INÊS CUSTÓDIO ALVES

OPERAÇÕES ABUSIVAS NA BANCA ELETRÓNICA

A IMPUTAÇÃO DE RESPONSABILIDADES PELAS PERDAS RESULTANTES DA MOVIMENTAÇÃO NÃO AUTORIZADA DE FUNDOS

Dissertação com vista à obtenção do grau de Mestre em Direito e Mercados Financeiros

Orientador:
Professor Doutor Frederico Costa Pinto, Professor da Faculdade de Direito da Universidade Nova de Lisboa

Janeiro, 2019

- DECLARAÇÃO DE COMPROMISSO ANTI-PLÁGIO -

Declaro por minha honra que o trabalho que apresento é original e que todas as citações estão corretamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui grave falta ética e disciplinar.

Lisboa, 19 de Janeiro de 2019

(Inês Custódio Alves)

Ao meu avô, Ricardo Custódio

- AGRADECIMENTOS -

A elaboração da presente dissertação de mestrado só foi possível com o apoio daqueles que em muito contribuíram para a sua conclusão.

Antes de mais, expresso o meu agradecimento ao Professor Doutor Frederico Costa Pinto por me ter acompanhado com disponibilidade, prontidão e rigor ao longo deste estudo.

À minha família, pais, irmã e avós pela presença, permanente apoio e inspiração que sempre me concederam.

Ao Pedro, pela motivação, companheirismo e amor.

- MENÇÕES –

Advertências:

Esta dissertação ocupa um total de 123530 caracteres

Siglas e Abreviaturas:

Art.- artigo

AIS - *Account Information Services*

Bdp – Banco de Portugal

CC – Código Civil

CE – Comissão Europeia

Cfr.- Conforme

CP- Código Penal

CPP- Código do Processo Penal

DL – Decreto - Lei

DSP 1 – Diretiva dos Serviços de Pagamento 1

DSP 2 - Diretiva dos Serviços de Pagamento 2

LC- Lei do Cibercrime

p.- página

PIN - *Personal Identification Number*

PIS - *Payment Initiation Services*

pp.- páginas

ob. cit.- obra citada

RSP – Regime Jurídico dos Serviços de Pagamento e Moeda Eletrónica

RGICSF - Regime Geral das Instituições de Crédito e Sociedades Financeiras

TPP - *Third Party Providers*

UE- União Europeia

Vol.- Volume

- RESUMO –

A difusão das novas tecnologias de informação e comunicação fez recrudescer a prática de "novos crimes": os crimes informáticos.

É variada a tipologia de ataques ao ciberespaço, todavia, no presente estudo, debruçamo-nos com mais detalhe sobre os ataques informáticos perpetrados nos serviços de *homebanking*. O *phishing* e o *pharming* surgem como as técnicas de fraude informática mais recorrentes, as quais nem sempre são fáceis de prever e combater, devido à capacidade de anonimato dos piratas informáticos.

De tais esquemas fraudulentos sobrevêm prejuízos que serão repartidos em conformidade com as condutas adotadas pelas partes no contrato – utilizador e prestador de serviço de pagamento. No seio de uma relação negocial complexa, a distribuição justa dos danos obtidos far-se-á em função do cumprimento de deveres ou falta deles. Assim, à luz do novo Regime Jurídico dos Serviços de Pagamento e Moeda Eletrónica, os deveres de conduta das partes na relação contratual são a pedra de toque em sede de repartição de tais prejuízos.

Serve o presente estudo para apurar a quem caberá a responsabilidade pelos danos causados em sede de utilização indevida do sistema de *homebanking.*

Atualmente, as alterações na área dos sistemas de pagamentos têm estado no centro das atenções devido à nova Diretiva de Sistemas de Pagamentos, Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro, relativa aos serviços de pagamento no mercado interno, que tem como foco a segurança, quer das instituições quer dos consumidores e na proteção de dados do utilizador.

Palavras-Chave: ciberespaço, cibersegurança, *homebanking*, fraude informática, *phishing*, *pharming*

- ABSTRACT –

The dissemination of new information and communication technologies has increased the practice of "new crimes": computer crimes.

The typology of attacks on cyberspace is varied, however, in the present study, we look in more detail about the cyber attacks perpetrated in the services of homebanking. Phishing and pharming appear as the most recurring computer fraud techniques, which are not always easy to predict and combat, due to hackers anonymity.

Such fraudulent schemes result in losses that will be allocated in accordance with the conduct of the parties in the user agreement. Within a complex negotiating relationship, the fair distribution of the damages obtained will be done in function of the fulfillment of duties or lack thereof. Thus, in light of the new Legal Regime of Payment and Electronic Currency Services, the parties' duties in the contractual relationship are the touchstone in the allocation of such damages.

The present study is used to determine who will be responsible for damages caused by improper use of the homebanking system.

Currently, changes in the area of payment systems have been in the spotlight due to the new Payment Systems Directive, Directive 2015/2366 of the European Parliament and of the Council of 25 November on payment services in the European Union internal market, which focuses on the security of both institutions and consumers and on user data protection.

Keywords: cyberspace, cybersecurity, homebanking, computer fraud, phishing, pharming

- INTRODUÇÃO –

As tecnologias de informação e comunicação são, indubitavelmente, um motor de desenvolvimento económico, facilitando a troca de informações de modo bastante célere. Estamos, atualmente, ante uma nova realidade, altamente dependente da tecnologia, que obriga ao armazenamento de grandes quantidades de informação, o que, por sua vez, incorpora graves riscos, capazes de pôr em causa a segurança e soberania de um país.

A Internet tem promissoras potencialidades, mas também um leque alargado de vulnerabilidades. Neste palco de tendência universal que é a Internet, coexistem fenómenos ilícitos e árduos de combater.

A veloz evolução tecnológica revolucionou, entre tantas outras coisas, as relações bancárias, assistindo-se atualmente à possibilidade de realizar operações bancárias e de aceder à distância a todos os serviços prestados pelos bancos por via da Internet.

É deste fenómeno que nos ocuparemos ao longo do presente estudo: o *homebanking*.

Debruçar-nos-emos, em particular, sobre as práticas ilícitas a ele associadas, onde ganha papel de destaque a pirataria e fraude informáticas, mormente quando o anonimato surge como elemento potenciador desse tipo de comportamentos.

Para o efeito, a estrutura do trabalho estará centralizada primeiramente na análise do *homebanking*, enquanto contrato-quadro, no qual as partes ficam vinculadas ao exercício de condutas diligentes.

De seguida, teremos a oportunidade de aprofundar a fraude informática no *homebanking*, *maxime* através do *phishing*, *spyware* e do *pharming*.

Como resultado dos esquemas fraudulentos violadores da segurança na utilização dos instrumentos de pagamento, impõe-se a questão central do nosso estudo e à qual, a devido tempo, daremos resposta - quem suporta os prejuízos decorrentes de tal utilização indevida?

Por fim, concluiremos com a abordagem comunitária sobre este problema, transposta para o ordenamento jurídico português através do novo Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (DL n.º 91/2018, de 12 de novembro), fazendo a

análise dos seus objetivos no seio de um setor sujeito a práticas fraudulentas constantes em sede de *homebanking*.

Apresentados o objeto e a estrutura do nosso trabalho, estamos em condições de dar início ao nosso percurso pelo tema.

- CAPÍTULO I -
A TRANSFORMAÇÃO DIGITAL DO SETOR BANCÁRIO

A informatização da sociedade é uma realidade tão coetânea quanto a inovação tecnológica do setor bancário, assistindo-se a um indubitável aumento das transferências de fundos através de meios eletrónicos.

A utilização da informática nas operações do quotidiano tornou-se inevitável e o setor bancário esteve sempre na vanguarda do fenómeno da *digitalização financeira*.[1]

Compreende-se facilmente esta progressiva desmaterialização dos meios de pagamento. Se por um lado o cliente é cada vez mais exigente com os serviços disponibilizados pelo seu banco, por outro a digitalização desses serviços traz uma redução notória no tempo de execução das operações bancárias e, bem assim, uma melhoria da qualidade dos serviços prestados.

O recurso à Internet e aos dispositivos móveis, como meios de viabilização do acervo de produtos e serviços bancários, tornou-se, pois, um imperativo e marca a modernização do setor bancário, movido pelo desiderato de um aperfeiçoamento constante e da satisfação das necessidades dos seus clientes.[2]

Em rigor, a comercialização de produtos e serviços bancários de *homebanking* através da Internet, de dispositivos móveis (*smartphones* e *tablets*) e de aplicações móveis (*apps)* espelham aquilo que se pode designar hoje como um *ecossistema digital.* São estes os canais digitais que permitem ao cliente aceder aos serviços bancários a qualquer momento, em qualquer lugar e de um modo mais rápido que os canais tradicionais.

---

[1] Tornaram-se vulgares as expressões *cashless society* ou *paperless society*, caracterizando o rumo da evolução da sociedade no que respeita aos meios de pagamento, cfr. GUIMARÃES, MARIA RAQUEL**,** *As Transferências electrónicas de fundos e os cartões de débito*, Almedina, Coimbra, 1999, p.13.

[2] Nas palavras de MONTEIRO, VASCO, "Transformação digital do sector bancário. Desenvolvimentos recentes e futuros no quadro legal e regulatório" in *InforBANCA 111, nov'17-fev'18,* p. 25, "A transformação digital representa para o sector bancário: uma *necessidade* de acompanhar as novas tendências tecnológicas, demográficas e os hábitos de consumo e de comportamento das novas gerações – *millenials*; uma oportunidade para represar os seus processos internos, de forma a tornar-se mais eficiente, reduzindo custos e aumentando a eficácia; um *desafio* decorrente da alteração no modelo de negócio". No mesmo sentido FERREIRA, ANTÓNIO PEDRO DE AZEVEDO, *A relação negocial bancária – conceito e estrutura*, Lisboa, Quid Iuris, 2005, pp.70-73.

Ora, é este o *punctum saliens* do *homebanking*: permitir aos seus clientes realizar as operações bancárias (tradicionalmente levadas a cabo nos balcões das sucursais), em qualquer parte e em tempo real, servindo-se para o efeito dos *supra* especificados canais digitais.

A segurança dos serviços de *homebanking* é assegurada através da existência de chaves e combinações numéricas que são do exclusivo conhecimento do utilizador. Todavia, paradoxalmente, o principal óbice com que a utilização dos canais digitais se depara é precisamente a segurança dos clientes, das suas transações e dos seus dados pessoais, surgindo o *phishing*, o *pharming*, o roubo de identidade e o *malware* como alguns dos principais riscos de segurança identificados pelas instituições bancárias.[3]

Em rigor, *"A Internet tem vindo a converter-se num novo campo de batalha não convencional, cujos rostos invisíveis tendem paulatinamente a dominar o ciberespaço, dotando-se de uma arma que representa uma maior perigosidade e ameaça do que a nuclear, num cenário virtual dotado de soldados digitais devidamente preparados para actuar em ambiente de ciberguerra. A arma por excelência no ciberespaço reside na capacidade de enviar códigos que consigam quebrar todo o tipo de protocolos de segurança nas mais diversas redes informáticas*.".[4]

Partindo desta ideia, o ciberespaço, enquanto *domínio caracterizado pelo uso de equipamentos electrónicos e de espectro electromagnético para armazenar, modificar e trocar dados por via de sistemas em rede*[5], detém uma série de caraterísticas que fazem dele uma realidade detentora de um leque de vulnerabilidades.

Convém, pois, antes de mais, densificar o alcance do conceito de ciberataques, entendidos como "*ataques lançados geralmente a partir de um computador, recorrendo ao método de intrusão e que tem como finalidade adquirir, explorar, perturbar, romper, negar, degradar ou destruir informação constante em computadores ou em redes de*

[3] *Vide* a este propósito o contributo dos resultados do questionário às instituições financeiras, de 2016, elaborado pelo Banco de Portugal, *Comercialização de produtos e serviços bancários nos canais digitais em Portugal*, disponível em www.clientebancario.bportugal.pt.
[4] Cfr. MARTINS, MARCO, "Ciberespaço: uma nova realidade para a segurança internacional", *in Nação e Defesa*, 2012, Instituto da Defesa Nacional, p. 133.
[5] Cfr. FREIRE, VICENTE, " Cibersegurança e Ciberdefesa: a inevitabilidade de adoção de uma estratégia nacional", in *Revista Segurança e Defesa*, 21, maio-agosto de 2012, p. 53.

computadores, com sistemas e equipamentos electrónicos ligados a outros equipamentos ou sistemas, ou que partilhem a mesma estrutura de energia ou o mesmo espaço de emissão electromagnética, bem como os próprios computadores, redes de computadores, sistemas e equipamentos".[6]

Ora, o modo como a Internet está arquitetada, a capacidade de ubiquidade do ciberespaço e o incremento do problema do anonimato são os ingredientes necessários à prática de intrusões e incidentes[7], pelo que o conceito de *cibercrime* abrange todos os atos criminosos cometidos por via da utilização de redes de comunicação eletrónicas contra essas mesmas redes ou sistemas.

Assim, entende-se que a prática de *cibercrime* não corresponde, naturalmente, a uma categoria específica de crime, mas, pelo contrário, está geralmente associado a um grupo de infrações relacionadas com o uso de computadores e de redes eletrónicas.[8]

E é justamente daquelas que afetam o setor bancário, que nos ocuparemos nos capítulos subsequentes.

---

[6] Cfr. MOREIRA, JOÃO MANUEL DIAS, "O impacto do ciberespaço como nova dimensão nos conflitos", in *Boletim Ensino*, Investigação n.º 13, 2012, disponível em www.ium.pt.

[7] Segundo SANTOS, RITA COELHO, *O tratamento jurídico-penal da transferência de fundos monetários através da manipulação ilícita dos sistemas informáticos*, Coimbra, Coimbra Editora, 2005, p. 239, os ataques informáticos podem ser cometidos por qualquer pessoa, não obstante a sua prática se encontrar socialmente referenciada a indivíduos com particulares conhecimentos técnicos; De acordo com GAMEIRO, CARLOS, "O risco da informação em ambiente electrónico", in *AAVV, Estudos de Direito e Segurança*, Coimbra, Almedina, 2007, p. 130, apesar de reconhecer que a figura dos piratas informáticos traz associada a sua experiência e investimento na área tecnológica, não descura que agressores com conhecimentos técnicos limitados também possam levar a cabo ataques bem sucedidos, pois "*estão disponibilizadas muitas ferramentas de fácil consulta e execução"*.

[8] A este propósito, *vide* com mais detalhe GILMOUR STAN, "Policing crime and terrorism in cyberspace: ano overview", 2014, disponível em www.s3.amazonaws.com

- CAPÍTULO II -
HOMEBANKING

Decorrentes do fenómeno de evolução tecnológica, recrudesceram novas práticas no setor bancário, nomeadamente associadas à digitalização financeira, fenómeno que trouxe novos serviços financeiros de retalho caracterizados pela simplicidade e celeridade na utilização dos serviços de pagamento. Assim, assistimos ao acesso à distância de operações bancárias, assim como aos inúmeros serviços decorrentes da utilização de serviços de pagamento, cujo *modus operandi* decorre por via da Internet.

Surge, assim, o serviço de *homebanking* que se revela, no *plano jurídico, como uma 'teia' de contratos, a uma série de relações jurídicas complexas*.[9]

Neste domínio, dedicaremos as próximas reflexões à análise do negócio jurídico através do qual é possível utilizar um instrumento de pagamento eletrónico.

