ISSN 2529-9824

Artigo de Investigação

O enquadramento da responsabilidade bancária pelos riscos inerentes à utilização do sistema de homebanking

The framework of bank liability for the risks inherent in the use of the homebanking system

Maria Emília Teixeira[1]: Universidade Portucalense, Portugal.
emiliat@upt.pt
Maria Manuela Magalhães: Universidade Portucalense, Portugal.
mmdmms@upt.pt

Data de receção: 11/06/2024

Data de aceitação: 12/09/2024

Data de publicação: 12/02/2025

Como citar o artigo:

Teixeira, M. E., & Magalhães, M. M. (2025). O enquadramento da responsabilidade bancária pelos riscos inerentes à utilização do sistema de homebanking. [The framework of bank liability for the risks inherent in the use of the homebanking system]. *European Public & Social Innovation Review*, 10, 1-17. https://doi.org/10.31637/epsir-2025-1448

Resumo:
Introdução: No presente artigo pretendemos efetuar um enquadramento jurídico e legal da utilização do *homebanking* como sistema de pagamento, abordando os principais riscos da sua utilização e de que forma poderá o banco ser responsabilizado pelos danos resultantes para o cliente bancário. **Metodologia**: A metodologia utilizada no presente artigo científico combina as abordagens descritiva e explicativa, utilizando como métodos de pesquisa a revisão bibliográfica, a análise documental e a análise jurisprudencial. **Resultados:** Para aferir dos riscos de utilização do sistema de *homebanking* e sobre quem recairá a responsabilidade pelos prejuízos provenientes desta utilização, iremos analisar alguns casos já tratados jurisprudencialmente e identificar os riscos inerentes ao uso deste sistema de pagamento. **Discussão**: Uma vez identificados os riscos, pretendemos discutir e comparar as obrigações a que a entidade bancária e o cliente bancário se encontram adstritos e qual o fundamento para a respetiva responsabilização. **Conclusões**: Com o presente artigo pretendemos definir critérios objetivos que permitam balizar os limites da responsabilidade de cada uma das partes pela utilização do sistema de pagamento *homebanking*.

[1] **Maria Emília Teixeira:** Universidade Portucalense (Portugal).

Palavras-Chave: sistema financeiro; homebanking; responsabilidade bancária; Serviços financeiros; Serviços de pagamento; phishing; pharming; E-banking.

Abstract:
Introduction: This article aims to provide a legal framework for using homebanking as a payment system, addressing the main risks of its use and how the bank can be held liable for the resulting damage to the banking customer. **Methodology:** The methodology used in this scientific article combines descriptive and explanatory approaches, using bibliographical review, documentary analysis and jurisprudential analysis as research methods. **Results:** In order to assess the risks of using the homebanking system and who will be responsible for the losses arising from this use, we will analyze some cases already dealt with in case law and identify the risks inherent in the use of this payment system. **Discussion:** Once the risks have been identified, we intend to discuss and compare the obligations to which the bank and the bank customer are bound and the grounds for their respective liability. **Conclusions:** The aim of this article is to define objective criteria that allow us to define the limits of each party's liability for using the home banking payment system.

Keywords: financial system; homebanking; bank liability; financial services; payment services; phishing; pharming; E-banking.

1. Introdução

A Constituição da República Portuguesa consagra no seu art. 101.º que a lei deve estruturar o sistema financeiro de forma a garantir a formação, a captação e a segurança das poupanças dos cidadãos, bem como deve regular a aplicação dos meios financeiros de forma a prover ao desenvolvimento económico e social, o que assume particular relevância dado que não é apenas uma questão técnica, mas também uma questão de determinação constitucional e que, como tal, deve ser observada quer pela legislação, quer pelas políticas públicas a desenvolver neste âmbito. O advento da internet propiciou avanços significativos em todas as áreas e o sector bancário não foi alheio às potencialidades que a mesma proporcionou para o exercício da atividade bancária e modo de relacionamento da Banca com os seus clientes. A Banca tradicional, associada a burocracia, procedimentos morosos e dispendiosos, cedeu à era da digitalização e desmaterialização dos serviços bancários. Este fenómeno, transversal a toda a sociedade, muitas vezes apelidado de *paperless society*, fez emergir a Banca *online* ou o *e-banking*[2]. Assiste-se à era da descentralização dos serviços prestados pela Banca.

No que concerne à segurança financeira e à proteção dos dados e transações financeiras dos clientes, torna-se imperativo o desenvolvimento de sistemas que garantam a o acesso rápido aos serviços financeiros, de forma segura e capazes de transmitir fiabilidade no seu uso, não comprometendo a confiança dos seus utilizadores. A segurança cibernética é atualmente uma das principais preocupações dos prestadores de serviços de pagamento, onde se incluem as instituições de crédito, considerando a crescente ameaça de crimes financeiros *online*. Sabendo-se que o sistema de *homebanking* se traduz numa ferramenta que não está isenta de riscos, desde logo porque a sua utilização potencia e está suscetível à ocorrência de fraudes e de outros crimes cibernéticos, sendo vulnerável a ataques de *crackers* que visam o furto de dados e adulterar as ordens de transações financeiras, com o consequente desvio de fundos, pretendemos analisar no presente estudo quem e em que moldes responderá por este risco informático. Na verdade, os sistemas informáticos, que por mais seguros que sejam estarão sempre vulneráveis a novas técnicas de fraude, cada vez mais sofisticadas, propiciando a

[2] Neste sentido, veja-se Moura, 2013, p. 3.

ocorrência de danos, para os quais nenhuma das partes pode até ter contribuido e que derivam de ataques de terceiros, externos ao contrato de *homebanking* celebrado entre o prestador de serviços de pagamento e o utilizador, e cuja identidade a maioria das vezes é impossível de determinar, torna-se vital definir com clareza as regras de imputação de responsabilidade civil aplicáveis.

Tendo em mente este propósito, analisaremos o enquadramento jurídico do contrato de *homebanking* e os regimes jurídicos aplicáveis ao prestador de serviços de pagamento, determinando quais as suas obrigações, por contraposição à análise das obrigações a que os utilizadores dos serviços se encontram adstritos. Impõe-se ainda que se faça uma análise dos tipos de ilícitos criminais mais comuns a que estarão sujeitos os utilizadores deste sistema de *homebanking*, como os fenómenos de phishing e pharming, determinando quando se considera que o utilizador é ou não o responsável pelos danos do ataque de que foi vítima, tendo em consideração se o mesmo atuou com negligência grosseira ou não. Começaremos então por efetuar uma breve descrição sobre a natureza e estrutura contratual do contrato de *homebanking*, seguido do seu atual enquadramento legal em Portugal, decorrente da transposição de Diretivas Europeias e Regulamentos, identificando as principais vantagens da utilização do sistema *homebanking* quer para os prestadores de serviços de pagamento quer para os seus utilizadores. Identificar-se-á igualmente quais os principais riscos a que tal sistema de pagamento se encontra sujeito, aludindo-se a casos concretos e respetivo tratamento jurisprudencial. Após tal análise, tentar-se-á contribuir para fornecer uma visão mais transparente sobre quais as regras que definem o responsável civilmente pelos prejuízos provenientes de uma incorreta utilização ou de fraude perpetrada por terceiros, designadamente quando a identidade destes terceiros não seja possível apurar.

