell'utente degli strumenti di pagamento contro le transazioni fraudolente: problematiche giuridico-applicative e possibili evoluzioni.

User protection of payment instruments against fraudulent transactions: legal-application problems and possible evolutions.

LUIGI IZZO

Dottorando di ricerca *Sugli ambiti di interazione e integrazione tra le scienze umane e le tecnologie avanzate*, Università degli Studi di Napoli Suor Orsola Benincasa

Abstract

In circa trenta anni si è assistito a una evoluzione radicale del sistema finanziario, tanto nel panorama europeo quanto con riferimento a quello globale, mediante il processo di globalizzazione dei mercati, l'interconnessione delle economie, l'introduzione di una moneta unica a livello europeo, l'abbattimento delle frontiere nella prestazione dei servizi e lo sviluppo delle ICT (information and communications technologies).

Questi fenomeni, tra loro interconnessi, hanno innescato processi con conseguenze significative per numerosi ambiti, in particolare per quello dei servizi di pagamento., che ha visto la nascita e la diffusione della cd. "moneta elettronica".

Tuttavia, ciò ha portato con sé le inevitabili conseguenze negative, sostanziatesi nelle diverse e numerose metodologie di accesso truffaldino ai servizi di pagamento elettronici, tali da richiedere la predisposizione di sistemi a tutela dei titolari degli stessi, che non paiono essere idonei allo scopo dichiarato di proteggere i conti e i depositi, sovente violati da terzi.

In about thirty years there has been a radical evolution of the financial system, both in the European panorama and regarding the global one, through the process of globalization of the markets, the interconnection of economies, the introduction of a single currency at the European level, the abolition of borders in the provision of services and the development of ICT (information and communications technologies).

These phenomena, interconnected with each other, have triggered processes with significant consequences for numerous areas, in particular for that of payment services., Which saw the birth and spread of the so-called "Electronic money".

However, this has brought with it the inevitable negative consequences, resulting in the various and numerous methods of fraudulent access to electronic payment services, such as to require the preparation of systems to protect the holders of the same, which do not appear to be suitable for the declared purpose of protect accounts and deposits, often violated by third parties.

Parole chiave: Strumenti di pagamento; moneta elettronica; ICT; Data Protection.

Keywords: payment instruments; e-money; ICT; Data Protection.

Summary: Introduzione. – 1. Il quadro normativo europeo e nazionale. – 1.1 Il concetto di “moneta elettronica”. – 1.2 I profili di responsabilità previsti in tema di e-money. – 2. Problematiche interpretative in tema di responsabilità degli intermediari. – 2.1 I primi orientamenti in materia di diligenza bancaria. – 2.2 La novella *post* PSD2 e l’operato dell’Arbitro Bancario Finanziario. – 3. La sostanziale inefficacia del sistema di tutele. – 3.1 Le statistiche sull’andamento delle transazioni fraudolente. – 3.2 Una possibile evoluzione dei sistemi di pagamento attraverso IA e *blockchain*. – Conclusioni.

Introduzione.

La cd. “moneta elettronica”, altrimenti detta *e-money*¹ in correlazione al fenomeno del commercio elettronico, ossia l’*e-commerce*, è una delle innovazioni più importanti nell’ambito delle transazioni bancarie, basata sul concetto di trasferimento di somme di denaro slegato dalla materialità della consegna e attuato a mezzo di impulsi elettronici. In verità, tale modalità di pagamento era già molto diffusa prima dell’attuale crisi pandemica globale, per quanto quest’ultima abbia determinato un ricorso sempre più intenso ai sistemi di pagamento dematerializzati². Tuttavia, se è vero che circa nove milioni di italiani sono oramai avviati sulla strada dei pagamenti digitali (anche per le piccole spese quotidiane), è altrettanto vero che ben diciotto milioni sono coloro che, per svariati motivi, rinunziano ad abbracciare (in parte o totalmente) la strada della digitalizzazione e tra le motivazioni risalta il timore di essere oggetto di furti e clonazioni (16,8% degli intervistati)³.

Tale paura non è assolutamente infondata, anzi. Si può tranquillamente

¹ L’espressione è usata in P. PACILEO, *L’attuazione in Italia delle direttive comunitarie in materia di e-money*, in *La moneta elettronica: profili giuridici e problematiche applicative*, a cura di SICA-STANZIONE-Z. ZENCOVICH, Giuffrè, 2006, p. 191.

² Si consideri che nel commercio e nei pagamenti si attuano operazioni che vengono svolte (ancora, per ora) toccando, prendendo, usando oggetti che, spesso e volentieri, cambiano possesso più volte nel corso della stessa giornata. Ma proprio per questo si è verificato un forte ricorso al digitale, attesa l’incompatibilità di simili procedure fisiche in ragione della perdurante pandemia da SARS-CoV-2. Anche l’utilizzo del denaro contante, ovviamente, ha risentito di simili tendenze, per quanto, in questo specifico caso, parte della “colpa” sia da rinvenirsi più in una certa “informazione giornalistica” condotta male e che ha dominato la prima parte della pandemia (cfr. B. GARDNER, *Dirty banknotes may be spreading the coronavirus*, WHO suggests, articolo comparso il 2 marzo 2020 su www.telegraph.co.uk/news/2020/03/02/exclusive-dirty-banknotes-may-spreading-coronavirus-world-health/). L’articolo in questione, per l’autorevolezza della testata, è stato immediatamente ripreso da diversi giornali in tutto il mondo, con conseguenze facilmente immaginabili). Questa tendenza è stata poi confermata in occasione della presentazione della nuova edizione dell’Osservatorio Innovative Payments della School of Management del Politecnico di Milano, avvenuta durante l’evento «*Innovative Payments: da alternativa a necessità*», nella quale risulta che un terzo degli acquisti effettuati dagli italiani è avvenuto per mezzo dei sistemi di pagamento elettronici (cfr. A. LAR., *Covid e cashback spingono i pagamenti digitali: nel 2020 senza contanti un acquisto su tre*, 11 marzo 2021 su www.ilsole24ore.com/art/covid-e-cashback-spingono-pagamenti-digitali-nel-2020-senza-contanti-acquisto-tre-ADPXnZPB).

³ L. INCORVATI, *La paura del contagio porta a dire addio al contante*, 22 ottobre 2020 su www.ilsole24ore.com/art/la-paura-contagio-porta-dire-addio-contante-ADaCrZx

asserire che, in parallelo con la diffusione dei servizi di pagamento digitali, si è avuta una sempre più alta circolazione di truffe e attacchi informatici quali *phishing*, *SIM Swap* e clonazione, a danno dei sistemi di pagamento come le carte di credito.

Ovviamente, il *trend* pare destinato unicamente ad acuirsi. Tant'è vero che da un rapporto statistico relativo al nostro Paese, pubblicato nel 2020 dal Ministero dell'Economia e delle Finanze (MEF)⁴ e aggiornato al 2019, emerge testualmente che «Le frodi, sia in valore che in numero, sono in forte aumento rispetto all'anno precedente (circa +28%). Quelle in valore sono dunque salite a un livello leggermente superiore (102,3) rispetto a quello del 2009, mentre quelle in numero si mantengono molto più elevate (207,1). In termini di valore, senza tenere conto delle transazioni totali genuine, si assiste a un aumento del fenomeno su tutti i canali. Nello specifico, colpisce l'incremento dei prelievi ATM (+44,1%), accompagnato da un incremento del 27,6% sul canale Internet e del 25% su POS. La maggior parte delle frodi su Internet risulta avvenuta all'estero.»⁵.

Un simile aumento non deve certo stupire, anche in considerazione di come i malviventi abbiano a disposizione una variegata panoplia di strumenti per perpetrare le loro frodi. In generale, tali metodi atti a frodare vengono suddivisi in due macrocategorie:

- La macrocategoria delle frodi CNP, acronimo con cui si intende una transazione del tipo "*card-not-present*", ossia che prescinde dall'utilizzo di una carta di pagamento per l'autenticazione dell'utente, dovendosi "solo" inserire, seguendo le indicazioni del sistema che gestisce il pagamento, il codice CCV, il numero della carta, il PIN ovvero un codice monouso fornito dal proprio intermediario a mezzo SMS o tramite apposita app. Pertanto, rientrano in questa categoria tutte le transazioni che avvengono su store online, su servizi di home banking, su sistemi di tipo e-wallet. Ovviamente, nell'ipotesi di frode il soggetto che inserisce manualmente i dati in questione non è assolutamente identificabile con il titolare dello strumento di pagamento;
- La macrocategoria delle frodi "materiali", attuate tramite terminali ATM e POS vedono una modifica dei dispositivi che leggono le carte in modo da carpirne i dati, uniti a microtelecamere per vedere la digitazione del PIN, così da utilizzarli per clonare materialmente le carte e successivamente utilizzarle.

Tuttavia, la modifica dei dispositivi può risultare oggettivamente rischiosa da operare⁶ e, invero, sono oramai comunemente diffusi una serie di

⁴ MEF – DIPARTIMENTO DEL TESORO, *Rapporto statistico sulle frodi con le carte di pagamento 2020*, a cura della DIREZIONE V UFFICIO VI – UCAMP – UFFICIO CENTRALE ANTIFRODE DEI MEZZI DI PAGAMENTO, disponibile al link http://www.dt.mef.gov.it/modules/documenti_it/antifrode_mezzi_pagamento/antifrode_mezzi_pagamento/Rapporto_statistico_sulle_frodi_con_le_carte_di_pagamento_-_edizione_2020.pdf

⁵ *Ivi*, p. 7-8

⁶ Si consideri, a titolo esemplificativo, una tecnica alquanto "artigianale" e, per questo, ben più rischiosa, definita "*lebanese loop*". Questa consiste nella manomissione della sola fessura di inserimento della carta di un ATM, inserendo nella stessa un dispositivo che blocca fisicamente la carta di pagamento (cfr. https://www.axisbank.com/bank-smart/safe-banking/atm/lebanese_loop.html). In quel momento, poi, il malcapitato, generalmente un anziano, viene avvicinato da un soggetto che, guarda caso, transitava nelle vicinanze e si poneva subito a disposizione dell'utente al solo scopo di carpire il codice PIN, in modo da utilizzarlo con la carta di pagamento originale, che avrebbe estratto in seguito all'allontanamento del

comportamenti prudenziali⁷ a scopo di contrasto.

Ne consegue che le tecniche tipo CNP dominano letteralmente le statistiche di settore. Di queste tecniche, certamente la più conosciuta e diffusa è quella del *phishing*⁸, una forma di adescamento della quale numerosi cadono vittime grazie a un abile sfruttamento delle loro stesse paure.

Per esempio, per mezzo di una mail ovvero di un SMS (nel qual caso si parla di *smishing*) si viene avvisati di un supposto problema relativo al nostro account, solitamente legato alla sicurezza. Magari in tale comunicazione si avverte l'utente di un blocco (ovviamente inventato) dell'account e per risolverlo invita a cliccare su un link che, però, riporta a un sito fittizio, controllato dal cracker e che riproduce molto bene il portale dell'istituto bancario o della posta, rendendo difficile rendersi conto di quel che si sta facendo.

In tal modo, senza rendersi conto che li sta letteralmente regalando al criminale, l'utente ingenuamente inserisce i dati sensibili relativi alla propria carta di pagamento in quelli che sembrano i campi di compilazione di una pagina apparentemente appartenente al proprio intermediario.

Non solo mail e SMS sono i vettori di queste frodi, dal momento che sono divenute ancora più insidiose grazie all'utilizzo del *vishing* (ossia il *voice-phishing*), che è attuato a mezzo telefonate da parte di presunti operatori che avvertono (o meglio, allarmano) l'utente in merito a non meglio dichiarate anomalie delle carte di pagamento⁹.

