Universidade Católica Portuguesa de Lisboa

As debilidades do serviço de *homebanking*, em especial quanto aos crimes de fraude informática de *phishing* e *pharming*. A questão da responsabilidade no âmbito das operações bancárias não autorizadas.

Dissertação de Mestrado

Orientador: Professor, Dr. Francisco Mendes Correia

Discente: Verónica Santos

Mestrado em Direito Empresarial

2018

Ao meu pai, mãe e avós,

E ao meu namorado,

Pelo amor e suporte incondicional,

Obrigada.

Termo de pesquisa

Home banking; Contrato quadro de home banking; Instrumento de pagamento; Deveres jurídicos; Internet; Fraude Informática; Repartição dos prejuízos; Autenticação; Phishing; Pharming

Índice

Lista de Abreviaturas

Ac.	Acórdão
Art.	Artigo
CC	Código Civil
Cfr.	Confrontar
Cit.	Citado
DL	Decreto-lei
Nº	Número
p.	Página
pp.	Páginas
Proc.	Processo
PSD	Diretiva relativa aos Serviços de Pagamento 2007/64/CE
PSD	Diretiva relativa aos Serviços de Pagamento 2015/2366 do Parlamento Europeu e do Conselho que revoga a Diretiva 2007/64/CE
RGICSF	Regime Geral dos Serviços de Pagamento e Moeda Eletrónica
RSP	Regime Jurídico dos Serviços de Pagamento e Moeda Eletrónica
STJ	Supremo Tribunal de Justiça

TRE	Tribunal da Relação de Évora
TRG	Tribunal da Relação de Guimarães
TRL	Tribunal da Relação de Lisboa
TRP	Tribunal da Relação do Porto
Vol.	Volume

1. Introdução

A internet tem, no final de junho de 2017, perto de 3.885.567.619 milhares de utilizadores mundiais[1]. Na Europa, em particular, é corrente assumir-se que uma em cada duas pessoas é utilizadora diária de Internet. Ou seja, seguramente cerca de metade dos europeus utiliza a Internet com regularidade e habitualidade, em casa, no seu local de trabalho, para desenvolver as suas atividades de trabalho ou de lazer[2].

Paralela a esta expansão deparamo-nos também com outra realidade económica em constante crescimento: o comércio eletrónico que apresenta cada vez maiores índices de utilização.[3]

Assim e fruto desta evolução tecnológica que sem tem vindo fazer sentir nas últimas décadas, encontramos hoje, um paradigma das relações bancárias, diferente do que se apresentava há uns anos atrás. Começo primeiramente por referir-me, a todo o progresso a que assistimos desde de a emissão de cartões de crédito e de débito, que vieram possibilitar que fossem realizadas várias operações, como por exemplo, operações de pagamento, de transferência, depósito entre outras, através de um terminal de caixa automática, também denominado por ATM[4].

Toda esta revolução tecnológica proporcionou também a convergência de muitas transações de gestão financeira que anteriormente eram consideradas díspares. Todos estes fatores abriram o caminho para que se ofereçam produtos e serviços bancários a diferentes clientes com diferentes necessidades bancárias, como corporações, pequenas empresas e indivíduos, todos dentro de uma plataforma baseada na Internet.[5]

Os clientes das instituições bancárias veem-se agora munidos de uma serie de instrumentos que lhes permitem de forma rápida e instantânea realizar uma serie de operações, como refere e muito pertinentemente o Professor FRANCISCO MENDES

[1] Este dado refere-se a junho de 2017. Vejam-se as estatísticas atualizadas em: www.internetworldstats.com/stats.htm
[2] VERDELHO, PEDRO em: "*Phishing* e outras formas de defraudação nas redes de comunicação", p. 407.
[3] Ibidem Verdelho, Pedro p.409
[4] Vide Acódão do STJ de 18/12/2013 (Ana Paula Boularot).
[5] "*Technology has permitted the convergence of many financial management transactions that previously were considered disparate. This has opened the path for offering banking products and services to different customers with different banking needs, such as corporations, small businesses and individuals all within one internet-based platform".* Law & Regulation of Eletronic Finance & Internet Banking – Introduction and Overview (2014), p. 4

CORREIA[6], as operações de pagamento executadas por bancos e outros prestadores de serviços são já incontornáveis no cumprimento quotidiano das obrigações pecuniárias assumidas nos mais diversos contextos desde comerciais a pessoais, tanto por particulares como por empresas. É neste contexto que surge o tão conhecido serviço de *home banking*. Através deste sistema é possível aceder a uma multiplicidade de operações bancárias utilizando para o efeito um instrumento com acesso à internet.

Tanto o alargamento do comércio eletrónico como a evolução que se constatou quanto aos meios de pagamento[7], tiveram a sua razão de ser na Internet, que de facto possibilitou todas estas mudanças com que agora nos deparamos. Nomeadamente, hoje, a celebração de contratos prescindiu do fator "físico ou presencial" conseguindo-se agora aceder a diferentes mercados e certos bens, sendo fácil e rápido pagar qualquer bem ou serviço adquirido. A distância deixou de ser um obstáculo à celebração de contratos bem como às várias transações comerciais.

Contudo, e se por um lado a Internet e consequentemente toda esta evolução associada ao desenvolvimento do mundo digital a que aqui me refiro, trouxeram enumeras vantagens, das quais faço sobressair a celeridade e a comodidade de certos serviços em especial, no que diz respeito ao serviço de *home banking*, por outro lado e a ela estão associados vários malefícios.

É neste contexto de desvantagens, nomeadamente nos serviços de banca eletrónica que o conceito de fraude assume uma especial relevância. Não são raras as situações em que uma pessoa se vê confrontada com a utilização abusiva do seu cartão de débito ou de créditos por variados motivos, ou porque os mesmos foram clonados, ou furtados, ou ainda porque foram usados de forma abusiva e indevida por um sujeito que não era titular da conta de pagamento a que os mesmos estavam associados.

No âmbito do serviço de *home banking*, a atuação típica que configura uma situação fraudulenta baseia-se na intromissão de pessoa não autorizada em determinada rede informática através de um computador, acompanhada da movimentação de saldo bancário para contas de terceiro, ou seja, existe um acesso não autorizado a certa conta

[6] CORREIA, FRANCISCO MENDES em "Operações não autorizadas e o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, p.701 in Revista de Direito Civil, Ano II (2017) nº 3.

[7] Sobre os meios de pagamento, vide MARIA VICTORIA ROCHA em: "Novos meios de pagamento no comércio eletrónico (e-commerce), in: Direito da sociedade de informação/ Alberto de Sá e Mello… [et al.] – Coimbra: Coimbra Editora, 2004. – Vol. 5, p. 203-214.

de depósito através da introdução não autorizada das credenciais de acesso ao serviço em causa, situação esta que pela sua relevância estatística é merecedora de análise e destaque.

Os ataques cibernautas tornaram-se assim comuns, tendo surgido novas modalidades de atuações ilícitas como o *phishing* e o *pharming*. As mesmas constituem uma das formas mais lucrativas do cibercrime. Segundo os indicadores do APWG (*Anti-Phishing Working Group*[8]), o número de ataques não para de aumentar e o setor dos serviços de pagamento é o mais afetado.[9]

A questão da repartição dos prejuízos que decorrem de situações que configuram operações fraudulentas através do serviço de *home banking*, tem merecido a atenção dos nossos tribunais superiores nos últimos anos. Mais precisamente desde 2010, data da primeira decisão dos tribunais superiores portugueses sobre este assunto e que foi proferida pelo TRL em 26/10/2010.[10]

De entre os vários cenários que uma ordem de pagamento pode criar, sendo o primeiro uma operação realmente autorizada pelo utilizador/ cliente, o segundo uma operação não autorizada e a sua execução se deva a factos imputáveis ao prestador de serviços a título censurável, o terceiro visa uma operação novamente não autorizada e a sua execução fique a dever-se a factos imputáveis a título censurável ao utilizador e por fim o quarto e último cenário que reflete uma operação não autorizada cuja execução fique a dever-se a factos imputáveis a terceiro a título censurável.

Face ao exposto, cabe referir que a presente dissertação versará sobre a questão da repartição responsabilidade o mesmo será dizer dos prejuízos decorrentes de operações fraudulentas e não autorizadas pelos titulares legítimos das contas bancárias afetadas, através de ataques de *phishing* e de *pharming*, realizados através do serviço de *home banking*, problematizando por um lado a questão da tutela do cliente bancário, e por outro o ónus que recai sobre o prestador de serviços em termos de prova. Em suma e perante uma operação não autorizada pelo titular da conta e feita em benefício de

[8] *O Anti -Phishing Working Group*, é uma aliança a nível mundial que visa unificar a resposta global ao cibercrime. O APWG opera através de uma organização sem fins lucrativos, com sede nos EUA e do APWG.EU, fundação de pesquisa sem fins lucrativos estabelecida em Barcelona, em 2013. In: http://apwg.org/about-APWG/

[9] BARREIRA, CAROLINA FRANÇA "*HOME Banking*, a repartição dos prejuízos decorrentes da fraude online" P.29

[10] Ac. TRL de 20.10.2010, Proc. Nº 1943/09.1TJLSB1.7, Relator: Maria Amélia Ribeiro, Disponível em: http://www.dgsi.pt/jtrl1.nsf/0/20a5cc803440273e802577ed003c0299?OpenDocument

terceiro, serão sobretudo discutidas as pretensões de cada uma das partes bem como o seu respetivo fundamento.

Para o efeito será analisado o regime especial constante no DL 317/2009, bem como o regime comum previsto no Código Civil, deixando de fora a vertente penal da matéria em causa. A isto acresce uma breve análise da jurisprudência nos casos de fraude *online* em sede de *home banking*, bem como uma tomada de posição critica sobre certas decisões dos tribunais e na minha opinião, na pesada exigência de prova que recai sobre o Banco sobretudo nos casos de *phishing*, que a meu ver deveriam colocar o utilizador numa posição merecedora de um maior grau de censura, ao contrário do que se passará nos casos de *pharming,* situação esta que irei descortinar.