2. Metodologia

A metodologia utilizada no presente artigo científico combina as abordagens descritiva e explicativa, utilizando como métodos de pesquisa a revisão bibliográfica, a análise documental e a análise jurisprudencial. A pesquisa descritiva tem como objetivo identificar os possíveis riscos a que a utilização do sistema de pagamento através de *homebanking* se encontra vulnerável, proporcionando uma compreensão o problema da responsabilização pelos prejuízos daí provenientes. Este tipo de pesquisa permitirá desde logo expor o principal problema com que a jurisprudência atual se depara que é a imputação da responsabilidade civil e seu enquadramento legal, bem como viabilizará a correta subsunção jurídica de cada uma das situações possíveis, de acordo com as doutrinas e teorias jurídicas relevantes aplicáveis. A revisão bibliográfica, útil à fundamentação da pesquisa para proporcionar uma base teórica sólida, constitui a primeira etapa metodológica, onde se pretende expor o atual estado da arte sobre o tema, contextualizando o presente tema face às discussões atuais e assegurando que as perspetivas relevantes pré-existentes sejam consideradas.

A análise documental utilizada no presente artigo reveste-se de extrema utilidade uma vez que pretender-se-á alcançar conclusões cuja validade jurídica assente em fundamentos legais sólidos e vigentes, pelo que efetuaremos um enquadramento jurídico-legal com base nos atuais diplomas legais, o que será fundamental para compreender o regime jurídico que norteia o tema em análise. Complementarmente, efetuaremos uma análise jurisprudencial de forma a percecionar-se, em concreto, como os tribunais interpretam a atual legislação e como procedem à sua aplicação. Não se pretende ser exaustiva na identificação de todas as decisões judiciais, mas antes selecionando as decisões judiciais relevantes que possam caracterizar e demonstrar os principais tipos de riscos inerentes ao uso do sistema de *homebanking*, identificando-se padrões interpretativos e eventuais divergências jurisprudenciais.

Com a abordagem explicativa da pesquisa pretendemos esclarecer as relações de causa e efeito entre os tipos de riscos possíveis e a consequente responsabilização, tentando-se compreender que fatores influenciaram na criação das normas e as razões justificativas da aplicação das mesmas no âmbito das decisões judiciais identificadas no presente estudo.

3. O contrato de *homebanking* e o seu enquadramento legal em Portugal

3.1. O contrato de homebanking

A relação jurídica bancária, entre cliente e o banco, inicia-se com a celebração de um contrato de abertura de conta bancária, consubstanciando este o contrato matriz, a partir do qual se poderá celebrar outros contratos, como por exemplo o contrato de depósito bancário, que é a convenção que tem por objeto o depósito de dinheiro na conta do respetivo titular, ou o contrato de conta-corrente bancária, que se traduz na convenção cujo objeto é o registo contabilístico das operações realizadas entre os contraentes e de que resulta o saldo[3].

Todavia não se pode confundir o contrato de *homebanking* com o contrato de depósito bancário nem com contrato de abertura de conta bancária, tratando-se de contratos distintos embora interligados e coligados entre si e embora sejam contratos distintos não são contratos autónomos, tratando-se antes de uma verdadeira união de contratos com dependência. A este propósito, Galvão Telles refere que o vínculo de dependência significará que a validade e vigência de um contrato ou de cada um dos contratos depende da validade do outro na medida em que um contrato só será válido se o outro também o for[4].

Após estabelecida a relação jurídica bancária entre cliente e Banco, surge então o contexto para a celebração do contrato de *homebanking*, concluindo-se que este é um contrato acessório do contrato de abertura de conta bancária e do contrato de depósito bancário. Os bancos enquanto prestadores de serviços de pagamento[5] disponibilizam ao cliente um instrumento de pagamento e realização de operações bancárias à distância, sem que estes tenham de se deslocar fisicamente às agências bancárias, assumindo e garantindo a segurança do sistema na sua utilização e que os dispositivos de segurança inerentes a tal instrumento sejam acessíveis apenas ao utilizador/ cliente, o qual, por sua vez, deve guardar segredo sobre as suas chaves de acesso a este instrumento e cartão de coordenadas para validação de operações, evitando que tais dados sejam fornecidos a terceiros estranhos à relação jurídica bancária estabelecida. O contrato de *homebanking* implica, para a sua constituição, uma disponibilização do instrumento de pagamento ao cliente e a aceitação por parte deste na sua utilização, mas não se trata de um contrato unilateral, pois do mesmo surge para ambas as partes um conjunto de obrigações, conforme descrito, sendo um contrato comutativo, obrigacional e sinalagmático.

[3] Cfr. Antunes, 2009, pp. 484–487.
[4] Cfr. Telles, 1989, p. 71.
[5] Cfr. Artigo 2.º, al. pp) e artigo 11.º, n.º 1, al. a) do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica.

O contrato *homebanking* é inominado e atípico, mas considera-se socialmente típico e não obedece a exigência de forma. Pode ser gratuito ou oneroso, dependendo das condições gerais e particulares estabelecidas entre as partes. Considera-se um contrato de execução continuada ou duradoura e sujeito a denúncia *ad nutum*, ou seja, sujeito a uma desvinculação unilateral, sem necessidade de justificação, sem estar sujeito a prazo limitativo para o seu exercício[6] e sem aviso prévio. No que se refere à denúncia *ad nutum* importa salientar que tal se aplica sempre ao cliente, já para a entidade bancária, contratualmente pode ser estipulada a necessidade de aviso prévio.

Com relevância para a presente análise importará referir que o contrato de *homebanking* se caracteriza como um contrato-quadro[7], na medida em que estabelece as diretrizes gerais a que irão obedecer os contratos de execução de operações bancárias que lhe vão suceder, ou seja, o contrato *homebanking* dita o quadro normativo, os direitos e deveres de ambas as partes na realização das subsequentes operações bancárias que serão executadas através desse sistema.

O contrato de *homebanking* caracteriza-se também por ser um contrato de adesão na medida em que as suas cláusulas são pré-elaboradas e disponibilizadas ao cliente o qual apenas se limita a aderir e a aceitar as mesmas, não lhe sendo viabilizada a possibilidade de negociar as mesmas. Assim, este contrato está sujeito ao Regime Jurídico das Cláusulas Contratuais Gerais[8].