Poi, a testimoniare l'evoluzione delle frodi CNP, si può ricordare anche l'*e-skimming*¹⁰ (che prende ispirazione da una tecnica descritta nel prossimo paragrafo) e che, mediante l'installazione di codice malevolo nelle pagine *web* in cui erano presenti moduli da compilare per effettuare pagamenti online, provocava una "sostituzione" di questi moduli compilabili con altri predisposti dai cybertruffatori e che avrebbero trasmesso a questi i dati inseriti dagli utenti.

Ciò conduce necessariamente a chiedersi se, contro simili minacce, l'attuale sistema di tutele sia adeguato ovvero necessiti di essere rivisto.

legittimo titolare, convinto di aver perso la carta e di doverla far estrarre fisicamente dall'ATM ad opera dei tecnici della filiale (cfr. A. ZURLO, *La truffa del cd. "lebanese loop" - Nota a ABF, Collegio di Roma, 11 gennaio 2021, n. 540*, su www.dirittodelrisparmio.it).

⁷ Vedasi quelli descritti in una pagina del sito istituzionale dei Carabinieri, disponibile al link <http://www.carabinieri.it/cittadino/consigli/tematici/giorno-per-giorno/la-carta-di-credito/carta-di-credito>

⁸ R. RIJTANO, *Phishing, cos'è e come proteggersi: la guida completa*, 29 maggio 2018 su www.cybersecurity360.it. Ma si considerino pure le pagine ad essa dedicate dai vari intermediari, quali Intesa San Paolo (<https://www.intesasanpaolo.com/it/common/landing/anti-phishing/phishing-vishing-smishing-come-proteggersi.html>) e Poste Italiane (<https://www.poste.it/psd2-e-sicurezza---come-difendersi-dalle-truffe.html>). Secondo la giurisprudenza penale (cfr. *ex multis* Trib. Monza, 7 maggio 2009, in *Riv. pen.*, 2010) tale condotta è configurabile anche mediante intrusione nel sistema informatico ed è sussumibile nella fattispecie di "truffa", come pure quella di accesso abusivo in sistema informatico (cfr. PERRI, *Analisi informatico-giuridica dei reati di frode informatica e accesso abusivo a un sistema informatico o telematico con l'aggravante dell'abuso della qualità di operatore del sistema*, in *Giur. merito*, 2008, 1651).

⁹ REDAZIONE, *La nuova cybertruffa in auge è il vishing*, 30 maggio 2020 su www.ilsole24ore.com

¹⁰ S. LOMBARDO, *E-skimmer nascosti nei siti Web, così ci clonano le carte di credito: che c'è da sapere*, 14 maggio 2020 su www.cybersecurity360.it

1. Il quadro normativo europeo e nazionale.

Al fine di analizzare compiutamente l'attuale scenario sul piano giuridico, non è possibile prescindere da una previa analisi della normativa di riferimento e va chiarito, anzitutto, cosa sia la "moneta elettronica" e quali ipotesi di responsabilità siano state previste dal legislatore tanto per l'utente della stessa e degli strumenti che di essa si avvalgono quanto per l'intermediario che la fornisce.

1.1 Il concetto di "moneta elettronica".

Trattasi di espressione che, in verità, è oramai datata, poiché coniata all'inizio del processo di rinnovamento dei sistemi di pagamento, i quali sono attualmente arrivati a quella che sarebbe la quarta generazione degli stessi¹¹. Infatti, questo concetto fa la sua comparsa per la prima volta in un testo normativo europeo con la Raccomandazione della Commissione 97/489/CE 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", dove si legge testualmente, nel terzo Considerando, «che ai fini della presente raccomandazione, gli strumenti di pagamento comprendono inoltre gli strumenti di moneta elettronica ricaricabili aventi forma di carte con valore immagazzinato e di memorie di elaboratori elettronici collegati in rete»¹².

Il primo atto effettivamente vincolante in tale ambito è, piuttosto, la prima Direttiva IMEL (così denominata perché introduce, accanto ai classici intermediari, anche gli Istituti di Moneta Elettronica, gli IMEL), attuata in Italia con il d.lgs. n. 39/2002 e il cui terzo Considerando qualifica la moneta elettronica come un *surrogato elettronico* del normale denaro contante¹³.

Tale Direttiva è stata poi superata dalla seconda Direttiva IMEL¹⁴, recepita dal nostro Legislatore con il d.lgs. n. 45/2012 e nella quale viene indicato come prioritario un aggiornamento della definizione stessa di "moneta elettronica", tant'è vero che nei Considerando dell'atto – elementi imprescindibili al fine di

¹¹ P. SPADA, *Carte di credito, terza generazione dei mezzi di pagamento*, in *Rivista di Diritto Civile*, 1976, I, pag. 489, dove la prima generazione dei mezzi di pagamento è identificata con la moneta avente corso legale, la seconda nei titoli di credito, la terza nelle carte di credito. Pertanto, molto probabilmente, la quarta potrebbe essere ragionevolmente rappresentata dagli attuali trasferimenti elettronici di fondi e nei pagamenti elettronici.

¹² Invero, vi è chi fa notare come questa espressione sia ancor più risalente nel tempo (cfr. L. CAPALDO, *Moneta elettronica e trasparenza*, in *La moneta elettronica: profili giuridici e problematiche applicative*, a cura di SICA-STANZIONE-Z. ZENCOVICH, Giuffrè, 2006, p. 158). in quanto rinvenibile nel report del 1996 *SECURITY OF ELECTRONIC MONEY*, stilato a cura del *Committee on Payment and Settlement System* (disponibile su www.bis.org/cpmi/publ/d18.pdf). Vi è poi il GUERRIERI (cfr. G. GUERRIERI, *La moneta elettronica – profili giuridici dei nuovi sistemi di pagamento*, Il Mulino, 2015, p. 41 nota n. 2) che la retrodata ulteriormente al 1994, anno in cui fu presentato il "Report to the Council of the European Monetary Institute on prepaid cards" (disponibile su www.ecb.europa.eu/pub/pdf/other/prepaidcards1994en.pdf), nel quale si parla, molto profeticamente, di *cashless money* (pag. 9) ed *electronic purse money* (pag. 6).

¹³ Direttiva 2000/46/CE "riguardante l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica", art. 1, co. 2, lett. b), dove si definisce la "moneta elettronica" come «un valore monetario rappresentato da un credito nei confronti dell'emittente che sia: i) memorizzato su un dispositivo elettronico; ii) emesso dietro ricezione di fondi il cui valore non sia inferiore al valore monetario emesso; iii) accettato come mezzo di pagamento da imprese diverse dall'emittente.»

¹⁴ Direttiva 2009/110/CE, "concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE"

fornire una chiave di lettura preziosa per risolvere le ambiguità che spesso sono presenti nel testo legislativo¹⁵ – si asserisce che «(7) È opportuno introdurre una definizione chiara di moneta elettronica che sia tecnicamente neutra. [...]. (8) È opportuno che la definizione di moneta elettronica copra la moneta elettronica, sia se detenuta su un dispositivo di pagamento in possesso del detentore di moneta elettronica, sia se memorizzata a distanza su un server e gestita dal detentore tramite un conto specifico per la moneta elettronica. Tale definizione dovrebbe essere abbastanza generale da non ostacolare l'innovazione tecnologica e da includere non soltanto tutti i prodotti di moneta elettronica disponibili oggi sul mercato, ma anche i prodotti che potrebbero essere sviluppati in futuro.».

1.2 I profili di responsabilità previsti in tema di e-money.

Chiarita la nozione base di e-money, si procede ad illustrare il regime di responsabilità delineato a mezzo delle ultime novelle legislative.

Questi profili sono stati disciplinati per mezzo di separati atti comunitari, ossia le due Direttive sui sistemi di pagamento (PSD1¹⁶ e PSD2¹⁷), le cui innovazioni sono confluite tutte nel d.lgs. n. 11/2010.

Innanzitutto, è necessario separare la responsabilità dell'emittente della moneta elettronica da quella che si pone in capo all'utilizzatore della stessa, la quale è disciplinata dall'art. 7 del d.lgs. n. 11/2010, relativo agli obblighi dell'utente della Moneta Elettronica¹⁸. Secondo questa disposizione, l'utente ha, sostanzialmente, due obblighi, di cui il primo configurabile come obbligo di *comunicazione* e il secondo quale obbligo di *custodia* e di *uso conforme* dello strumento di pagamento.

È a detti obblighi che si ricollega l'art. 12¹⁹, il quale disciplina appunto la

¹⁵ R. BARATTA, *Complexity of EU law in the domestic implementing process*, articolo tra gli atti del seminario *Quality of legislation - EU Legislative Drafting: Views from those applying EU law in the Member States*, tenutosi a Bruxelles il 3 luglio 2014 e disponibile su ec.europa.eu/dgs/legal_service/seminars/20140703_baratta_speech.pdf, p. 13, laddove si ricorda come «Recitals can help to explain the purpose and intent behind a normative instrument. They can also be taken into account to resolve ambiguities in the legislative provisions to which they relate». Ciononostante, valga l'avvertimento della Corte di Giustizia dell'Unione Europea che ricorda come questi Considerando non abbiano «binding legal force and cannot be relied on as a ground for derogating from the actual provisions of the act in question» (cfr. Case C-162/97, Nilsson, [1998] ECR I-7477, para. 54, disponibile su <https://eur-lex.europa.eu>).

¹⁶ Direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE, che abroga la direttiva 97/5/CE (*Payment Services Directive*)

¹⁷ Direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE

¹⁸ «1. L'utente abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di: a) utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso e che devono essere obiettivi, non discriminatori e proporzionati; b) comunicare senza indugio, secondo le modalità previste nel contratto quadro, al prestatore di servizi di pagamento o al soggetto da questo indicato lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza.

2. Ai fini di cui al comma 1, lettera a), l'utente, non appena riceve uno strumento di pagamento, adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate.».

¹⁹ «1. Salvo il caso in cui abbia agito in modo fraudolento, l'utente non sopporta alcuna perdita derivante dall'utilizzo di uno strumento di pagamento smarrito, sottratto o utilizzato indebitamente intervenuto dopo la comunicazione eseguita ai sensi dell'articolo 7, comma 1, lettera b).

responsabilità del pagatore, valutabile sotto tre profili:

- Che abbia agito con intenti fraudolenti nei confronti dell'emittente di moneta elettronica²⁰;
- Che abbia dolosamente omesso di adempiere agli obblighi di custodia dello strumento di pagamento;
- Che abbia, con colpa grave, omesso di adempiere compiutamente agli obblighi di custodia dello strumento di pagamento.

Ora, se nei primi due casi è possibile, in qualche modo, qualificare il "livello" di imputabilità della relativa condotta, più difficile è, invece, definire quando si sia in presenza di colpa grave ovvero di colpa lieve/assente.

In tal caso, si dovrà avere riguardo al contenuto delle disposizioni contrattuali, le quali, spesso e volentieri, sono fornite di esempi che chiariscono la condotta da tenersi²¹.

Per contro, la responsabilità del *provider* di servizi di pagamento appare definita in modo molto meno articolato. Si consideri quanto previsto nell'art. 8, d.lgs. n. 11/2010:

«1. Il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo di:

a) assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento, fatti salvi gli obblighi posti in capo a quest'ultimo ai sensi dell'articolo 7;

b) astenersi dall'inviare strumenti di pagamento non richiesti, a meno che lo strumento di pagamento già consegnato all'utente debba essere sostituito;

c) assicurare che siano sempre disponibili strumenti adeguati affinché l'utente dei servizi di pagamento possa eseguire la comunicazione di cui all'articolo 7, comma 1, lettera b), nonché, nel caso di cui all'articolo 6, comma 4, di chiedere lo

2. Salvo il caso in cui abbia agito in modo fraudolento, l'utente non è responsabile delle perdite derivanti dall'utilizzo dello strumento di pagamento smarrito, sottratto o utilizzato indebitamente quando il prestatore di servizi di pagamento non ha adempiuto all'obbligo di cui all'articolo 8, comma 1, lettera c).