1. CONTRATO DE UTILIZAÇÃO DE INSTRUMENTOS DE PAGAMENTO

Em consonância com as considerações expendidas no Acórdão do Tribunal da Relação de Coimbra, de 20 de setembro de 2016, "*a emissão/utilização de cartões bancários, assenta numa relação triangular que tem como vértices um banco ou outra entidade autorizada (emitente) e o cliente (aderente) através do qual se atribui a este um direito de acesso ao sistema operativo especial de pagamentos, criado e gerido pela entidade emitente, constituindo o cartão um instrumento de pagamento que permite ao respectivo titular a respectiva utilização para a aquisição de bens e serviços, com pagamento diferido, junto de um terceiro*".[10]

Para a utilização de um instrumento de pagamento eletrónico, pressupõe-se a prévia celebração de um contrato, concluído entre o cliente e o prestador de serviços, do qual resulta não só a emissão do cartão bancário de crédito ou débito, como ainda são preconizadas as regras de utilização do instrumento de pagamento eletrónico, bem como os direitos e deveres implícitos às partes no contrato.

---

[9] *Vide* a este propósito GUIMARÃES, MARIA RAQUEL, *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos*, Coimbra, Wolters Kluwer/Coimbra Editora, 2011, pp.174 – 175;
[10] Processo n.º 183554/14.0YIPRT.C1, disponível em http://www.dgsi.pt, consultado em 03.01.2018;

Acompanhamos, neste sentido, a posição propugnada por Maria Raquel Guimarães, que destaca que *o contrato de utilização de um cartão de pagamento não surge "desgarrado", como facto jurídico isolado, mas antes aparece como um desenvolvimento de relações jurídicas anteriores (ou contemporâneas) à sua conclusão.*[11]

No seguimento da génese do contrato de utilização de instrumento de pagamento *supra* referida, assente na anterioridade do contrato celebrado entre o utilizador e a instituição bancária, cumpre relevar a cronologia das subsequentes relações jurídicas provenientes das sucessivas utilizações do cartão, que fazem deste contrato um contrato-quadro.

Destarte, *o contrato de emissão ou de utilização não surge como uma "ilha", como um facto jurídico isolado, gerador de uma relação jurídica única entre determinados sujeitos jurídicos. Antes integra um conjunto mais complexo de relações que se estabelecem, por um lado, entre os mesmos sujeitos, e, por outro, entre estes e terceiros.*[12]

Rege-se, assim, o contrato de utilização de instrumento de pagamento, que se afigura como uma manifestação da revolução tecnológica sentida nas transferências eletrónicas de fundos, o qual suscita complexos problemas de direito probatório, nomeadamente quanto à repartição do ónus da prova e distribuição do risco.[13]

A) CONTRATO-QUADRO

Num momento precedente à celebração de operações de transferência eletrónica de fundos, decorre a celebração de um *contrato - quadro* o qual se funda numa "*relação de colaboração estável, duradoura, de conteúdo múltiplo, cuja execução implica designadamente, a celebração de futuros contratos entre as partes (…)".*[14]

[11] Cfr. GUIMARÃES, MARIA RAQUEL, *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos*, Coimbra, Wolters Kluwer/Coimbra Editora, 2011, p.179.
[12] *Idem*, p.180.
[13] Acórdão do Tribunal da Relação de Lisboa, de 26 de dezembro de 2010, processo n.º 1943/09.1TJLSB.L-7, disponível em http://www.dgsi.pt, consultado em 12.01.2018.
[14] MONTEIRO, ANTÓNIO PINTO, *Contratos de distribuição comercial*, Almedina, 2004, p.108.

Gradualmente, a locução *contrato-quadr*o e a complexidade contratual que sustenta a estrutura de contratos para utilização de instrumentos de pagamento foi ganhando reconhecimento e ponderação por parte do legislador nacional, conseguindo, assim, enquadramento no nosso ordenamento jurídico.

Com o DL n.º 91/2018 de 12 de novembro, que aprova o novo Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, transpondo a Diretiva (UE) 2015/2366, é clarificada a conceção de *contrato-quadro* e os elementos basilares sobre os quais assenta a sua estrutura contratual. Assim, do disposto no artigo 2.º, alínea *i)* do presente diploma, consta uma definição clara de contrato-quadro, o qual representa o *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.*

Ao dia de hoje, com a entrada em vigor Diretiva 2015/2366/CE, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, que revogou a Diretiva 2007/64/CE, verificamos que a definição de contrato-quadro se mantém nos mesmos termos que a anterior Diretiva. De igual modo, também o âmbito de aplicação e definição dos diferentes momentos contratuais do contrato-quadro, são expressamente contemplados à luz da nova Diretiva.

Neste sentido, no plano jurídico, o contrato - quadro enforma-se numa complexidade de relações jurídicas que se complementam entre si, sustentando uma verdadeira teia de contratos.[15]

Da complexidade contratual que o contrato-quadro envolve em relação às sucessivas operações de transferência eletrónica de fundos ordenadas através da Internet, cumpre

[15] Cfr. GUIMARÃES, MARIA RAQUEL, *O contrato-quadro (…),* pp. 174 e 175; Refere ainda a autora, a propósito da utilização de cartões, que "*os procedimentos necessários para desencadear uma transferência electrónica de fundos que satisfaça o credor do titular de um cartão de pagamento, na sua aparente singeleza, são na realidade sustentados por três feixes de relações jurídicas interligadas entre si, que se estabelecem entre o titular do cartão e o beneficiário da ordem de pagamento, entre o mesmo titular e o banco emissor do cartão e entre este último e o beneficiário do pagamento. Isto para não mencionar uma quarta relação, que se estabelece entre o banco emissor do cartão e o banco beneficiário do pagamento - uma vez que estes, as mais das vezes, não coincidirão -, na medida em que este último não assume um papel autónomo na operação de pagamento electrónico, actuando como um auxiliar o primeiro banco".*

salientar que *sempre que o utilizador de um serviço de banca electrónica emite uma ordem de pagamento – mandato de pagamento – a favor de um terceiro, é celebrado um novo contrato de execução ou de aplicação do contrato de base anterior, que se rege pelo programa contratual definido, num primeiro momento, no contrato-quadro.*[16]

Conforme anteriormente explanado, somos de referir que cada ato de pagamento configura um ato isolado neste leque de operações agregadas ao contrato-quadro, sendo que da execução de cada uma individualmente resultam diferentes destinatários, montantes, circunstâncias temporais, entre outras condições.

Também a doutrina ecoa a ideia *supra,* referindo que a cada utilização do instrumento de pagamento decorre uma operação isolada da qual resulta uma declaração de vontades, existindo, por isso, uma *renovação de vontades*[17] a cada operação de pagamento, quer da parte do utilizador, quer da parte do prestador de serviços.[18]

Cumpre, pois, avultar que uma nova emissão de uma ordem de pagamento a favor de terceiro, decorrente da utilização dos canais digitais colocados à disposição pelo banco, desencadeia a celebração de um novo contrato de execução do contrato de *homebanking.* Assim, o contrato de *homebanking é, por sua vez, também um contrato – quadro relativamente às sucessivas operações de transferência eletrónica de fundos ordenadas através da internet*.[19]

Destarte, a inserção do contrato de *homebanking* numa relação contratual complexa, potencia a celebração de uma panóplia de contratos subsequentes, intrinsecamente

[16] GUIMARÃES, MARIA RAQUEL, "A repartição dos prejuízos decorrentes de operações fraudulentas de banca eletrónica *(home banking*): anotação ao Acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09", in *Cadernos de Direito Privado*. Braga: CEJUR. Nº 41 (janeiro/março 2013) p. 59.

[17] De acordo com GUIMARÃES, MARIA RAQUEL, *I Congresso de Direito Bancário*, Almedina, 2015, p. 123,*"a autorização genérica que possa ser prestada no contrato base de utilização do instrumento de pagamento (no contrato-quadro), não é suficiente para desencadear a operação. A lei exige uma renovação da vontade do utilizador do serviço, embora se baste, com a adopção dos comportamentos fixados no contrato para o efeito: marcação de um código secreto num terminal de um computador instalado no estabelecimento do beneficiário, assinatura manual, inserção de uma ou mais chaves de acesso no site do banco, através do teclado do computador do utilizador, no caso do homebanking, etc".* Do lado do utilizador de serviços, também é referido pela autora que também estará implícita a manifestação da sua vontade na concretização da ordem de pagamento. Assim, leia-se *"o prestador de serviço de pagamento é chamado a conferir a conformidade da ordem de pagamento recebida e a manifestar a sua concordância com a mesma".*

[18] *Idem.*

[19] GUIMARÃES, MARIA RAQUEL, "A repartição dos prejuízos (…)", p. 59.

ligados ao contrato quadro, afigurando-se, assim, como um *contrato de contratos, um contrato que antecipa futuros contratos*.[20]

Conforme exposto no Acórdão de 29 de fevereiro de 2018, o Tribunal da Relação do Porto considerou que "*a utilização do serviço de pagamento através da respetiva conta de pagamento pressupõe, todavia, a prévia celebração de um contrato quadro – "o) 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; ou no caso de operação de pagamento de caráter isolado a celebração de um contrato de serviço de pagamento de caráter isolado (cfr. artigos 46º e segs. e 51º e segs. do RJSP). No caso, pelas operações individuais e sucessivas que ocorreram, necessariamente que a sua execução estava dependente da celebração de um contrato quadro".*[21]

Face ao exposto, e em resposta à recorrente utilização eletrónica diária da multiplicidade de operações de transferências de fundos, com recurso aos diversos canais digitais disponibilizados pelas instituições financeiras, que permitem a sua execução e conclusão de uma forma célere, eficaz e simples, cumpre avultar que cada operação individualmente concluída, não é mais do que um *acordo de vontades, não se cingindo a simples atos de execução de um contrato anterior*.[22]

B) INSERÇÃO NO COMPLEXO CONRATUAL

O enquadramento do *homebanking* no seio da relação bancária inicia-se com a celebração do contrato de abertura de conta, entendido como um *contrato bancário matriz,* [23] no qual é constituído o quadro geral de regulação de negócio que venha a ser posteriormente celebrado pelas partes.

Neste sentido, e nas palavras de Maria Raquel Guimarães, *a realização de operações de home banking – transferências electrónicas, pagamentos de serviços, entre outras – pressupõe um complexo de contratos que permite regular, de antemão, as relações*

[20] *Idem.* p.151.
[21] Processo n.º 572/17.0T8PRT.P1, disponível em http://www.dgsi.pt, consultado em 03.04.2018.
[22] GUIMARÃES, MARIA RAQUEL, *O Contrato-quadro* (…), p.133.
[23] ANTUNES, JOSÉ ENGRÁCIA, *Direito dos Contratos Comerciais*. Coimbra: Almedina, 2009, p.484.

entre o banco prestador do serviço e o seu cliente, utilizador do mesmo, simplificando os procedimentos a adoptar no momento em que essas operações são concretizadas.[24]

Entendeu ainda o Tribunal da Relação de Lisboa, no Acórdão de 24 de maio de 2012, processo n.º 192119/11.8YIPRT.L1-2, disponível em www.dgsi.pt, que "*O contrato de conta bancária - enquanto contrato nuclear instituinte do tronco comum sobre o qual repousarão todas as relações jurídicas entre banco e cliente, inclusive contratuais, possui um conteúdo negocial complexo do qual fazem parte, necessária ou usualmente, outras convenções acessórias embora autónomas: tal o caso do contrato de conta-corrente bancária e do contrato de depósito*."

Ao abrigo de tal entendimento o contrato de *homebanking* afigura-se distinto dos restantes contratos, apesar de conexos entre si. E conexos mas independentes são, por sua vez, os contratos subsequentes que derivam da *convenção "troncal" da relação banco-cliente*.[25]

Assim, a autonomia do contrato de *homebanking* resulta do acordo de vontades autónomas mas convergentes e articuladas, com fim a permitir a movimentação de fundos na conta pelo cliente através de recurso informático. Deste modo, o contrato de banca eletrónica não é mais do que um contrato de prestação de serviços reconhecido eletronicamente e que constitui a faculdade de utilização do serviço pelo cliente, mediante a adesão ao contrato de banca eletrónica,[26] funcionando autónoma mas intrinsecamente ligado ao contrato de abertura de conta.

Igualmente conexo aos contratos de abertura de conta e de *homebanking* está o contrato de depósito bancário. No seio do nexo funcional que complementa a relação jurídica bancária, o contrato de depósito e o de *homebanking* afiguram-se complementares uma vez que, havendo interesse da parte do cliente na movimentação de fundos disponíveis depositados na conta bancária, poder-se-á recorrer à utilização dos instrumentos de pagamento eletrónico. Assim, o contrato de *homebanking* funciona como um contrato

[24] GUIMARÃES, MARIA RAQUEL, "A repartição dos prejuízos (…)", p. 58.
[25] *Idem.*
[26] Cfr. Acórdão do Tribunal da Relação de Guimarães, de 23 de outubro de 2012, processo n.º 305/09.5TBCBT.G1, disponível em www.dgsi.pt, consultado em 23.02.2018.

acessório e instrumental em relação ao contrato de depósito, fazendo apenas sentido se existir uma relação negocial subjacente, assente na disponibilização de fundos disponíveis para movimentação.

Em suma, da *complexidade constituída a partir da celebração de um contrato de conta e da constituição de depósitos de montantes em conta por parte do cliente ou de abertura de crédito*[27], surge o *homebanking.* Enquadrado numa relação bancária complexa, a utilização de um instrumento de pagamento eletrónico surge como uma faculdade concedida ao cliente mediante a adesão ao contrato de banca eletrónica.

Autónomo mas interdependente em relação a outros contratos, da celebração do contrato de *homebanking* decorre uma complexidade de direitos e deveres que regulam a relação obrigacional duradoura entre as partes utilizador e prestador de serviços de pagamento, aspeto com que nos iremos deter seguidamente.

[27] BARREIRA, CAROLINA, "*Home banking*: a repartição dos prejuízos decorrentes de fraude informática", in *Revista Eletrónica de Direito*, n.º 3, outubro de 2015, Faculdade de Direito da Universidade do Porto, p.8.

- CAPÍTULO III –
DEVERES ASSOCIADOS À UTILIZAÇÃO DE SERVIÇOS DE PAGAMENTO

Do contrato de *homebanking* e da relação obrigacional complexa daí oriunda, emerge uma variedade de direitos e obrigações que recaem sobre as partes na utilização do serviço de pagamento.

A alusão ao Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, adiante designado por RSP, abordado no prévio desenvolvimento relativo ao contrato de *homebanking*, também assumirá, na presente análise, um enquadramento legal relevante, relativo ao conjunto de direitos subjetivos, direitos potestativos e deveres principais nas relações jurídicas estabelecidas entre o utilizador e o prestador de serviços de pagamentos.[28]

1. DO UTILIZADOR

A entidade bancária confere aos seus clientes a possibilidade de utilização de um serviço de *homebanking* para movimentação dos fundos. Trata-se, pois, da prestação principal do banco que confere aos utilizadores a possibilidade de usufruir de um serviço que lhes permita a gestão e movimentação dos fundos disponíveis nas suas contas bancárias.

Assim, a entidade bancária confere a possibilidade de os seus clientes usufruírem de um serviço que lhes permita a gestão e movimentação dos fundos disponíveis nas suas contas bancárias.