Em suma, com este trabalho para além da análise formal de todas as figuras aqui mencionadas, desde do contrato de *home banking* como os crimes de fraude informática de *phishing* e de *pharming*, a presente dissertação trará como novidade uma nova perspetiva critica sobre os critérios a ter em conta no momento da tomada de decisão dos Tribunais, bem como uma proposta de análise de certos casos concretos.

2.Do Sistema

2.1 Noção e especificidades do serviço de *home banking*

Conhecido por *home banking* (banco internético (do inglês *internet banking), e-banking*, banco *online*, *online banking*, às vezes também denominado de banco virtual, banco eletrónico), este serviço posto à disposição pela entidade bancária, possibilita aos seus clientes, mediante a aceitação de determinados condicionalismos a utilização de uma panóplia de operações bancárias *online,* relativamente às contas de que sejam titulares, utilizando para o efeito canais telemáticos que conjugam os meios informáticos com os meios de comunicação à distância, através de uma página segura do banco. Este serviço reveste uma grande utilidade, especialmente no que diz respeito

à utilização de serviços do banco fora do seu horário de atendimento ou qualquer lugar onde haja acesso à internet.[11]

Através do referido serviço, os clientes podem efetuar operações como a consulta de saldos, pagamentos de serviços/compras, carregamentos de telemóveis, transferências de valores depositados para contas próprias ou de terceiros, para a mesma ou para diversa instituição de crédito.

A banca eletrónica tem por isto apresentado uma crescente utilização pelo facilitismo que proporciona aos seus utilizadores, acabando com o fator físico ou presencial criando assim a possibilidade de se realizarem todas as operações acima mencionadas, bem como variadíssimas transações comerciais.

Neste serviço de *home banking*, a entidade bancária entrega ao cliente as chaves de acesso ao serviço: o número de contrato, um código secreto e um cartão matriz de coordenadas. Assim e para aceder ao serviço, o cliente dirige-se à página do banco, seleciona a área destinada ao registo do cliente autentica-se inserindo o seu número de contrato e a respetiva senha de acesso.[12]

Caso o utilizador pretenda somente consultar informações sobre a sua conta bancária, não terá que efetuar mais nenhum mecanismo de segurança, ao contrário do que se passa nas situações em que o utilizador/cliente pretende efetuar uma operação bancária, como por exemplo uma transferência para outra conta. Aqui o banco exige que o cliente indique não só o número de contrato e a senha que lhe foi concedida pelo Banco, como ainda se exige certa coordenada do cartão matriz que lhe foi também fornecido.

Estas senhas de acesso são assim solicitadas no final de cada operação realizada por meios telemáticos, de modo a autenticá-las, uma vez que o cartão matriz apenas deverá ser do conhecimento do cliente/utilizador, sendo este o único a poder utilizá-lo, não lhe sendo permitido fornecer nenhum dos dados nele inseridos a terceiros, uma vez que, quer o protocolo da página bancária, quer o tráfego de toda a informação nela processada, o que inclui as sobreditas senhas de acesso, são encriptadas, tornando quase impossível que um terceiro obtenha ou altere a informação depois de enviada.[13]

[11] Ac. STJ 18.12.2013, Proc. 6479/09 (Ana Paula Bularout). Disponível em: www.dgsi.pt.
[12] BARREIRA, CAROLINA FRANÇA "*HOME Banking*, a repartição dos prejuízos decorrentes da fraude online" p. 38
[13] Ac. STJ, de 18/12/2013 Proc. 6479/09 (Ana Paula Bularout). Disponível em: www.dgsi.pt.

Por sua vez, o contrato de banca eletrónica configura um contrato socialmente típico, mas legalmente atípico uma vez que, e apesar de não se encontrar previsto na lei, é comummente solicitado na prática, pelo que adota um figurino comum conhecido por todos[14]. Este modelo que referi como comum, deriva da utilização pelos bancos de cláusulas contratuais gerais[15] muito semelhantes nos contratos de banca eletrónica.

2.2 O complexo contratual que sustenta as operações de *home banking*

A realização de operações de *home banking,* transferências eletrónicas, pagamentos de serviços entre outras, pressupõem um complexo de contratos que permitem regular de antemão, as relações entre o banco prestador do serviço e o seu cliente, utilizador do mesmo, simplificando os procedimentos a adotar no momento em que essas operações são concretizadas.

O contrato de *home banking* insere-se numa relação negocial complexa por englobar várias figuras jurídicas. O mesmo inicia-se através de um CONTRATO DE ABERTURA DE CONTA, e da constituição de DEPÓSITOS de quantias em conta por parte do titular, numa verdadeira coligação de contratos[16], em que há certa dependência entre os mesmos[17]. Esta dependência é criada pela relação de motivação que afeta estes contratos. Contudo, este nexo de ligação não destrói a individualidade dos mesmos.[18]

a) Contrato de abertura de conta como contrato – quadro

Designa-se por contrato de conta bancária (ou abertura de conta) o acordo havido entre uma instituição bancária e um cliente «*através do qual se constitui, disciplina e baliza a respetiva relação jurídica bancária*».[19]

---

[14] CORDEIRO, ANTÓNIO MENEZES – Tratado de Direito Civil Português, Tomo I. 3ª Edição (reimpressão). Coimbra: Almedina, 2007, p.472-473.
[15] Exemplo de um contrato de adesão com recurso às clausulas contratuais gerais: https://www.montepio.pt/iwov-resources/SitePublico/documentos/pt_PT/pdf-pmc/mbway-condicoes-gerais-utilizador.pdf.
[16] Entendimento perfilhado pelo Ac. do TRG de 23/10/2012, Proc. 305/09.
[17] Neste sentido, veja-se o entendimento do TRL nos acórdãos de 26/10/2010 e de 24/5/2012.
[18] A, VARELA- Das obrigações em Geral, Vol. I, 10ª Ed., Almedina, 2003, p.202-284.
[19] ANTUNES, ENGRÁCIA em Direito dos Contratos Comerciais, p. 483

A relação bancária que se estabelece entre o banco e os seus clientes é desencadeada por um contrato de abertura de conta. Se atentarmos na letra dos considerandos do Aviso do Banco de Portugal nº 11/2005, de 21/7[20], o Banco de Portugal afirma que "*a abertura de conta de depósito bancário constitui uma operação bancária central pela qual se inicia, com frequência uma relação de negócio duradoura entre o cliente e a instituição de crédito"*. Na esteira do entendimento de que a abertura de conta funda a relação com o banco, os professores ANTÓNIO MENEZES CORDEIRO, LUÍS MIGUEL PESTANA DE VASCONCELOS e ainda o professor JOÃO CALVÃO DA SILVA.[21]

Nas palavras da Professora MARIA RAQUEL GUIMARÃES a abertura de conta funciona como um "contrato dos contratos".[22] Dai a sua classificação como contrato-quadro celebrado mediante a adesão do cliente bancário a um conjunto de cláusulas contratuais gerais pré-determinadas pela instituição financeira. Esta classificação foi adotada não só pelo STJ, nomeadamente no Ac. de 3/4/2003[23], como também pelo próprio legislador nacional no texto preambular do DL nº 95/2006, de 29/5 que transpôs para o direito interno a Diretiva 2002/65/CE do Parlamento Europeu e do Conselho, de 23/9. No contrato de abertura de conta são assim convencionadas as condições em que os posteriores atos de execução (i.e. transferências, débitos diretos, pagamentos de serviços entre outras) da relação bancária vão ser concretizados.

Associado a essa abertura de conta, aparece-nos o depósito bancário (regulado pelo DL 430/91, de 2 de novembro com as alterações introduzidas pelo DL 88/2008, de 29 de maio), operação essa que se encontra indissociavelmente ligada à abertura de conta e que constitui um pressuposto *sine qua non* desta, já que nenhuma conta poderá ser aberta sem quaisquer fundos.[24]Assim, e nos casos em que perante certa ordem de pagamento do ordenante não se verifique a existência de saldo bancário na conta do cliente, o mesmo será dizer que não se encontra verificada uma condição material para que seja realizada a operação em causa, condição esta que já foi previamente acordada aquando da realização do contrato de abertura de conta.

---

[20] Aviso do Banco de Portugal nº 11/2005, de 21/7 (publicado no DR, nº139, I Série-B, de 21/5/2005).

[21] Vide, CORDEIRO, ANTÓNIO MENEZES: Manual de Direito Bancário, 4ª Edição, Coimbra, Livraria Almedina, 2010, p.260-264,505-511; PESTANA DE VASCONCELOS, L. MIGUEL: Dos contratos de depósito bancário, in Revista da Faculdade de Direito da Universidade do Porto, ano VIII, Coimbra, Coimbra Editora, 2011, p. 141, 165-166.

[22] GUIMARÃES, MARIA RAQUEL em: "A repartição dos prejuízos decorrentes de operações fraudulentas de banca electrónica (*home banking*) : acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09" in: Cadernos de Direito Privado. - Braga: Centro de Estudos Jurídicos do Minho, 2003- . - n.º 41 (2013), p. 45-69

[23] Ac. STJ, de 3/4/2003 (Quirino Soares). Disponível em: www.dgsi.pt.

[24] As operações fraudulentas de *homebanking* na jurisprudência recente, Ac. do STJ de 18.12.2013, GUIMARÃES, MARIA RAQUEL in Cadernos do Direito Privado nº 49, 2015.

Pelo exposto, é percetível o porque do título na medida em que o contrato de abertura de conta está na base de enumeras operações bancárias, e até de outro tipo de contratos, servindo por isso de base e fundamento a todos eles.

b) O contrato de *home banking* como contrato-quadro

Este contrato pode também ser classificado como um contrato-quadro em relação às sucessivas operações de transferência eletrónica de fundos ordenadas através da internet.[25][26]Isto porque as operações de transferência eletrónica de fundos realizadas através de um sistema de banca ao domicílio não surgem de forma isolada ou descontextualizada, mas sim correspondem a atos de execução de um contrato previamente celebrado.