2-bis. Salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente.

2-ter. Il pagatore non sopporta alcuna perdita se lo smarrimento, la sottrazione o l'appropriazione indebita dello strumento di pagamento non potevano essere notati dallo stesso prima di un pagamento, salvo il caso in cui abbia agito in modo fraudolento, o se la perdita è stata causata da atti o omissioni di dipendenti, agenti o succursali del prestatore di servizi di pagamento o dell'ente cui sono state esternalizzate le attività.

3. Negli altri casi, salvo se abbia agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi di cui all'articolo 7, con dolo o colpa grave, il pagatore può sopportare, per un importo comunque non superiore a euro 50, la perdita relativa a operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita.

4. Qualora abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'articolo 7, con dolo o colpa grave, l'utente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di 50 euro di cui al comma 3.».

²⁰ Trattasi dei casi in cui il cliente operi una falsa denuncia di operazioni non autorizzate ovvero eseguite in modo inesatto, trasmettendo una comunicazione ai sensi dell'art. 9, d.lgs. n. 11/2010

²¹ Per esempio, si considerino le Condizioni Generali della FinecoBank S.p.A., aggiornate al 18 marzo 2021 e disponibili al link https://images.fineco.it/pub-fineco/pdf/apriconto/condizioni_generali.pdf, nello specifico il contenuto degli artt. 4, rubricato "Custodia della Carta e del P.I.N. e del Codice di Sicurezza", e 5, inerente all'ipotesi di smarrimento/sottrazione delle credenziali. Ebbene, avendo quale riferimento un ipotetico caso con, quale "protagonista", un cliente della FinecoBank S.p.A., si dovrà innanzitutto verificare se la sua condotta sia stata aderente alle raccomandazioni presenti nello stesso testo contrattuale o meno, così da poter verificare se si sia quantomeno nell'ambito della cd. "colpa grave" ai fini di una imputabilità, nei confronti dell'utente, delle conseguenze negative delle operazioni di cui questi chiede il rimborso.

sblocco dello strumento di pagamento o l'emissione di uno nuovo, ove il prestatore di servizi di pagamento non vi abbia già provveduto. Ove richiesto dall'utente, il prestatore di servizi di pagamento gli fornisce i mezzi per dimostrare di aver effettuato la comunicazione di cui all'articolo 7, comma 1, lettera b), entro i 18 mesi successivi alla comunicazione medesima;

c-bis) fornire all'utente la possibilità di procedere alla comunicazione di cui all'articolo 7, comma 1, lettera b), a titolo gratuito, addebitandogli eventualmente solo i costi di sostituzione dello strumento di pagamento;

d) impedire qualsiasi utilizzo dello strumento di pagamento successivo alla comunicazione di cui all'articolo 7, comma 1, lettera b).

2. I rischi derivanti dalla spedizione di uno strumento di pagamento o delle relative credenziali di sicurezza personalizzate sono a carico del prestatore di servizi di pagamento.».

Quindi, pure il *provider* è soggetto a degli obblighi, solo che sembrano essere limitati piuttosto alla "semplice" garanzia dell'integrità dei dati in suo possesso, da intendersi tanto come condotta volta a prevenire intrusioni nel sistema informatico quanto come condotta idonea, *ex post*, a porre rimedio ad eventuali anomalie²².

E, invero, i profili di responsabilità previsti all'art. 11, d.lgs. n. 11/2010 sono strettamente attinenti alla custodia del sistema informatico in sé, stante il fatto che le ipotesi di utilizzo fraudolento ovvero omissione colposa/dolosa delle precauzioni in tema di custodia sono chiaramente definite nel successivo art. 12, delineato in precedenza. Infatti, se si considera che l'art. 11²³ non delinea

²² R. CELELLA, *Principi generali della protezione dei dati personali: qualità e integrità dei dati*, su www.dataprotectionlaw.it, 15 luglio 2018

²³ Art. 11, d.lgs. n. 11/2010 - «1. Fatto salvo l'articolo 9, nel caso in cui sia stata eseguita un'operazione di pagamento non autorizzata, il prestatore di servizi di pagamento rimborsa al pagatore l'importo dell'operazione medesima immediatamente e in ogni caso al più tardi entro la fine della giornata operativa successiva a quella in cui prende atto dell'operazione o riceve una comunicazione in merito. Ove per l'esecuzione dell'operazione sia stato addebitato un conto di pagamento, il prestatore di servizi di pagamento riporta il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo, assicurando che la data valuta dell'accredito non sia successiva a quella dell'addebito dell'importo.

2. In caso di motivato sospetto di frode, il prestatore di servizi di pagamento può sospendere il rimborso di cui al comma 1 dandone immediata comunicazione per iscritto alla Banca d'Italia all'((...)).

2-bis. Se l'operazione di pagamento è disposta mediante un prestatore di servizi di disposizione di ordine di pagamento, il prestatore di servizi di pagamento di radicamento del conto rimborsa al pagatore immediatamente e, in ogni caso, entro la fine della giornata operativa successiva, l'importo dell'operazione non autorizzata, riportando il conto di pagamento addebitato nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo. In caso di operazione di pagamento non autorizzata, se il relativo ordine di pagamento è disposto mediante un prestatore di servizi di disposizione di ordine di pagamento, quest'ultimo è tenuto a rimborsare immediatamente e, in ogni caso, entro la fine della giornata operativa successiva, senza che sia necessaria la costituzione in mora, al prestatore di servizi di pagamento di radicamento del conto su richiesta di quest'ultimo, gli importi rimborsati al pagatore. Se il prestatore di servizi di disposizione di ordine di pagamento è responsabile dell'operazione di pagamento non autorizzata, risarcisce immediatamente e, in ogni caso, entro la fine della giornata operativa successiva senza che sia necessaria la costituzione in mora il prestatore di servizi di pagamento di radicamento del conto, su richiesta di quest'ultimo, anche per le perdite subite. In entrambi i casi è fatta salva la facoltà del prestatore di servizi di disposizione di ordine di pagamento di dimostrare, in conformità a quanto disposto dall'articolo 10, comma 1-bis, che, nell'ambito delle sue competenze, l'operazione di pagamento è stata autenticata, correttamente registrata e non ha subito le conseguenze di guasti tecnici o altri inconvenienti relativi al servizio di pagamento da questo prestato, con conseguente diritto in questi casi alla restituzione delle somme da quest'ultimo versate al prestatore di servizi di pagamento di radicamento del conto ai sensi del presente comma.

3. Il rimborso di cui ai commi precedenti non preclude la possibilità per il prestatore di servizi di pagamento di dimostrare, anche in un momento successivo, che l'operazione di pagamento era stata autorizzata. In tal caso, il

chiare ipotesi a carico del prestatore di servizi di pagamento, mentre, al contrario, sono precisamente descritte quelle previste a carico dell'utente del sistema di pagamento, ne consegue logicamente che, per esclusione, tutte quelle possibili fattispecie di responsabilità non ricomprese (e non ricomprendibili) nel disposto dell'art. 12 vanno intese come rientranti nel campo di applicazione dell'art. 11²⁴.

1.3 I presidi di sicurezza adottati dopo la PSD2.

Spostando ora l'attenzione sui metodi di autenticazione, va chiarito che questi non si riducono unicamente alla combinazione PIN/striscia magnetica – come nel caso di pagamenti con POS o prelievi presso gli ATM – ovvero all'utilizzo dei dati presenti sulla carta, magari in combinazione con i normali dati di autenticazione utilizzati per l'accesso al portale di *home banking* del proprio intermediario (*password* o indirizzo *e-mail* di riferimento)²⁵.

Infatti, è stato adottato un differente approccio, consacrato con la Direttiva PSD2, il quale sfocia nell'adozione della cd. "*Strong Customer Authentication*" (d'ora in avanti SCA) in relazione a qualsiasi operazione avvenga *online*²⁶.

In virtù del Regolamento di attuazione di questa Direttiva, quindi "*l'autenticazione si basa su due o più elementi che sono classificati nelle categorie della conoscenza, del possesso e dell'inerenza e comporta la generazione di un codice di autenticazione.*"²⁷, peraltro indipendenti tra loro e interscambiabili, in modo tale che la violazione di uno di questi tre fattori di autenticazione non comporti l'automatica compromissione degli altri due²⁸. Questi tre elementi tra cui è possibile scegliere sono:

- identificazione con una password o con un PIN: quindi qualcosa di criptato che l'utente *conosce*²⁹ può essere una parola chiave

prestatore di servizi di pagamento ha il diritto di chiedere direttamente all'utente e ottenere da quest'ultimo la restituzione dell'importo rimborsato ai sensi dei commi 1 e 2-bis.

4. Il risarcimento di danni ulteriori subiti può essere previsto in conformità alla disciplina applicabile al contratto stipulato tra l'utente e il prestatore di servizi di pagamento compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento.»

²⁴ G. GUERRIERI, *La moneta elettronica – profili giuridici dei nuovi sistemi di pagamento*, cit., p. 158, dove pone, quale esempio, l'ipotesi di un malfunzionamento proprio del sistema informatico, tale da comportare una "duplicazione" della medesima operazione di pagamento, la quale venga effettuata due volte, senza che vi sia responsabilità alcuna del pagatore

²⁵ Per i quali, tra l'altro, valgono i normali "presidi di sicurezza" identificabili come le misure dettate dal buon senso e descritte dalla Banca d'Italia al link <https://economiepertutti.bancaditalia.it/notizie/pagamenti-in-sicurezza/>

²⁶ Art. 10-bis, co. 1, d.lgs. n. 11/2010 – "*Conformemente all'articolo 98 della direttiva (UE) 2015/2366 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente:*

a) accede al suo conto di pagamento on-line;

b) dispone un'operazione di pagamento elettronico;

c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi."

²⁷ Art. 4 del 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

²⁸ Art. 9 del Regolamento Delegato (UE) 2018/389

²⁹ Art. 6 del Regolamento Delegato (UE) 2018/389 – "*1. I prestatori di servizi di pagamento adottano misure volte ad attenuare il rischio che gli elementi dell'autenticazione forte del cliente classificati come **conoscenza** siano acquisiti da soggetti non autorizzati o divulgati a questi ultimi. 2. L'uso di detti elementi da parte del*

- piuttosto che un codice o una domanda di sicurezza;
- identificazione con qualcosa che sia in *possesso*³⁰ all'utente e che l'utente può utilizzare, tipicamente un device come lo smartphone piuttosto un device portatile o ancora un token bancario;
- identificazione con qualcosa di fisico: impronta digitale o lineamenti biometrici del viso, ovvero tratti che, in qualche modo, sono *in grado di caratterizzare il cliente*³¹ identificandolo nella sua persona in modo univoco.

Per esempio, laddove si intenda acquisire un biglietto del treno a mezzo *PayPal*, si dovrà in primo luogo inserire il primo fattore di autenticazione, che è quello che dà accesso al servizio stesso di *PayPal*, per poi inserire il secondo fattore di autenticazione, fornito direttamente dall'intermediario che gestisce la carta di pagamento collegata all'*e-wallet*.

Di conseguenza, nel caso di acquisti *online* sarà necessario utilizzare questa autenticazione forte, seguendo una regola particolarmente rigida.