O contrato de *homebanking* é pois o contrato instituidor de serviço que permitirá ao cliente bancário/ uitlizador, consultar os dados da sua conta, como saldos, a movimentação, o IBAN, os titulares de conta, convenções acessórias à conta bancária subscritas e outros serviços. Permitirá ainda movimentar os fundos depositdos na conta, efectuar transferências para terceiros, configurando-se por isso desde logo como um serviço de pagamento, permitirá também pagar serviços e compras, solicitar cartões de débito ou crédito, efectuar ordens de investimento, consultar cheques, gerir pagamentos, ordenar ou cancelar débitos diretos, subscrever seguros, entre muitas outras operações, a custos mais baixos, em qualquer local e hora.

3.2. Enquadramento legal no ordenamento jurídico português

Nos termos do artigo 3.º do Regime Geral das Instituições de Crédito e Sociedades Financeiras, os bancos são, para além de outras aí contempladas, instituições de crédito, podendo, nos termos do artigo 4.º do mesmo diploma legal efetuar, entre outras, a operação de receção de depósitos ou outros fundos reembolsáveis para utilização de conta própria[9], assim como podem prestar serviços de pagamento tal como definidos no artigo 4.º do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica[10].

---

[6] O que distingue este direito do direito de livre resolução, previsto nos artigos 19.º e 20.º do Regime Jurídico dos Contratos à Distância relativos a Serviços Financeiros celebrados com Consumidores.

[7] O artigo 2.º, al. i) do Decreto-Lei n.º 91/2018 de 12 de novembro, define contrato-quadro como "um contrato de prestação de serviços de pagamento que rege a execução futura de operações de pagamento individuais e sucessivas e que pode enunciar as obrigações e condições para a abertura de uma conta de pagamento".

[8] Decreto-Lei n.º 446/85, de 25 de outubro.

[9] Cfr. Art. 8.º, n.º 1 do Regime Geral das Instituições de Crédito e Sociedades Financeiras.

[10] Refere que constituem serviços de pagamento as seguintes atividades:

a) Serviços que permitam depositar numerário numa conta de pagamento, bem como todas as operações necessárias para a gestão dessa conta;

b) Serviços que permitam levantar numerário de uma conta de pagamento, bem como todas as operações necessárias para a gestão dessa conta;

c) Execução de operações de pagamento, incluindo a transferência de fundos depositados numa conta de pagamento aberta junto do prestador de serviços de pagamento do utilizador ou de outro prestador de serviços de pagamento, tais como:

Assim, e por força da conjugação dos artigos 2.º, als. dd), pp), 3.º, 4.º, al. g) e 11.º do Decreto-Lei n.º 91/2018, de 12 de novembro[11], é aplicável ao contrato de *homebanking* o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica[12], uma vez que se traduz num "serviço de pagamento fornecido através da internet ou de outros canais à distância, cujo funcionamento não depende do local onde estão fisicamente situados o dispositivo utilizado para iniciar a operação de pagamento ou o instrumento de pagamento utilizado"[13]. Simultaneamente, é ainda aplicável ao contrato de *homebanking* o Regime Jurídico dos Contratos à Distância relativos a Serviços Financeiros celebrados com Consumidores regulado pelo Decreto-lei nº 95/2006, de 29 de maio[14].

Este regime afigura-se de extrema importância para efeitos de enquadramento da responsabilidade das partes no que concerne aos contratos relativos a serviços financeiros prestados a consumidores através de meios de comunicação à distância pelos prestadores autorizados a exercer a sua atividade em Portugal[15].

Com base neste regime legal, os bancos são prestadores de serviços financeiros nos termos do artigo 2.º, al. d), entendendo-se por serviço financeiro "qualquer serviço bancário, de crédito, de seguros, de investimento ou de pagamento e os relacionados com a adesão individual a fundos de pensões abertos"[16]. Se pelo contrato de *homebanking* se estipulam as diretrizes a que obedecerá a prestação de serviços financeiros, através de meios de comunicação à distância, a consumidores[17], então estamos no âmbito de aplicação deste regime[18], o qual prevê uma proteção de conteúdo mínimo imperativo do consumidor, não sendo lícito a este renunciar aos direitos que lhe são conferidos por lei, nem será válida qualquer cláusula contratual que derroguem esses direitos[19].

---

i) Execução de débitos diretos, incluindo os de carácter pontual;
ii) Execução de operações de pagamento através de um cartão de pagamento ou de um dispositivo semelhante;
iii) Execução de transferências a crédito, incluindo ordens de domiciliação;
d) Execução de operações de pagamento no âmbito das quais os fundos são cobertos por uma linha de crédito concedida a um utilizador de serviços de pagamento, tais como:
i) Execução de débitos diretos, incluindo os de carácter pontual;
ii) Execução de operações de pagamento através de um cartão de pagamento ou de um dispositivo semelhante;
iii) Execução de transferências a crédito, incluindo ordens de domiciliação;
e) Emissão de instrumentos de pagamento ou aquisição de operações de pagamento;
f) Envio de fundos;
g) Serviços de iniciação do pagamento;
h) Serviços de informação sobre contas.

[11] Alterado pelo Decreto-lei n.º 66/2023, de 8 de agosto e pela Lei n.º 82/2023, de 29 de dezembro.

[12] Que transpôs para o ordenamento jurídico português a Diretiva (UE) 2015/2366, revogando o Decreto-Lei n.º 317/2009, de 30 de outubro, que havia transposto para a ordem jurídica portuguesa a Diretiva 2007/64/CE.

[13] Cfr. Preâmbulo do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica.

[14] Que transpôs para a ordem jurídica portuguesa a Diretiva 2002/65/CE.

[15] Cfr. Artigo 1.º, n.º 1, do Decreto-lei nº 95/2006, de 29 de maio.

[16] Cfr. Art. 2.º, al. c) do Regime Jurídico dos Contratos à Distância relativos a Serviços Financeiros celebrados com Consumidores.

[17] Entende-se como consumidor qualquer pessoa singular que, nos contratos à distância, atue de acordo com objetivos que não se integrem no âmbito da sua atividade comercial ou profissional, nos termos do art. 2.º, al. e) do Regime Jurídico dos Contratos à Distância relativos a Serviços Financeiros celebrados com Consumidores.

[18] De realçar que este regime se aplicará também aos intermediários de serviços financeiros, nos termos do artigo 3.º do Regime Jurídico dos Contratos à Distância relativos a Serviços Financeiros celebrados com Consumidores.

[19] Cfr. Artigo 5.º do Regime Jurídico dos Contratos à Distância relativos a Serviços Financeiros celebrados com Consumidores.

Como referimos *supra*, o contrato de *homebanking* é um contrato-quadro ao abrigo do qual se realizarão subsequentemente operações de execução continuada, pelo que o Regime Jurídico dos Contratos à Distância relativos a Serviços Financeiros celebrados com Consumidores apenas se aplica ao acordo inicial e não a cada uma das operações que subsequente e individualmente se realizem no âmbito desse acordo inicial[20].