Citando um parágrafo do comentário da Professora MARIA RAQUEL GUIMARÃES ao acórdão do TRG de 23/10/2012 a autora refere que: "Sempre *que o utilizador de um serviço de banca eletrónica emite uma ordem de pagamento – um mandato de pagamento- a favor de um terceiro, é celebrado um novo contrato de execução ou de aplicação do contrato base anterior e que se rege pelo programa contratual definido, num primeiro momento, no contrato-quadro".*

Será que é de facto correto afirmar que a cada nova operação de pagamento se celebra um novo contrato de execução? Neste ponto, terei que apresentar a minha discordância com a Professora Maria Raquel Guimarães que defende um "desdobramento contratual", bem como qualifica as novas operações como novos contratos[27], na medida em que cada nova operação de pagamento consubstancia nada mais do que um ato de execução de um contrato previamente celebrado, refiro-me ao contrato de abertura de conta, veja-se para devido efeito o artigo 76 nº 1 do RJSPME em que o prestador de serviços de pagamento está obrigado a executar as operações de pagamento : no caso de estarem reunidas todas as condições previstas no contrato –

[25] "O contrato de *home banking*

[26] GUIMARÃES, MARIA RAQUEL – A repartição dos prejuízos decorrentes de operações fraudulentas de banca eletrónica (*home banking*) – Ac. do TRG de 23/10/2012, Proc. 305.09 in Cadernos do Direito Privado nº 41.

[27] GUIMARÃES, MARIA RAQUEL em: "O contrato- Quadro no âmbito da utilização de meios de pagamento Eletrónicos, Coimbra, Coimbra Editora, p. 507 e sgs.

quadro celebrado com o ordenante, o prestador de serviços de pagamento não pode recusar a execução de uma ordem de pagamento autorizada[28].

Para além do exposto veja-se que, se por um lado o prestador de serviços está obrigado a executar a instrução do ordenante conforme dispõe o artigo 76º do RSP, por outro lado, por outro lado devemos ter presente o facto de também não existir em cada nova operação de pagamento liberdade de celebração, pressuposto essencial para que possamos reiterar a afirmação de que cada ato de execução consubstancia um novo contrato.

Segundo a autora, entende-se por contrato – quadro, o contrato de base que tem por objetivo definir as principais regras sob as quais irão ser submetidos acordos a celebrar sucessivamente no futuro, referindo-se aos contratos de execução do contrato-quadro, destinados a preparar, facilitar a sua conclusão, porém sem com eles se confundirem[29].

Este entendimento do contrato de *home banking* como contrato-quadro decorre da Diretiva 2007/64/CE[30] do Parlamento Europeu e do Conselho, de 13 de novembro, relativa aos serviços de pagamento. Este conceito foi também acolhido pelo próprio Regime de Sistemas de Pagamento (RSP), que foi aprovado pelo DL nº 317/2009, de 30/10. Neste diploma o legislador define contrato-quadro como: "*um contrato de prestação de serviços de pagamento que rege a execução futura de operações de pagamento individuais e sucessivas e que pode enunciar as obrigações e condições para a abertura de uma conta de pagamento".*[31]

Este contrato servirá então de base a uma serie de atos contemporâneos ou futuros uma vez que irá determinar e estipular uma parte substancial do seu conteúdo.[32]

Em termos práticos sempre que é realizada uma operação de pagamento eletrónica através do serviço de *home banking* é celebrado um novo ato de execução deste contrato-quadro de banca eletrónica, cuja celebração apenas se torna possível devido à adesão do cliente a este serviço, por via do contrato-quadro. Assim e tendo em conta que este instituto consubstancia uma prestação de serviços, a sua subscrição faz-se

---

[28] CORREIA, FRANCISCO MENDES em "Operações não autorizadas e o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, in Revista de Direito Civil, Ano II (2017) nº 3, p. 705.

[29] GUIMARÃES, MARIA RAQUEL – O contrato-quadro. (2011),cit, p.62

[30] A presente Diretiva relativa aos serviços de pagamento no mercado interno altera as Diretivas 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE e revoga a Diretiva 97/5/CE. A presente Diretiva é de harmonização plena (artigo 86º). Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32007L0064.

[31] Vide art. 2 alínea o) do DL 317/2009

[32] ALMEIDA, CARLOS FERREIRA – Contrato bancário geral e depósito bancário, in: Coleção de Formação Continua – Direito bancário, Lisboa: Centro de Estudos Judiciários (2015) cit.., p. 26.

mediante um contrato de adesão, contrato este em que o cliente solicita à instituição bancária a utilização de um serviço informático de forma a movimentar os fundos depositados, e cujo direito de utilização do serviço surge apenas com a adesão ao contrato de banca eletrónica, mais especificamente às condições de utilização nele previstas.[33]

Conforme refere a Professora MARIA RAQUEL GUIMARÃES: "*celebrado um contrato de home banking*[34] *é acordada a prestação de um serviço de banca eletrónica ao domicílio por uma entidade bancária a um seu cliente, ambos partes no contrato".*[35]

Neste ponto julgo por conveniente mencionar as semelhanças existentes com a estrutura contratual do mandato, isto porque o prestador de serviços de pagamento atua em nome e por conta do utilizador, executando ordens de pagamento conforme as for recebendo. Os instrumentos de pagamento configuram formas pré acordadas de transmissão de ordens de pagamento, e na medida em que o prestador de serviços atua em nome e por conta do utilizador, ao abrigo de uma relação contratual não discricionária impera o princípio da autorização prévia, ou seja, é o consentimento prévio do utilizador, emitido de forma pré-determinada com o prestador de serviços, que vai legitimar a atuação em nome e por conta do utilizador.

A isto acresce o facto de o prestador de serviços ter direito a debitar da conta do utilizador as despesas incorridas por sua conta, situação está que está prevista nas condições gerais utilizadas pelos prestadores de serviços, ou seja, tal como no mandato também aqui e perante a celebração do contrato quadro é convencionada uma forma de recuperação de despesas. O prestador de serviços obriga-se a realizar certos atos jurídicos e materiais por conta do cliente ao mesmo tempo que convenciona uma forma de recuperação de despesas, tal como funciona no mandato em que o mandatário tem o direito a recuperar as despesas que teve por conta do mandante, veja-se para o efeito o artigo 1157º e 1116º al. a) do CC. Assim nas relações entre utilizador e o banco, o modo contratualmente convencionado para este reembolso será o débito na conta corrente, atendendo à convenção de conta corrente celebrada entre ambos.

---

[33] As consequências jurídicas do *Home Banking*.

[34] Estes contratos de *home banking*, assentam num conjunto de clausulas contratuais gerais, definidas de forma unilateral pela entidade bancária e antecipadamente, relativamente à celebração do contrato, tendo como destinatários os seus clientes aderentes ao serviço.

[35] GUIMARÃES, MARIA RAQUEL – As transferências eletrónicas de fundos e os cartões de débito. Alguns problemas jurídicos relacionados com as operações de levantamento de numerário e de pagamentos por meio eletrónico, Coimbra, Livraria Almedina, 1999, p. 41-45

2.3 O conteúdo da relação contratual – As obrigações que vinculam as partes

No quadro de um relacionamento estável e duradouro em que as operações bancárias individuais se sucedem, encontramos uma relação de clientela, uma relação continua de negócios entre a instituição bancária e o cliente.

Relação esta que nas palavras do Professor JOÃO CALVÃO DA SILVA[36] configura uma relação obrigacional complexa e duradoura, assente em estreita confiança pessoal entres as partes, que se inicia nas negociações de um primeiro contrato e se desenvolve continuadamente através de subsequentes e repetidas ou renovadas operações de negócio firmadas pela instituição financeira e pelo cliente, em que, a par das prestações primárias ou secundárias, surgirão obrigações acessórias de cuidado ou deveres de proteção cominados por acordo dos contraentes, por lei ou pelo principio da boa fé, para satisfação e interesse do cliente.

Assim a celebração do contrato de *home banking* irá gerar esta mesma relação complexa e duradoura da qual surgem direitos subjetivos, deveres primários de prestação, deveres secundários e acessórios, os quais muitos deles podemos encontrar no RSP diploma que regula esta matéria, nomeadamente nos artigos 67º e 68º e agora na Diretiva 2015/2366 do Parlamento Europeu e do Conselho de 25 de Novembro de 2015, doravante DSP 2 com efeitos a partir de 13 de Janeiro de 2018, relativa aos Serviços de Pagamento e que revoga a Diretiva 2007/64/CE do Parlamento Europeu e do Conselho, de 13 de novembro de 2007, relativa aos serviços de pagamento no mercado interno (DSP1) e que estabelece entre outros, deveres que devem ser observados tanto pelo prestador de serviço como pelo utilizador.

[36] SILVA, JOÃO CALVÃO DA – Serviços de pagamento e responsabilidade civil in "Estudos em homenagem a Rui Manchete, Coimbra, Almedina 2015, p. 347

2.3.1 Deveres do utilizador

I. Dever de utilização correta do serviço de *home banking*

Se atentarmos na letra do artigo 67º alínea a) do RSP conseguimos visualizar as duas obrigações principais que recaem sobre o cliente/ utilizador do serviço de banca eletrónica. Por um lado, está adstrito a utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização, ou seja, as estipuladas no contrato, e por outro a comunicar à instituição bancária, sem atrasos injustificados, logo que deles tenha conhecimento, a perda, o roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento que consubstancia um dever acessório de conduta.

A utilização correta do serviço, apesar de não consubstanciar um dever principal em sentido técnico-jurídico, apresenta-se como um dos deveres mais importantes no que diz respeito ao utilizador por se tratar de uma condição *sine qua non* do bom funcionamento do serviço, e que comporta um conjunto de deveres acessórios de conduta ligados à segurança do sistema.

Ainda sobre a utilização correta do serviço cabe referir que a mesma é um dever secundário acessório[37] da prestação principal, que visa a utilização do serviço dentro dos limites da provisão existente na conta bancária do cliente, no caso da conta à ordem, não podendo o mesmo efetuar operações a descoberto. Caso se trate de uma conta de abertura de crédito, esta atuação pautar-se-á dentro dos limites do crédito que tenha sido previamente concedido.