Ebbene, va riconosciuto che la stessa opera indubbiamente a vantaggio sia dei consumatori che degli esercenti di *e-commerce*, in quanto consente di tenere sotto controllo pressoché qualsiasi movimento di fondi sui propri mezzi di pagamento elettronici, con delle esenzioni ben tipizzate.

Tuttavia, queste nuove procedure in materia di autenticazione non paiono aver sortito pienamente l'effetto sperato (anzi, sono pure contestate dagli esercenti in quanto disincentiverebbero gli acquirenti dal proseguire acquisti già iniziati³²).

Tale risultato è da attribuirsi all'evoluzione costante delle tecniche con cui si appropria delle credenziali di accesso ai sistemi di pagamento a fini fraudolenti³³.

pagatore è soggetto a misure di attenuazione allo scopo di impedire che vengano divulgati a soggetti non autorizzati."

³⁰ Art. 7 del Regolamento Delegato (UE) 2018/389 – "1. I prestatori di servizi di pagamento adottano misure volte ad attenuare il rischio che gli elementi dell'autenticazione forte del cliente classificati come **possesso** siano utilizzati da soggetti non autorizzati. 2. L'uso di detti elementi da parte del pagatore è soggetto a misure volte a impedirne la duplicazione."

³¹ Art. 8 del Regolamento Delegato (UE) 2018/389 – "1. I prestatori di servizi di pagamento adottano misure volte ad attenuare il rischio che gli elementi di autenticazione classificati come **inerenza** e letti dai dispositivi e dal software di accesso forniti al pagatore siano acquisiti da soggetti non autorizzati. Come minimo, i prestatori di servizi di pagamento garantiscono che la probabilità che soggetti non autorizzati effettuino l'autenticazione a nome del pagatore utilizzando detti dispositivi e software sia molto bassa. 2. L'utilizzo di detti elementi da parte del pagatore è soggetto a misure volte ad assicurare che detti dispositivi e software garantiscano la resistenza contro l'utilizzo non autorizzato degli elementi mediante l'accesso ai dispositivi e al software."

³² Infatti, una ricerca condotta dalla AXERVE S.p.A., società operante nel settore dei pagamenti digitali, sulla base di dati forniti da Mastercard, fa emergere come siano numerose le transazioni che non vengono concluse a causa di *timeout* di sistema ovvero di disagi sul piano della *user experience* – cfr. A. S., *E-commerce, transazioni più sicure grazie all'analisi in real time*, 3 maggio 2021 su www.pagamentidigitali.it

³³ Per esempio, si consideri la tecnica definita "SIM Swap", con cui il truffatore cambia il numero di telefono del titolare con il proprio, al fine di "bucare" i sistemi SCA che sfruttano l'elemento della conoscenza unito a quello del possesso. Cfr. S. GALEOTTI, *Truffa sim swap, le banche: "L'addio alle chiavette token ha aumentato sicurezza. I clienti devono essere più attenti al phishing"*, 31 gennaio 2020 su www.ilfattoquotidiano.it dove sono riportate le dichiarazioni in materia del Segretario Generale di ABI Lab (www.abilab.it/web/guest/chi-siamo), il centro di ricerca promosso dall'ABI (Associazione Bancaria Italiana).

2. Problematiche in tema di responsabilità degli intermediari.

Chiarito, quindi, come siano disciplinate le ipotesi di responsabilità per i soggetti parte del rapporto contrattuale inerente alla gestione dello strumento di pagamento e quali siano i presidi di sicurezza adottati, è necessario ora delineare brevemente gli orientamenti formati nel nostro Ordinamento in relazione specificamente alla responsabilità dell'intermediario, sia nell'ambito della giurisprudenza (arbitrale e ordinaria) sia nell'ambito della dottrina.

Ciò in quanto sussiste un chiaro *favor* verso l'utente dei sistemi di pagamento, come risulta dai Considerando della Direttiva PSD2³⁴.

2.1 I primi orientamenti in materia di diligenza bancaria tra dottrina e giurisprudenza.

Invero, è bene considerare che in ambito dottrinale, spesso e volentieri, sono state precorse le successive elaborazioni giurisprudenziali.

Più nello specifico, è necessario considerare quanto scritto in tema di

³⁴ Si consideri per esempio quanto disposto nei Considerando 91, 95 e 96 di detta Direttiva: «(91) I prestatori di servizi di pagamento sono responsabili delle misure di sicurezza. Tali misure devono essere proporzionate ai relativi rischi di sicurezza. È opportuno che i prestatori di servizi di pagamento stabiliscano un quadro per attenuare i rischi e mantenere procedure efficaci di gestione degli incidenti. È opportuno mettere in atto un meccanismo di segnalazione periodica in modo da garantire che i prestatori di servizi di pagamento forniscano periodicamente alle autorità competenti una valutazione aggiornata dei rischi di sicurezza cui sono confrontati e delle misure che hanno adottato per contrastarli. Inoltre, affinché i danni agli utenti, ad altri prestatori di servizi di pagamento o ad altri sistemi di pagamento, tra cui disfunzioni sostanziali di un sistema di pagamento, siano ridotti al minimo, è essenziale che i prestatori di servizi di pagamento siano tenuti a segnalare senza indugio i principali incidenti di sicurezza alle autorità competenti. Dovrebbe essere affidato un ruolo di coordinamento dell'ABE.

[...]

(95) La sicurezza dei pagamenti elettronici è fondamentale per garantire la protezione degli utenti e lo sviluppo di un contesto affidabile per il commercio elettronico. Tutti i servizi di pagamento offerti elettronicamente dovrebbero essere prestati in maniera sicura, adottando tecnologie in grado di garantire l'autenticazione sicura dell'utente e di ridurre al massimo il rischio di frode. Non si ravvisa la necessità di garantire lo stesso livello di protezione per le operazioni di pagamento disposte ed eseguite con modalità diverse rispetto all'uso di piattaforme o dispositivi elettronici, ad esempio operazioni di pagamento su supporto cartaceo, ordini per corrispondenza o ordini telefonici. Una crescita robusta dei pagamenti tramite Internet e dispositivi mobili dovrebbe essere accompagnata da un potenziamento generalizzato delle misure di sicurezza. I servizi di pagamento offerti via Internet o tramite altri canali a distanza - il cui funzionamento non dipende dal luogo fisico in cui sono situati il dispositivo per disporre l'operazione di pagamento o lo strumento di pagamento - dovrebbero pertanto comportare l'autenticazione delle operazioni attraverso codici dinamici, affinché l'utente sia, in ogni momento, al corrente dell'importo e il beneficiario dell'operazione che l'utente sta autorizzando.

(96) Le misure di sicurezza dovrebbero essere compatibili con il livello di rischio insito nel servizio di pagamento prestato. Al fine di permettere lo sviluppo di mezzi di pagamento di facile uso e accessibili per pagamenti a basso rischio, come i pagamenti di importo ridotto senza contatto fisico al punto vendita, basati o meno su telefono cellulare, le esenzioni dall'applicazione dei requisiti di sicurezza dovrebbero essere specificate in norme tecniche di regolamentazione. L'uso sicuro di credenziali di sicurezza personalizzate è necessario per limitare i rischi connessi al phishing e ad altre attività fraudolente. Al riguardo, l'utente dovrebbe poter fare affidamento sull'adozione di misure che tutelano la riservatezza e l'integrità delle credenziali di sicurezza personalizzate. Tali misure comprendono di norma sistemi di cifratura basati su dispositivi personali del pagatore, tra cui lettori di carte o telefoni cellulari, o forniti al pagatore dal proprio prestatore di servizi di pagamento di radicamento del conto mediante canali diversi, come SMS o posta elettronica. Le misure, comprendenti normalmente i sistemi di cifratura, che possono dar luogo a codici di autenticazione quali password monouso, sono in grado di potenziare la sicurezza delle operazioni di pagamento. L'uso di tali codici di autenticazione da parte degli utenti dei servizi di pagamento dovrebbe essere considerato compatibile con i relativi obblighi in relazione agli strumenti di pagamento e alle credenziali di sicurezza personalizzate, anche quando sono coinvolti prestatori di servizi di disposizione di ordine di pagamento o prestatori di servizi di informazione sui conti.»

diligenza dell'intermediario nell'esecuzione dei contratti.

Ebbene, si può pacificamente asserire che la dottrina più risalente (nonché consolidata) abbia mostrato di individuare una responsabilità particolarmente approfondita in capo alle banche. Ciò in ragione del dibattito sorto intorno ai canoni di condotta esigibili dalle aziende di credito nell'erogazione dei loro servizi alla clientela, nel corso del quale si è giunti al punto da postulare una vera e propria "diligenza del buon banchiere"³⁵, istituto così caratterizzato da portare una parte della dottrina a teorizzare una vera e propria responsabilità da status³⁶ in capo all'intermediario³⁷ sulla scorta della teoria del cd. "contatto sociale", indicazione successivamente raccolta dagli Ermellini.

Infatti, quasi trent'anni fa³⁸ la Corte di Cassazione ha chiarito come la diligenza del *bonus argentarius* sia caratterizzata da quel maggior grado di prudenza ed attenzione che la connotazione professionale dell'agente richiede. Non solo, essa deve trovare applicazione tanto in riferimento ai contratti bancari in senso stretto quanto ad ogni tipo di atto o di operazione posta in essere, nell'esercizio della sua attività, dalla banca, la quale deve predisporre qualsiasi mezzo idoneo onde evitare il verificarsi di eventi pregiudizievoli comunque prevedibili.

Altro orientamento, invero, postula l'applicazione della disciplina prevista per il mandato e, seguendo un percorso ermeneutico strettamente aderente alla lettera della norma, è stato evidenziato come l'art. 1856 c.c. prescriva, nell'esecuzione degli incarichi bancari, di attenersi alle regole del mandato³⁹. Detta norma opera un doppio richiamo, in quanto si ricollega prima al concetto di diligenza del buon padre di famiglia di cui all'art. 1710 c.c. e, per suo tramite, richiama il comma 1 dell'art. 1176 c.c.. Così facendo, però si postulerebbe un canone di condotta diverso rispetto a quello — assai più severo — della diligenza professionale, enunciata al comma 2 della medesima disposizione e alla quale va ricondotta la "diligenza del buon banchiere"⁴⁰.

Altri interpreti, ancora, hanno inquadrato l'attività in questione nell'ambito

³⁵ Dibattito, peraltro, che ha radici risalenti alla seconda metà dello scorso secolo, visto che già è affrontato in G. FERRI, *La diligenza del buon banchiere*, in *Banca borsa tit. cred.*, 1958, I, 1 e in P. VITALE, *Fondamento e limiti della "libertà" del banchiere nel pagamento degli assegni bancari*, 1959, I, 513. In giurisprudenza (cfr. Cass., 12.04.2018, n. 9158, questa con nota di M. C. DOLMETTA, *Responsabilità dell'intermediario in caso di operazioni fraudolente effettuate a mezzo di strumenti elettronici*, su www.dirittobancario.it, del 16 maggio 2018; Cass., 03.02.2017, n. 2950 con nota di L. ASTORRI, *Home banking: responsabilità del prestatore dei servizi di pagamento per operazioni disposte da terzi*, su www.dirittobancario.it, del 1° marzo 2017; Cass., 19.01.2016, n. 806 su <http://www.italgiure.giustizia.it/sncass/>; Cass., 12.06.2007, n. 13777 su <https://plusplus24diritto.ilsole24ore.com/>; Coll. Coord., 12.06.2019, n. 14447 su <https://www.arbitrobancariofinanziario.it/decisioni/index.html>) si parla della figura dell'*accorto banchiere*, che va ritenuta identica a quella teorizzata in dottrina.