Não obstante o direito de utilização de tais serviços, à luz do artigo 110.º do DL n.º 91/2018, de 12 de novembro, relativo ao *supra* referido Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, e que revogou o anterior artigo 67.º constante do DL n.º 317/2009, de 30 de outubro, ao utilizador de serviços de pagamento recaem determinados deveres:

[28] MARIA RAQUEL GUIMARÃES, *O contrato-quadro (…), p*. 279.

A) Dever de utilização correta do serviço de *homebanking*

Ao abrigo do artigo 110.º n.º 1 alínea a) do RSP, o cliente utilizador fica sujeito a deveres de conduta, os quais constituem uma condição *sine qua non* da correta utilização do serviço de *homebanking.*

Do ponto de vista técnico-jurídico, a utilização do serviço de *homebanking* por parte do utilizador, não constitui um dever principal, mas sim instrumental de conduta, mediante o qual o processamento da relação contratual se torna exequível.

Assim, a fim de beneficiar de tal serviço, o utilizador do serviço de *homebanking*, deverá cumprir com determinadas exigências de conduta, às quais estão aliados outros deveres no âmbito obrigacional, nomeadamente o princípio da boa fé, consagrado no artigo 762.º n.º 2 do Código Civil.

B) Dever de comunicação imediata ao banco de qualquer operação abusiva do instrumento de pagamento não autorizada ou do extravio dos códigos de acesso e cartão matriz

Aos deveres acessórios *supra* referidos, acresce ainda um outro dever na ótica do utilizador, consagrado nos termos do artigo 110.º n.º 1, alínea b) do RSP, segundo o qual incumbe ao cliente notificar "sem atrasos injustificados" o banco logo que tenha conhecimento da perda, roubo, ou apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento.

Com efeito, compete ao cliente o dever de comunicação à instituição bancária caso se verifique qualquer irregularidade derivada da utilização abusiva do instrumento de pagamento.

Por outro lado, deverá a instituição bancária disponibilizar a todo o tempo os meios adequados à realização da correspondente notificação por força do artigo 111.º n.º 1 alínea *c)* do RSP. Esta notificação assume uma importância decisiva, uma vez que, estabelece o momento a partir do qual o cliente não suporta as consequências

financeiras resultantes das operações de pagamento, questão que mais adiante analisaremos.

C) Dever de confidencialidade dos dados pessoais e chaves de acesso associados ao *homebanking* e dever de guarda do cartão matriz

À luz do artigo 110.º n.º 2 do RSP, o cliente do serviço de *homebanking* deve adotar medidas que garantam a preservação da eficácia dos respetivos códigos de acesso a este serviço.

Trata-se, pois, de um dever que se reporta à confidencialidade das senhas de acesso inscritas no cartão matriz, facultadas pela instituição bancária e que permitem o acesso ao serviço de *homebanking* e correspondentes operações disponibilizadas ao utilizador.

Assim, uma vez digitados os códigos de acesso e os três dígitos do cartão matriz, o sistema reconhece o utilizador do serviço de banca eletrónica como o legítimo portador de tais dispositivos e, consequentemente, enquanto cliente, poderá usufruir dos serviços disponibilizados eletronicamente.

Sendo este serviço não presencial e realizado à distância, com recurso a um formato eletrónico, mediante a introdução dos dados entregues ao cliente, a instituição bancária valida-os presumindo que está perante o seu verdadeiro portador.[29] Ora, sendo as respetivas operações devidamente autorizadas, mediante a introdução das chaves de acesso, compete a natural exigência do banco ao cliente de um dever de sigilo, guarda e de não transmissão a terceiros, ainda que seus mandatários, dos dispositivos de segurança em causa, sob pena de toda a base de confiança em que assenta este contrato se desvirtuar.

[29] FARIA, JOSÉ MANUEL, "Acesso a contas bancárias por terceiros no âmbito de operações de pagamento", in *Revista da Banca*, Lisboa: Associação Portuguesa de Bancos. N.º 71 (janeiro/junho 2011), p.32.

2. DO PRESTADOR DE SERVIÇOS

A) Dever de emissão e entrega do cartão matriz e códigos de acesso

Com a utilização do serviço de *homebanking,* surge o dever de emissão e entrega ao utilizador do respetivo cartão matriz e correspondentes códigos de acesso (credenciais), com vista à correta e legítima autenticação.[30]

Trata-se de um dever acessório ao dever principal constante da alínea a) do n.º 1 do artigo 111.º do RSP.

Deste modo, cabe ao prestador de serviços o dever de, exclusivamente, entregar ao utilizador do serviço de *homebanking* as credenciais necessárias para autenticação, assegurando a não interceção por parte de terceiros. A manifestação deste dever de cuidado por parte do prestador de serviço, é feita logo que se proceda ao envio do cartão e códigos de acesso. Neste sentido, e à luz do disposto no artigo 111.º n.º 2 do RSP, aquando do envio ao ordenante do instrumento de pagamento ou dos respetivos dispositivos de segurança personalizados, e se verificados quaisquer riscos associados ao extravio ou interceção dos dispositivos de segurança personalizados por terceiros estranhos à relação contratual, tais correrão por conta do prestador do serviço de pagamento.

O cartão matriz, bem como os códigos de acesso conferidos ao cliente pelo prestador de serviços, assumem a função de autenticação, sendo que a introdução dos mesmos pelo cliente, torna possíveis as operações de crédito ou de débito.

O sistema de autenticação é hoje um ponto de fragilidade nos serviços de pagamento eletrónicos, pelo que a nova Diretiva 2015/2366, de 25 de novembro de 2015, relativa

[30] No entendimento plasmado no Acórdão do Tribunal da Relação de Coimbra, de 15 de junho de 2010, processo n.º 1408/08.9TBACB.C1, disponível em www.dgsi.pt, consultado em 15.02.2018: *"A emissão de um cartão de débito tem assim como requisito necessário a existência de um contrato de depósito bancário, contrato este que é, digamos, a sua causa remota. No entanto a causa próxima da emissão de um cartão de débito é, já não o depósito bancário, mas sim um outro contrato, comummente designado "contrato de utilização". Mediante a conclusão de um contrato de utilização, o cliente do banco adquire um direito obrigacional que lhe permite utilizar um "cartão de plástico" em terminais POS e ATM, conservando o banco, todavia, o direito de propriedade sobre o mesmo cartão".*

aos serviços de pagamento no mercado interno, transposta para a ordem jurídica portuguesa no DL n.º 91/2018, de 12 de novembro, veio implementar exigências adicionais a nível de autenticação forte na autorização da operação de pagamento, tendo sido

A autenticação forte pressupõe uma utilização mais rigorosa para o início e processamento de pagamentos eletrónicos, com vista à redução de risco de fraude para todos os meios de pagamento, sejam os mais tradicionais ou os mais atuais. A confidencialidade dos dados financeiros do utilizador, são uma premissa que se pretende assegurar com as novas exigências comunitárias definidas na nova Diretiva de Serviço Pagamentos, que adiante se abordará.

B) Dever de garantia de disponibilidade a todo o momento dos meios adequados que confiram ao utilizador a possibilidade de comunicação de fraude

No seguimento dos deveres de conduta *supra* referidos, compete ao banco prestador de serviço de pagamento o dever de garantir a disponibilidade a todo o momento dos meios adequados para que, em caso de ocorrência de fraude, o utilizador do serviço possa comunicar ao banco o ocorrido.

Assim, caso se verifique uma situação de operação não autorizada pelo utilizador incumbe ao banco o dever de disponibilizar, a todo o tempo, os meios adequados à realização desta notificação por força do artigo 111.º n.º 1, alínea c) do RSP. Tal notificação assume relevância decisiva, uma vez que estabelece o momento a partir do qual o cliente não suporta as consequências resultantes de fraude ou operações não autorizadas.

Além disso, pelo artigo 111.º n.º 1, alínea d) do RSP, e no seguimento do *supra* referido, incumbe ao banco o dever de disponibilizar ao utilizador de serviços de pagamento, os meios necessários para fazer prova de que efetuou tal comunicação, sendo um dever que deverá ser cumprido a pedido do respetivo utilizador do serviço.

C) Dever de prestação de um serviço de *homebanking* eficaz e seguro

A celeridade e eficiência que o serviço de *homebanking*, tem inerentes riscos próprios associados ao seu funcionamento. Em virtude dos mesmos, espera-se, quer da parte do cliente, quer do prestador de serviços de pagamento, condutas diligentes, cabendo em particular à entidade bancária o dever de assegurar a robustez dos sistemas informáticos e, bem assim, garantir que não se verificam falhas técnicas durante as operações de pagamento. Daqui resulta um dever acessório de conduta que assenta na qualidade e segurança do serviço conferido ao cliente, conforme resulta do artigo 73.º do Regime Geral das Instituições de Crédito e Sociedades Financeiras, doravante "RGICSF".

Assim, compete ao banco, enquanto prestador do serviço de banca eletrónica, criar um sistema informático de acesso à conta bancária que seja seguro e no qual o utilizador tenha a necessária confiança para realizar as suas operações de pagamento.[31]

Pese embora o *supra* referido, e não descurando a exigência da prestação de um serviço seguro, importa notar que o banco deverá, da mesma forma, prestar um serviço eficiente na sua utilização, conforme se estipula no artigo 111º n.º 1 alíneas *b) e e)* do RSP.

D) Dever de informação acerca das medidas que o utilizador deve adotar para preservar a segurança dos códigos de segurança e cartão matriz, como forma de prevenção antifraude

Da relação de confiança gerada entre o banco e o seu cliente, aquando da abertura de conta, nasce um dever lateral de conduta da entidade prestadora de serviços, assente na obrigação de informação das medidas que o utilizador deve adotar para preservar a segurança dos códigos e cartão matriz.

[31] No mesmo sentido, *vide* Acórdão do Tribunal da Relação de Lisboa, de 22 de março de 2018, processo n.º 14202/16.4T8LSB.L1-2, disponível em www.dgsi.pt, consultado em 18.05.2018: *Os clientes reconhecem aos bancos um superior conhecimento da sua atividade proveniente da sua profissionalização e especialização, confiando que estes atuarão, não só de acordo com normais padrões de diligência e correção ao nível da genérica boa-fé exigida na execução dos contratos (art.º 762.º n.º 2 do CC) ou da sua negociação prévia (art.º 227.º n.º 1 do CC), mas, mais do que isso, esperarão que estes, tal como expressamente enunciado no RGICSF, pautarão a sua atuação por elevados padrões de competência técnica (art.º 73.º do RGICSF), os quais se refletirão na "diligência, neutralidade, lealdade, discrição e respeito consciencioso dos interesses que lhes estão confiados", que deverão nortear as suas relações com os clientes (art.º 74.º RGICSF)".*

Nas palavras de Maria Raquel Guimarães, trata-se de "um dever imposto à entidade bancária de explicar as situações mais comuns de fraude e os perigos específicos dos diferentes serviços que fornece, em função do tipo de utilizador envolvido e dos seus conhecimentos técnicos".[32]

Regulado no artigo 84.º do RSP, o dever de informação é fulcral para elucidar o utilizador das medidas preventivas de deverá adotar para preservação e segurança do instrumento de pagamento.

Qualificado como uma máquina industrial complexa e perigosa,[33] por acarretar um sistema sofisticado e complexo de onde podem brotar técnicas de fraude eletrónica por terceiros, cabe à entidade bancária proteger os utilizadores do serviço de *homebanking*, acautelando-os dos perigos inerentes à sua utilização.[34]

Assim, deve a instituição bancária descrever ao utilizador do serviço de *homebanking* um conjunto de medidas que o mesmo deve adotar para preservar a segurança dos seus cartões de acesso e cartão matriz.

Não obstante o artigo 83.º do RSP caracterizar este dever como um dever de informação pré-contratual, por força da sua remissão para o artigo 84.º, certo é que tal dever acompanhará o decurso do contrato estabelecido.

Assim, numa ótica de prevenção antifraude, os utilizadores deverão ser notificados das condições de acesso ao seu portal de banca eletrónica, bem como de todas as recomendações e regras de segurança, com vista a acautelar eventuais ocorrências fraudulentas. A título de exemplo, salientamos alertas como os de não abertura de mensagens de correio eletrónico com remetente desconhecido; proteção do computador ou dispositivo móvel com antivírus; evitar o acesso à plataforma de correio eletrónico por links; utilização de rede doméstica no momento do acesso às páginas de

[32] Cfr. GUIMARÃES, MARIA RAQUEL, "A repartição dos prejuízos (…)", p. 62.
[33] *Idem.*
[34] Neste domínio, *vide* o Acórdão do Tribunal da Relação de Guimarães, de 25 de novembro de 2013, processo n.º 2869/11.4TBGMR.G1, disponível in http://www.dgsi.pt, consultado em 18.02.2018.

homebanking, entre outras medidas preventivas que visam impedir possíveis esquemas de fraude, como as técnicas de *phishing* e *pharming*, já comumente conhecidas.

- CAPÍTULO IV -
ESQUEMAS FRAUDULENTOS NA BANCA ELETRÓNICA

Feito o enquadramento geral da relação obrigacional inerente ao contrato de *homebanking*, versemo-nos agora sobre a temática da fraude informática da banca eletrónica.

A banca eletrónica (frequentemente designada por *homebanking*, *e-banking*, bancos virtuais ou bancos *online*) corresponde à prestação de serviços bancários com recurso a meios tecnológicos, através da Internet.

Partilhamos, pois, do entendimento de António Menezes Cordeiro, a respeito da simplicidade que os meios informatizados apresentam na prática dos mais variados atos bancários.[35]

Por ser elucidativo, transcreve-se ainda o que sobre o assunto refere o Supremo Tribunal de Justiça, no Acórdão de 18 de dezembro de 2013, a propósito do conceito de *homebanking* que se concretiza *"pela possibilidade conferida pela entidade bancária aos seus clientes, mediante a aceitação de determinados condicionalismos, a utilizar toda a panóplia de operações bancárias, online, relativamente às contas de que sejam titulares, utilizando para o efeito os canais telemáticos que conjugam os meios informáticos com os meios de comunicação à distância, por meio de uma página segura do banco, o que se reveste de grande utilidade, especialmente para utilizar os serviços do banco fora do horário de atendimento ou de qualquer lugar onde haja acesso à Internet*".[36]

---

[35] Cfr. CORDEIRO, MENEZES ANTÓNIO, *Manual de Direito Bancário*, 3.ª edição, Coimbra, Almedina, 2006, pp. 147-150. Em consonância com o entendimento defendido pelo autor, refere GUIMARÃES, MARIA RAQUEL, " As transferências eletrónicas (…)", pp. 43-44, que, "*em todos os sistemas de homebanking o utilizador tem a possibilidade de realizar operações bancárias em tempo real, na medida em que tem acesso direto ao computador do seu banco, que imediatamente debita ou credita a conta do seu cliente, consoante o sentido das ordens emitidas por este (...) A segurança destes serviços é normalmente garantida através da existência de várias combinações numéricas de conhecimento exclusivo do utilizador, que funcionam como códigos secretos de acesso ao sistema, e que terão que ser marcados no teclado do equipamento utilizado para comunicar com a instituição bancária respetiva (...) No entanto, estes dispositivos de segurança revelam-se por vezes insuficientes, principalmente quando é utilizada uma rede de telecomunicações, na medida em que não é possível a um terceiro intercetar uma comunicação deste tipo e decifrar códigos marcados para posteriormente aceder ao sistema."*

[36] Processo n.º 6479/09.8TBBRG.G1.S1, disponível em http://www.dgsi.pt, consultado em 21.02.2018.