II. Dever de sigilo relativamente aos dispositivos de segurança associados ao *home banking*

No âmbito dos deveres acessórios de conduta criados no seio de uma relação obrigacional complexa e duradoura entre a instituição bancária e o cliente,

[37] Sobre os deveres secundários acessórios veja-se o Professor VARELA, ANTUNES – Das obrigações em geral…, cit., p.122. Assim os deveres secundários acessórios da prestação principal distinguem-se dos deveres secundários com prestação autónoma. Os deveres secundários acessórios visam assegurar a correta e integral execução da prestação principal.

aparecem-nos clausulados deveres como os de confidencialidade[38] e sigilo quanto aos dados pessoais e senhas de acesso ao sistema, nomeadamente as coordenadas do cartão matriz, a não divulgação a terceiros, bem como o dever de preservar a eficácia dos mecanismos de segurança personalizados associados ao instrumento de pagamento art. 67º nº 2 do RSP e 69º nº 2 da DSP2.

O dever de confidencialidade ou a não divulgação dos códigos de acesso consta expressamente do contrato de banca eletrónica a que o cliente aderiu. Para além disso decorrerá também daquilo a que vulgarmente chamamos de padrão de normalidade, ao qual face a ele o utilizador médio/comum de internet sabe que deverá observar.[39]

Tudo isto compreende-se, por um lado pelo facto deste serviço não ser presencial, mas sim eletrónico, e por outro pelo facto de apenas ser somente possível ao banco através desta via de disponibilização de códigos de acesso confidenciais autenticar a operação e assim aferir da legitimidade do ordenante. A isto acresce que depois de digitados os códigos de acesso e os três dígitos do cartão matriz o sistema irá reconhecer o utilizador como sendo o portador legitimo daqueles dados, bem como o cliente com o qual a instituição bancária celebrou o contrato de *home banking*, validando de imediato a operação, como referi através destes códigos de acesso o banco tem como finalidade assegurar a correspondência entre a pessoa que acedeu ao serviço com o cliente que subscreveu o contrato, ou seja, credor do serviço de banca eletrónica.

A DSP2 no considerando 72[40] refere expressamente que o utilizador, que por exemplo conserve as credenciais utilizadas para autorizar uma operação de

---

[38] Veja-se a clausula nº 2.2 do ponto IV – Prestação de serviços via telemática, disponível em: https://www.bancoctt.pt/contentAsset/raw-data/da49ab94-76e0-48de-9f77-43db8fd51558/ficheiro/ae25658c-b70b-4282-b2cb-44cf71220766/export/CG_ContaSMB.PDF

[39] Ac. TRL de 18/04/2013 (Anabela Calafate)

[40] "*Para avaliar a eventual negligência ou negligência grosseira cometida pelo utilizador dos serviços de pagamento, deverão ser tidas em conta todas as circunstâncias. Os elementos de prova e o grau da alegada negligência deverão ser avaliados nos termos do direito nacional. Todavia, embora o conceito de negligência implique uma violação do dever de diligência, a negligência grosseira deverá significar mais do que mera negligência, envolvendo uma conduta que revela um grau significativo de imprudência; por exemplo, conservar as credenciais utilizadas para autorizar uma operação de pagamento juntamente com o instrumento de pagamento, num formato que seja aberto e facilmente detetável por terceiros. As modalidades e condições contratuais relativas ao fornecimento e à utilização de um instrumento de pagamento que tenham por efeito agravar o ónus da prova que recai sobre o consumidor ou atenuar o ónus da prova que recai sobre o emitente deverão ser consideradas nulas e sem efeito. Além disso, em situações específicas e, nomeadamente quando o instrumento de pagamento não estiver presente no ponto de venda, como sucede no caso de pagamentos em linha, é adequado que o prestador de serviços de pagamento seja obrigado a apresentar provas da alegada negligência, uma vez que o ordenante apenas dispõe de meios muito limitados para o efeito em tais casos*." Considerando 72 da Diretiva 2015/2366

pagamento juntamente com o instrumento de pagamento, num formato que seja aberto e facilmente detetável por terceiros, revela por parte do utilizador uma conduta que demonstra um grau significativo de imprudência, caindo mesmo numa situação de negligencia grosseira. Ainda no contexto da referida Diretiva cabe sublinhar que tal como a DSP1 ambas referem a importância de preservar a segurança das credenciais de segurança personalizadas como forma de proteger os fundos do utilizador de serviços de pagamento e de limitar os riscos de fraude e de acesso não autorizado à conta de pagamento.

As obrigações acessórias de cuidado ou deveres de proteção derivam como vimos de acordo dos contraentes, da lei, ou do princípio da boa fé para satisfação do interesse do próprio cliente.[41]

No que diz respeito ao incumprimento destes deveres, o mesmo gera responsabilização do utilizador pelos prejuízos que ocorram nos termos do artigo 798º do CC. O utilizador responde por todos os prejuízos a título de dolo ou negligencia conforme se prevê no artigo 72º do RSP.

III. Dever de comunicação imediata ao Banco de qualquer operação de pagamento não autorizada ou do extravio dos códigos de acesso e cartão matriz

Nos termos do artigo 67º nº 1. Alínea b) do RSP e 69º nº 1 al. b) da DSP2 surge, como já referi, a obrigação do utilizador comunicar ao banco, sem atrasos injustificados, logo que deles tenha conhecimento, a perda, o roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento. Este dever é imposto contratualmente, mas mesmo que não o fosse decorreria sempre do próprio dever de guarda e sigilo a que utilizador está vinculado. Por sua vez, ao Banco competirá disponibilizar a todo o tempo os meios adequados e necessários à realização da notificação, veja-se para o efeito o artigo 70º nº 1 al. c) da Diretiva.

[4141] SILVA, JOÃO CALVÃO – Serviços de pagamento e responsabilidade civil in "Estudos em homenagem a Rui Manchete, Coimbra, Almedina 2015 p. 347.

A notificação vai ter uma importância decisiva no que toca à responsabilidade por operações bancárias não autorizadas, como veremos adiante.

De acordo com o considerando 70 da segunda Diretiva de Serviços de Pagamento, a fim de reduzir os riscos e as consequências de operações de pagamento não autorizadas ou incorretamente executadas, o utilizador dos serviços de pagamento deverá informar o mais rapidamente possível o prestador desses serviços de quaisquer reclamações relativas a operações de pagamento alegadamente não autorizadas ou incorretamente executadas, desde que o prestador de serviços de pagamento tenha cumprido as suas obrigações de informação nos termos da presente diretiva. Se o prazo de notificação for cumprido pelo utilizador do serviço de pagamento, este deverá poder tramitar essas reclamações de acordo com os prazos nacionais de prescrição. A presente diretiva não deverá afetar outras reclamações entre utilizadores e prestadores de serviços de pagamento.

2.3.1. Deveres do prestador de serviços

Nas palavras do Professor JOÃO CALVÃO DA SILVA a relação obrigacional complexa e duradoura que se gera entre a instituição financeira e o cliente, envolve deveres de diligencia e cuidado, deveres de lealdade, deveres de alerta, aviso, advertência e prevenção para certos riscos e a sua repartição, deveres de informação esclarecimento e conselho, deveres de descrição e sigilo profissional, cuja inobservância ou violação poderá por em causa a *uberrina fides* do cliente e o intituitus personae da relação e assim originar a responsabilidade da instituição financeira não criteriosa e ordenada na sua conduta leal de promoção e respeito consciencioso dos interesses que lhe estão confiados (arts. 74 e 75 do RGICSF).

O contrato de *home banking* permite como já vimos ao cliente que usufrua de um serviço de movimentação de fundos. Assim a obrigação principal do banco será a de aceitar os mandatos para pagamento que são emitidos sob a correta autenticação ao serviço por parte do cliente, como já vimos no limite do saldo disponível da sua conta à

ordem, ou caso de trate de uma conta de abertura de crédito, no limite do crédito que lhe tenha sido concedido.

I. Dever de emissão e entrega ao utilizador dos códigos de acesso e cartão matriz.

A entrega dos códigos de acesso e do cartão matriz, constitui nada mais do que o pressuposto essencial ao acesso ao serviço de banca eletrónica, uma vez que sem a entrega dos dispositivos de segurança ao utilizador, o mesmo não conseguiria aceder ao serviço online. Está aqui em causa um dever secundário acessório[42] que tem a sua base legal no artigo 68º nº 1 do RSP.

Os códigos de acesso e o cartão matriz revelam-se imprescindíveis na medida em que sem eles o cliente/ utilizador fica inviabilizado de aceder aos serviços abrangidos pelo *home banking,* nomeadamente da realização de operações de pagamento, uma vez que somente com a inserção dos dados presentes nos mesmos é que a respetiva operação de pagamento se considera autenticada e autorizada pelo cliente, o que significa que estará apta para ser executada pelo prestador de serviço.

Se atentarmos na letra do artigo 97º nº 1 da DSP2, percebemos que o sistema de autenticação que é atualmente exigido pelo RSP se encontra aquém das medidas comunitárias, uma vez que a nova Diretiva impõe a implementação de uma "autenticação forte". Nesta autenticação os Estados-Membros deverão assegurar que os prestadores de serviço apliquem esta autenticação, o mesmo será dizer que os estados devem assegurar que se inclua elementos que associem de forma dinâmica a operação a um montante específico e a um beneficiário específico.

Para melhor compreensão do conceito trazido pela DSP2 de "autenticação forte" devemos debruçar-nos sobre a definição contida no artigo 4º nº 30 da Segunda Diretiva, a qual faz menção a uma autenticação baseada " [43]*na utilização de dois ou mais*

[42] ALMEIDA COSTA, MÁRIO JÚLIO DE., em: Direito das Obrigações, 17ª edição, Almedina, Coimbra, 2009, p.77
[43] Diretiva (EU) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/EU e o Regulamento (EU) nº 1093/2010, e que revoga a Diretiva 2007/64/CE. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015L2366&from=FR

elementos pertencentes às categorias conhecimento (algo que só o utilizador conhece), posse (algo que só o utilizador possui) e inerência (algo que o utilizador é), os quais são independentes, na medida em que a violação de um deles não compromete a fiabilidade dos outros, e que é concebida de modo a proteger a confidencialidade dos dados de autenticação".