³⁶ C. SCOGNAMIGLIO, *Sulla responsabilità dell'impresa bancaria per violazione di obblighi discendenti dal proprio status*, in *Giur. it.*, 1995, I, 1, 356; *Id.*, *Ancora sulla responsabilità della banca per violazione di obblighi discendenti dal proprio status*, in *Banca borsa tit. cred.*, 1997, II, 655; N. MARZONA, *Lo status (professionalità e responsabilità) della banca in una recente sentenza della Cassazione*, 1994, II, 266.

³⁷ Tale responsabilità da status potrebbe benissimo ricollegarsi, poi, alla necessità che l'intermediario si accolli interamente il cd. "rischio di impresa" delineato in accorta dottrina e recentemente accolto nella giurisprudenza arbitrale di cui si dirà nel prossimo paragrafo (cfr. Coll. Coord., 26.07.2018, n. 16237 <https://www.arbitrobancariofinanziario.it/decisioni/index.html>; Coll. Coord., 26.10.2012, n. 3498 su <https://www.arbitrobancariofinanziario.it/decisioni/index.html>; Coll. Roma, 15.10.2010, n. 1111 su <https://www.arbitrobancariofinanziario.it/decisioni/index.html>)

³⁸ Cass., 07.05.1992, n. 5421 su <https://plusplus24diritto.ilsole24ore.com/>

³⁹ Cass., 18.03.2010, n. 6624 su <https://plusplus24diritto.ilsole24ore.com/>

⁴⁰ In questo senso vedasi Cass., 12.05.2021, n. 12573 su <http://www.italgiure.giustizia.it/sncass/>

della responsabilità da trattamento dei dati ai sensi dell'art. 31, d.lgs. n. 196/2003, con la conseguenza che veniva altresì considerato il rinvio operato dall'art. 15, d.lgs. n. 196/2003 al regime delle attività pericolose ex art. 2050 c.c.⁴¹.

2.2 La novella *post* PSD2 e l'operato dell'Arbitro Bancario Finanziario.

Tali impostazioni ermeneutiche sono state, poi, arricchite in seguito alle novità introdotte dalla Direttiva PSD2, nonché dalla maggior rilevanza acquisita da un ulteriore *player*, l'Arbitro Bancario Finanziario⁴².

Attore che, oltre ad aver accolto quell'impostazione basata sulla responsabilità professionale qualificata⁴³ – ex art. 1176, co. 2, c.c. – ha fatto propria anche quella giurisprudenza di legittimità che, con specifico riferimento ai servizi e strumenti che si avvalgono di mezzi meccanici o elettronici (compresi i servizi di pagamento), ha chiarito come l'istituto bancario non possa non adottare misure idonee a garantire la sicurezza del servizio stesso, attesa la natura tecnica della diligenza posta a suo carico, da valutarsi tenendo conto dei rischi tipici della sfera professionale di riferimento⁴⁴.

Tuttavia, va precisato come l'operato ermeneutico dell'Arbitro sia differente in quanto, da un lato è giunto a postulare persino un dovere di monitoraggio delle operazioni di pagamento svolte dai propri utenti e a ricomprenderla nel perimetro della diligenza del buon banchiere⁴⁵ mentre, dall'altro lato, richiama

⁴¹ Trib. Palermo, 12.01.2010, n. 81 su <https://plusplus24diritto.ilsole24ore.com/>, recentemente ripresa in Cass., 12.04.2018, n. 9158 su <http://www.italgiure.giustizia.it/sncass/>. Nello stesso senso ma con considerazioni pure sull'operatività del disposto ex art. 1176 c.c. vedasi Trib. Siracusa, 15 marzo 2012 su <https://plusplus24diritto.ilsole24ore.com/>

⁴² Vero è che l'Arbitro Bancario Finanziario (ABF) è stato istituito nel 2009 in attuazione dell'articolo 128-bis del Testo unico bancario (TUB), introdotto dalla legge sul risparmio (legge n. 262/2005). Ma è pure vero che ha acquisito rilevanza solo con il trascorrere del tempo, iniziando con un "carico" di 3.409 ricorsi presentati nel primo anno di operatività (cfr. BANCA D'ITALIA (a cura della), *Relazione sull'attività dell'Arbitro Bancario Finanziario*, n. 1, 2010) per arrivare ai 13.575 ricorsi del 2015 e ai 30.918 ricorsi nel 2020 (vedasi la *Relazione sull'attività dell'Arbitro Bancario Finanziario* del 2015 e la si confronti anche con quella del 2020).

⁴³ Cfr. Coll. Coord., 26.10.2012, n. 3498, che richiama anche Coll. Roma, 15.10.2010, n. 1111, entrambe su <https://www.arbitrobancariofinanziario.it/decisioni/index.html>. Nello stesso senso Coll. Roma, 17.06.2010, n. 544 e Coll. Napoli, 10.09.2019, n. 21064 – Rel. GATT, su <https://www.arbitrobancariofinanziario.it/decisioni/index.html>

⁴⁴ Cass., 12.06.2007 n. 13777, su <https://plusplus24diritto.ilsole24ore.com/>; nello stesso senso anche Cass., 24.09.2009, n. 20543 su <https://plusplus24diritto.ilsole24ore.com/>, mentre per la giurisprudenza merito vedasi Trib. Parma, 06.09.2018, n. 1268 su <https://plusplus24diritto.ilsole24ore.com/>, Trib. Verona, 02.10.2012 su <https://plusplus24diritto.ilsole24ore.com/>.

⁴⁵ Coll. Napoli, 14.01.2013, n. 311 su <https://www.arbitrobancariofinanziario.it/decisioni/index.html>; vedasi anche Coll. Napoli, 28.11.2018, n. 25152 – Rel. GATT su <https://www.arbitrobancariofinanziario.it/decisioni/index.html>, dove è stigmatizzata la condotta dell'intermediario per aver mancato in una attività che rientra chiaramente nel monitoraggio delle operazioni degli utenti, in quanto «*Nel caso di specie il Collegio, pur ritenendo sussistere detta serie univoca e concordante di elementi atti a dimostrare un contegno colposo da parte del ricorrente - in ragione del fatto che le operazioni sono avvenute a non rilevante distanza di tempo dal furto dello strumento di pagamento - circostanza che lascia presumere la conservazione dei codici PIN unitamente alla carta stessa (Coll. Napoli, n. 11185/2016) - non può non rilevare altresì l'allegazione di 13 tentativi non andati a buon fine, nell'arco della medesima giornata e a distanza ravvicinata l'uno dall'altro. Elemento questo che induce a ritenere anche l'intermediario corresponsabile dell'evento dannoso ai sensi dell'art. 1227 c.c. Peraltro, anche la circostanza che i sette prelievi disconosciuti si siano susseguiti tra le 11:58 e le 12:59, vale a dire nell'arco temporale di circa un'ora nel medesimo giorno, rappresenta un elemento idoneo a distribuire parte della responsabilità alla negligenza dell'intermediario.*». All'interno dell'obbligo di monitoraggio (ma con più stretta connessione alla corretta esecuzione del contratto) si può ricondurre anche l'ipotesi dell'intermediario che consenta un uso della carta oltre i limiti di importo pattuiti (Coll. Napoli, 14.05.2019, n. 12125 – Rel. GATT su

ampiamente la disciplina settoriale predisposta con il d.lgs. n. 11/2010.

Per cui, se la giurisprudenza ordinaria tende ad applicare le norme codicistiche, i Collegi arbitrali fondano le loro decisioni soprattutto sul disposto del d.lgs. n. 11/2010 e sviluppano gli orientamenti già affrontati dai loro "collegi" magistrati.

Anzi, si può ben dire che i membri dei Collegi arbitrali affrontino con maggior severità i casi di lamentata negligenza in capo ai *provider* di servizi di pagamento.

Infatti, se applicando i parametri della responsabilità professionale ex artt. 1176, co. 2 e 2050 c.c., si giunge a chiedere all'intermediario una prova liberatoria particolarmente approfondita, si ha comunque un regime differente rispetto a quello delineato dagli artt. 10, 11 e 12, d.lgs. n. 11/2010, i quali, tra l'altro, paiono configurare una fattispecie di responsabilità oggettiva frequente in ambito bancario⁴⁶, che caratterizza proprio gli orientamenti della giurisprudenza arbitrale⁴⁷.

È così che se la prova richiesta in tema di responsabilità professionale attiene alla dimostrazione di aver adottato tutte le misure necessarie e idonee a qualificare concretamente la propria diligenza come rientrante nell'art. 1176, co. 2, c.c., a questa si aggiunge la necessità di provare, alternativamente, la colpa grave, il dolo ovvero l'intento fraudolento del titolare dello strumento di

<https://www.arbitrobancariofinanziario.it/decisioni/index.html>), in quanto per potersi avere un "blocco" di simili operazioni è necessario monitorare le stesse.

⁴⁶ M. C. PAGLIETTI, *Questioni in materia di prova nei casi di pagamenti non autorizzati*, in *Innovazione e regole nei pagamenti digitali – Il bilanciamento degli interessi nella PSD2*, a cura di M. C. PAGLIETTI e M. I. VANGELISTI, Roma TrE-PRESS, 2020, p. 49, dove si legge «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, coesivamente, far gravare il costo degli incidenti), è il cuore delle disposizioni e delle scelte politiche in materia, che, nei vari ordinamenti, propongono un'allocatione articolata delle perdite subite, risentendo della maggiore propensione ad optare per la soluzione della responsabilità oggettiva limitata laddove l'attività bancaria venga ascritta alle attività pericolose.»

⁴⁷ Posizione, tra l'altro, che trova numerosi echi anche nella giurisprudenza di legittimità in tema di contratti bancari, tant'è vero che, per esempio, in Cass., 19.07.2012, n. 12448 su <https://plusplus24diritto.ilsole24ore.com/>, il collegio giudicante si esprime nei seguenti termini testuali (richiamando numerose pronunce): «A norma dell'art. 2049, la società di intermediazione è responsabile degli illeciti commessi dal promotore finanziario anche a titolo oggettivo, cioè indipendentemente da comportamenti negligenti o colposi suoi propri, in relazione ai danni che l'investitore possa avere subito per avere fatto affidamento sull'esistenza del rapporto di preposizione. Ciò in considerazione dei rischi inerenti all'esercizio di attività finanziarie e delle gravi perdite a cui gli eventuali illeciti degli addetti possono esporre la clientela: rischi che la società di intermediazione è in grado di gestire, e danni contro i quali ha la possibilità di premunirsi (anche tramite l'assicurazione), in termini più efficaci, più razionali e meno costosi, che non il singolo investitore. Trattasi dei noti principi da tempo elaborati dalla dottrina in tema di responsabilità per rischio di impresa, che nell'ambito delle attività finanziarie trovano particolari ragioni per essere riaffermati, e che in questo campo la giurisprudenza di legittimità ha effettivamente ribadito con rigore (cfr., proprio con riferimento ad un caso di indebita appropriazione del denaro dei clienti da parte del promotore finanziario, Cass. civ. Sez. 1, 24 luglio 2009 n. 17393: "Sussiste la responsabilità indiretta della banca nei confronti dei terzi per il comportamento illecito del promotore finanziario allorché, indipendentemente dall'esistenza di un rapporto di lavoro subordinato e dal carattere di continuità dell'incarico, l'attività del promotore sia stata agevolata o resa possibile dal suo inserimento nell'attività d'impresa (dalla sua presenza nella sede, dall'utilizzo della modulistica di pertinenza, dalla spendita del nome, ecc.), e sia stata realizzata nell'ambito e coerentemente alle finalità in vista delle quali l'incarico è stato conferito, in maniera tale da far apparire al terzo in buona fede che l'attività posta in essere per la consumazione dell'illecito rientrasse nell'ambito dell'incarico affidato dalla mandante". Vedi anche, fra le tante, Cass. civ. Sez. 1, 22 ottobre 2010 n. 21729; Cass. civ. Sez. 3, 25 gennaio 2011 n. 1741, che ha ravvisato la responsabilità in un caso in cui il promotore aveva provocato il danno svolgendo attività in conflitto di interessi con la società mandante, cioè vendendo i prodotti di altra società, per il solo fatto che l'illecito è stato compiuto nel quadro delle attività funzionali all'esercizio delle incombenze affidate al promotore. Per un caso analogo, con riferimento alla L. n. 1 del 1991, art. 5, Cass. civ. Sez. 3, 19 luglio 2002 n. 10580).»

pagamento⁴⁸ nell'ottica di una esclusione della propria responsabilità di tipo oggettivo.