Através desta forma de relacionamento entre o banco e o cliente, o banco deve reforçar o compromisso com os seus clientes com vista ao aperfeiçoamento e desenvolvimento da atividade bancária, designadamente pela capacidade de resposta rápida e eficiente, sem descurar, naturalmente, os deveres de informação, lealdade, diligência e transparência inerentes à confiança recíproca entre as partes, tal como se encontra vertido nos artigos 74.º e 77.º do Regime Geral das Instituições de Crédito e Sociedades Financeiras (Decreto-Lei n.º 298/92, de 31/12, com as alterações introduzidas pela Lei n.º 71/2018, de 31/12).

Do anonimato, simplicidade e celeridade nas transações que a Internet facvorece, nasce um palco propício a atuações ilícitas por parte de terceiros.

Como já referido *supra*, é particularmente dramático quando as transferências bancárias pela Internet são feitas à revelia dos titulares das contas.

As modalidades de fraude informática mais recorrentes são o *phishing*, o *spyware* e o *pharming*.

1. *O PHISHING*

O *phishing* traduz-se numa técnica fraudulenta que se concretiza através do envio em massa de mensagens de correio eletrónico com vista à obtenção de dados para o acesso às contas bancárias de terceiros, desenvolvendo-se em duas etapas: primeiramente são enviadas, em massa, mensagens de correio eletrónico não solicitadas, vulgo, *spam*[37], as quais incluem uma ligação para uma página na *web*, com vista a ludibriar a vítima, fazendo-a crer que está a receber um *e-mail* cujo remetente é o seu banco. Clicando na hiperligação, a vítima é automaticamente reencaminhada para uma página, em tudo semelhante à da entidade bancária, mas que, todavia, não corresponde ao seu *site* oficial.

[37] Atento o seu envio maciço, criam não apenas incómodos ao utilizador, como podem, inclusive, bloquear o sistema de receção de mensagens por saturação.

A vítima depara-se, portanto, com uma página *web* que é uma réplica da página oficial do banco[38], onde lhe será solicitada a identificação, informação pessoal e confidencial (tais como o número da conta ou o número de contribuinte) e a aposição das palavras-passe relativas à sua conta bancária, passando os piratas informáticos a conhecer os códigos secretos e a aceder à conta da vítima, sem o seu consentimento.[39]

A página *web* replicada cria no destinatário uma falsa representação da realidade, induzindo-o em erro, gerando a crença de que existe um fundado motivo para agir, razão que leva a vítima a fornecer os seus dados.

Chegados aqui, cumpre aprofundar o elenco de ilícitos criminais contidos no *phishing*. São eles: a falsidade informática, o dano informático, o acesso ilegítimo, a interceção ilegítima e a burla informática, os quais iremos, seguidamente, detalhar.

A) Falsidade informática (artigo 3.º da Lei do Cibercrime)

O crime de falsidade informática, previsto no artigo 3.º da Lei do Cibercrime (Lei n.º 109/2009, de 15/09, doravante "LC") consiste na falsificação de programas ou dados informáticos, consumado pela produção de *dados ou documentos não genuínos*.

Os elementos objetivos tipificadores deste crime são "(…) introduzir, modificar, apagar ou suprimir dados informáticos ou, por qualquer outra forma, interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos (…)".

Por sua vez, são elementos subjetivos específicos deste crime " a intenção de provocar engano nas relações judiciais" e a intenção de que os documentos não genuínos produzidos "sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem".

---

[38] Os *websites* fraudulentos para os quais a vítima é redirecionada, ao serem réplicas da imagem, linguagem e marca identificativas da entidade fidedigna, reconduzem-nos a outro tipo de ilícito criminal: o crime de contrafação, imitação e uso ilegal de marca, plasmado no artigo 320.º do Código da Propriedade Industrial (DL n.º 110/2018, de 10 de dezembro).
Esta contrafação é, no entanto, entendida como um mero ato de execução do crime informático consubstanciado no *phishing*, não sendo, pois, autonomizável.

[39] Cfr. VERDELHO, PEDRO*, "*Phishing e outras formas de defraudação nas redes de comunicação", in *Direito da Sociedade de Informação*, vol. III, Coimbra Editora, 2009, p. 42.; A técnica do *phishing* é ainda descortinada no Acórdão do Supremo Tribunal de Justiça, de 18 de dezembro de 2013, processo n.º 6479/09.8TBBRG.G1.S1 e no Acórdão do Tribunal da Relação do Porto de 07 de outubro de 2014, processo n.º 747/12.9TJPRT.P1, ambos disponíveis em www.dgsi.pt, consultados em 21.02.2018.

Por força da relevância do bem jurídico aqui em causa (segurança das relações jurídicas), este ilícito criminal tem uma natureza pública.

A previsão deste crime visa proteger a segurança das relações jurídicas enquanto interesse público essencial que ao próprio Estado de Direito compete assegurar, e não a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e de dados informáticos.[40]

B) Dano informático, acesso ilegítimo e interceção ilegítima (artigos 4.º, 6.º e 7.º da LC)

A atividade de *phishing* é prosseguida através de *malware*, usado tanto para espiar o computador da vítima, como para redirecionar o seu *browser* para URL´s falsos.[41]

Ora, a utilização desse *malware* origina a consumação dos três tipos de ilícitos criminais em epígrafe. Vejamos:

i) A instalação de *malware* no computador ou no *browser* para alterar ou afetar a sua capacidade de acesso à Internet configura um crime de dano relativo a programas informáticos, tal como se encontra vertido no artigo 4.º, n.º 1 da LC;[42]

ii) A utilização de *malware*, consubstanciando o *modus operandi* do pirata informático com vista à monitorização do computador da vítima, configura um crime de acesso ilegítimo, tal como previsto no artigo 6.º da LC, cujos elementos tipificadores se encontram nos n.ºs 1 e 2 do referido artigo.[43] Por se mostrar elucidativo, transcreve-se o

[40] Nas considerações expendidas pelo Acórdão do Tribunal da Relação do Porto, de 24 de abril de 2013, processo n.º 585/11.6PAOVR.P1, disponível em www.dgsi.pt, consultado em 21.02.2018, "O bem jurídico tutelado pelo crime de falsidade informática p. e p. pelo artigo 3º, n.ºs 1 e 3 da Lei n° 109/2009, de 15.09, não é o património, mas antes a "integridade dos sistemas de informação" através do qual se "pretende impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados".
No mesmo sentido, *vide* acórdão do Tribunal da Relação do Porto, de 21 de novembro de 2012, processo n.º 1001/11.9JAPRT.P1 e acórdão do Tribunal da Relação de Lisboa, de 30 de junho de 2011, processo n.º 189/09.3JASTB.L1-5, disponíveis em www.dgsi.pt, consultados em 21.02.2018.

[41] Cfr. GERALDES, ANA VAZ, "*Phishing*: fraude online", in *Revista da Faculdade de Direito da Universidade de Lisboa,* 2013, Coimbra Editora, p. 93.

[42] "Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa".

[43] "1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.
2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto

entendimento no Tribunal da Relação de Coimbra, no Acórdão de 17 de fevereiro de 2016, processo n.º 2119/11.TALRA.C2, disponível em www.dgsi.pt: "*Comete o crime de acesso ilegítimo (Artigo 6º, nºs 1 e 4, al a, da Lei nº 109/2009), o inspetor tributário que, por motivos estritamente pessoais, acede ao sistema informático da Autoridade Tributária, consultando declarações de IRS de outrem. O tipo subjetivo daquele ilícito penal não exige qualquer intenção específica (como seja o prejuízo ou a obtenção de benefício ilegítimo), ficando preenchido com o dolo genérico de intenção de aceder a sistema)".*

O bem jurídico protegido nesta sede é a segurança dos sistemas informáticos, como esclareceu o Tribunal da Relação do Porto, no Acórdão, de 08 de janeiro 2014, processo n.º 1170/09.8JAPRT.P2, disponível em www.dgsi.pt, ao entender que "*O crime de acesso ilegítimo, previsto no Artigo 6º da Lei do Cibercrime (Lei nº 109/2009) incrimina exatamente a mesma factualidade que era incriminada pelo crime correspondente (Artigo 7º da Lei nº 109/91). Todavia, na lei nova, não se exige qualquer intenção específica (por exemplo, a de causar prejuízo ou a de obter qualquer benefício ilegítimo), apenas se exigindo dolo genérico. O bem jurídico protegido é a segurança dos sistemas informáticos*."

iii) Por fim, a utilização de *malware* pode ainda ser visto como a concretização de um crime de interceção ilegítima, ao abrigo do artigo 7.º, n.º 1 da LC. Trata-se de "intercetar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes", "sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele", especificando-se ainda no n.º 2 que constitui crime de interceção ilegítima "disseminar ou introduzir num ou mais sistemas informáticos, dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas", descritas no n.º 1.[44]

executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior."

[44] Cfr. GERALDES, ANA VAZ, "*Phishing*: fraude online", in Revista da Faculdade de Direito da Universidade de Lisboa, 2013, Coimbra Editora, p. 94.

Para efeitos do artigo 2.º, alínea e) da LC, a interceção é "o ato destinado a captar informações contidas num sistema informático através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros".

Nesta sede, somos de salientar engenharias enganosas, que se afiguram como variantes do *phishing,* tais como o *Smishing* e *Vishing*, mecanismos ilícitos de captação de informação pessoal do cliente, através de mensagens de texto (*SMS*) e sistema de voz automático, enviadas para o telefone do usuário, criando uma sensação de urgência para facultar de imediato as suas informações pessoais, nomeadamente dados bancários.

Face a tais riscos, torna-se imperativa a proteção do bem jurídico segurança e privacidade das comunicações eletrónicas.

C) Burla informática (art. 221.º do Código Penal)

O crime de burla surgiu para penalizar as formas de captação do alheio por via de meios ardilosos. Com a crescente utilização dos computadores e da Internet, o legislador sentiu a necessidade de introduzir um novo tipo de crime: a burla informática (art. 221.º do Código Penal).[45] [46]

A dimensão típica do crime de burla informática remete para a realização de actos e operações específicas de intromissão e interferência em programas ou utilização de

[45] Com precisão, CORREIA, PEDRO RIBEIRO e JESUS, INÊS ANDRADE, "Combate às transferências bancárias ilegítimas pela Internet no direito português: entre as experiências domésticas e políticas globais concertadas", in *Revista Direito GV*, maio-agosto 2016, p. 545, assinalam a conveniência em se encontrar previsto o crime de burla informática, evidenciando a insuficiência do crime de burla, vertido no art. 217.º do CP, para as manipulações dos sistemas e dados informáticos: "Atentando nos casos em que os burlões enviam um e-mail a pedir os dados bancários do titular da conta e, depois de saberem o código de acesso à conta bancária através da Internet, transferem uma quantia monetária sem a sua autorização, verifica-se que o elemento típico consistente na prática, pelo burlado, de atos causadores de prejuízo patrimonial não está preenchido. Na verdade, o e-mail enviado sob a capa do banco pode ser considerado como um facto provocado astuciosamente. Além disso, o titular da conta é efetivamente induzido em erro por esse e-mail. No entanto, não é a cedência do código de acesso pelo titular, mas antes a transferência pelo burlão que provoca o prejuízo patrimonial. Logo, o crime de burla não se mostra completo. Pode ainda afirmar-se que os computadores não são suscetíveis de erro ou engano, uma vez que essa é uma característica especificamente humana."

[46] A burla informática prevista no n.º 1 do art. 221.º do CP é um crime semipúblico. Por conseguinte, o procedimento criminal depende da apresentação de queixa por parte do ofendido ou de outra pessoa a quem a lei confira esse direito, ao abrigo dos artigos conjugados 113.º e 116.º do CP e artigo 49.º do CPP. O n.º 3 do art. 221.º do CP consagra a punibilidade da burla informática na forma tentada e o n.º 5 do mesmo preceito prevê a burla informática qualificada, a qual assume a natureza pública, o que significa que é o Ministério Público que promove o procedimento criminal, conforme dispõe o art. 48.º do CPP.

dados nos quais está presente e aos quais está subjacente algum modo de engano, de fraude ou de artifício que tenha a finalidade, e através da qual se realiza a específica intenção de obter enriquecimento ilícito, causando a outra pessoa prejuízo patrimonial.[47]

A clareza deste entendimento proferido pelo Supremo Tribunal de Justiça permite descortinar os elementos objetivos e subjetivo do ilícito criminal de burla informática.

Assim, são elementos objetivos a interferência no resultado de tratamento de dados, a estruturação incorreta de programa informático e a utilização ou intervenção não autorizada, por qualquer outro modo, no processamento.[48] [49]

Para a técnica do *phishing*, aqui sob esmiúça, tem relevância o elemento objetivo que se configura na utilização de dados sem autorização.

Por outro lado, emerge como elemento subjetivo a intenção de o agente obter, para si ou para terceiro, um locupletamento ilegítimo, o que reflete, indubitavelmente, o dolo na sua ação, porquanto tem plena consciência de que a sua conduta viola a lei, causando prejuízo a terceiro.

Nos termos conjugados do art. 13.º e do art. 221.º do CP, a burla informática é um crime doloso, não admitindo punição a título de negligência. Além disso, é um crime intencional, que exige a verificação de uma intenção específica de enriquecimento ilegítimo.

Em consonância com o referido, evidenciou o Tribunal da Relação do Porto, em acórdão, de 03 de fevereiro de 2016, processo n.º 482/10.2SJPRT.P1, disponível em www.dgsi.pt, que *"A burla informática consiste num erro consciente provocado por intermédio da manipulação de um sistema de dados ou de tratamento informático. Não*

[47] Cfr. Acórdão do Supremo Tribunal de Justiça de 20/09/2006, processo n.º 06P1942, disponível em www.dgsi.pt, consultado em 22.02.2018.
[48] Neste sentido, *vide* GERALDES, ANA VAZ, ob. cit., p. 95.
[49] Evidencia GERALDES, ANA VAZ, ob. cit., p. 96, que existe um concurso aparente entre a burla informática e demais crimes relacionados com o acesso ilegítimo e sabotagem informáticos, uma vez que todos eles têm como finalidade um enriquecimento ilegítimo, servindo estes últimos de meros atos de execução, e ainda por respeito ao princípio *ne bis in idem*, segundo o qual ninguém pode ser duplamente punido pelo mesmo ilícito criminal (art. 29.º, n.º 5 da Constituição da República Portuguesa).
Além disso, considerou ainda o Tribunal da Relação do Porto, em Acórdão de 30 de agosto de 2009, processo n.º 15273/02.6TDLSB.P1, disponível em www.dgsi.pt, consultado em 25.02.2018, que a burla informática consubstancia um crime de resultado: "Na burla informática a lesão do património produz-se através da intromissão nos sistemas e da utilização em certos termos de meios informáticos - é um crime de resultado, exigindo-se que seja produzido o prejuízo patrimonial de alguém.".

se exige um qualquer engano ou artifício por parte do agente, mas sim a introdução e utilização abusiva de dados no sistema informático.".

Deslindados os elementos tipificadores da burla informática, cumpre precisar qual é o bem jurídico aqui protegido.