No seio das novidades trazidas pelas DSP2 encontramos a componente da segurança, que aqui nos aparece num conjunto de obrigações, nomeadamente a já referida "autenticação forte" das transações *on line* por via do utilizador/cliente, neste caso trata-se da segurança das transações e da informação que lhes dá origem, desde logo com o intuito primeiro de prevenir situações de fraude, assim no artigo 74º n º 2 conseguimos perceber como a segurança é um dos pilares sobre os quais assentou a DSP2, uma vez esta Diretiva sanciona o prestador do serviço de pagamento quando o mesmo não impõe, como é suposto, a realização da autenticação forte.

Com a omissão por parte da instituição bancária deste dever, a mesma agrava a sua responsabilidade, uma vez que, conforme dispõe o supra referido artigo, o cliente apenas suportará as perdas relativas a operações de pagamento não autorizadas quanto atue fraudulentamente. Fora destes casos em que existe esta atuação fraudulenta, será o banco, que não exigiu a autenticação forte do cliente, a suportar as perdas financeiras do mesmo, até quando o cliente/ utilizador não tenha atuado em cumprimento dos seus deveres de sigilo e confidencialidade relativamente aos dipositivos de segurança que lhe estão associados.

II. Dever de correta execução das ordens de pagamento autorizadas, quando se verifiquem reunidas todas as condições previstas no contrato.

Apesar de celebrado e acordado entre o cliente e a entidade bancária, o contrato de banca eletrónica não constitui per si uma autorização genérica para todas e quaisquer ordens de pagamento que o utilizador/cliente pretenda realizar. Assim para cada operação em concreto carece da reunião de várias manifestações negociais por parte do cliente, ou seja, a sua autorização, bem como do prestador de serviços no que diz respeito à sua concordância, para que tais ordens possam ser executadas.

É neste contexto, que o instituto do consentimento previsto no artigo 65º nº1 do RSP, bem como na DSP2 no seu artigo 64º, releva grande importância. Se atentarmos

no regime do consentimento previsto tanto no RSP como na DSP 2 percebemos que no essencial, o mesmo não difere, pelo que uma operação de pagamento só se considera autorizada e assim suscetível de execução quando o ordenante/cliente que subscreveu o serviço de banca eletrónica consentir na sua execução. O consentimento para executar uma operação de pagamento ou uma serie de operações de pagamento é dado na forma acordada entre o ordenante e o prestador de serviços de pagamento. A não observação do consentimento por parte do cliente consubstancia uma falta de autorização para a operação em causa.

Neste caso em concreto, o consentimento pelo cliente verifica-se através do sistema de autenticação, onde o utilizador digita as suas credenciais, ou seja, tanto os códigos de acesso, como os números do cartão matriz que lhe foram concedidos pelo Banco. Através deste sistema, permite-se ao utilizador que solicita o acesso ao serviço de *home banking*, identificar-se perante a instituição bancaria como sendo o cliente que solicitou aquele serviço, e que assim se apresenta como credor legitimo do serviço bancário que o Banco se obrigou a prestar.

A isto acresce que o Banco terá por devidamente consentida e por isso autorizada aquela ordem de pagamento, podendo assim executá-la.

Contudo e apesar do exposto cabe ao Banco verificar se estão reunidos os pressupostos que legitimam a execução de determinada ordem de pagamento, sendo lícito ao Banco recusar executar a ordem de pagamento tendo por motivo a inexistência de fundos que suportem tal operação. Tal será o caso de um cliente que emita uma ordem de pagamento que ultrapasse os limites do saldo disponível da conta à ordem, não estando sequer previsto no contrato a possibilidade do mesmo realizar operações a descoberto, bem como a falta de existência de quaisquer créditos.

Assim por via do artigo 76º nº 2 do RSP, bem como do artigo 79º da DSP2 o prestador de serviços de pagamento que se recuse a executar uma ordem de pagamento ou a iniciar uma operação de pagamento, a recusa, e se possível, as razões para a mesma e o procedimento a seguir para retificar os erros factuais que tenham conduzido a essa recusa são comunicados ao utilizador de serviços de pagamento.

Pelo contrário, quando estiverem reunidas as condições previstas no contrato-quadro do ordenante, o prestador de serviço não poderá recusar a execução de uma ordem de pagamento autorizada, devendo assim a instituição bancária cumprir o seu dever que sobre ela impende e que decorre da celebração do contrato de *home banking*.

III. Dever de manutenção de um serviço eficaz e seguro

Se atentarmos na letra dos artigos 73º e 75º do RGICSF "*as instituições de crédito devem assegurar, em todas as atividades que exerçam, elevados níveis de competência técnica, garantindo que a sua organização empresarial funcione com os meios humanos e materiais adequados a assegurar condições apropriadas de qualidade e eficiência*" e ainda se todos aqueles que exerçam cargos de direção, gerência, chefia ou similares procedam " com a *diligência de um gestor criterioso e ordenado, de acordo com o principio da repartição de riscos e da segurança das aplicações, tendo em conta o interesse dos depositantes*". Como refere o professor CALVÃO DA SILVA[44] trata-se da responsabilidade profissional de um bónus *paterfamilias* elevado, de quem a própria lei exige diligência qualificada. Daqui se depreende a uma imposição da própria lei que impõe à instituição bancária especiais deveres de proteção dos clientes contra os riscos operacionais de deficiências e fraudes associados à prestação dos serviços de levantamentos, pagamentos ou transferências eletrónicas, como riscos próprios da industria financeira cujos custos devem ser disseminados por todos os potenciais utilizadores (e não ficarem a cargo apenas de cada concreto utente) para potenciar a confiança no seu uso generalizado, no interesse de todos, das instituições de pagamento, dos empresários, dos comerciantes e dos consumidores.

Assim competirá ao Banco[45], enquanto prestador de banca eletrónica, criar um sistema informático de acesso à conta bancária que seja seguro e no qual o utilizador confie para realizar as suas operações de pagamento.

A par da evolução da indústria financeira, também as técnicas utilizadas pelos criminosos evoluem, sendo natural que o" combate" a este vírus caiba à indústria em termos de oferecer serviços financeiros, inovadores, cómodos, eficientes e seguros, evitando assim a interferência fraudulenta ou abusiva de terceiro, como veremos no ponto 3. com os ataques de *phishing* e de *pharming,* conducente à realização de operações não autorizadas ou ordenadas pelo cliente. Esta obrigação de manter um

[44] CALVÃO DA SILVA, JOÃO em "Estudos em Homenagem a Rui Manchete, Coimbra, Almedina 2015.

[45] Segundo MARIA RAQUEL GUIMARÃES, o Banco ao disponibilizar o serviço de *home banking* tem o dever de manter operacionais os sistemas informáticos que o sustentam, bem como de assegurar que não se verificam falhas técnicas durantes as operações de pagamento, em: "A repartição dos prejuízos decorrentes de fraude eletrónica (2013), p.60

sistema seguro e eficaz deve-se por um lado ao facto do banco ser a parte com mais capacidade patrimonial para neutralizar este tipo de risco ou perigo operacional com investimento em inovação segura, redistribuindo-o por todos os potenciais utilizadores através do preço dos instrumentos de pagamento, por outro lado, é a parte que também está em melhor posição de reduzir e redistribuir os danos provenientes de fraude ou abuso de terceiro ao menor custo através de seguros.

Logo, se o prestador de serviço está em melhor posição de evitar o risco de operação não autorizada também por ser ele que domina o seu sistema, deverá ser ele o responsável por assegurar um sistema credível e eficaz com vista a potenciar a confiança no seu uso generalizado, o mesmo será dizer que cria um incentivo à popularização do uso dos serviços, em benefício de todos, da indústria financeira, dos utilizadores e dos comerciantes.

IV. Dever de o Banco assegurar que os códigos de acesso estão somente acessíveis ao cliente

Neste ponto tanto o RSP no artigo 68º nº 1 al. a), como a DSP2 no artigo 70º nº 1 al. a) preveem um dever que impende sobre o Banco de assegurar que os mecanismos de segurança personalizados associados ao instrumento de pagamento sejam somente acessíveis ao utilizador que subscreveu o contrato de adesão, e ao qual foi conferido o direito à sua utilização.

Assim, o Banco deverá adotar todas as medidas que estejam ao seu alcance para impedir que os códigos de acesso bem como o cartão matriz sejam intercetados por terceiro, o que significa que sobre ele recai um especial dever de cuidado no momento em que procede ao envio dos mesmos. Esta mesma questão chegou a ser levantada pelo Banco de Portugal no artigo 11º do Aviso 11/2001[46] de 20 de novembro, onde se referiu que "a *entrega aos titulares quer do cartão quer do respetivo código (...) deve ser rodeada de especial cuidado, devendo ser adotadas adequadas regras de segurança que impeçam a utilização do cartão por terceiros*".

Caso se verifique esta situação, em que os códigos de acesso e cartão matriz foram intercetados por terceiro, o risco irá correr por conta do prestador do serviço de

[46] Aviso 11/2001 de 20 de novembro do Banco de Portugal, Disponível em: https://www.cgd.pt/Ajuda/Espaco-Cliente/Informacao-util/Documents/Aviso-BdP-11_2001.pdf

pagamento conforme dispõe o artigo 68º nº 2 do RSP bem como o artigo 70º nº 2 da Segunda Diretiva, o que significa que será a entidade bancária que neste caso irá suportar as perdas resultantes de extravio ou interceção dos dispositivos de segurança personalizados, nomeadamente os códigos de acesso e cartão matriz, o que é desde já compreensível uma vez que o cliente e utilizador em momento algum detém o controlo do envio destes elementos.