E, invero, tale è l'unica conclusione cui si può giungere in tema di riparto dell'onere probatorio, giusto il disposto dell'art. 10, d.lgs. n. 11/2010, rubricato "*Prova di autenticazione ed esecuzione delle operazioni di pagamento*"⁴⁹, dove si prevede al comma 1 un onere probatorio ben inquadrabile nel solco della diligenza ex art. 1176, co. 2 c.c., cui si *aggiunge*, però, quello relativo alla prova della frode, del dolo o della colpa grave in capo all'utente disposto al comma 2, a chiusura della disposizione.

Per cui, è oramai pacifico come l'intermediario sia chiamato a provare tanto la propria diligenza quanto, almeno, la colpa grave dell'utente, dovendosi raggiungere entrambe le prove ai fini di una esclusione della propria responsabilità.

Tuttavia, nella consapevolezza che così procedendo si rischia di prospettare una quasi sistematica responsabilità del *provider* che fornisce il servizio di *home banking*, i Collegi territoriali⁵⁰ hanno evidenziato l'importanza di una analisi approfondita delle circostanze del singolo caso al fine di vagliare attentamente possibili profili di negligenza dell'utente⁵¹.

Pertanto, se può sostenersi la netta responsabilità del *provider* che trascuri l'adozione dei più avanzati accorgimenti tecnici di prevenzione in spregio all'obbligo di diligenza⁵², la medesima responsabilità potrebbe essere esclusa, in tutto o quantomeno in parte, nell'ipotesi in cui il cliente, debitamente informato circa l'aggiornamento dei presidi di sicurezza (quale è, per esempio, un sistema di generazione e invio di codici *One Time Password*), ometta di avvalersene, venendo meno ai propri personali obblighi di custodia.

⁴⁸ In tal senso, successivamente alla novella del d.lgs. n. 11/2010, va chiarito come vi sia una vera e propria unanimità nella giurisprudenza degli Ermellini e in quella dell'ABF (cfr. Cass., 26.05.2020, n. 9721, con nota di G. SPATARO, *Bancomat: prelievi abusivi da parte di terzi e riparto di responsabilità tra banca e correntista*, su www.dirittobancario.it, del 13 ottobre 2020; Cass., 03.02.2017, n. 2950 su <http://www.italgiure.giustizia.it/sncass/>; Coll. Coord., 26.10.2012 n. 3498, *cit.*), pur permanendo un maggior ricorso dell'ABF ai suddetti dati normativi.

⁴⁹ « 1. Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti.

1-bis. Se l'operazione di pagamento è disposta mediante un prestatore di servizi di disposizione di ordine di pagamento, questi ha l'onere di provare che, nell'ambito delle proprie competenze, l'operazione di pagamento è stata autenticata, correttamente registrata e non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti connessi al servizio di disposizione di ordine di pagamento prestato.

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

⁵⁰ Coll. Milano, 25.07.2012, n. 2594 e Coll. Napoli, 03.04.2013, n. 1802 su <https://www.arbitrobancariofinanziario.it/decisioni/index.html>.

⁵¹ Per esempio, in Coll. Napoli, 15.05.2019 n. 12269 – Rel. GATT su <https://www.arbitrobancariofinanziario.it/decisioni/index.html> è stata affrontata una ipotesi di *phone hijacking*, dove si è avuto il rigetto del ricorso per carenza probatoria da parte della ricorrente, la quale non ha dimostrato la presenza di un *man in the middle*

⁵² Coll. Napoli., 05.11.2019 n. 24101 su <https://www.arbitrobancariofinanziario.it/decisioni/index.html>

E, proprio in tal senso, gli Arbitri hanno dato vita a differenti filoni interpretativi in merito alla valutazione della condotta dell'utente, che qui non saranno illustrati⁵³.

3. La sostanziale inefficacia del sistema di tutele.

Come si è visto, la *ratio* complessiva della normativa settoriale in tema di strumenti di pagamento e di operazioni di acquisto su base elettronica è basata su due elementi principali⁵⁴:

- favorire la diffusione di tali modalità di pagamento alternative al classico contante fornendo la massima sicurezza dei sistemi informatici;
- ottenere la fiducia degli utenti.

Ciononostante, tale obiettivo è perseguito operando un bilanciamento di interessi molto particolare, caratterizzato soprattutto dalla previsione di obblighi e responsabilità che, alla prova dei fatti, ricadono quasi unicamente sugli intermediari, sbilanciando l'impianto normativo stesso a favore del consumatore, tradizionalmente considerato la parte debole nei rapporti contrattuali di tipo *business to consumer* (B2C).

Tale sbilanciamento, tra l'altro, è alquanto "rafforzato" dalla giurisprudenza predominante in materia di contratti bancari e preesistente rispetto alle ultime novelle operate nei confronti del d.lgs. n. 11/2010.

Però, non può dirsi che una simile disciplina, così *astrattamente* favorevole verso l'utente dei servizi di pagamento, abbia sortito l'effetto sperato, dal momento che la fiducia dei consumatori negli strumenti di pagamento elettronici è effettivamente aumentata in tempi recenti, ma certamente non in conseguenza delle larghe tutele previste per gli stessi all'interno del d.lgs. n. 11/2010, quanto, piuttosto, in considerazione dei vantaggi derivanti dal cd. "cashback di Stato" avviato nell'ambito del "Piano Italia Cashless", previsto dalla Legge di Bilancio 2020 (art. 1, co. 288 - 290, l. n. 160/2019) e dal Decreto del Ministero dell'Economia e delle Finanze n. 156 del 24 novembre 2020, unitamente alle esigenze derivanti dal distanziamento sociale disposto a causa della pandemia.

⁵³ Comunque, valga quanto segue ai fini di un approfondimento. Alcuni degli orientamenti risultano essere quali più rispondenti alla *ratio* e alla lettera della norma e tendenti all'esclusione di automatismi in sede probatoria che ribaltino il rapporto di *favor* previsto dalla norma per il titolare dello strumento di pagamento (cfr. Coll. Napoli, 08.10.2012 n. 3192 su <https://www.arbitrobancariofinanziario.it/decisioni/index.html>, che si esprime nei seguenti termini: «gli orientamenti di questo Collegio sono nel senso che "l'adozione da parte dell'intermediario di valide ed efficaci misure di tutela degli interessi dell'utilizzatore, se non può ritenersi valere ad escludere senz'altro la sua responsabilità e, di riflesso, a dimostrare che l'intromissione fraudolenta nel sistema di protezione da lui predisposta sia imputabile alla grave (in rapporto alla massima sicurezza offerta dall'intermediario) negligenza o imprudenza dell'utilizzatore (per non avere custodito adeguatamente le proprie credenziali: art. 12, n. 4), vale sicuramente ad elevare in modo significativo il livello delle allegazioni richieste al cliente, al fine di rendere adeguatamente verosimigliante il carattere fraudolento dell'operazione" (così nella decisione n. 1334/1912), venendo, in difetto, altrimenti sancito – a fronte di soluzioni tecnologicamente avanzate – una inammissibile sottrazione del prestatore dei servizi di pagamento a ogni forma di responsabilità». In senso conforme all'orientamento degli arbitri partenopei si veda anche il Collegio di Roma con varie decisioni (*ex multis*, 28.06.2012, n. 2264, nonché 30.07.2012, n. 2660) e altri di senso opposto (vedasi Coll. Milano, 17.02.2012 n. 528, di recente superato per accogliere l'impostazione del Collegio di Napoli), tutti su <https://www.arbitrobancariofinanziario.it/decisioni/index.html>

⁵⁴ M. C. PAGLIETTI, *Questioni in materia di prova nei casi di pagamenti non autorizzati*, cit., p. 44

Al tempo stesso, non solo le disposizioni del d.lgs. n. 11/2010 non sembrano garantire adeguate tutele effettive all'utente del servizio di pagamento – ciò in quanto una cosa è ottenere un rimborso, magari parziale, del danaro trafugato e ben altra cosa è usufruire di un sistema che riconosce e blocca efficacemente le frodi impedendole *in toto* – ma, in ragione dei tempi comunque relativamente (e fisiologicamente) lunghi per far valere le proprie ragioni, ad esempio in sede arbitrale (generalmente previo reclamo al proprio *provider*), l'impianto complessivo delle tutele risulta inadeguato a perseguire il fine di ottenere la *fiducia* dell'utente stesso⁵⁵.

Poi, siffatta modalità di pagamento ovviamente non incontra, lato tutele, il favore degli intermediari per gli oneri probatori che pone in capo agli stessi per dimostrare di aver adempiuto ai propri obblighi di diligenza "bancaria" ma, soprattutto, è osteggiata dagli stessi esercenti (tanto dei negozi fisici che degli *store online*) per via degli *step* di autenticazione che richiede per limitare il rischio di transazioni non autorizzate⁵⁶, che rendono farraginose le operazioni di pagamento.

Ne consegue la necessità di riflettere e verificare se non sia il caso, piuttosto, di spostare il *focus* complessivo, dagli strumenti di tutela ordinari previsti per il titolare dello strumento di pagamento a un ripensamento dell'architettura internazionale (e interna, dal momento che sono simili) dei sistemi di pagamento digitali in sé (in considerazione del fatto che buona parte dei fondi distratti dai conti correnti italiani vengono dirottati in altri Paesi).

Infatti, è oramai pacifico che, pur attuando tutte le tutele volte a prevenire le frodi e pur ponendo un obbligo di rimborso a carico dei *provider*, comunque queste non sono scelte idonee a ridurre concretamente il rischio di operazioni non riconosciute derivante dalla diffusione di strumenti di pagamento digitali, le quali stanno, anzi, aumentando.

Ciò in quanto, da un lato corrisponde al vero che sono migliorate le modalità di autenticazione dell'utente ma, dall'altro, è pur vero che l'architettura di sistema su cui "viaggiano" le transazioni è complessivamente rimasta la medesima dalla seconda metà dello scorso secolo⁵⁷, senza che si siano avuti aggiornamenti sufficientemente radicali da rendere obsolete numerose modalità di captazione dei dati di accesso le quali, *de facto*, sono rimaste le stesse.

⁵⁵ Per esempio, in un caso seguito dal Collegio di Napoli (Coll. Napoli, 25.03.2021 n. 8323, su <https://www.arbitrobancariofinanziario.it/decisioni/index.html>) la frode si è verificata il 18 febbraio 2020 e, tra reclamo all'intermediario, presentazione del ricorso, calendarizzazione e adunanza del Collegio, la decisione – di rigetto del ricorso, tra l'altro – è arrivata più di un anno dopo. Tempi parimenti lunghi si possono riscontrare in altri Collegi. Vedasi Coll. Milano, 01.03.2021 n. 5357 su <https://www.arbitrobancariofinanziario.it/decisioni/index.html>, dove non risulta, dalla lettura della decisione, che vi sia stata una previa interlocuzione tra utente e intermediario e comunque ci sono voluti diversi mesi per arrivare a una decisione. Tempi pari a quelli del Collegio partenopeo (ossia un anno circa a partire dalla data della frode) si hanno anche in quello capitolino in presenza di un previo reclamo al proprio intermediario, come si evince da Coll. Roma, 01.03.2021 n. 5436 su <https://www.arbitrobancariofinanziario.it/decisioni/index.html>.