A generalidade da doutrina portuguesa apologiza que o bem jurídico protegido é o património, com fundamento, essencialmente, na localização sistemática que o crime ocupa no Código Penal.[50]

Porém, há vozes na doutrina e jurisprudência que entendem que este tipo criminal visa também tutelar um interesse coletivo: o regular funcionamento dos sistemas e das redes informáticas.[51]

2. O *SPYWARE*

Proveniente do *malware*, o *spyware* afigura-se um programa malicioso, *instalado no computador ou tablet do cliente, sem que este se aperceba. Uma vez instalado, deteta se o cliente está a aceder a uma página de internet protegida e regista os dados inseridos pelo utilizador*.[52]

À semelhança do que acontece com o *keylogger*, programa de vigilância que procede à recolha e armazenamento de toda a informação digitalizada, tais como endereços pessoais de correios eletrónicos, dados e informações bancárias, nomeadamente números de cartão bancário e senhas, o *spyware* vem recolher a informação de um sistema de computação sem o consentimento do seu titular. Posteriormente, a recolha dos dados será enviada para destinos alheios.

---

[50] De igual modo entendeu o Tribunal da Relação de Lisboa, em acórdão de 24/01/2007, processo n.º 5990/2006-3 e o Supremo Tribunal de Justiça, em acórdão de 05/11/2008, processo n.º 08P2817, disponíveis em www.dgsi.pt, consultados em 25.02.2018, considerando que a burla informática é um crime de dano, uma vez que pressupõe uma efetiva lesão do património, e um crime material ou de resultado, exigindo a verificação de um prejuízo patrimonial.

[51] Assim, SANTOS, RITA, *O tratamento jurídico-penal da transferência de fundos monetários através da manipulação ilícita dos sistemas informáticos*, Coimbra, Coimbra Editora, 2005, p. 217, ao assinalar que "existem normas relativamente às quais, não obstante a sua localização sistemática, se reconhece protegerem bens jurídicos diversos daqueles que identificam a sua concreta integração no Código Penal". Ao nível da jurisprudência, acompanham o mesmo entendimento o Supremo Tribunal de Justiça, em acórdão de 14/07/2004, processo n.º 04P3287 e em acórdão de 06/10/2005, processo n.º 05P2253, bem como o Tribunal da Relação de Lisboa, em acórdão de 03/5/2007, processo n.º 10042/06-5, disponíveis em http://www.dgsi.pt, consultados em 25.02.2018.

[52] *Cfr.* Notícia do Banco de Portugal, disponível em https://clientebancario.bportugal.pt/pt-pt/noticias/proteja-se-contra-fraude-na-internet-banco-de-portugal-divulga-boas-praticas-nas-operacoes

Este programa pode ser instalado de forma inofensiva pelo próprio usuário, aquando da realização de um simples *download* aparentemente normal.

Alerta-se, pois, para os riscos inerentes às práticas do quotidiano realizadas no seio do *ecossistema digital* cada vez mais revolucionário, mas igualmente potenciador de práticas fraudulentas na banca eletrónica.

3. O *PHARMING*

O *pharming* é outra recorrente técnica fraudulenta, mas mais sofisticada e perigosa que o *phishing.*

À semelhança do *phishing*, faz os utilizadores crerem que estão a aceder a um *site* legítimo, quando não estão.

Inversamente ao que sucede no *phishing*, a difusão de ficheiros via *spam* é feita de forma oculta, os quais, também de modo encoberto se autoinstalam nos computadores dos utilizadores.

"*Estes ficheiros ocultos são programas que captam os códigos de pulsação do teclado, key loggers, e permitem que, sempre que o utilizador digita o endereço de determino site, o sistema, por via das mencionadas alterações, redirija-o para uma outra página, para além de registarem tudo o que é digitado no teclado do utilizador*".[53]

Ou seja, o utilizador, mesmo que digite o *site* oficial do seu banco, é involuntariamente redirecionado para um outro *site* (falso), através do qual são recolhidas as informações e códigos da vítima.

Este tipo de disseminação oculta de *software* malicioso é extremamente eficaz para os criminosos, porquanto, contrariamente ao que acontece no *phishing* onde os criminosos tentam ardilosamente enganar os utilizadores com o envio de mensagens de correio eletrónico, admitindo uma suficiente margem de falibilidade uma vez que nem todos caem no engano do esquema fraudulento, no *pharming*, o utilizador é enganado sem se

[53] Conforme elucidativamente refere BARREIRA, CAROLINA, ob. cit., p. 27.

aperceber, uma vez que o *software* malicioso ultrapassou de forma oculta a barreira de proteção do computador.[54]

Quanto a este tópico, é muito claro o Tribunal da Relação do Porto, no acórdão de 07 de dezembro de 2014, processo n.º 747/12.9TJPRT.P1, disponível em http://www.dgsi.pt, quando considera que o *pharming "(...) opera pelo mesmo princípio do phishing, ou seja, fazendo os internautas pensarem que estão a aceder a um site legítimo, quando na verdade não estão. Mas ao contrario do phishing, o qual uma pessoa mais atenta pode evitar simplesmente não respondendo ao e-mail fraudulento, o pharming é praticamente impossível de ser detectado por um utilizador comum da internet, que não tenha maiores conhecimentos técnicos. Nesse novo tipo de fraude, os agentes criminosos valem-se da disseminação de softwares maliciosos que alteram o funcionamento do programa de navegação (browser) da vítima. Quando esta tenta aceder a um site de um banco, por exemplo, o navegador infectado redireciona-a para o spoof site (o site falso com as mesmas características gráficas do site verdadeiro). No site falseado, então, ocorre a recolha das informações privadas e sensíveis da vítima, tais como números de cartões de crédito, contas bancárias e senhas."*

[54] No entendimento de VERDELHO PEDRO, ob. cit., p. 415, o *pharming* é muito difícil de se deslindar, mesmo para utilizadores experientes e alertados, fazendo dele uma técnica muito mais perigosa para os utilizadores dos serviços de *homebanking*.

- CAPÍTULO V -
DISTRIBUIÇÃO DE PREJUÍZOS E IMPUTAÇAO DE RESPONSABILIDADES RESULTANTES DAS OPERAÇÕES NÃO AUTORIZADAS NO CONTRATO DE HOMEBANKING

No seio do *ecossistema digital*, o *homebanking* confere ao seu utilizador a comercialização de produtos e a prática de diversos atos bancários de uma forma célere, cómoda e prática. Todavia, de tal serviço emergem vicissitudes na segurança pelo que, aos dias de hoje, a segurança das contas bancárias torna-se imperativa.

As ameaças cada vez mais recorrentes à segurança colocam em perigo as contas bancárias dos clientes, que são alvo de intromissões não autorizadas acompanhadas da movimentação do saldo dos depósitos bancários.

Neste domínio, Maria Raquel Guimarães denota que *os prejuízos causados por este tipo de actuação são tendencialmente elevados, podendo decorrer um espaço de tempo considerável entre o momento em que a intromissão tem lugar e a sua detecção.*[55]

Ora, perante tais ilícitos, sendo debitados montantes das contas dos clientes sem o seu consentimento através do uso eletrónico do Instrumento de Pagamento, urge questionar quem suporta os prejuízos decorrentes da utilização indevida dos serviços de pagamento, questão com que nos ocuparemos.

A segurança do sistema de banca eletrónica está dependente da atuação diligente de todos os seus utilizadores. Assim, para efeitos de repartição dos prejuízos entre as partes, deverá ser apurada a atuação dos seus intervenientes, confirmando se foram cumpridos os deveres que lhes estão adstritos pelo contrato celebrado. A repartição de tais danos assentará *numa ideia de distribuição equitativa dos prejuízos causados, na medida do incumprimento dos deveres contratuais que sobre cada um impende, decorrentes do princípio geral da boa fé*.[56]

[55] *Idem.*
[56] Cfr. Acórdão do Tribunal da Relação de Lisboa de 04 de julho de 2013, processo n.º 103841/11.3YIPRT.L1-2, disponível em http://www.dgsi.pt, consultado em 03.03.2018.

Nestes termos, dispõe o Acórdão do Tribunal da Relação de Guimarães, de 23 de dezembro de 2012, disponível em http://www.dgsi.pt, que "*I- A complexidade dos sistemas bancários homebanking, concebidos e controlados pelos Bancos, assim como a grande exigência dos mecanismos relacionados com a segurança das operações bancárias através deles realizadas, a par da propriedade do banco sobre os valores depositados pelos seus clientes, em ambiente contratual, justificam o funcionamento da regra da presunção de culpa prevista pelo art.º 799º, nº 1, do Código Civil, que recai sobre a entidade bancária na responsabilidade pela utilização fraudulenta daqueles meios.*

II- Em todo o caso, o banco pode elidir aquela presunção, afastando a sua culpa ou demonstrando mesmo a culpa do cliente pela deficiente utilização daqueles meios expeditos, designadamente, alegando e demonstrando que o cliente beneficiário violou o contrato, divulgando na internet dados pessoais, secretos e intransmissíveis relativos ao seu acesso, em benefício de hackers.

III- No primeiro caso, o Banco pode ainda ser responsabilizado pelo risco, enquanto na segunda hipótese a responsabilidade é do cliente." [57]

1. Imputação de responsabilidade ao utilizador

Em sede de repartição de riscos provenientes da utilização indevida do serviço de banca eletrónica, regula o artigo 113.º, n.º 1 do RSP [58] que, caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada ou alegue que a operação não foi corretamente efetuada, incumbe ao respetivo prestador do serviço de pagamento o ónus de provar 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.

Porém, para efeitos de prova, não é suficiente alegar apenas que foram cumpridos os deveres que lhe estão implícitos, pelo que o prestador de serviços, *vulgo* banco, deverá igualmente fazer prova de que o utilizador do serviço de *homebanking* agiu

[57] Acórdão com o número de processo 305/09.5TBCBT.G1, disponível em http://www.dgsi.pt, consultado em 06.03.2018.

[58] Anexo ao DL nº 91/2018 de 2 de novembro, que transpõe para a ordem jurídica interna a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno (segunda Diretiva de Serviços de Pagamento), que procedeu a uma revisão do enquadramento jurídico europeu em matéria de serviços de pagamento.

negligentemente, incumprindo com os seus deveres de diligência a que está sujeito por força do presente diploma.

Torna-se, pois, imperativo concretizar que a utilização indevida do serviço de pagamento eletrónico correu por conta do seu utilizador que agiu de forma fraudulenta, ou que não cumpriu, com dolo ou negligência grosseira, uma ou mais obrigações previstas no artigo 110.º do RSP.[59]

Nesta sede, veja-se o disposto no Acórdão do Tribunal da Relação de Guimarães que concretiza que, numa ótica de responsabilização pelos riscos decorrentes de esquemas fraudulentos, "*no contrato de homebanking, o prestador de serviços de pagamento (normalmente um Banco), tem a obrigação de assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento, sendo seu o risco do envio ao utilizador de um instrumento de pagamento ou dos respetivos dispositivos de segurança personalizados. O utilizador de serviços de pagamento responde pelas perdas resultantes de operações de pagamento não autorizadas se tiver agido fraudulentamente ou com incumprimento deliberado de uma ou mais das suas obrigações. Pode ainda responder por aquelas perdas se tiver atuado com negligência grave, conceito que se pode definir como "negligência grosseira, erro imperdoável, desatenção inexplicável, incúria indesculpável, vistos em confronto com o comportamento do comum das pessoas, mesmo daquelas que são pouco diligentes".*[60]

Importa ter em consideração a regra da presunção de culpa estabelecida no artigo 799.º n.º 1 do Código Civil, nos termos da qual recai sobre o banco depositário o ónus da prova de que a falta de cumprimento ou o cumprimento defeituoso da obrigação, nomeadamente deficiências técnicas que possam potenciar eventuais utilizações fraudulentas, não procedem por culpa sua.

Sustenta o Acórdão do Tribunal da Relação de Évora, datado de 25 de junho de 2015 que, "*em todo o caso, avultando neste tipo de contratos de home banking a obrigação de utilização correcta do serviço por parte do utente, o qual assenta em boa parte na*

[59] Com remissão para o Artigo 113.º, n.ºs 3 e 4 do RSP.
[60] Cfr. Acórdão do Tribunal da Relação de Guimarães de 17 de dezembro de 2014, processo n.º 1910/12.8TBVCT.G1, disponível em http://www.dgsi.pt, consultado em 15.05.2018.

não divulgação dos seus elementos de segurança e códigos de acesso, o Banco pode elidir aquela presunção, afastando a sua culpa ou demonstrando mesmo a culpa do cliente pela deficiente utilização daqueles meios expeditos, designadamente, alegando e provando que o cliente beneficiário violou o contrato, divulgando na internet dados pessoais, secretos e intransmissíveis relativos ao seu acesso, em benefício de hackers." [61]

Chegados a este ponto, urge questionar a aceção das expressões *dolo* e *negligência grosseira* do utilizador, constantes do artigo 113.º do RSP, para que possamos apurar nos mais variados casos, se houve quebra dos deveres e consequente imputação de responsabilidades.

Apreciados os comportamentos do utilizador, deverá ser verificado se o mesmo incumpriu de forma dolosa e deliberada os seus deveres previstos no artigo 110.º do RSP ou se facilitou a execução desta operação de pagamento movido por intuitos fraudulentos, não cumprindo as regras de conduta diligente que lhe é vedado pela lei.

Ademais, tal disposição legal refere ainda que, havendo negligência grosseira por parte do utilizador, isto é, um *erro imperdoável, desatenção inexplicável, incúria indesculpável, vistos em confronto com o comportamento do comum das pessoas, mesmo daquelas que são pouco diligentes*[62], a responsabilidade incidirá por conta do ordenador.

Consubstanciam situações de negligência grave não só aquelas em que o cliente forneceu os códigos de acesso e credenciais disponíveis no cartão matriz, como também nos casos em que, pese embora o correto funcionamento dos serviços do banco e do cumprimento do dever de informação ao cliente com a disponibilização de alertas de segurança na página de *homebanking* perfeitamente claros e elucidativos na detetação de interações fraudulentas, o mesmo procede com descuido e desatenção, conduta vista, aos olhos da jurisprudência, como censurável, com a qual concordamos.

[61] Cfr. Acórdão do Tribunal da Relação de Évora, processo n.º 3052/11.4TBSTR.E1, disponível em http://www.dgsi.pt, consultado em 18.06.2018.
[62] Cfr. Acórdão do Tribunal da Relação de Guimarães, de 17 de Dezembro de 2014, processo n.º 1910/12.8TBVCT.G1, abordado *supra*.

Ainda assim, cumpre referir que tais condutas pouco cautelosas em muito decorrem da iliteracia tecnológica que abrange muitos clientes. A falta de domínio de tecnologia no acesso a meios informáticos é uma realidade comum num segmento de clientes, nomeadamente idosos ou aqueles que apresentem um fraco domínio de tais ferramentas para a realização de operações financeiras *online*.

Assim, deverá a entidade prestadora de serviços acautelar os clientes que, aparentemente, demonstrem pouco domínio de tal ferramenta, recomendando o recurso aos serviços tradicionais.

Ainda assim, de acordo com estudos efetuados em sede de segurança no *homebanking*, mostram *que as vítimas de fraudes não são necessariamente pessoas com baixa educação, ingénuas ou idosos*, pelo que em qualquer dos casos, sempre que haja uma conduta negligente com incumprimento de tais obrigações, será o utilizador de tal serviço a responsabilizar-se pelos prejuízos causados. [63]

A título exemplificativo, somos de salientar situações constantes na nossa jurisprudência, nomeadamente nos Acórdãos da Relação de Lisboa, de 12 de dezembro de 2013 [64]; de 15 de março de 2016 [65] e ainda o Acórdão datado de 12 de outubro de 2017 [66], nas quais o Banco fica isento de quaisquer responsabilidades.