V. Dever de informação qualificada nomeadamente das medidas que o utilizador deve adotar para assim preservar a segurança dos seus códigos de acesso

Se atentarmos na letra do artigo 53º do RSP nomeadamente na al. e), subalínea i), o mesmo faz menção as informações que devem ser fornecidas ao utilizador do serviço de pagamento, em especial informações de caráter preventivo e retificativo que se traduzem numa descrição das medidas que o utilizador do serviço de pagamento deve tomar para preservar a segurança dos instrumentos de pagamento, bem como a forma de notificar o prestador do serviço de pagamento, dever este que deverá subsistir ao longo de toda a execução do contrato de *home banking,* e não só aplicar-se como sendo um dever de informação pré contratual como nos aparece caracterizado no artigo 52º nº 1 do RSP.

A DSP2 como já referi anteriormente, assenta um dos seus pilares na segurança dos serviços apresentado como uma das ferramentas essenciais à prossecução deste objetivo, o dever de informação que impende sobre os prestadores de serviço face aos seus utilizadores, veja-se para o efeito o considerando 57[47] da referida Diretiva, onde são mencionados os requisitos de informação prévia sobre os contrato-quadro.

[47] Considerando 57 da Diretiva (EU) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015. "Na prática, os contratos-quadro e as operações de pagamento por eles abrangidas são de longe mais comuns e importantes de um ponto de vista económico do que as operações de pagamento de caráter isolado. Se existir uma conta de pagamento ou um instrumento de pagamento específico, é necessário um contrato-quadro. Por conseguinte, os requisitos de informação prévia sobre contratos-quadro deverão ser exaustivos, devendo as informações ser sempre prestadas em papel ou noutro suporte duradouro, tais como extratos de conta impressos em terminais automáticos, CD-ROM, DVD, discos rígidos de computadores pessoais onde possa ser armazenado correio eletrónico, e sítios na Internet, desde que tais sítios possam ser consultados posteriormente durante um período de tempo suficiente aos fins a que o acesso às informações se destina e desde que esses sítios permitam a reprodução da informação aí armazenada num formato sem alterações. Todavia, o prestador de serviços de pagamento e o utilizador desses serviços deverão ter a possibilidade de acordar no contrato-quadro o modo como devem ser dadas informações subsequentes sobre as operações de pagamento executadas, estabelecendo, por exemplo, que na banca via Internet estejam disponíveis em linha todas as informações sobre a conta de pagamento." Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015L2366&from=FR

A informação deverá ser clara sobre o serviço em causa de modo a permitir que os futuros utilizadores possam efetuar uma escolha com conhecimento de causa (considerando 54).

Citando a Professora MARIA RAQUEL GUIMARÃES, está em causa "*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."* Assim, à instituição bancária é imposto um dever de elucidação do cliente, nomeadamente no que tocas aos crimes de fraude informática suscetíveis de se verificarem neste tipo de serviços.

Assim e tendo em conta que ao mesmo tempo que a indústria financeira evolui também as técnicas utilizadas pelos criminosos evoluem, cabe mencionar que não basta, para o cumprimento deste dever de informação que o Banco preste informações prévias à execução do contrato, mas sim que o faça durante toda a sua execução. Isto significa a criação de alertas existentes no momento em que qualquer cliente acede ao serviço, ou seja, avisos que aparecem ao abrir a ligação de acesso ao *home banking* e que tem de ser fechados pelo próprio cliente para que o mesmo consiga aceder serviço, situação que cria a obrigatoriedade ao cliente de o ver. O exemplo mais frequente é aquele que avisa o utilizador de que o Banco nunca pede a confirmação dos dados do cartão matriz e que as combinações que nele constam nunca deverão ser facultadas a terceiros, uma vez que este é o principal método utilizados pelos piráticas informáticos. A estes acrescem outros alertas como o de não abrir mensagens de correio eletrónico com remetente desconhecido, ou não aceder à página do banco através de links que constem em mensagens de correio eletrónico ou da lista de favoritos do browser, devendo o site oficial da instituição bancária em causa ser digitado na barra de pesquisa.

Em suma, os bancos têm atualmente aquilo que denomino de três níveis de informação: i) informação prévia à execução do contrato, ii) a informação constante no menu da página oficial do banco e por fim iii) os avisos que vão surgindo consoante a navegação do utilizador no seu serviço de *home banking*, e que como já foi explicado, implicam que esses avisos sejam fechados para que o cliente consiga avançar na sua ligação.

3. Da fraude

Como se referiu na introdução da presente dissertação, a fraude informática no *home banking* constitui uma das formas mais lucrativas do *ciber* crime[48], sobretudo no que toca ao setor dos serviços de pagamento. [49]

A realização de operações fraudulentas através de um sistema de banca ao domicílio pressupõe que o autor da fraude consiga ceder on-line, a uma conta de um determinado cliente de um banco, levando a cabo transferências de fundos, aí inscritas a débito para contas terceiras, sem a autorização do utilizador do serviço.[50]

Este acesso on-line à conta de terceiros poderá ser conseguido através de diferentes vias, nomeadamente através da utilização de programas informáticos, usurpando os mecanismos de segurança do sistema, ou mais comumente utilizando as chaves de acesso de um cliente. Quanto ao acesso às chaves de acesso, estas podem ser obtidas em situações de furto, roubo ou de perda, situação que não consubstancia um caso de fraude e que por isso não será aqui analisado, e ainda quando disponibilizadas pelo utilizador na Internet, situação que iremos aprofundar no ponto que diz respeito à responsabilidade.

Estas hipóteses em que o cliente fornece as coordenadas de acesso ao serviço na Internet, correspondem às duas modalidades de fraude informática, sobre as quais nos debruçaremos: o *phishing* e o *pharming*.

Apesar disto, oportuno será referir as situações em que existe uma utilização fraudulenta pelo próprio utilizador, quando este realiza transferências bancárias para uma terceira conta e notifica a instituição bancária, da ocorrência de uma operação não autorizada, não correspondendo com a verdade. Nesta situação, à luz do que se passa com os casos de fraude informática aqui analisados, o utilizador de *home banking* age de forma consciente e deliberada, tendo como fim a obtenção de benefícios ilegítimos, neste caso, à custa da entidade bancária.

---

[48] Em março de 2005 a polícia britânica detetou uma tentativa de apropriação de 315 milhões de euros, pertencentes à sucursal de Londres de um banco japonês, com utilização de *keylogging* e acesso à distância aos computadores do Banco. A história foi pormenorizadamente relatada pelo Público de 18 de março de 2005. Tal situação motivou o anúncio no primeiro trimestre de 2008 da formulação de propostas parlamentares britânicas no sentido da criação de um Ministério do Cibercrime e da Cibersegurança. Veja-se o Diário Digital de 10 de março de 2008.

[49] Informação disponível em: http://docs.apwg.org/reports/apwg_trends_report_h1_2017.pdf p.7

[50] A repartição de prejuízos decorrentes,,

Os ataques de *phishing* e de *pharming* subsistem na esteira da constante evolução tecnológica, que permite por um lado a obtenção de novos esquemas informáticas que detonem a segurança da banca eletrónica, e que por outro dificulta a prevenção e deteção deste tipo de fraude, permitindo por isso a sua continua proliferação.

3.1 Phishing

A ação de phishing contém um catálogo de meios destinados à obtenção de dados ou de informação confidencial dos utilizadores. Esta informação é utilizada para posterior benefício ilícito dos agentes que capturam estes dados. O *phishing* é então uma atividade fraudulenta que consiste na remessa massiva de mensagens de correio eletrónico, utilizando, portanto, a técnica de spam[515253] Estas mensagens surgem com uma aparência credível e fidedigna, e que como refere a Professora MARIA RAQUEL GUIMARÃES "camufladas" muitas vezes como sendo mensagens da própria instituição bancária. Tais mensagens incluem um link para uma página WWW[54], esta página por sua vez será uma réplica, ou seja, a reprodução aproximada da página autêntica (aqui especialmente as páginas da banca e comércio), contendo para o efeito elementos identificadores da entidade autêntica e imagens a ela referentes.

Fazendo uso da clara explicação de ANA VAZ GERALDES[55] os ataques de *phishing* desenrolam-se da seguinte forma: o *phisher* envia uma mensagem de correio eletrónico, ou um site aparentemente legitimo quanto à sua origem e conteúdo. A mensagem enviada ou o website utilizado como já referi, irá usar imagens e linguagem identificativa da entidade fidedigna. Posteriormente o *Internet Service*

[51] Segundo a empresa de segurança Symantec em dezembro de 2007 o spam constituía mais de 72% das mensagens de correio eletrónico de todo o mundo. Para o efeito, veja-se o relatório citado no Diário Digital de 15 de janeiro de 2008.
[52] O spam consiste no envio mensagens não solicitadas, isto é relativamente às quais o emissor não tem comprovativo da permissão de envio dada pelo recetor, enviadas para um grande número de destinatários, sendo o conteúdo substancialmente idêntico e que frequentemente têm objetivos comerciais. Informação disponível em: https://www.anacom.pt/render.jsp?categoryId=346972
[53] A regular esta matéria a lei 46/2012 de 29 de agosto.
[54] Neste sentido, VERDELHO, PEDRO em: "Phishing e outras formas de defraudação nas redes de comunicação" p. 413
[55] GERALDES, ANA VAZ em : " Phishing: Fraude On line, *In:* Revista da Faculdade de Direito da Universidade de Lisboa. - Lisboa: F.D.U.L . -Coimbra. V. 54, n.º 1 e 2 (2013), p. 87-102

Provider entrega a mensagem ao utilizador, que irá suscitar um falso sentido de urgência no destinatário, ao indicar que o mesmo deverá fornecer dados, aceder a determinado URL, ou descarregar um ficheiro para a resolução de determinado problema (por exemplo, a necessidade de reativação de conta de e-mail ou validação de acesso à conta bancária).

No momento em que o destinatário da mensagem realiza a ação pretendida e o *phisher* fica na posse dos dados fornecidos, é que se dá o expoente máximo do ataque. Na posse destes elementos *phisher* irá obter benefícios patrimoniais através da sua utilização ilegítima.