⁵⁶ A. S., *E-commerce, transazioni più sicure grazie all'analisi in real time, su [www.pagamentidigitali.it/ecommerce/e-commerce-transazioni-piu-sicure-grazie-allanalisi-in-real-time/#:~:text=Grazie%20ad%20%22Advice%22%2C%20il,frodi%20con%20%22Guaranteed%20Payments%22](http://www.pagamentidigitali.it/ecommerce/e-commerce-transazioni-piu-sicure-grazie-allanalisi-in-real-time/#:~:text=Grazie%20ad%20%22Advice%22%2C%20il,frodi%20con%20%22Guaranteed%20Payments%22;)*.

⁵⁷ Il sistema *SWIFT* per le transazioni internazionali è nato nel corso degli anni Settanta ad opera della Society for Worldwide Interbank Financial Telecommunication

3.1. Le statistiche sull'andamento delle transazioni fraudolente.

Infatti, ponendo ora l'attenzione sulle dimensioni del fenomeno stesso – ci si riporta a un report annualmente prodotto dalla Nilson Report⁵⁸, rivista specializzata nell'ambito dei sistemi di pagamento – si nota quanto sia vasto lo stesso. Infatti, le frodi su carte di pagamento a livello globale per emittenti, esercenti e *acquirers*, utilizzate per acquisti o prelievi di contante, hanno raggiunto nel 2019 i 28,65 miliardi di dollari, con un aumento del 2,9% rispetto all'anno precedente, da rapportare a un volume di transazioni a mezzo pagamenti elettronici pari a oltre 42 trilioni di dollari, pure aumentato del 4,2% rispetto al 2018.

L'anno precedente, invece, le frodi su carte di pagamento a livello globale hanno avuto una crescita pari a oltre il 16% per un valore complessivo di 27,85 miliardi di dollari, rapportata a un totale di transazioni complessive pari a oltre 40 trilioni di dollari, in aumento del 17,7% rispetto al 2017⁵⁹.

Quindi, l'incidenza complessiva delle frodi, espressa in termini percentuali rispetto al totale delle operazioni svolte, è costantemente in diminuzione, come si evince dai dati illustrati nella tabella qui allegata (vedasi la figura che segue – terza colonna verso destra). Ciononostante, secondo le proiezioni statistiche si prevede una recrudescenza delle stesse frodi proprio in questi due anni caratterizzati dalla pandemia.

| YEAR | Total Volume | Fraud | Cents per |
|------|--------------|----------|--------------|
| | TRILLIONS | BILLIONS | \$100 VOLUME |
| 2015 | \$31.310 | \$21.84 | 6.97¢ |
| 2016 | \$31.878 | \$22.80 | 7.15¢ |
| 2017 | \$34.472 | \$23.97 | 6.95¢ |
| 2018 | \$40.582 | \$27.85 | 6.86¢ |
| 2019 | \$42.274 | \$28.65 | 6.78¢ |
| 2020 | \$42.241 | \$30.93 | 7.32¢ |
| 2021 | \$44.829 | \$32.04 | 7.14¢ |
| 2022 | \$47.627 | \$31.52 | 6.62¢ |
| 2023 | \$50.375 | \$32.96 | 6.54¢ |
| 2024 | \$53.245 | \$34.40 | 6.46¢ |
| 2025 | \$56.182 | \$35.31 | 6.28¢ |
| 2026 | \$59.284 | \$36.93 | 6.23¢ |
| 2027 | \$62.614 | \$38.50 | 6.15¢ |
| 2028 | \$66.188 | \$40.05 | 6.05¢ |

© 2020 Nilson Report

60

Variazione del valore delle frodi con sistemi di pagamento elettronici nel mondo rapportato al valore complessivo delle transazioni.

⁵⁸ REDAZIONE, *Card Fraud Losses Worldwide*, in *Nilson Report*, n. 1187 del dicembre 2020, disponibile gratuitamente al link https://nilsonreport.com/content_promo.php?id_promo=16

⁵⁹ REDAZIONE, *Card Fraud Losses Reach \$27.85 Billion*, in *Nilson Report*, n. 1164 del novembre 2019, disponibile gratuitamente al link <https://nilsonreport.com/mention/407/1link/#>

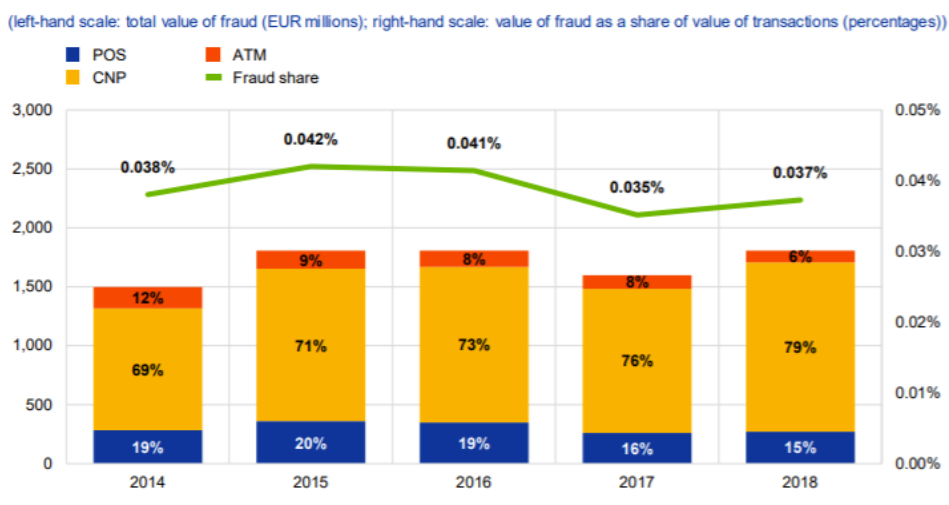
⁶⁰ REDAZIONE, *Card Fraud Losses Worldwide*, cit., p. 5

Concentrando lo sguardo sull'area SEPA, poi, si rinviene un simile trend di crescita delle frodi, forse anche più pronunciato, anche se i dati statistici analizzati nel *Sixth report on card fraud* della BCE sono limitati al 2018.

Per la precisione, se le transazioni totali hanno quasi raggiunto il valore di 5 trilioni di euro nel 2018 con una crescita del 6,5% rispetto al 2017, si è registrato un aumento assai più rilevante delle frodi, tanto in termini di valore assoluto (1,8 miliardi di euro) che in termini percentuali rispetto all'anno precedente (+13%), con una incidenza delle transazioni fraudolente sul totale che è tornata a crescere.

Chart 1a

Evolution of the total value of card fraud using cards issued within SEPA



Source: All reporting card payment service operators.

61

Variazione del valore delle frodi con sistemi di pagamento elettronici nell'area SEPA con indicazione dell'incidenza sul totale delle transazioni.

3.2 Una possibile evoluzione dei sistemi di pagamento attraverso IA e blockchain.

Da quanto finora delineato, si comprende come sia necessario intervenire a monte, ossia sull'architettura tecnica del sistema di pagamento, per poi modificare e adeguare anche il relativo substrato di previsioni giuridiche.

Una prima ipotesi di innovazione sarebbe l'applicazione della *blockchain* all'ambito dei sistemi di pagamento elettronici (che pure è il suo "ambiente" naturale, visto che è nata come mezzo di scambio delle criptovalute⁶²), soluzione che pare già tenuta in considerazione, tant'è vero che in una pubblicazione molto lungimirante della Cassa Depositi e Prestiti si analizza

⁶¹ BCE, *Sixth report on card fraud*, 2020, p. 8, disponibile al link <https://www.ecb.europa.eu/pub/pdf/cardfraud/ecb.cardfraudreport202008~521edb602b.en.pdf>

⁶² S. NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, disponibile al link https://www.uscc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf. Si noti che il nome dell'autore è uno pseudonimo che nasconde l'inventore della criptovaluta Bitcoin

proprio l'attuale sistema di pagamenti *cross border* basato su SWIFT⁶³ e si ipotizza la sua sostituzione con un sistema completamente nuovo, su base *blockchain*, che prevede perfino l'utilizzo di *digital asset* ai fini della gestione dei pagamenti stessi, in modo da rendere più certe e celeri le transazioni transfrontaliere operate da Piccole e Medie Imprese.

Ora, laddove dovesse essere sperimentata con successo nell'ambito della PMI, una architettura informatica simile ben si presterebbe ad essere adeguata e applicata su scala ben più vasta, ossia a livello *retail*⁶⁴, anche per assolvere non solo al monitoraggio antifrode ma anche per garantire il corretto funzionamento del sistema contro ipotesi quali quella del *double spending*⁶⁵.

La tecnologia a "registri distribuiti", tuttavia, non sarebbe idonea da sola a porre un freno alle transazioni fraudolente, laddove i sistemi di *autenticazione* degli utenti e quelli di *monitoraggio* delle operazioni dovessero rimanere sostanzialmente gli stessi.

E, invero, se l'autenticazione biometrica è già prevista, non può dirsi lo stesso per l'utilizzo di Intelligenze Artificiali quali sistemi di monitoraggio.

Anzi, potrebbe affermarsi che vi sia un divieto di essere sottoposti a decisioni automatizzate⁶⁶, la cui *ratio* è quella di garantire in ogni momento la possibilità di ottenere la modifica ovvero la disattivazione degli algoritmi impiegati in tal senso.

Tuttavia, sussistono delle eccezioni a tale divieto:

- l'ipotesi che l'utilizzo dell'IA sia necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
- l'utilizzo dell'IA sia autorizzato a livello europeo o nazionale, fatti salvi i diritti e le libertà fondamentali;
- l'utilizzo dell'IA sia fondato sul consenso dell'interessato.

Ebbene, per quanto concerne il caso del monitoraggio delle transazioni di un individuo (che già avviene, per la verità), va detto che anche ora, senza alcuna modifica normativa da effettuarsi, potrebbero sussistere, cumulativamente, i presupposti per l'applicazione delle IA al monitoraggio bancario.

⁶³ CDP-SIA-IBM, *Ipotesi di adozione della tecnologia blockchain in ambito finanziario*, su www.cdp.it/resources/cms/documents/White_paper_tecnologia_blockchain_CDP_SIA_IBM.pdf, p. 36 ss.

⁶⁴ Un progetto più *retail* è perseguito proprio a livello nazionale con il progetto *Spunta* di ABILab (link <https://www.abilab.it/aree-ricerca/blockchain-dlt/spunta-banca-dlt>), finalizzato a gestire i conti interbancari con una tecnologia *blockchain* condivisa in luogo della precedente, basata su registri bilaterali

⁶⁵ M. F. MONTEROSI, *Intelligenza artificiale e blockchain: implicazioni reciproche*, in *Intelligenza artificiale e diritto – come regolare un mondo nuovo*, a cura di A. D'ALOIA, Franco Angeli S.r.l., 2020, p. 480

⁶⁶ Cfr. Art. 22 GDPR – « 1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

2. Il paragrafo 1 non si applica nel caso in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
c) si basi sul consenso esplicito dell'interessato.

3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.»

Infatti, è chiaro che ricorrerebbe la prima eccezione, dal momento che tutti i contratti bancari fanno espresso riferimento al trattamento dei dati ai fini dell'esecuzione degli stessi.

Parimenti, essendovi una normativa che consente il trattamento dei dati dell'utente ai fini della prevenzione delle frodi, si rientrerebbe nel campo di applicazione della seconda eccezione⁶⁷.