Atento o exposto, à luz do artigo 115.º n.º4 do anexo ao DL n.º 91/2018, de 12 de novembro, havendo negligência grosseira por parte do ordenante, e tendo a entidade

[63] De acordo com a notícia publicada no Jornal Expresso a 31 de agosto de 2009, disponível em www.expresso.pt

[64] Cfr. Acórdão do Tribunal da Relação de Lisboa, processo n.º 164/11.8TBSRT.L1-6, disponível em http://www.dgsi.pt, consultado em 18.06.2018, que refere que "*Provando a Ré que a Autora fez uma utilização imprudente, negligente e descuidada desse serviço, revelando a terceiros, na internet, os seus códigos pessoais de acesso ao serviço, bem como dos elementos necessários para a confirmação/validação da operação bancária, não lhe é exigível o pagamento das quantias por eles indevidamente movimentadas".*

[65]Acórdão do Tribunal da Relação de Lisboa, processo n.º 1063/12.1TVLSB.L1-1, disponível em http://www.dgsi.pt, consultado em 18.06.2018, que decidiu que, "*7.1-O Banco não será, em caso algum, responsável pelos prejuízos derivados de erros de transmissão, deficiências técnicas, interferências ou desconexões ocorridas por via e no âmbito dos sistemas de comunicação utilizados para a prestação do Serviço.*
7.2-O Cliente e os Utilizadores assumem inteira responsabilidade pela utilização negligente, indevida ou fraudulenta das Chaves de Acesso e Cartão de Coordenadas.
7.3-O Cliente é responsável e suportará todos os prejuízos resultantes de uma utilização abusiva do Serviço por intermédio de pessoas diferentes dos Utilizadores, quer estes sejam membros do órgão de administração ou colaboradores do Cliente ou outras pessoas."

[66] Cfr. Acórdão do Tribunal da Relação de Guimarães de 17 de Dezembro de 2014, processo n.º 1910/12.8TBVCT.G1, disponível em http://www.dgsi.pt, consultado em 18.06.2018.

prestadora de serviços provado que o utilizador incumpriu com as obrigações a que está adstrito pelo artigo 110.º do mesmo diploma, será o utilizador do serviço responsável pelos prejuízos causados pela utilização indevida dos serviços de banca eletrónica, ficando sujeito a um pagamento superior ao limite definido pelo n.º 1 do mesmo artigo, de € 50,00 (cinquenta euros),[67] montante máximo para situações de negligência leve pelo utilizador.

Por fim, não sendo possível ao banco provar que no decurso da operação fraudulenta foram disponibilizado aos clientes informações acerca daquela fraude em concreto, ou sendo um utilizador que não dispõe dos conhecimentos eletrónicos suficientes, ou ainda quando se prove que logo que teve conhecimento comunicou imediatamente à entidade prestadora de serviço o sucedido, a jurisprudência entende que ainda que seja um comportamento passível de censura, o mesmo responsabilizar-se-á pelos prejuízos resultantes de operações de pagamento não autorizadas a título de negligência leve, conforme dispõe o artigo 115.º n.º1 do RSP. [68]

2. Imputação de responsabilidade ao prestador de serviços de pagamento

Uma temática correlacionada com a fraude no *homebanking*, que se perscrutará seguidamente, é a eventual responsabilidade da instituição bancária pelos danos sofridos pelos seus clientes, fruto da pirataria informática.

Existe um amplo consenso na jurisprudência no que concerne à responsabilidade por parte da entidade bancária. Vejamos:

Numa ótica, sobretudo, de defesa do consumidor, não havendo culpa nem negligência grave do cliente na movimentação fraudulenta da conta, recairá sobre o banco a responsabilidade, o qual terá que suportar as consequências da fraude, as quais

[67] O montante de € 50,00 (cinquenta euros), definido no artigo 115.º n.º1 do presente diploma, constitui uma alteração introduzida pela transposição para a ordem jurídica interna da Diretiva (UE) 2015/2366 de 25 de novembro de 2015.

[68] Assim, *"O cliente do banco vê a sua posição agravada conforme vai aumentando o grau de censura sobre a sua conduta. Na medida em que seja, ele próprio, o autor da fraude, então já o banco não assumirá qualquer prejuízo pelas operações realizadas", cfr.* GUIMARÃES, MARIA RAQUEL, "A repartição dos prejuízos decorrentes de operações fraudulentas de banca eletrónica *(home banking*): anotação ao Acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09", *Cadernos de Direito Privado,* Braga: CEJUR. Nº 41 (janeiro/março 2013), p. 66.

conseguiram pôr em causa a confiança que ele próprio se comprometeu a garantir perante o cliente.[69]

Nas considerações expendidas pelo Tribunal da Relação de Lisboa, no acórdão de 26 de outubro de 2010, processo n.º 1943/09.1TJLSB.L1-7, disponível em www.dgsi.pt,*"(...) na sociedade de informação em que vivemos, só o banco tem hipótese de controlar os riscos que para ele são mínimos e que poderão ser desastrosos para a A.. Por isso, numa ótica de defesa do consumidor, não tendo o banco demonstrado culpa da A. na movimentação fraudulenta da conta, o mesmo terá de suportar as consequências da fraude no circuito cuja fiabilidade, de resto, ele próprio se comprometeu contratualmente a garantir".*

Existe, aliás, uma presunção de culpa que recai sobre a entidade bancária, aquando das transferências fraudulentas nas contas dos seus clientes, cabendo-lhe ilidir essa presunção.[70]

[69] Havendo negligência grave por parte do titular da conta bancária, por permitir ao criminoso o acesso às suas credenciais, não restam dúvidas de que a responsabilidade deixará de correr por conta do banco, passando a sê-lo por parte da vítima. *Vide* a este propósito o acórdão do Tribunal da Relação de Lisboa de 15/03/2016, processo n.º 1063/12.1TVLSB.L1-1, disponível em www.dgsi.pt, consultado em 03.03.2018, quando explica que " Apenas há responsabilidade da vítima, se se determinar que ela, com negligência grave, permitiu ao defraudador o acesso às credenciais de acesso. Negligência grave (ou grosseira) corresponde à falta grave e indesculpável, consistente na omissão dos deveres a que se está adstrito, que só uma pessoa especialmente desleixada, descuidada e incauta deixaria de observar. Não se provando como o agente do crime obteve as credenciais, não pode qualificar-se a atuação da vítima como gravemente negligente."
Sufraga também o mesmo entendimento o Tribunal da Relação de Guimarães em acórdão de 17/12/2014, processo n.º 1910/12.8TBVCT.G1, disponível em www.dgsi.pt, consultado em 03.03.2018, quando evidencia que " Num contrato de *home banking*, o Banco tem a obrigação de assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento. O utilizador de serviços de pagamento responde pelas perdas resultantes de operações de pagamento não autorizadas se tiver agido com incumprimento deliberado de uma ou mais das suas obrigações. Pode ainda responder por aquelas perdas se tiver atuado com negligência grave, conceito que se pode definir como "negligência grosseira, erro imperdoável, desatenção inexplicável, incúria indesculpável, vistos em confronto com o comportamento do comum das pessoas, mesmo daquelas que são pouco diligentes".

[70] Assim entendeu o Tribunal da Relação de Lisboa, em acórdão de 21/05/2015, processo n.º 337/14.1YXLSB.L1-2, disponível em www.dgsi.pt, consultado em 04.03.2018: "(…) para ilidir a presunção de culpa que a onera, em caso de transferência fraudulenta, nos quadros de serviços de *internet banking*, não basta à instituição de crédito a alegação e prova dos procedimentos de segurança adotados, relativos à emissão do cartão respetivo e códigos de acesso, e às advertências e recomendações publicitadas e transmitidas ao utilizador, quando, não se demonstrando a culpa de banda daquele, tão pouco se tenha sequer comprovado qual o tipo de intromissão fraudulenta concretamente verificado. Para além disso, em relação a uma operação de pagamento não autorizada, presume-se a culpa do prestador de serviços de pagamento do ordenante, que não proceda ao imediato reembolso deste do montante da dita operação".

Assim, sempre que o prestador de serviços de pagamento não consiga fazer prova do incumprimento deliberado pelo utilizador do serviço, recairá sobre ele o reembolso imediato do montante da operação de pagamento não autorizada.[71]

Deste modo, sendo-lhe imputados os prejuízos pelos débitos indevidos, ao abrigo do novo Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, fica o prestador de serviços responsável por um reembolso imediato ao ordenante, após ter tomado conhecimento da operação ou após lhe ter sido comunicada, sendo que o atraso no cumprimento dessa obrigação acarretará o pagamento de juros moratórios. [72] [73]

Além disso, cumpre referir que o incumprimento do dever de reembolso é considerado uma infração especialmente grave, punível com uma coima de € 10.000,00 (dez mil euros) a € 5.000.000,00 (cinco milhões de euros), conforme artigo 151.º, alínea *dd)* do DL n.º 91/2018 de 12 de novembro.

Ora, havendo quebras de segurança e de eficácia dos serviços prestados na banca eletrónica, bem como o incumprimento dos deveres que competem ao prestador de serviço de pagamento, contantes no artigo 111.º do RSP, deverá a instituição bancária assumir tais responsabilidades decorrentes dos débitos indevidos nas contas dos seus clientes.

Das decisões judiciais analisadas, e ainda que definidas ao abrigo do anterior Regime dos Serviços de Pagamento e da Moeda Eletrónica, DL n.º 157/2014, de 24 de outubro, verificamos que a maioria dos tribunais tem condenado a entidade prestadora de serviços de pagamento pela totalidade dos prejuízos decorrentes dos mais variados esquemas fraudulentos assistidos nos serviços de *homebanking.*[74]

Neste sentido, em matéria de cumprimento dos deveres que à entidade prestadora de serviços compete, veja-se o disposto no Acórdão do Tribunal da Relação de Lisboa, de 5 de novembro de 2013[75], no Acórdão do Tribunal da Relação de Lisboa, de 12 de

[71] GUIMARÃES, MARIA RAQUEL, *I Congresso de Direito Bancário*, Almedina, 2015, p. 139.
[72] Cfr. Artigo 114.º n.º 1 do RSP.
[73] Cfr. Artigo 114.º n.º 10 RSP.
[74] *Vide* Capítulo IV do presente estudo.
[75] O Acórdão, com o n.º de processo 9821/11.8T2SNT.L1-1, esclarece que "*O home banking é um s erviço prestado ao cliente pelo Banco, sendo este que tem de diligenciar para que seja seguro e nele possa o cliente confiar, devendo este utilizar esse serviço seguindo as regras de segurança que lhe*

dezembro de 2013[76] e no Acórdão do Tribunal da Relação de Guimarães, datado em 17 de dezembro de 2014,[77] que entenderam ser responsável a instituição de crédito por tais prejuízos.

Ademais, e conforme referido, não sendo possível provar este incumprimento ou imputar a operação ao titular do instrumento de pagamento, *recairá sobre a entidade o risco de autorizar operações de pagamento realizadas com um instrumento de pagamento*. [78] Veja-se, neste sentido, o Acórdão do Tribunal da Relação de Lisboa, com data em 3 de março de 2015 [79] e o Acórdão do Tribunal da Relação de Coimbra, de 2 de fevereiro de 2016,[80] nos quais, uma vez mais, a entidade prestadora de serviços de pagamento fica adstrita a suportar os danos causados.

---

tenham sido comunicadas pelo Banco", processo disponível em http://www.dgsi.pt, consultado em 25.07.2018.

[76] Deste Acórdão, com o n.º de processo 164/11.8TBSRT.L1-6, consta que "*1. Sendo o "homebanking" um serviço prestado ao cliente pelo Banco, a este compete diligenciar pela sua segurança de modo a que o seu utilizador não fique privado dos valores nele depositados pelo abusivo acesso a terceiros, sem a sua autorização ou consentimento, ou seja, o cliente tem de poder confiar nesse sistema de acesso à sua conta bancária e respectiva movimentação.*
2. Sobre o Banco impende a obrigação de prestar um serviço eficaz e seguro (...)", disponível em http://www.dgsi.pt, consultado em 25.07.2018.

[77] Refere o acórdão, com o n.º de processo 1910/12.8TBVCT.G1, que "*IV – Num contrato de homebanking, o prestador de serviços de pagamento (normalmente um Banco), tem a obrigação de assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento, sendo seu o risco do envio ao utilizador de um instrumento de pagamento ou dos respectivos dispositivos de segurança personalizado",* disponível em http://www.dgsi.pt, consultado em 25.06.2018.

[78] GUIMARÃES, MARIA RAQUEL, "*A* fraude no comércio eletrónico: o problema da repartição do risco por pagamentos fraudulentos" in *Infrações Económicas e Financeiras: Estudos de Criminologia e Direito* (J. Cruz, C. Cardoso, A. L. Leite, R. Faria, *coordenação*). Coimbra Editora, 2013, p. 593.

[79] O Acórdão, com o nº de processo 1727/13.2TJLSB.L1-1, refere que "*Não se tendo apurado ter o cliente permitido o acesso de terceiros às suas credenciais, não se pode concluir ser imputável ao mesmo a quebra da confidencialidade dos dispositivos de segurança",* disponível em http://www.dgsi.pt, consultado em 25.06.2018.

[80] O Acórdão, cujo n.º de processo é o 902/13.4TBCNT.C1, concretiza que "*Não se tendo provado que o cliente forneceu a terceiros (ao aceder a página ilícita) as chaves de acesso ao serviço de home banking nem que, ao navegar na internet, permitiu que outrem tenha capturado as credenciais de acesso e validação, recai sobre o banco a responsabilidade pela movimentação fraudulenta da sua conta bancária, através da internet (Serviços Homebanking)", disponível em* http://www.dgsi.pt, consultado em 25.06.2018.

- CAPÍTULO VI -
SOLUÇÕES DECORRENTES DA LEGISLAÇÃ COMUNITÁRIA - DIRETIVA (UE) 2015/2366 DO PARLAMENTO EUROPEU E DO CONSELHO RELATIVA AOS SERVIÇOS DE PAGAMENTO NO MERCADO INTERNO

O fenómeno da digitalização financeira tem ganho cada vez mais visibilidade e impacto numa sociedade cada vez mais dependente da Internet e dos produtos por ela disponibilizados.

Com efeito, a utilização da informática nas operações do quotidiano tornou-se inevitável e o setor bancário sentiu a necessidade de acompanhar as exigências e expectativas dos seus clientes, desmaterializando os serviços de pagamento e acompanhando a atual era digital.[81] [82]

Fruto das alterações dos hábitos dos clientes e face à necessidade de concorrerem em igualdade de circunstâncias com os bancos da União Europeia, o sector bancário vem apostar na tecnologia como modelo de negócio, adotando a sua estratégia digital, potenciando a eficiência e redução de custos operacionais, alargando-a a mais processos de negócio e aproximando-se mais das necessidades e expetativas dos clientes.[83]

Todavia, a capitalização da experiência digital dos bancos acarreta, de igual modo, um impacto negativo na segurança dos serviços disponibilizados, conforme temos vindo a analisar, razão que tem preocupado as instituições bancárias.

[81] Ideia reforçada por GUIMARÃES, MARIA RAQUEL**,** *As Transferências electrónicas de fundos e os cartões de débito*, Almedina, Coimbra, 1999, pp.42 e 43: "*o homebanking veio revolucionar a concepção clássica do modo de funcionamento das instituições bancarias, permitindo aos seus clientes realizar as operações tradicionalmente levadas a cabo nos balcões das sucursais nos seus próprios domicílios"*.