O *phisher* no seu fim de obter informação confidencial ou pessoal, dirige-se a vítimas especificas, fazendo recair o ataque em dois fatores cruciais. Por um lado, explorando a relação de confiança e o medo que existe entre as vítimas /utilizadores perante a mensagem, e por outro, na urgência criada para a prática da ação em causa. Assim as mensagens apresentam um conteúdo bastante específico, refiro-me às fórmulas utilizadas ou de recompensa "para evitar a fraude", "para garantir a segurança", ou com ameaça "terá de pagar uma taxa" entre outras, com o fim de atrair a vítima a aceder a certos sites, ou a descarregar ficheiros pretendidos pelo fisher.

A tudo isto acresce o facto de que as vítimas podem ser previamente estudadas[56], levando a que o *phisher* adapte o conteúdo das mensagens isco ao seu perfil.

Nas palavras de PEDRO VERDELHO, o *phishing* tem dimensão transacional, pelo que é difícil combate-lo, a não ser pela prevenção. Este tipo de fraude começou dirigido à obtenção de dados de cartões de crédito, e esta atualmente dirigido para a defraudação na área do *home banking*, em que o *phisher* na posse dos códigos de acesso *on line* que foram capturados, irá movimentar as quantias depositadas nas contas e causa, ou caso se trate de dados confidencias de cartões de crédito, com eles fazer transações não autorizadas em nome dos respetivos titulares, e em seu simultâneo prejuízo.

[56] Trata-se de Spear Phishing, dirigido na maioria das vezes a empresas e indivíduos específicos

3.2. Pharming

O *pharming* ao contrário do *phishing* apresenta-se como sendo uma técnica mais perigosa, na medida em que e mais difícil para os utilizadores de *homebanking* a detetarem, mesmo os mais avançados, isto porque este tipo de fraude consubstancia uma técnica mais sofisticada na medida em que corrompe o próprio nome de domínio de determinada instituição financeira, levando o utilizador para um site falso, que em tudo se assemelha à página verdadeira e oficial do banco. Para tal acontecer, basta que o utilizador digite o endereço web do seu banco.

Esta técnica assenta na difusão de vírus por via de spam, ou seja, por correio eletrónico, de ficheiros ocultos que se auto instalam nos computadores e sistemas informáticos das vítimas, alterando de forma oculta e sem o conhecimento do dono do computador, os arquivos do sistema, designadamente os ficheiros contendo os populares "favoritos" e o registo de cookies.[57]

Assim, sempre que determinado utilizador aceda à página do seu banco, o sistema automaticamente dirige-o para outro site, que em muito se assemelha à página verdadeira do banco (tal com acontece no *phishing*), disponibilizado *on line* e com uma oferta de serviços também idêntica ao verdadeiro site da instituição bancária. Acreditando na veracidade da página, o utilizador / cliente digita as suas palavras de acesso ao serviço de banca eletrónica, ao mesmo tempo que está a permitir ao pirata informático que aceda às suas passwords bem como realize operações de transferência de fundos não autorizadas, e é neste ponto que a fraude atinge o seu expoente máximo.

Porém, o *pharming* não esgota aqui o seu método, apresentado outras formas de captar passwords do utilizador para posteriormente poder aceder à sua conta e realizar transferências. O *pharming* pode também ocorrer quando o cliente escreve o nome de um banco real e legitimo na barra de direções da internet, mas com um erro ortográfico, sendo o utilizador redirecionado para um site falso e clonado.

Em suma, enquanto que no *phishing* o utilizador recebe como "isco" uma mensagem de correio eletrónico que parece proveniente de uma instituição bancária e que contem uma ligação que leva o cliente até uma página clonada pelo *phisher*, nos

[57] Verdelho, Pedro em: "*Phishing* e outras formas de defraudação nas redes de comunicação" In Direito da Sociedade e da informação, Organização da faculdade de Direito de Lisboa e Associação Portuguesa do Direito Intelectual-Coimbra 2009.

casos de *pharming*, o utilizador do serviço é induzido em erro sem sequer se aperceber, uma vez que é o próprio sistema de segurança do computador que foi suplantado. Neste tipo de fraude e tendo em conta que o ficheiro oculto já se auto instalou, o cliente ao digitar o endereço web do seu banco é instantaneamente levado ate à página forjada, motivo pelo qual a desconfiança gerada neste tipo de situações é pouca ou mesmo nenhuma, o que se percebe.

4. Da Responsabilidade

4.1 A repartição da responsabilidade no que toca a operações bancárias não autorizadas por motivos decorrentes de fraude informática no contrato de *home banking*. Analise à luz do RSP e da Diretiva 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015

Chegados aqui e cientes das vantagens de um serviço de *home banking*, nomeadamente no que diz respeito à comodidade de operações feitas à distância bem como a celeridade com que as mesmas são realizadas, tal facto comporta-nos também para as desvantagens deste serviço. Refiro-me aos dois fenómenos de fraude informática que mais são reconhecidos pelos Tribunais, o *phishing* e o *pharming* já explicados anteriormente no ponto 3.

No âmbito do serviço de *home banking* o paradigma das atuações fraudulentas consiste na intromissão de pessoa não autorizada em certa rede informática, utilizando para o efeito um computador cujo sistema será corrompido e cujo ataque tem por fim a movimentação de saldo bancário para conta de terceiro, de forma deliberada e com o fim imediato de obtenção de uma vantagem patrimonial.

A presente dissertação irá então debruçar-se sobre a questão da responsabilidade de operações não autorizadas em sede do serviço de *home banking* e que se devem a motivos de fraude.

Estas questões surgem hoje resolvidas pelo Regime Jurídico que regula o acesso à atividade das instituições de pagamento e a prestação de serviços de pagamento, contido no Anexo I do DL nº 317/2009, de 30/10 que veio regular entre nós a prestação e utilização de serviços de pagamento, transpondo para a ordem jurídica interna a Diretiva

2007/64/CE do Parlamento Europeu e do Conselho, de 13/11 que por sua vez foi revogada pela Segunda Diretiva (DSP2) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, com efeitos a partir de 13 de janeiro de 2018.

Na sequencia do lançamento em 2012 do Livro Verde[58] *para um mercado europeu integrado dos pagamentos por cartão, por internet e por telemóvel*, o legislador aprovou em 2013 a proposta sobre a segunda Diretiva sobre matéria dos sistemas de pagamento, que para além de equacionar a atuação de novos intervenientes e a oferta de outro tipo de serviços, a DSP2 tem outra componente de grande importância e que diz respeito Às obrigações na área de segurança, nomeadamente no instituto da "autenticação forte" das transações *online* por via do utilizador/cliente, neste casa tratar-se-á da segurança de transações e da informação que lhes dá origem, desde logo com o fim de prevenir situações de fraude.

A par disto a Diretiva 2015/2366 apela ainda à uniformização na transposição para os diferentes Estados Membros.

É sobre a repartição de perdas resultantes dos ataques de fraude informática que versarão os próximos pontos, nomeadamente no regime constante no direito comum, bem como em legislação especifica. No âmbito da legislação especifica sobre esta matéria iremos focar a questão da presunção de culpa que recai sobre o Banco, sobre o juízo de valor que recai sobre o utilizador/ cliente, a questão da notificação ao Banco bem como do reembolso. Sobre a lei a aplicar cabe mencionar, como refere a autora CAROLINA FRANÇA BARREIRA[59] "*devemos ter presente durante a análise desta problemática que podem ser aplicadas disposições legais diferentes aos utilizadores de serviços de pagamento que sejam consumidores e aos que não o sejam pois, geralmente, estes últimos encontram-se em melhor posição para avaliar o risco de fraude e tomar medidas de salvaguarda*". Tratando-se de consumidores ser-lhes-á aplicado o regime previsto nos artigos 70º a 72º do RSP.

---

[59] BARREIRA, CAROLINA FRANÇA, **"***Home Banking:* A repartição dos prejuízos decorrentes da fraude informática", Revista Eletrónica de Direito (2015), disponível em: https://www.cije.up.pt/content/home-banking-repartição-dos-prejuízos-decorrentes-de-fraude-informática , p.36;

4.2 A responsabilidade de operações bancárias não autorizadas no seio do direito comum

Como refere o Professor CALVÃO DA SILVA, é no seio da relação de clientela como relação obrigacional complexa de confiança mútua e deveres de proteção dos legítimos interesses do cliente que deve ser encontrada a solução para a questão axial que se discute em torno da responsabilidade do ente bancário no que toca as operações não autorizadas, bem como se sobre ele recai a obrigação de reembolso do cliente.

Para dar resposta e focando neste ponto concreto a nossa análise nas soluções que vigoram no direito comum, seria de recorrer ao instituto da responsabilidade contratual geral por via do disposto no artigo 796º do CC. Sendo assim, o risco inerente à conta do cliente, o risco relacionado com a obrigação de restituir coisa do mesmo género e qualidade, não pode deixar de correr por conta do banqueiro. Como se refere no artigo 796º nº 1 do CC nos contratos que importem a transferência do domínio sobre certa coisa ou que constituam ou transfiram um direito real sobre ela, o perecimento ou deterioração da coisa por causa não imputável ao alienante corre por conta do adquirente. Mais atendendo aos artigos 540º, 799º nº 1, 1144º, 1185º, 1205 e 1206º e 1611º alínea e) todos do CC. É ao Banco que cabe o ónus da elisão da presunção legal que sobre ele impende, demonstrando para o efeito a culpa do cliente depositante na não restituição do dinheiro.

Esta foi a linha de entendimento seguida pelo STJ no ac. 10/11/2011, bem como no ac. do TRG de 23.10.2012[60]. No primeiro o STJ entende que "*através do ato de depósito o tradens aceita transferir para a esfera de domínio (propriedade) do accipiens o risco sobre a gestão da quantia que transferiu, sendo que a partir desse momento se alheia da responsabilidade quanto ao uso e fruição, por transferência para a esfera de responsabilidade do depositário. Cabe ao depositário, enquanto proprietário da coisa transferida, responder pelo risco de extravio ou dissipação da coisa até ao montante exigível no momento da solicitação da restituição*".