In ultimo, sarebbe possibile soddisfare anche l'ultima eccezione in considerazione del fatto che, in sede di stipula dei contratti bancari, è oramai richiesto il consenso dell'interessato al fine del trattamento dei suoi dati⁶⁸.

Così ragionando e ricomprendendo il monitoraggio a mezzo IA nell'ambito del concetto di "trattamento automatizzato", è possibile ipotizzare che già a legislazione vigente si possano adottare le Intelligenze Artificiali nei processi di monitoraggio interno delle banche.

Rimane comunque, in una ottica *de iure condendo*, la necessità di adottare una apposita normativa, quantomeno a livello europeo, per regolamentare l'uso dell'IA in ambito bancario, non potendocisi affidare unicamente a un procedimento di ermeneusi, stante la sua inadeguatezza a fornire contorni più certi a scenari attualmente molto sfumati⁶⁹, con tutti i rischi del caso.

Tale necessità diventa ancor più impellente se si considerano i profili inerenti tanto alla soggettività giuridica di simili sistemi automatizzati quanto all'etica stessa, dovendosi *progettare* sistemi automatizzati così evoluti da soddisfare la necessità di un comportamento etico delle macchine.

Anzi, nel corso di una intervista alla Prof.ssa Gatt⁷⁰ quale direttore del *Research Centre of European Private Law* (ReCEPL) per la rivista *Diritto Mercato Tecnologia*⁷¹, alla domanda su quali possano essere i rischi di un

⁶⁷ Art. 29, d.lgs. n. 11/2010 - «1. I prestatori di servizi di pagamento e i gestori di sistemi di pagamento possono trattare dati personali ove ciò sia necessario a prevenire, individuare e indagare casi di frode nei pagamenti. La fornitura di informazioni a persone fisiche in merito al trattamento dei dati personali e ad altro trattamento ai fini del presente decreto avviene in conformità al decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni.

1-bis. I prestatori di servizi di pagamento hanno accesso, trattano e conservano i dati personali necessari alla prestazione dei propri servizi solo previo consenso esplicito dell'utente dei servizi di pagamento.»

⁶⁸ Vedasi, ad esempio, il contratto della Fineco Bank sopra descritto in relazione agli obblighi dell'utente, il quale è tenuto a prendere visione dell'Allegato A (informativa privacy) e a fornire il relativo consenso. Ovviamente, si rende necessaria una corretta informazione dello stesso, come si ribadisce in M. F. MONTEROSSO, *Intelligenza artificiale e blockchain: implicazioni reciproche*, cit., p. 485

⁶⁹ Infatti, si consideri quanto dice E. TROISI (cfr. *AI e GDPR: l'Automated Decision Making, la protezione dei dati e il diritto alla 'intelligibilità' dell'algoritmo*, in *European Journal of Privacy Law & Technologies*, Giappichelli, issue 1/2019) laddove scrive che «L'ADM è ammesso solo in presenza di quelle condizioni autorizzative per così dire "consensuali", idonee ad assicurare una più ampia consapevolezza dell'interessato, con la conseguenza che deve ritenersi illegittimo in tutti i casi in cui l'interessato non vi abbia acconsentito espressamente attraverso una propria consapevole manifestazione di volontà, o direttamente[1], o nell'ambito di un più complesso rapporto contrattuale, sul presupposto però, in quest'ultimo caso, che il trattamento automatizzato sia da considerarsi necessario[2] alla conclusione o all'esecuzione dell'accordo». Il problema è proprio capire quando ricorrano chiaramente le eccezioni previste dall'art. 29 GDPR, specialmente con riferimento a tecnologie *disruptive* come l'utilizzo della IA, a prescindere dal fatto che sia unita o meno ad altre tecnologie quali la *blockchain*.

⁷⁰ Docente ordinario presso l'Università Suor Orsola Benincasa di Napoli e titolare della Cattedra in Diritto delle Nuove Tecnologie

⁷¹ REDAZIONE, *Per un'Intelligenza Artificiale antropocentrica. Intervista a Lucilla Gatt*, 21 febbraio 2020, su www.dimt.it; nello stesso senso vedasi L. AULINO, *Intelligenza artificiale e giustizia tra nuove soggettività giuridiche e nuove problematiche etiche e deontologiche*, in *Intelligenza artificiale e diritto – come regolare un mondo nuovo*, a cura di A. D'ALOIA, Franco Angeli S.r.l., 2020, p. 229 ss. dove affronta la questione etica in relazione al comparto dell'amministrazione della giustizia. Ciononostante, trattasi di principi generali applicabili astrattamente a qualsiasi ambito la IA si trovi ad operare, ivi compreso anche quello bancario e della prevenzione delle frodi.

approccio normativo che non tenga conto dell'utente umano e dell'etica, si è avuta la seguente risposta:

«Questa recente esortazione del Parlamento europeo alla Commissione si pone in linea di continuità con almeno due risoluzioni del Parlamento medesimo, adottate l'una nel febbraio 2017 e l'altra nel febbraio 2019 dal titolo "European industrial policy on artificial intelligence and robotics". Già da tempo, infatti, il Parlamento sollecita la Commissione ad emanare regole mandatory in materia di AI. Allo stato, tuttavia, la Commissione, pur non ignorando affatto il tema dell'AI, non ha accolto completamente le indicazioni del Parlamento. Ha emanato, infatti, due comunicazioni in materia di AI nel 2018 e nel 2019. Quest'ultima si intitola "Building Trust in Human-Centric Artificial Intelligent" e si accompagna a due rilevanti atti non vincolanti della Commissione o, più esattamente, dell'High-Level Expert Group on AI (AI HLEG) costituito dalla Commissione medesima nel giugno del 2018. L'AI HLEG ha elaborato e pubblicato on line due deliverables denominati "Ethics Guidelines for Trustworthy AI" dell'aprile 2019 e "Policy and Investment Recommendations for Trustworthy AI" del giugno 2019. Si vede, dunque, come entrambi gli organi europei, e la Commissione in particolare, siano profondamente consapevoli della necessità di realizzare un quadro di regole per lo sviluppo di una AI antropocentrica nel senso di tutelante e potenziante l'essere umano in quanto tale. Questa consapevolezza, però, ha finora condotto verso l'elaborazione di raccomandazioni, comunicazioni, linee guida che, tra l'altro, si focalizzano sull'esigenza di fare delle scelte etiche e, tralasciano, comunque, in maniera più o meno evidente, di formulare regole a carattere cogente provviste di sanzione.»

Conclusioni.

Stante il panorama in rapido rinnovamento, specialmente dal lato dell'innovazione tecnologica, si pone la questione dell'aggiornamento delle disposizioni normative.

Per ironia della sorte, proprio la corrente disciplina già è stata il prodotto di un "inseguimento" della tecnologia in sé e ugualmente pare non aver sortito effetti.

A parere dello scrivente, forse, l'errore – o, meglio, l'imprudenza – commessa in sede di stesura della PSD2 e della normativa ad essa connessa è stato quello di focalizzare l'intero comparto delle misure di sicurezza unicamente sulla fase dell'autenticazione del pagatore, trascurando il complesso delle misure di *raccolta, conservazione e analisi* dei dati delle transazioni, che ricadono in capo alle banche.

Infatti, si potrebbe quasi dire che si è posto pressoché interamente a carico dell'utente l'obbligo di tutelare in via preventiva i propri fondi, mentre le conseguenze della mancata custodia delle credenziali tendono a ricadere, per converso, sull'intermediario stesso, spesso e volentieri tacciato di mancata *vigilanza*, di mancato *monitoraggio*, di mancata *prevenzione*⁷².

⁷² Per tutte valga Coll. Napoli, 14.01.2013 n. 311 su <https://www.arbitrobancariofinanziario.it/decisioni/index.html>, dove si legge testualmente: «La condotta dell'intermediario appare, inoltre, priva della necessaria diligenza anche con riguardo ad ulteriori e connessi obblighi derivanti dalla propria posizione contrattuale, con particolare riguardo al costante e scrupoloso

Eppure, per come è pensato attualmente, proprio il sistema di autenticazione e di pagamento in sé non è idoneo a consentire un monitoraggio che vada oltre l'analisi basica dei dati raccolti, atteso che consente (in tal modo evitando di gravare con ulteriori costi sull'intermediario) unicamente la verifica della mera regolarità dell'accesso e della disposizione dell'ordine di pagamento. Né si potrebbe introdurre una IA a legislazione vigente e senza cambiare l'architettura dei sistemi di pagamento, giacché la base normativa è, interpretativamente parlando, troppo confusa, mentre l'attuale sistema di pagamento non è in grado di garantire una piena integrità dei dati, quantomeno non al livello della *blockchain*.

Per contro, una novella che da un lato apra all'utilizzo della *blockchain* e della IA nelle transazioni *retail*, ponendo però in contemporanea l'obbligo – per il *provider* – di adottare tali innovazioni, unitamente alla previsione di un obbligo – questo in capo al titolare di strumenti di pagamento – di utilizzo di dati biometrici per aversi una SCA adeguata a proteggere transazioni di una certa importanza (altrimenti si avrebbe una grande falla nel sistema di monitoraggio delle operazioni), potrebbe costituire una formula idonea a garantire una vera prevenzione contro le transazioni fraudolente.

Inoltre, si avrebbero due ulteriori effetti:

- da una parte, vi sarebbe l'abbandono di una fattispecie di responsabilità oggettiva, in considerazione del fatto che con *blockchain* e IA l'intermediario ben potrebbe evitare transazioni fraudolente, senza che possa limitarsi ad allegare la mera regolarità formale delle stesse. Infatti, tecniche quali il *phishing* e similari sarebbero efficaci solo in caso di mancata adozione di queste tecnologie, con la conseguenza che sarebbe possibile ricercare profili di responsabilità soggettiva nella condotta dell'intermediario stesso il quale non abbia adottato o compiutamente/correttamente implementato tali sistemi di sicurezza;
- dall'altra parte, un impianto che prevenga le frodi anziché fornire una tutela *ex post* ha dalla sua anche il non trascurabile vantaggio di costituire uno strumento di deflazione del contenzioso davanti agli Arbitri e ai Magistrati ordinari, dal momento che assai poche sarebbero le frodi che riuscirebbero ad essere condotte a termine, dovendo superare uno "sbarramento" assai più complesso di quello che ora violano con relativa facilità.

In tal modo, da un lato si avrebbe un miglior riparto di responsabilità per i vari soggetti chiamati a operare nel caso di una transazione e, dall'altro, si otterrebbe una tutela effettiva e rapida a vantaggio dell'utente.

monitoraggio delle transazioni on line da parte dei correntisti (già più volte richiamato da questo Collegio; cfr., per tutte, dec. n. 1477/2011); tale dovere, infatti, consente all'intermediario di verificare il regolare andamento delle operazioni e di segnalare quelle che appaiono anomale, come è avvenuto nel caso di specie, tenuto conto che – per i bonifici di cui si discute – si tratta di operazioni effettuate in un ristretto lasso temporale e nei confronti del medesimo beneficiario, ponendosi in contraddizione con la usuale operatività del conto del ricorrente. A dimostrazione della bontà dell'assunto, va presa in considerazione la condotta tenuta dal resistente nell'immediatezza della denuncia del medesimo fatto alle autorità, in seguito alla quale ha prontamente bloccato l'ultimo dei tre bonifici contestati. La condotta tenuta, dunque, deve considerarsi contraria alla diligenza professionale, di cui all'art. 1218 cod.civ. letto in combinazione con l'art. 1176, comma 2, cod.civ., come specificamente descritta anche dalla giurisprudenza, con espresso riferimento agli intermediari bancari (cfr., tra le tante, Cass. civ., sent. nn. 20543/2009; 13777/2007, 11382/2002; 3389/2003; 6756/2001).»