Salientamos que este regime jurídico consagra no seu artigo 7.º que é proibida a prestação de serviços financeiros à distância que acarretem um pedido de pagamento, seja imediato ou diferido, ao consumidor que os não tenha prévia e expressamente solicitado, mais estipulando que o silêncio do consumidor no âmbito de tal proposta não vale como consentimento para efeitos da aceitação desse serviço e pagamento. Caso tal ocorra, entender-se-á que o serviço financeiro que banco prestou será a título gratuito. A par desta proibição, consagra o artigo 8.º do mesmo diploma legal que também não é permitido o envio de mensagens relativas à prestação de serviços financeiros não solicitados, carecendo sempre do consentimento prévio do consumidor tal envio. Os bancos, para se precaverem e como forma de recolherem este consentimento prévio que é exigido, costumam consagrar desde logo nas cláusulas do contrato de *homebanking* que o cliente declara prestar o seu consentimento para a receção de tais propostas, seja através dos canais de comunicação remota do banco, seja através de correio eletrónico, SMS ou outras vias a comunicação, ainda que tais propostas impliquem um pedido de pagamento. No entanto cabe aqui diferenciar o estipulado nos artigos 7.º e 8.º, dado que no primeiro caso trata-se da prestação efetiva de serviços financeiros não solicitados, no segundo trata-se apenas de comunicações não solicitadas.

Consagra-se ainda que para efeitos de melhor clareza na perceção das cláusulas contratuais, a informação pré-contratual, os termos do contrato à distância e todas as demais comunicações relativas a esse contrato sejam efetuadas na língua oficial portuguesa a menos que o consumidor consinta na utilização de outro idioma devendo especificá-lo. A informação a prestar deve ser efetuada de modo claro, objetivo, percetível, personalizada ao meio de comunicação utilizado para o efeito e de acordo com os princípios da boa-fé. O conteúdo da informação a prestar reporta-se à identificação do prestador de serviços, ao serviço financeiro a prestar em concreto, ao contrato e aos mecanismos de proteção ao dispor dos consumidores. A informação a prestar deve ser prévia à realização do contrato e à consequente vinculação do consumidor. Exige-se ainda que seja disponibilizada em papel ou noutro suporte duradouro disponível e acessível ao consumidor, podendo este exigir que lhe seja fornecido, a qualquer momento e durante a manutenção do contrato a informação em suporte de papel. Importa salientar aqui que disponibilizar a informação em papel ou em suporte duradouro não significa cumprir com o dever de informação, mas tão-somente indiciar o cumprimento do dever de comunicar.

O direito de livre resolução[21] assume maior importância no âmbito do dever de informação que impende sobre o prestador de serviços financeiros celebrados com consumidores através de meios de comunicação à distância. Os artigos 19.º e 20.º do Regime Jurídico dos Contratos à Distância relativos a Serviços Financeiros celebrados com Consumidores prevê que o consumidor possa livremente resolver o contrato à distância sem necessidade de indicar qualquer motivo e sem que lhe possa ser exigida qualquer indemnização ou aplicada qualquer penalização. O prazo para exercer este direito de livre resolução é de 14 dias, todavia, se se tratar de contratos de seguro de vida e relativos à adesão individual a fundos de pensões abertos, o prazo para o exercício do direito de livre resolução sobe para 30 dias. A contagem

[20] Cfr. Artigo 4.º, n.º 1 do Regime Jurídico dos Contratos à Distância relativos a Serviços Financeiros celebrados com Consumidores.
[21] Não existe nos casos especificados no artigo 22.º do Regime Jurídico dos Contratos à Distância relativos a Serviços Financeiros celebrados com Consumidores.

de tais prazos apenas se inicia a partir da data da celebração do contrato à distância ou, se for em data posterior, da data da receção pelo consumidor das informações em suporte duradouro ou em papel[22].

Por fim e a este propósito, salientar ainda que a prova do cumprimento da obrigação de informação ao consumidor assim como o consentimento deste para a celebração do contrato e a sua execução cabe ao prestador, considerando-se proibida qualquer cláusula que determine a inversão contratual deste ónus de prova.

Por fim, cumpre referir que configurando-se o sistema de *homebanking* como um sistema de pagamento eletrónico, os prestadores de serviços de pagamento, onde se incluem os bancos, que o disponibilizam estão obrigados a implementar regras de segurança na sua utilização, pelo que se torna obrigatório a adoção de medidas de segurança que garantam que os serviços de pagamento eletrónico oferecidos estejam o mínimo possível expostos a riscos de fraude e roubo de dados. Ciente desta necessidade, a União Europeia emanou o Regulamento Delegado (UE) 2018/389, de 27 de novembro de 2017, que veio complementar a Diretiva dos Serviços de Pagamento[23], impondo aos prestadores de serviços de pagamento a implementação do sistema de autenticação forte dos clientes na realização de operações através do *homebanking* ou *app*. Assim, sempre que um cliente bancário utilize o sistema de *homebanking* para aceder à sua conta de pagamento, para efetuar uma operação de pagamento eletrónico ou para realizar a generalidade das ações possíveis através desse canal remoto, cuja utilização evolve um risco de fraude ou outro abuso, deverão autenticar-se segundo regras que permitam aferir e verificar a identidade do utilizador, bem como a sua legitimidade para efetuar tais operações.

O sistema de autenticação forte imposto por aquele Regulamento é um método que exigirá ao cliente bancário o fornecimento de elementos que permitam atestar a sua identidade e legitimidade. Os elementos exigidos para efetuar a autenticação forte estão elencados por categorias: a categoria do "conhecimento", a de "posse" e a de "inerência". Na categoria de "conhecimento" será solicitado ao cliente o fornecimento de algo que apenas o próprio conheça, como por exemplo uma *password*, na categoria "posse" será exigido ao cliente que forneça algo que esteja na sua posse, como por exemplo um código que foi gerado no âmbito da operação que se encontra a realizar e a que só o cliente tenha acesso por lhe ter sido enviado para o número de telemóvel que fidelizou e certificou como seu junto do prestador do serviço de pagamento, e na categoria "inerência", pode ser necessário que o cliente viabilize o acesso a uma característica única sua, como por exemplo a sua impressão digital. Será o prestador do serviço de pagamento que decidirá quais os elementos escolhidos para efetuar esta autenticação forte, que chamamos de dupla autenticação por ser bastante a exigência de dois elementos pertencentes àquelas categorías.

[22] O consumidor que queira exercer o direito de livre resolução deve notificar o prestador do serviço financeiro por qualquer meio que seja suscetível de prova podendo fazê-lo através de envio de carta registada para a morada do prestador de serviço ou endereço de correio eletrónico que tenham sido indicados pelo prestador de serviço termos dos artigos 13.º e 15.º, n,º 1, al. a). Salienta-se que notificação não é uma declaração recetícia, no sentido em que ela não tem de ser recebida até ao último dia do prazo, mas antes enviada até ao último dia do prazo de exercício de tal direito.

[23] Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro (Diretiva de Serviços de Pagamento revista – DSP2).