[82] Da evolução tecnológica têm surgido propostas inovadoras e cada vez mais atuais, cfr. notícia divulgada pelo Jornal Diário de Notícias, a 26 de junho de 2017, disponível em www.dn.pt e notícia publicada no Jornal Expresso a 06 de Junho de 2018, disponível em www.expresso.pt.

[83] Cfr. Artigo publicado no Jornal Económico "Banco de Portugal aprova abertura de contas bancárias através de canais digitais" de 02 de agosto de 2017, disponível em www.jornaleconomico.sapo.pt.

O risco é assim *algo evidente para as instituições que trabalham afincadamente no sentido de proteger os seus sistemas, ao mesmo tempo que modernizam infra-estruturas e abraçam definitivamente o conceito de transformação digital*. [84]

As instituições de crédito estão sujeitas ao risco operacional, isto é, ao risco das perdas resultantes da inadequação ou falhas dos processos internos, pessoas, sistemas ou de eventos externos, que acarretam exposição das instituições bancárias ao pagamento coercitivo de verbas, fruto de ações judiciais e regulatórias, propostas como consequência de falhas operacionais.

Neste sentido, no seio dos serviços bancários digitais e dos mais variados esquemas fraudulentos a que tal serviço está sujeito, torna-se imperativa a criação de mecanismos de sensibilização para as nefastas consequências trazidas a ambas as partes (utilizador e prestador de serviços), bem como adoção de medidas preventivas e de proteção dos intervenientes.

Tais preocupações ocuparam a União Europeia naquela que tem sido uma realidade bastante evolutiva em torno do regime dos serviços de pagamentos eletrónicos.

Assim, com a consciência da importância de tais realidades, e no seguimento do Livro Verde lançado pela Comissão Europeia em 2012, o legislador comunitário aprovou em 2013 uma proposta de uma nova Diretiva de Serviços de Pagamentos, adiante designada por "DSP 2", isto é, a Diretiva 2015/2366 do Parlamento Europeu e do Conselho de 25 de Novembro, relativa aos serviços de pagamentos eletrónicos, que vem alterar as Diretivas 2002/65/CE, 2013/36/CE e 2009/110/CE e revogar a Diretiva 2007/64/CE.

Nas palavras de Vasco Monteiro, "*o foco das preocupações com esta diretiva tem estado na segurança, quer das instituições quer dos consumidores, e na proteção de dados, em resultado do acesso, por terceiros, às contas dos clientes bancários, tanto*

[84] Artigo publicado no Jornal de Negócios de 05 de julho de 2017, disponível em www.jornaldenegocios.pt.

para efeitos de serviços de informação sobre contas como para serviços de iniciação de pagamentos.'' [85]

A DSP 2 veio, assim, ampliar aquele que era o âmbito da DSP 1, 2007/64/CE, entretanto revogada.

Para além da criação de um mercado de pagamentos mais integrado e eficiente, que dispõe de novas entidades que disponibilizam aos consumidores serviços de pagamento inovadores, conforme dispõe o artigo n.º 19 e *ss.*, a DSP 2 vem ainda realçar a importância da segurança nos sistemas de pagamento, de forma a proteger os seus consumidores.

Neste sentido, a nova diretiva de Sistemas de Serviços de Pagamentos vem introduzir medidas de segurança melhoradas, dirigidas a todos os fornecedores de serviços de pagamento, instituições bancárias entre outros agentes de mercado, designadamente aos *Third Party Providers*, adiante designados por TPP, que beneficiam do mercado único digital.[86]

[85] Cfr. MONTEIRO, VASCO "Transformação digital do sector bancário. Desenvolvimentos recentes e futuros no quadro legal e regulatório" in *InforBANCA 111, nov'17-fev'18,* p.27.

[86] Desde a adoção da PSD1, surgiram novos serviços na área de pagamentos na Internet, onde os chamados intermediários de pagamentos *third party providers* (TPP) oferecem soluções ou serviços de pagamento específicos aos clientes. Ou seja, existem serviços que compilam e consolidam informações sobre as diferentes contas bancárias de um consumidor em um único lugar "serviços de informações de conta (AIS - Account Information Services)". Esses serviços normalmente permitirão que os consumidores tenham uma visão global sobre sua situação financeira e analisem seus padrões de gastos, despesas, necessidades financeiras de maneira amigável. Outros intermediários de pagamentos third party providers (TPPs) tentam facilitar o uso de serviços bancários on-line para fazer pagamentos pela Internet (os chamados "serviços de iniciação de pagamento (PIS - Payment Initiation Services"). Estes ajudam a iniciar um pagamento da conta do cliente para a conta comercial criando uma "ponte" de software entre essas contas, preenchendo as informações necessárias para uma transferência (quantidade da transação, número da conta, mensagem) e informam o comerciante quando a transação é iniciada.
Até agora, entrar no mercado de pagamentos era complicado para estes fornecedores de serviços (TPPs), já que muitas barreiras os impediam de oferecer as suas soluções em larga escala e em diferentes Estados Membros. Com estas barreiras removidas, espera-se uma maior concorrência com novas entidades que entram em novos mercados e oferecem soluções mais baratas para pagamentos a mais e mais consumidores em toda a Europa. Os fornecedores de serviços de: pagamentos, TPPs, terão de seguir as mesmas regras que os prestadores tradicionais de serviços de pagamento registo, licenciamento e supervisão pelas autoridades competentes. Além disso, os novos requisitos de segurança incluídos no texto da PSD2 obrigarão todos os fornecedores de serviços de pagamento a aumentar a segurança em torno dos pagamentos *online*.

O alto nível de segurança que a nova diretiva de serviços de pagamento vem introduzir, exige a todos os fornecedores de serviços de pagamento prova de que os seus sistemas possuem medidas apropriadas e preventivas de eventuais riscos operacionais no seio das transações eletrónicas efetuadas.

Para tornar os pagamentos de serviços mais seguros, a DSP 2 introduz requisitos de segurança rigorosos para o processamento de pagamentos eletrónicos, dirigidos a todos os prestadores de serviços de pagamento, inclusive os recentemente regulamentados, como forma de prevenção de operações fraudulentas dos pagamentos *online* para todos os meios, bem como para proteger a confidencialidade dos dados financeiros do utilizador.

Assim, os prestadores de serviços de pagamento serão obrigados a aplicar a chamada autenticação forte, regulada no artigo 30.º n.º 4 da DSP 2, quando se proceda à iniciação de uma transação de pagamento eletrónico.

Entende-se por autenticação forte do cliente, um processo que valida a identidade do utilizador de um serviço de pagamento e a transação de pagamento por ele realizada, ou seja, um processo que apura se o uso de um instrumento de pagamento está efetivamente autorizado.

À luz do disposto no artigo 2.º alínea *d)* do DL n.º 91/2018 de 2 de novembro, que transpõe para a ordem jurídica interna a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro, a autenticação forte do cliente baseia-se no uso de elementos tais como, o conhecimento, posse e inerência do utilizador, elementos de validação da identidade do utilizador e da sua transação, afigurando-se como essenciais num sistema de segurança projetado a proteger a confidencialidade dos dados de autenticação.

A ideia *supra* materializada assenta no conhecimento do utilizador das senhas de acesso ou PIN associados; que o mesmo possua o cartão ou um dispositivo gerador de código

de autenticação; e que a identidade do mesmo seja reconhecida pelo uso de uma impressão digital ou reconhecimento de voz para validar a identidade ou a transação.[87]

Face ao exposto, sendo a resolução de litígios a questão nuclear da nova Diretiva de Serviços de Pagamento, salientamos aquele que é o *punctum saliens* da nosso estudo – a segurança na banca eletrónica.

Assim, a autenticação forte nos sistemas de pagamento introduzida pela DSP 2, e, aos dias de hoje, acolhida na ordem jurídica portuguesa no DL n.º 91/2018 de 12 de novembro, "*afigura-se como um aspeto fundamental para assegurar a proteção dos utilizadores e a promoção adequada do desenvolvimento do comércio eletrónico em condições concorrenciais"*[88]. Numa realidade coetânea marcada pela dinâmica dos serviços de pagamento eletrónicos, sufragamos tais iniciativas. Acreditamos, pois, que os mecanismos trazidos acautelarão a exposição ao risco operacional proveniente de eventuais esquemas fraudulentos cada vez mais comuns.

Face ao exposto, e em sede de distribuição de prejuízos resultantes dos esquemas fraudulentos na banca eletrónica, salientamos a importância dos mecanismos trazidos pela DSP 2, capazes de fazer face aos condicionalismos tão comuns em matéria de fraude no *homebanking*.

Assim, com as melhorias de segurança trazidas com a nova diretiva comunitária, nomeadamente em torno da autenticação forte no acesso aos serviços de pagamento *online*, reforça-se a proteção do consumidor e, consequentemente, da instituição bancária que, em sede de repartição dos riscos, suporta a maior parte dos prejuízos provenientes dos esquemas fraudulentos na banca eletrónica, conforme referido ao longo do presente estudo.

[87] Cumpre referir que nem todos os pagamentos eletrónicos estão sujeitos a autenticação forte do cliente, ficando isentas todas as situações cuja necessidade e conveniência de segurança não se justifique. Assim, dever-se-á atender ao risco que cada meio acarreta, bem como o valor das transações e os canais digitais para o pagamento. Neste sentido, leia-se a informação do BdP, disponível em www.bportugal.pt.
[88] Cfr. preâmbulo do DL 91/2018 de 12 de novembro.

Em nosso entendimento, tais iniciativas pretendem acautelar e tornar robusta a segurança nos pagamentos, tentando, assim, mitigar a exposição a riscos quer da entidade prestadora de serviços, quer do utilizador.

Para além disso, os novos procedimentos de segurança incluídos na DSP 2 são extensíveis às novas entidades fornecedoras de serviços de pagamento, TPP, construindo, deste modo, um mercado de pagamentos europeu mais integrado, competitivo, eficiente e seguro em torno dos pagamentos *online.*

Cremos por isso que, num setor onde a exposição ao risco operacional é tão recorrente, a introdução de benefícios económicos, de proteção do consumidor e segurança nos pagamentos conferem robustez ao sector bancário, principalmente em matéria antifraude, pelo que a entrada da nova Diretiva de Serviços de Pagamento se afigura uma boa via para o mercado de sistemas de pagamento e moeda eletrónica.

- CONCLUSÃO –

O recurso à Internet e aos dispositivos móveis, como meios de viabilização do acervo de produtos e serviços bancários, afigura-se um marco na modernização do setor bancário, movido pelo aperfeiçoamento constante e da satisfação dos serviços disponibilizados, com vista à satisfação das necessidades dos seus clientes.

Neste sentido, face às exigências de uma sociedade digital globalizada, e numa ótica de simplificação e de redução dos custos de transação, assiste-se à diversificação de canais utilizados para a contratação de serviços bancários, surgindo assim o sistema de *homebanking*.

O *homebanking* permite aos seus clientes realizar as operações bancárias, tradicionalmente levadas a cabo nos balcões das sucursais, em qualquer parte e em tempo real, servindo-se para o efeito dos canais digitais.

Este fenómeno de desmaterialização foi alcançado pelos progressos que a Internet trouxe, sendo um traço inequívoco da nossa era. Todavia não podemos descurar o que, no seu âmago, é palavra de ordem: segurança.

Este é a principal preocupação na utilização dos canais digitais.

Ora, ainda que os acessos aos serviços de pagamento eletrónicos sejam feitos através de chaves e combinações numéricas que são do exclusivo conhecimento do utilizador, a infalibilidade de tais serviços tem vindo a perder robustez com os esquemas fraudulentos cada vez mais frequentes na banca eletrónica. O *phishing*, o *pharming*, o roubo de identidade e o *malware* são realidades cada vez mais frequentes no nosso quotidiano.

Assim, perante tais ilícitos, sendo debitados montantes das contas dos clientes sem o seu consentimento através do uso eletrónico do Instrumento de Pagamento, mostra-se essencial saber quem suporta os prejuízos decorrentes da utilização indevida dos serviços de pagamento.

Das decisões judiciais analisadas no presente estudo, concluímos que a regulação é maioritariamente protetora do cliente, que se limita a aderir ao contrato de utilização, libertando-o do ónus da prova, consagrando um princípio de limitação dos prejuízos a assumir pelo titular, caso não atue com culpa, recaindo o remanescente sobre a entidade prestadora do serviço, sendo reembolsado imediatamente pelas operações não autorizadas.

Assim, numa ótica de proteção e prevenção de fraude, consideramos imperativo dar resposta às vicissitudes que a digitalização no setor bancário apresenta. A necessidade de salvaguardar a segurança e a eficiência de tais mecanismos obrigaram a União Europeia a avançar com serviços melhorados, capazes de dar resposta às necessidades dos utilizadores, assim como indicar os procedimentos de autenticação que permitam verificar a identidade de um utilizador de serviços de pagamento e, bem assim, acautelar eventuais infrações na segurança dos mesmos.

Do ponto de vista da imputação de responsabilidades decorrentes da fraude na banca eletrónica, cremos que a implementação de novos mecanismos com a DSP 2 veio não só proteger a identidade do utilizador, mas também minimizar os prejuízos para as partes, nomeadamente na condenação que, em sede judicial, tendencialmente recai sobre a entidade prestadora de serviços.

Face ao exposto, concluímos que, em regra, compete à instituição bancária arcar com os prejuízos decorrentes dos esquemas fraudulentos no *homebanking.* Nesta sede, torna-se, assim, imperativa a necessidade de atenuar a responsabilidade que aos bancos compete, através de políticas e procedimentos de autenticação forte no exercício eficiente de tal serviço, que carece da introdução de credenciais de segurança personalizada do utilizador.

Além disso, tal mecanismo vem introduzir nas páginas oficiais avisos de detetação de indícios de fraude, servindo de meio preventivo e, igualmente, de exigência do cumprimento do dever de confidencialidade dos códigos de acesso do cartão matriz por parte do utilizador.

Assim, sempre que sejam incumpridos os deveres que ao utilizador estão adstritos, seja por indiferença aos avisos cautelosos e de alerta da entidade prestadora de serviços, seja por comportamentos dolosos, imputam-se ao cliente tais responsabilidades.

Feita a análise dos comportamentos das partes, para apurar como se e fará a repartição dos prejuízos decorrentes dos ilícitos no serviço *homebanking*, entendemos que, havendo um comportamento doloso ou negligente e censurável do utilizador, o prestador de serviços ficará liberado de qualquer responsabilidade.

Tal entendimento é acompanhado pelo novo Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (DL n.º 91/2018, de 12 de novembro), bem como pela DSP 2.

A responsabilidade em matéria de fraude no *homebanking* em muito difere do ponto de vista penal e civilístico. Assim, em termos criminais, o pirata informático não poderá ser senão punido pela prática dos crimes. Por outro lado, em termos civilísticos, concluiu-se que recai uma presunção de culpa sobre a entidade bancária, essencialmente, numa ótica de defesa do consumidor (neste caso, defesa do cliente titular da conta bancária), com exceção dos casos em que o próprio cliente, atuando com dolo ou negligência grosseira, permitiu a perpetração de movimentações fraudulentas na sua conta bancária.

É este o critério adotado pelo Regime Jurídico de Serviços de Pagamento e da Moeda Eletrónica, e também pela DSP 2, regulamentação que traz ainda consigo novos e importantes vetores em sede de segurança e proteção dos intervenientes, nomeadamente a introdução da autenticação forte aos utilizadores no momento da iniciação de uma transação de pagamento eletrónico.

Pretende-se, assim, proteger o cliente consumidor de eventuais condutas capazes de pôr em causa a segurança do cliente e do banco.