3.3. Obrigações contratuais e legais

3.3.1. Para os prestadores de serviços de pagamento

Como referido, sendo o contrato de *homebanking* um contrato-quadro que, acessoriamente ao contrato de abertura de conta, irá determinar as regras da relação jurídica estabelecida entre Banco e cliente, que se executarão *online*, nasce desde logo para o banco a obrigação de disponibilizar meios eletrónicos seguros e necessários ao estabelecimento dessa comunicação à distância. O Banco permanece obrigado a manter de forma constante e ao longo de todo o contrato regras de comunicação e de funcionamento seguras, devendo assegurar que o acesso à conta de certo cliente através desses dispositivos é feita exclusivamente por ele.

Os prestadores de serviços de pagamento, como o caso das entidades bancárias, estão vinculados a determinadas obrigações a partir do momento que emitem um instrumento de pagamento. Essas obrigações encontram-se previstas no art. 111.º, do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, traduzindo-se no dever de assegurar que as credenciais de segurança personalizadas do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento. Cabe-lhe ainda a obrigação de se abster de enviar instrumentos de pagamento não solicitados, salvo quando um instrumento deste tipo já entregue ao utilizador de serviços de pagamento deva ser substituído, deve também garantir a disponibilidade, a todo o momento, de meios adequados a permitir ao utilizador de serviços de pagamento que possa comunicar, logo que tenha conhecimento dos factos e sem atraso injustificado, ao prestador de serviços de pagamento ou à entidade designada por este último, a perda, o furto, o roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento, bem como deve providenciar por disponibilizar, a todo o momento, os meios adequados a permitir ao utilizador de serviços de pagamento solicitar o desbloqueio, nos termos do n.º 4 do artigo 108.º. Também é obrigação do prestador do serviço de pagamento, facultar ao utilizador do serviço de pagamento, a pedido deste, os meios necessários para fazer prova, durante 18 meses após a comunicação prevista na alínea b) do n.º 1 do artigo 110.º, de que efetuou essa comunicação ou solicitou o desbloqueio nos termos do n.º 4 do artigo 108.º e, finalmente, é ainda obrigação do prestador do serviço de pagamento impedir qualquer utilização do instrumento de pagamento logo que a comunicação prevista na alínea b) do n.º 1 do artigo 110.º tenha sido efetuada pelo utilizador.

Para além destas obrigações, os prestadores dos serviços de pagamento estão também adstritos ao cumprimento de deveres de informação muito concretos, devendo comunicar, informar e esclarecer os utilizadores do sistema de *homebanking* sobre as boas práticas a adotar na internet designadamente no que concerne a operações de pagamento, uma vez que para as executar necesariamente terão de fornecer dados sobre a sua identificação bancária ou do cartão a ela associado. A este propósito, veja-se o referido por:

> Quanto aos cartões, é aconselhável a utilização de IP com características de segurança acrescida (saldo/plafond limitado ou prazos de validade mais curtos) ou o uso de sistemas como o MBnet – permite a criação de um cartão de pagamento virtual e temporário (de uma utilização ou mensal), a que pode ser atribuído o plafond necessário para o pagamento pretendido, realizando compras on-line sem fornecer dados do cartão de pagamento verdadeiro. (Ribeiro De Lima, 2016, p. 34)

De referir que no caso de necessidade de envio ao utilizador de serviço de pagamento das credenciais de acesso a um instrumento de pagamento por parte do prestador de serviço, é sobre este que recai o risco se existir qualquer extravio ou violação de dados, sendo esse o

motivo pelo qual, por exemplo, no envio de um cartão, que é um instrumento de pagamento, o envio deste e do respetivo código de acesso sejam enviados em separado[24]. O art. 70.º, n.º 2 do mesmo diploma legal estabelece ainda que os prestadores de serviços de pagamento devem estabelecer e manter procedimentos eficazes de gestão de incidentes, inclusive para a deteção e classificação de incidentes operacionais e de segurança de carácter severo e nos termos do art. 113.º, n.º 1.

Caso um utilizador de serviços de pagamento negar ter autorizado uma operação de pagamento executada, ou alegar que a operação não foi corretamente efetuada, fica a cargo do prestador do serviço de pagamento o ónus de prova de que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência do serviço prestado pelo prestador de serviços de pagamento e para efeitos de tal prova não é necessariamente suficiente, por si só, provar que a operação de pagamento foi autorizada pelo ordenante e que este último agiu de forma fraudulenta, ou que não cumpriu, com dolo ou negligência grosseira, uma ou mais obrigações previstas no artigo 110.º, é necessário que o prestador de serviço de pagamento apresente elementos que demonstrem a existência de fraude, de dolo ou de negligência grosseira da parte do utilizador de serviços de pagamento. O mesmo é dizer que constitui ónus da prova da entidade bancária provar positivamente a ocorrência de comportamento negligente, gravemente negligente ou doloso do utilizador. E sobre este aspeto, é seguimos de perto as palavras de:

> Importa sublinhar que a negligência grosseira deve ser devidamente separada da diligência ordinária ou culpa leve. Não basta a falta de cuidado que um bom pai de família, que aqui significa simplesmente um utilizador cuidadoso, desses instrumentos tivesse adotado, dentro das circunstâncias do caso concreto. Vai para lá dessa medida. Implica um nível de falta de cuidado quase escandaloso, de um desleixo inadmissível seja para quem for (p. ex., deixar o seu nome de utilizador ou palavra passe à vista ou num local de acesso a terceiros fora do seu círculo familiar ou de confiança próxima). A porta para a imputação de perdas ao utilizador por esta via é, assim, bastante apertada. (Vasconcelos, 2020, p. 202).

3.3.2. Para o utilizador

Por sua vez, sobre o cliente/utilizador impõem-se essencialmente deveres de conduta, como de utilização correta do serviço e a obrigação de manter a confidencialidade relativamente ao código de acesso pessoal à conta e aos dispositivos de segurança personalizados fornecidos pela entidade bancária, onde se inclui cartões matriz, códigos gerados no momento das operações e enviados para o utilizador, os quais possuem uma função de autenticação das operações. Assim:

> O utilizador deverá, igualmente, evitar aceder à página do serviço de banca ao domicílio ou fazer pagamentos em computadores públicos, manter o antivírus atualizado, não clicar em hiperligações apresentadas em e-mails, digitar o endereço da página de homebanking, entre outros cuidados necessários a preservar a segurança do sistema de pagamentos eletrónicos e que poderão ser analisados pelos tribunais na ponderação da atuação do utilizador. (Ribeiro De Lima, 2016, p. 34)

Estes deveres a que os utilizadores se encontram adstritos surgem elencados no art. 110.º do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, onde se especifica que o utilizador deve tomar todas as medidas razoáveis, em especial logo que receber um

[24] Também neste sentido, veja-se Vasconcelos (2020, p. 203).

instrumento de pagamento, para preservar a segurança das suas credenciais de segurança personalizadas, debe utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização, as quais têm de ser objetivas, não discriminatórias e proporcionais e informadas pelo prestador do serviço de pagamento e, principalmente, deve comunicar, logo que tenha conhecimento dos factos e sem atraso injustificado, ao prestador de serviços de pagamento ou à entidade designada por este último, a perda, o furto, o roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento. Em caso de atuação fraudulenta ou incumprimento deliberado de uma ou mais destas obrigações, o utilizador suportará todas as perdas resultantes de operações de pagamento não autorizadas e, havendo negligência grosseira do utilizador, este suportará as perdas resultantes de operações de pagamento não autorizadas até ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, ainda que superiores à quantia de 50 euros[25].

3.4. Vantagens da utilização do sistema de homebankinhg para as partes

A grande vantagem para o cliente na celebração do contrato *homebanking* é a comodidade de a qualquer hora e momento e em qualquer local com acesso à internet poder efetuar a gestão da sua conta bancária sem a necessidade de se deslocar fisicamente a uma qualquer agência bancária ou caixa de multibanco. Através da utilização do sistema *homebanking*, o cliente tem acesso permanente e na hora à sua conta bancária, consultando o seu saldo, movimentações, posição integrada nos seus contratos de crédito, taxas de juro a estes aplicável, informações sobre investimentos efetuados, subscrição de novos produtos e serviços financeiros, realizar pagamentos, efetuar transferências, consultar débitos diretos, cancelar ou estipular novos limites, consultar informações referentes a novos produtos de investimento, consultar as suas poupanças e até constituir novas contas de depósito a prazo, contratar seguros, obter documentos referentes à sua conta bancária e situação creditícia junto do banco, solicitar a emissão de cartões, consultar a posição destes, solicitar emissão de cheques e até, em algumas circunstâncias, obter uma redução dos custos na gestão da sua conta bancária.

Mas a parte que colhe maiores benefícios no oferecimento de serviços bancários e financeiros através de meios de comunicação à distância é o banco, desde logo porque isso lhe permite reduzir significativamente os custos com recursos humanos, aumentando os seus lucros com a redução de tal despesa, permite ainda uma diminuição significativa das situações de erro humano, o que tem impacto positivo também na diminuição do risco operacional, permite o aumento da produtividade e eficiência na diversificação da oferta de produtos, personalizar essa oferta e realizar negócios sem recurso a transferência e circulação de dinheiro em papel, o que conduz à desnecessidade de reservas de moedas e notas físicas nas agências bancárias, o que reduz igualmente os prejuízos que possam decorrer de um eventual furto ou roubo nas instalações físicas dos bancos.

4. Riscos da utilização do sistema *homebanking*

Novos riscos surgiram na janela de oportunidade da utilização cada vez mais massificada do sistema de *homebanking*. (Câmara & Magalhães, 2012, p. 33) referem-se ao "risco informático", assente na "ideia de vulnerabilidade dos sistemas informáticos para a ocorrência de danos não imputáveis a qualquer das partes."

[25] Cfr. Art. 115.º, n.º 1, 3 e 4 do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica.

Efetivamente, existem riscos associados à utilização do serviço de *homebanking* diretamente relacionados com a vulnerabilidade da plataforma informática em que assenta a sua execução, suscetíveis de ataques informáticos e geradoras de situações de fraude praticadas por terceiros mal intencionados que pretendem violar direitos subjetivos do utilizador de tal sistema, tentando ilicitamente obter dados referentes à identidade do utilizador e as respetivas credenciais de acesso ao sistema e de validação de operações.

As fraudes são maioritariamente concretizadas com recurso à instalação nos dispositivos eletrónicos do utilizador de *malware* (*software* malicioso). O Banco de Portugal, enquanto regulador e supervisor do sistema bancário português, tem aconselhado os utilizadores a acederem sempre ao sítio de internet oficial do banco, digitando o endereço eletrónico (e nunca através de motores de busca), verificando sempre se o endereço começa por "https://" e se surge acompanhado de um cadeado. Aconselha ainda a que o utilizador não clique em *links* desconhecidos ou de origem duvidosa, inclusive constantes de mensagens provenientes de números desconhecidos ou emails cujo endereço eletrónico é de origem suspeita. Relembra ainda que o utilizador nunca pode divulgar as suas credenciais de acesso ao *homebanking* ou *app* do seu banco, nem os códigos de autorização que lhe sejam enviados pelo Banco para o seu telemóvel fidelizado no âmbito de uma operação bancária.

Entre as modalidades típicas de fraude informática destacam-se o *phishing* e o *pharming*. O *phishing* caracteriza-se pela tentativa de adquirir dados pessoais, costumando traduzir-se no envio de e-mails pretensamente remetidos pela entidade bancária solicitando elementos confidenciais do utilizador ou solicitando que este clique em *links* de sites alegadamente pertencentes ao banco, para aí proceder-se a supostas retificações de dados ou complemento de dados, ativação ou reativação de serviços, entre outras diligências supostamente necessárias à manutenção do funcionamento do sistema *homebanking* e, por vezes, a persuasão surge em forma de ameaça do bloqueio da conta se tais operações não forem efetuadas pelo utilizador. Ao abrir ou clicar em tais *links*, o utilizador poderá estar a proporcionar o furto de informações bancárias e a sua utilização subsequente.

O *pharming*, por sua vez, já se traduz numa técnica mais sofisticada, que consiste em suplantar o sistema de resolução dos nomes de domínio para conduzir o utilizador a uma página *web* falsa, clonada da página verdadeira da entidade bancária, baseando-se o processo, sumariamente, em alterar o IP numérico de uma direção no próprio navegador, através de programas que captam os códigos de pulsação do teclado (os ditos *keyloggers*), o que pode ser feito através da difusão de vírus via *spam*, o que leva o utilizador a pensar que está a aceder a um determinado site – por exemplo o do seu banco – e está a entrar no IP de uma página Web falsa, sendo que ao indicar as suas chaves de acesso, estas serão depois utilizadas pelos *crackers*, para acederem à verdadeira página da instituição bancária e aí poderem efectuar as operações que entenderem. Neste mesmo sentido, explica:

> O pharming, por seu turno, é uma técnica mais sofisticada e, por isso, mais perigosa, na medida em que é "corrompido" o próprio nome de domínio (domain name) de uma entidade financeira, redireccionando o utilizador para um site falso – que constitui um decalque do verdadeiro – sempre que este digita no teclado a morada correcta da sua entidade bancária. Uma vez na página falsa, o utilizador indica as suas chaves secretas de acesso que depois são utilizados na página verdadeira para transferências fraudulentas. (Santos, 2015, p. 12).

5. Casos concretos e respetivo tratamento jurisprudencial

Uma vez explicados os dois principais fenómenos de fraude eletrónica a que a utilização do sistema de *homebanking* se encontra sujeita, identificamos duas situações concretas, a título exemplificativo, para que se analise o tratamento jurisprudencial concedido e a que critérios obedeceram tais soluções judiciais.