Recentemente transposta para o ordenamento jurídico pelo DL n.º 91/2018 de 12 de novembro, espera-se que esta nova Diretiva de Serviços de Pagamentos confira uma maior robustez na segurança dos pagamentos eletrónicos, de forma a proteger os

consumidores e a prevenir os riscos operacionais das instituições bancárias, minimizando a imputação das responsabilidades que sobre as partes recaem.

-BIBLIOGRAFIA-

REFERÊNCIAS BIBLIOGRÁFICAS:

- ANTUNES, JOSÉ ENGRÁCIA, *Direito dos Contratos Comerciais*. Coimbra: Almedina, 2009;
- BARREIRA, CAROLINA, *"*Home banking: a repartição dos prejuízos decorrentes de fraude informática*"*, in *Revista Eletrónica de Direito*, n.º 3, Faculdade de Direito da Universidade do Porto, outubro de 2015;
- CORDEIRO, ANTÓNIO MENEZES - *Manual de Direito Bancário*, 3.ª edição, Coimbra, Almedina, 2006;
- CORREIA, PEDRO RIBEIRO e JESUS, INÊS ANDRADE, "Combate às transferências bancárias ilegítimas pela Internet no direito português: entre as experiências domésticas e políticas globais concertadas", in *Revista Direito GV*, maio-agosto 2016;
- FARIA, JOSÉ MANUEL, "Acesso a contas bancárias por terceiros no âmbito de operações de pagamento", in *Revista da Banca*, Lisboa: Associação Portuguesa de Bancos. N.º 71 (janeiro/junho 2011);
- FERREIRA, ANTÓNIO PEDRO DE AZEVEDO, *A relação negocial bancária – conceito e estrutura*, Lisboa, Quid Iuris, 2005;
- FREIRE VICENTE, " Cibersegurança e Ciberdefesa: a inevitabilidade de adoção de uma estratégia nacional", in *Revista Segurança e Defesa,* 21, maio-agosto de 2012;
- GAMEIRO, CARLOS "O Risco da Informação em Ambiente Electrónico", in Estudos de Direito e Segurança, (Coord. Bacelar Gouveia e Rui Pereira), Coimbra, Almedina, 2007;
- GERALDES, ANA VAZ - *"Phishing: fraude online"*, in *Revista da Faculdade de Direito da Universidade de Lisboa*, 2013, Coimbra Editora;
- GILMOUR STAN, "Policing crime and terrorismo in cyberspace: ano overview", 2014;
- GUIMARÃES, MARIA RAQUEL, *As transferências eletrónicas de fundos e os cartões de débito*, Coimbra, Almedina, 1999;
- GUIMARÃES, MARIA RAQUEL, *Comércio eletrónico e transferências eletrónicas de fundos. O Comércio Eletrónico – Estudos Jurídico-Económicos*, Coimbra, Almedina, 2002;

- GUIMARÃES, MARIA RAQUEL **"**As operações fraudulentas de *home banking* na jurisprudência recente - Ac. do STJ de 18.12.2013" in *Cadernos de Direito Privado*, 2015;
- GUIMARÃES, MARIA RAQUEL *O contrato-Quadro no âmbito da utilização de meios de pagamento electrónicos*, Coimbra, Wolters Kluwer/Coimbra Editora, 2011;
- GUIMARÃES, MARIA RAQUEL "O pagamento com cartão de crédito no comércio electrónico: evoluções legislativas recentes", in *Revista da Faculdade de Direito da Universidade do Porto*, ano IX, Coimbra, Coimbra Editora, 2012;
- GUIMARÃES, MARIA RAQUEL "Os cartões bancários e as cláusulas contratuais gerais na jurisprudência portuguesa e espanhola - Breve análise da jurisprudência mais recente dos tribunais superiores portugueses e espanhóis em matéria de cláusulas contratuais gerais inseridas nos contratos de utilização de cartões bancários", in *Revista de Direito e de Estudos Sociais*, ano XLIII, janeiro/março, n.º 1, Editorial Verbo, 2002;
- GUIMARÃES, MARIA RAQUEL, "A repartição dos prejuízos decorrentes de operações fraudulentas de banca eletrónica *(home banking*): anotação ao Acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09", in *Cadernos de Direito Privado*, Braga, CEJUR. Nº 41 (janeiro/março 2013);
- GUIMARÃES, MARIA RAQUEL, "Algumas considerações sobre o Aviso n.º 11/2001 do Banco de Portugal, de 20 de Novembro, relativo aos cartões de crédito e de débito", in *Revista da Faculdade de Direito da Universidade do Porto*, I;
- GUIMARÃES, MARIA RAQUEL, "(Ainda) a responsabilidade pelo uso indevido de instrumento de pagamento electrónicos em operações presenciais e á distancia - Análise do regime introduzido pelo Anexo I do Decreto-lei nº 317/2009, de 30 de outubro (RSP), e das alterações que se perspectivam face à proposta de directiva do Parlamento Europeu e do Conselho, de 24 de julho de 2013" in *I Congresso de Direito Bancário*, Coimbra, Almedina, 2015;
- GUIMARÃES, MARIA RAQUEL, "A fraude no comércio eletrónico: o problema da repartição do risco por pagamentos fraudulentos", in *Infrações Económicas e Financeiras: Estudos de Criminologia e Direito* (J. Cruz, C. Cardoso, A. L. Leite, R. Faria, *coordenação*). Coimbra Editora, 2013;

- MARTINS, MARCO, "Ciberespaço: uma nova realidade para a segurança internacional", *in Nação e Defesa*, Instituto da Defesa Nacional, 2012;
- MONTEIRO, ANTÓNIO PINTO, *Contratos de distribuição comercial*, Almedina, 2004;
- MONTEIRO, ANTÓNIO PINTO, "A Resposta do Ordenamento Jurídico Português à Contratação Bancária pelo Consumidor" in *Revista de Legislação e Jurisprudência,* n.º 3987, ano 143, julho/agosto de 2014, Coimbra Editora;
- MONTEIRO, VASCO, "Transformação digital do sector bancário. Desenvolvimentos recentes e futuros no quadro legal e regulatório" in *InforBANCA 111, nov'17-fev'18;*
- MOREIRA, JOÃO MANUEL DIAS, "O impacto do ciberespaço como nova dimensão nos conflitos", in Boletim Ensino, Investigação n.º 13, 2012
- PALMA, MARIA FERNANDA /DIAS, AUGUSTO SILVA /MENDES, PAULO SOUSA, *Direito Penal Económico e Financeiro*, Coimbra Editora;
- PEREIRA, JOEL TIMÓTEO RAMOS, *Direito da Internet e Comércio Eletrónico*, Lisboa, Quid Iuris, 2001;
- SANTOS, RITA COELHO, *O tratamento jurídico-penal da transferência de fundos monetários através da manipulação ilícita dos sistemas informáticos*, Coimbra, Coimbra Editora, 2005;
- SILVA, JOÃO CALVÃO DA, *Direito Bancário*. Coimbra: Almedina, 2001;
- SILVA, JOÃO CALVÃO DA, *Banca, Bolsa e Seguros – Direito europeu e português*, Tomo I, 2ª edição (revista e aumentada). Coimbra: Almedina, 2007;
- SOARES, QUIRINO, "Contratos Bancários", in *Scientia Iuridica,* separata janeiro-abril 2003, tomo LII, n.º 295, Universidade do Minho;
- VARELA, JOÃO DE MATOS ANTUNES, "Depósito Bancário – Depósito a prazo em regime de solidariedade", in *Revista da Banca*, Lisboa, Associação Portuguesa de Bancos. Nº 21 (Janeiro/Março de 1992);
- VERDELHO, PEDRO, "Phishing e outras formas de defraudação nas redes de comunicação" in *Direito da Sociedade da Informação* (Oliveira Ascensão, coordenação). Vol. VIII. Coimbra Editora, 2009;

JURISPRUDÊNCIA:

Tribunal da Relação de Lisboa:

- Acórdão do Tribunal da Relação de Lisboa, de 24 de janeiro de 2007, processo n.º 5990/2006-3;
- Acórdão do Tribunal da Relação de Lisboa, de 03 de maio de 2007, processo n.º 10042/06-5;
- Acórdão do Tribunal da Relação de Lisboa de 26 de outubro de 2010, processo n.º 1943/09.1TJLSB.L1-7;
- Acórdão do Tribunal da Relação de Lisboa, de 30 de junho de 2011, processo n.º 189/09.3JASTB.L1-5;
- Acórdão do Tribunal da Relação de Lisboa, de 24 de maio de 2012, processo n.º 192119/11.8YIPRT.L1-2;
- Acórdão do Tribunal da Relação de Lisboa de 04 de julho de 2013, processo n.º 103841/11.3YIPRT.L1-2;
- Acórdão do Tribunal da Relação de Lisboa, de 5 de novembro de 2013, processo n.º 9821/11.8T2SNT.L1-1;
- Acórdão do Tribunal da Relação de Lisboa, de 12 de dezembro de 2013, processo n.º 164/11.8TBSRT.L1-6;
- Acórdão do Tribunal da Relação de Lisboa, de 3 de março de 2015, processo n.º 1727/13.2TJLSB.L1-1;
- Acórdão do Tribunal da Relação de Lisboa, de 21 de maio de 2015, processo n.º 337/14.1YXLSB.L1-2;
- Acórdão do Tribunal da Relação de Lisboa, de 15 de março de 2016, processo n.º 1063/12.1TVLSB.L1-1;
- Acórdão do Tribunal da Relação de Lisboa, de 12 de outubro de 2017, processo n.º 4761/15.4T8VNG-2;
- Acórdão do Tribunal da Relação de Lisboa, de 22 de março de 2018, processo n.º 14202/16.4T8LSB.L1-2.

Tribunal da Relação de Coimbra:

- Acórdão do Tribunal da Relação de Coimbra, de 15 de junho de 2010, processo n.º 1408/08.9TBACB.C1;
- Acórdão do Tribunal da Relação de Coimbra, de 2 de fevereiro de 2016, processo n.º 902/13.4TBCNT.C1;
- Acórdão do Tribunal da Relação de Coimbra, no Acórdão de 17 de fevereiro de 2016, processo n.º 2119/11.TALRA.C2;
- Acórdão do Tribunal da Relação de Coimbra, de 20 de setembro de 2016 processo n.º 183554/14.0YIPRT.C1.

Tribunal da Relação do Porto:

- Acórdão do Tribunal da Relação do Porto, de 30 de agosto de 2009, processo n.º 15273/02.6TDLSB.P1;
- Acórdão do Tribunal da Relação do Porto, de 21 de novembro de 2012, processo n.º 1001/11.9JAPRT.P1;
- Acórdão do Tribunal da Relação do Porto, de 24 de abril de 2013, processo n.º 585/11.6PAOVR.P1;
- Acórdão do Tribunal da Relação do Porto, de 08 de janeiro 2014, processo n.º 1170/09.8JAPRT.P2;
- Acórdão do Tribunal da Relação do Porto de 07 de outubro de 2014, processo n.º 747/12.9TJPRT.P1;
- Acórdão do Tribunal da Relação do Porto, de 03 de fevereiro de 2016, processo n.º 482/10.2SJPRT.P1;
- Acórdão do Tribunal da Relação do Porto, de 29 de fevereiro de 2018, processo n.º 572/17.0T8PRT.P1.

Tribunal da Relação de Guimarães:

- Acórdão do Tribunal da Relação de Guimarães, de 23 de Outubro de 2012, processo n.º 305/09;

- Acórdão do Tribunal da Relação de Guimarães, de 23 de dezembro de 2012, processo n.º 305/09.5TBCBT.G1;
- Acórdão do Tribunal da Relação de Guimarães, de 25 de novembro de 2013, processo n.º 2869/11.4TBGMR.G1;
- Acórdão do Tribunal da Relação de Guimarães de 17 de Dezembro de 2014, processo n.º 1910/12.8TBVCT.G1.

Tribunal da Relação de Évora:

- Acórdão do Tribunal da Relação de Évora, datado de 25 de junho de 2015 processo n.º 3052/11.4TBSTR.E1;

Supremo Tribunal de Justiça:

- Acórdão do Supremo Tribunal de Justiça, de 14 de julho de 2004, processo n.º 04P3287;
- Acórdão do Supremo Tribunal de Justiça de 06 de junho de 2005, processo n.º 05P2253;
- Acórdão do Supremo Tribunal de Justiça de 20 de setembro de 2006, processo n.º 06P1942;
- Acórdão do Supremo Tribunal de Justiça, de 05 de novembro de 2008, processo n.º 08P2817;
- Acórdão do Supremo Tribunal de Justiça, de 18 de dezembro de 2013, processo n.º 6479/09.8TBBRG.G1.S1.

OUTRAS FONTES:

Sites consultados:

- www.dgsi.pt
- www.clientebancario.bportugal.pt
- www.bportugal.pt
- www.jornaldenegocios.pt

- www.sapo.pt
- www.dn.pt
- www.ifb.pt
- www.eba.europa.eu
- www.eur-lex.europa.eu
- www.expresso.pt
- www.jornaleconomico.sapo.pt
- www.ium.pt.

Conferências assistidas:

- "O *phishing* de dados bancários e o *pharming* de contas. Análise jurisprudencial", oradora Maria Raquel Guimarães, in *III Congresso de Direito Bancário*, 22 de Setembro de 2017

- ÍNDICE -

- ERRATA –

Errata referente à dissertação de Mestrado de Direito e Mercados Financeiros intitulada "Operações Abusivas na Banca Eletrónica - A Imputação de Responsabilidades pelas Perdas Resultantes da Movimentação Não Autorizada de Fundos", realizada por Inês Custódio Alves.

Página	Linha	Onde se lê	Deve ler-se
21	15	"Assim, a entidade bancária confere a possibilidade de os seus clientes usufruírem de um serviço que lhes permita a gestão e movimentação dos fundos disponíveis nas suas contas bancárias."	Trata-se de uma repetição, pelo que este parágrafo não deveria constar.
24	12	"Neste sentido, e à luz do disposto no artigo 111.º n.º 2 do RSP (…)"	"Neste sentido, e à luz do disposto no artigo 111.º n.º 3 do RSP (…)"
25	3	" (…) veio implementar exigências adicionais a nível de autenticação forte na autorização da operação de pagamento, tendo sido (…)"	" (…) veio implementar exigências adicionais a nível de autenticação forte na autorização da operação de pagamento."
25	8	" A confidencialidade dos dados financeiros do utilizador, são uma premissa que se pretende assegurar com as novas exigências comunitárias definidas na nova Diretiva de Serviço Pagamentos, que adiante se abordará."	" A confidencialidade dos dados financeiros do utilizador, são uma premissa que se pretende assegurar com as novas exigências comunitárias definidas na nova Diretiva dos Serviços de Pagamentos, que adiante se abordará."
27	6	"(…) para elucidar o utilizador das medidas preventivas de deverá adotar para preservação e segurança do instrumento de pagamento."	"(…) para elucidar o utilizador das medidas preventivas que deverá adotar para preservação e segurança do instrumento de pagamento."

30	9	“Do anonimato, simplicidade e celeridade nas transações que a Internet facvorece, nasce um palco propício a atuações ilícitas por parte de terceiros.”	“Do anonimato, simplicidade e celeridade nas transações que a Internet oferece, nasce um palco propício a atuações ilícitas por parte de terceiros.”
50	Nota rodapé 85, linha 4	“(…) contas bancárias de um consumidor em um único lugar”	“(…) contas bancárias de um consumidor num único lugar”