No primeiro caso, o utilizador do serviço de *homebanking* receciona no seu telemóvel, uma mensagem escrita proveniente de um número que surgia identificado como sendo do prestador de serviço de pagamento, no caso, o seu banco. Nessa mensagem escrita informa-se o cliente que deve aceder à página *web* do banco para ativar um serviço que estaria inativo, sendo que o utilizador já havia sido informado desse facto anteriormente pelo banco pelo menos duas vezes. Nessa mensagem escrita apela-se a que entre num *link* como sendo do *site* do banco. O utilizador clica no referido *link* constante da mensagem, surgindo-lhe uma página em tudo igual à do *site* do banco, nela entrando com o seu *username* e PIN, fornecendo depois números do seu cartão matriz como fora solicitado, tendo posteriormente detetado que foram efetuadas transferências e pagamentos que não fora o próprio a ordenar e a consentir.

Num segundo caso, o utilizador do serviço de *homebanking* julgou aceder ao *site* do prestador do serviço de pagamento, seu banco, mas na realidade acedeu a uma página da internet que não pertencia ao banco mas que era em tudo semelhante à mesma, não tendo o utilizador detetado qualquer anormalidade, pelo que aí forneceu, a pedido, todas as coordenadas do seu cartão matriz, tendo sido efectuadas transações posteriormente sem que tivesse sido o próprio a efetuá-las.

As situações expostas são recorrentes e, no primeiro caso (*phishing*/ *smishing*), o Supremo Tribunal de Justiça[26] decidiu que as perdas resultantes de operações de pagamento não realizadas e não autorizadas pelo utilizador do serviço de *homebanking* são da responsabilidade da entidade bancária pois esta não logrou provar que o comportamento do utilizador se traduziu numa atuação fraudulenta ou numa atuação grosseira e nem sequer logrou provar que tenha existido incumprimento deliberado das obrigações que sobre o utilizador impendiam no uso de tal sistema, afastando qualquer dolo ou de negligência grosseira por parte do utilizador. E em caso idéntico, o Tribunal da Relação do Porto[27] decidiu que a entidade bancária só não seria responsabilizada se alegasse e provasse que os danos resultaram de atuação dolosa ou grosseiramente negligente do utilizador do serviço. No segundo caso (*pharming*), o Tribunal da Relação de Évora[28] decidiu que a conduta do utilizador configurou negligência grave, cabendo-lhe a ele a responsabilidade pelas operações de pagamento não autorizadas executadas, até ao limite do saldo disponível, fundamentando que lhe havia sido dito pelo banco que se fosse solicitado mais de duas coordenadas do cartão matriz por cada operação isso indiciaria que poderia estar na presença de uma página fraudulenta, pelo que a ele se impunha cautela e teria de ter previsto a possibilidade de não se encontrar no *site* correto e, por conseguinte, se encontrar a facultar os seus dados a terceiros.

[26] Cfr. Acórdão do Supremo Tribunal de Justiça, datado de 12/12/2023, relatado por Manuel Capelo (Proc. N.º 9240720.5T8LSB.L1.S1).
[27] Cfr. Acórdão do Tribunal da Relação do Porto, datado de 16/05/2023, relatado por Rodrigues Pires (Proc. N.º 659/22.8T8PNF.P1).
[28] Cfr. Acórdão do Tribunal da Relação de Évora, datado de 12/04/2018, relatado por Ana Margarida Leite (Proc. N.º 9002/16.4T8STB.E1).

A jurisprudência portuguesa[29] utiliza como critério decisivo para a tomada de posição a prova carreada para os autos por parte da entidade bancária, impondo-lhe demonstrar se o utilizador teve ou não qualquer comportamento suscetível de pôr em causa a segurança do sistema, se contribuiu ou não, com dolo ou negligencia, para o acesso de terceiros às chaves de segurança e às combinações de coordenadas do cartão matriz do utilizador e, não logrando tal prova, o sentido da decisão será em desfavor da entidade bancária e esta terá a obrigação de reembolsar o utilizador pelos montantes das operações de pagamento que não tenham sido autorizadas.

6. Discussão: Repartição da responsabilidade pelos danos causados decorrentes da utilização do sistema *homebanking*

Como *supra* se deixou expresso, constitui ónus da prova da entidade bancária provar a ocorrência de comportamento negligente, gravemente negligente ou doloso do utilizador no cumprimento das obrigações a que se encontra adstrito para poder desresponsabilizar-se pelas perdas e danos decorrentes de fraude de que o utilizador tenha sido vítima no âmbito da sua utilização do sistema *homebanking*. A este propósito:

> Afigura-se tarefa árdua a interpretação e a aplicação do artigo 70.º, nomeadamente em virtude da utilização sucessiva de conceitos indeterminados. Assim, questiona-se qual o grau de prova que os prestadores devem assegurar para satisfazer este artigo, uma vez que se prevê que o registo da utilização do instrumento de pagamento – v.g. o registo da utilização do cartão de débito do utilizador com o PIN correto ou a introdução das credenciais de acesso ao homebanking – não é, só por si, necessariamente suficiente para provar que a operação de pagamento foi autorizada, que o utilizador agiu fraudulentamente, deliberadamente ou com negligência grave, quando o n.º 1 do artigo 70.º estatui que os prestadores devem demonstrar que a operação foi "devidamente registada" (Guerra, 2016, p. 26).

Cabe ao prestador do serviço de pagamento garantir o funcionamento seguro e eficaz do sistema de *homebanking* pelo que recairá sobre ele o risco de um funcionamento deficitário ou inseguro e, se em virtude dessa ineficácia ou insegurança, ocorrerem operações não autorizadas pelo cliente nem estas sejam devidas a uma utilização imprudente deste, as perdas e danos daí decorrentes correm por conta do prestador do serviço de pagamento.

Já o risco de mau uso dos dispositivos de segurança ou divulgação indevida de códigos de acesso ou das coordenadas do cartão matriz a terceiros não autorizados e que tenham sido utilizados para autenticar as operações bancárias realizadas através do sistema de *homebanking*, bem como o risco pela errada identificação do número de identificação bancária de destino de uma transferência ou errada indicação do montante a transferir, correrá por conta do utilizador.

Na verdade, o prestador do serviço só pode exonerar-se de responsabilidade se fizer a prova de que a operação foi regular e devidamente autenticada, registada e contabilizada, não tendo existido qualquer avaria técnica ou deficiência, e que tal operação se ficou a dever a fraude do utilizador ou a incumprimento doloso ou gravemente negligente, por parte deste, das suas obrigações. De outra forma, o prestador do serviço será sempre responsabilizado, inclusive, pelo risco de falha do sistema informático utilizado e pelos ataques cibernautas ao mesmo, sendo, de resto, o que sempre resultaria da regra geral prevista no art. 796.º, n.º1 do Código Civil.

---

[29] A título de exemplo, veja-se o Acórdão do Tribunal da Relação de Lisboa, datado de 21/12/2017, relatado por Manuel Rodrigues (Proc. N.º 1318/09.2TBTNV.L1-6).

O utilizador será responsabilizado se na sua utilização do sistema não cumpriu os deveres de conduta e legais que lhe são impostos e atuou com negligencia grosseira, a qual se entende como um comportamento que merece um grau de reprovação que ultrapasse a mera censura. A negligência grosseira decorre da inobservância das mais elementares regras de prudência e da não adoção do esforço e diligência minimamente exigíveis, nas circunstâncias concretas, correspondendo a um erro imperdoável, a uma desatenção inexplicável e a uma incúria indesculpável, vistos em confronto com o comportamento do comum das pessoas, mesmo daquelas pouco diligentes. Age com negligencia grosseira aquele que adota um comportamento que nunca seria adotado pela generalidade dos utilizadores do serviço de pagamento colocados perante as concretas circunstâncias do agente, pois que a diligência e cuidados exigíveis no caso os levariam a abster-se de o adotar e/ou prosseguir.

6. Conclusões

Chegados a este ponto, após a análise das principais características do contrato de *homebanking*, efetuado o seu enquadramento legal, elencadas as principais vantagens e obrigações decorrentes para ambas as partes deste tipo contratual, bem como identificados os principais tipos de fraudes informáticas que ocorrem no contexto da utilização do sistema de *homebanking*, pudemos concluir que o critério decisivo para a imputação de responsabilidade civil por perdas e danos decorrentes de fraudes informáticas perpretradas sobre utilizadores deste sistema de pagamento *online* dependerá da prova efetuada sobre se o utilizador teve ou não qualquer comportamento suscetível de pôr em causa a segurança do sistema, se contribuiu ou não, com dolo ou negligência, para o acesso de terceiros às chaves de segurança e às combinações de coordenadas do cartão matriz do utilizador e, não se logrando obter tal prova, será o prestador do serviço de pagamento o responsável e terá a obrigação de reembolsar o utilizador pelos montantes das operações de pagamento que não tenham sido autorizadas.

Concluimos ainda que a prova da culpa do utilizador pode ser extremamente difícil e variará casuisticamente, pelo que estaremos sempre no âmbito de critérios de apreciação alavancados em juízos subjetivos. No entanto, podemos afirmar que os prestadores de serviços de pagamento são os principais beneficiários da disponibilização e utilização do sistema de *homebanking*, conforme *supra* se demonstrou, dadas as inúmeras vantagens económicas que dele retiram para o funcionamento lucrativo da sua atividade, pelo que atendendo ao princípio *ubi commoda ibi incommoda*, cremos que legislador poderia ousar e consagrar uma verdadeira responsabilidade civil objetiva dos prestadores de serviços de pagamento que disponibilizem o sistema de *homebanking* ou outros meios de pagamento electrónicos quando, uma vez quebrada a segurança das repetivas plataformas, acarretem danos para os seus utilizadores, sem prejuízo, obviamente, da consagração de causas de exclusão dessa responsabilidade no caso de dolo ou negligência grosseira do utilizador, ou do ataque fraudulento perpetrado por terceiros que possam ser devidamente identificados.

7. Referências

Antunes, J. E. (2009). Direito dos contratos comerciais.

Câmara, P. y Magalhães, M. (2012). O novo direito bancário.

Guerra, P. (2016). The execution of unauthorised payment transactions and the payment service user protection under the legal framework governing the payment services and the electronic money. Revista electrónica de direito, 2. https://www.cije.up.pt/revistared

Moura, I. (25 de junio de 2013). O contrato de prestação de serviços bancários através da Internet. https://www.jusnetkarnovgroup.pt/jusjornal.php

Ribeiro De Lima, R. S. (2016). A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na jurisprudência portuguesa. Revista electrónica de direito, 3. https://WWW.CIJE.UP.PT/REVISTARED

Santos, H. L. D. (2015). Plaidoyer por uma "distribuição dinâmica do ónus da prova" e pela "teoria das esferas de risco" à luz do recente acórdão do Supremo Tribunal de Justiça, de 18/12/2013: o (admirável) "mundo novo" no homebanking? Revista electrónica de direito. https://WWW.CIJE.UP.PT/REVISTARED

Telles, I. G. (1989). Direito das obrigações, revista e actualizada. Coimbra Editora.

Vasconcelos, M. P. D. (2020). A responsabilidade do banco por operações de pagamento não autorizadas no online banking, decorrente do novo regime de serviços de pagamento (RSP II). JULGAR, 42.

CONTRIBUIÇÃO DOS AUTORES, FINANCIAMENTO E AGRADECIMENTOS

Contribuições dos autores:

Conceptualização: Teixeira, Maria Emília; Magalhães, Maria Manuela **Validação:** Teixeira, Maria Emília; Magalhães, Maria Manuela **Análise formal:** Teixeira, Maria Emília **Tratamento de dados:** Teixeira, Maria Emília; Magalhães, Maria Manuela **Redação - Preparação do projeto original:** Teixeira, Maria Emília **Redação-Revisão e Edição:** Teixeira, Maria Emília; Magalhães, Maria Manuela **Visualização:** Magalhães, Maria Manuela **Supervisão:** Teixeira, Maria Emília; Magalhães, Maria Manuela **Administração de Projecto:** Teixeira, Maria Emília **As autoras leram e aceitaram a versão publicada do artigo:** Teixeira, Maria Emília; Magalhães, Maria Manuela.

Financiamento: Este artigo teve o apoio do Contrato Programa UIDB/04112/2020, financiado por fundos nacionais através da FCT I.P.

Agradecimentos: O presente artigo contribui para a concretização dos objetivos de Investigação propostos pelo projeto de investigação "Regulação e Literacia Financeira", pertencente ao Grupo de Investigação "Património", do Instituto Jurídico Portucalense.

AUTORES:

Maria Emília Teixeira:

Licenciada em Direito pela Universidade Portucalense, Pós-Graduada em Direito da Banca, Bolsa e Seguros pela Universidade de Coimbra e Doutora em Direito Civil pela Universidade Portucalense. Professora Associada do Departamento de Direito da Universidade Portucalense, Investigadora do Instituto Jurídico Portucalense, Coordenadora Executiva do Doutoramento em Ciências Jurídicas e do Mestrado em Direito Europeu e Comparado da Universidade Portucalense. Coordenadora do Curso de Pós-Graduação em Direito Bancário e dos Valores Mobiliários da Universidade Portucalense.
emiliat@upt.pt

Orcid ID: https://orcid.org/0000-0001-9127-2148
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57658923700

Maria Manuela Magalhães:

Licenciada em Direito e Mestre em Relações Internacionais pela Universidade de Coimbra, Doutora em Direito Constitucional pela Universidade Portucalense. Professora Associada do Departamento de Direito da Universidade Portucalense e Diretora do Departamento de Direito da Universidade Portucalense. Atualmente desempenha ainda as funções de Diretora do Instituto Jurídico Portucalense, sendo também Investigadora deste Centro de Investigação.
mmdmms@upt.pt

Orcid ID: http://orcid.org/0000-0003-4261-7271
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57205592792