São aplicáveis ao depósito bancário, por força do artigo 1206º do CC, as disposições relativas ao mútuo designadamente a obrigação de restituição do *tantundem eiusdem generis*, mais os juros, quando convencionados, e a transferência da

[60] A repartição dos prejuízos decorrentes de operações fraudulentas de banca eletrónica (*home banking*), Acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305.09

propriedade sobre espécies monetárias pelo facto da entrega (1144º do CC). O risco corre por isso, por conta do Banco relativamente à subtração dessas espécies monetárias, a partir do momento em que são entregues.[61] Veja-se a definição do contrato de depósito: *depósito é o contrato pelo qual uma das partes entrega à outra uma coisa, móvel ou imóvel, para que a guarde e a restitua quando for exigida",* por sua vez o artigo 1205º estabelece que o depósito irregular é aquele que tem por objeto coisas fungíveis. Assim, e seguindo esta linha de raciocínio podemos afirmar que o contrato de depósito bancário é um contrato de depósito irregular, através do qual o depositante (proprietário) de recursos monetários transfere para uma instituição bancária a propriedade dos valores depositados, para que esta possa não só usá-los como dispõe deles com a obrigação de os restituir quando assim for exigido ou solicitado.

O mesmo entendimento é proferido num aresto do STJ de 18 de dezembro de 2013 (Proc. nº 6479/09.8TBBRG.G1.S19) quando refere que " *os riscos da falha do sistema informático utilizado, bem como dos ataques cibernautas, tem de correr por conta do reu Banco, por a tal conduzir o disposto no artigo 796º do CC, não se tendo provado, como não se provou, que tivesse havido culpa da autora (cliente)"* . Este entendimento tem por base a ideia de que o depósito bancário deverá ser considerado como um depósito irregular, sujeito a aplicação dos artigos já referidos 1205º,1206º 2 1114º do CC, contudo tal enquadramento não será já aceitável, para os que defendem o depósito bancário como um contrato atípico distinto do mútuo e do depósito.[62]

Este é o entendimento que partilho e que a meu ver o que deverá ser aplicado nestes casos, pese embora as opiniões em sentido diverso, nomeadamente a do Sr. Professor e meu orientador FRANCISCO MENDES CORREIA, que entende que não fará sentido perante operações bancárias modernas (de transferência eletrónicas de fundos) apelar ao artigo 796º do CC, que regula a distribuição do risco de perecimento de coisas corpóreas e determinadas. Apesar de entender bastaste bem o seu argumento quanto a este ponto, terei que discordar do mesmo, e partilhar do entendimento da maioria da doutrina e sobretudo do Professor Calvão da Silva, por entender que se trata de uma situação que se encaixa perfeitamente no escopo da norma do contida neste artigo.

[61] LEITÃO, LUÍS MENEZES, em: "Contratos em especial, Almedina, Vol.III, 2010, p.503, citando Menezes Cordeiros, Manuel de Direito Bancário, p.349

[62] V.J. SIMÕES PATRÍCIO, A operação bancária de depósito, Porto, ELCLA Editora, 1994, pp.29 e sgs; VASCONCELOS, L. MIGUEL PESTANA "Do contrato de depósito bancário", In Revista da Faculdade de Direito da Universidade do Porto, ano VIII,2011,P.166-171.

Ainda no âmbito da aplicação do direito comum, surge-nos o instituto da culpa do lesado previsto no artigo 570º do CC que deverá ser considerado aquando da análise da conduta do utilizador perante casos de fraude informática e de transferências de fundos não autorizadas. Neste sentido o professor CALVÃO DA SILVA, que defende uma interpretação evolutiva e atualista da norma[63], equacionando a aplicabilidade deste artigo quando a conduta do cliente possa ser censurável (por falta de precaução) ainda que o mesmo não tenha agido com culpa grave, ou quando a sua conduta não tenha sido determinante, causa exclusiva ou única da lesão. Pretende-se assim a ponderação, não acerca do dever de indemnizar, mas sim de uma redução da indemnização, que nas palavras do professor "*sinalizasse a função preventiva e sancionatória da auto-responsabilidade do cliente-vítima."*

4.3 A regra da responsabilidade do Banco por operações de pagamento não autorizadas

A regular esta matéria encontramos, como já foi referido ao longo do trabalho, um regime especial que dissipa com todas as dúvidas acerca do ónus *probandi* da autorização ou execução devida da operação efetuada e que esteja em causa em determinado momento. O regime especial consta do DL 317/2009 que transpôs para a ordem jurídica interna a Diretiva 2007/64/CE, agora revogada pela Segunda Diretiva (DSP2) 2015/2366. Tanto o regime que consta do RSP, nomeadamente no seu artigo 70º como da DSP2 artigo 72º fazem recair este encargo sobre o prestador do serviço, atribuindo-lhe assim o ónus de provar que as ordens de pagamento dadas pelo cliente foram devidamente autorizadas através da utilização efetiva dos mecanismos de autenticação disponibilizados, bem como foram corretamente registadas e contabilizadas, e que a sua execução foi isenta de qualquer avaria técnica ou devido a deficiência do serviço prestado pelo prestador de serviços de pagamento.

A isto acresce uma exigência de prova na medida em que são impostos certos limites, ou seja, o mero registo da operação de pagamento em causa não pode ser interpretado como um sinal inequívoco da autorização do titular, veja-se o artigo 7º nº 2

[63] Cfr. SILVA, JOÃO CALVÃO, Acidentes de Viação: concorrência do risco com a culpa do lesado (art.º. 505º) in, Revista de Legislação e de Jurisprudência, ano 134º (julho-agosto de 2001), p.115 e sgs. Especialmente p.117 e 118; João Calvão da Silva, Concorrência entre risco do veiculo e facto de lesado: o virar da pagina, In: Revista de Legislação e de Jurisprudência, ano 137º (setembro-outubro 2007), p.58 e sgs.

da DSP2 "*Caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, a utilização do instrumento de pagamento registada pelo prestador de serviços de pagamento, incluindo o prestador do serviço de iniciação do pagamento, se for caso disso, não é necessariamente suficiente, por si só, para provar que a operação de pagamento foi autorizada pelo ordenante ou que este último agiu de forma fraudulenta ou não cumpriu, com dolo ou por negligência grosseira, uma ou mais obrigações decorrentes do artigo 69. o . O prestador de serviços de pagamento, incluindo, se for caso disso, o prestador do serviço de iniciação do pagamento, apresenta elementos que demonstrem a existência de fraude ou de negligência grosseira da parte do utilizador de serviços de pagamento*".

Considerando que esta prova foi feita e caso o Banco se queira exonerar do dever de suportar os prejuízos decorrentes da operação de pagamento não autorizada, terá que provar face ao caso concreto, o grau de participação do cliente na operação em causa e o grau de culpa com que atuou, o mesmo será dizer que terá de ser feita prova de um comportamento negligente, ou fraudulento que traduza o incumprimento deliberado dos devedores do utilizador.

A presunção de culpa que recai sobre o Banco deve-se ao facto de não pode ser alocado ao utilizador o ónus de um sistema que ele não domina, sistema este informaticamente bastante complexo, estando por isso o prestador de serviços em melhor posição de evitar o risco de operação não autorizada pelo cliente.

4.4 A responsabilidade pelos prejuízos decorrentes de operações de pagamento não autorizadas, perante a notificação ao Banco –A importância da notificação

A notificação por parte do cliente/utilizador a dar conhecimento ao banco da ocorrência de determinação operação que não foi por si autorizada, tem um papel crucial na questão da repartição dos prejuízos decorrentes de operações fraudulentas.

Quando afirmo que o momento em que e feita a notificação tem um papel crucial, deve-se ao facto de ser este o momento a partir do qual o utilizador de serviços de pagamento *"não suporta quaisquer consequências financeiras resultantes da utilização de um instrumento perdido, roubado ou abusivamente apropriado, salvo em caso de atuação fraudulenta"*, artigo 72º nº 4 do RSP. Do exposto salta à vista desarmada a importância que tem para o utilizador/cliente, em ser diligente no cumprimento do dever de notificar ao Banco, a perda, o roubo, a apropriação abusiva ou qualquer operação não autorizada ou incorretamente executada, logo que tome conhecimento de qualquer destes factos, e sem atraso injustificado tendo por fim contribuir para prevenir riscos de fraude e minorar os danos existentes.

É a partir da notificação ou comunicação mencionada na alínea b) do artigo 67º nº 1 do RSP, que se constitui o dever no Banco de, por um lado bloquear o instrumento e assim impedir a sua posterior utilização e, por outro lado o dever de reembolsar imediatamente o utilizador do montante da operação de pagamento não autorizada, como veremos de seguida no ponto 4.5.

Tendo por fim minorar os riscos bem como as consequências das operações de pagamento não autorizadas, o utilizador, deve, como já foi referido comunicar ao Banco a situação sem atrasos injustificados logo que tenha conhecimento da utilização não autorizada do serviço.

Apesar do exposto, não são podem admitir cláusulas contratuais gerais que criem no cliente a obrigação de comunicar a situação ocorrida de "forma imediata", "com a maior urgência" ou dentro de um determinado lapso de tempo "24 horas depois". Isto porque, é possível e até bastante comum que um cliente agindo de boa fé e que tenha adotado sempre uma conduta prudente e diligente, não tenha tido conhecimento da operação não autorizada durante vários dias ou horas.[64] A DSP2 no artigo 71º nº1 que

[64] BARREIRA, CAROLINA FRANÇA, home banking: A repartição dos prejuízos decorrentes de fraude informática (2015).

remeto para o 69º nº 1 alínea b), como o RSP dispõe no mesmo sentido, acrescentado um prazo nunca superior a 13 meses a contar da data do débito, para a comunicação[65].

Este prazo de 13 meses deve-se por um lado a uma forma do Banco não se olvidar da sua responsabilidade, alegando para o efeito o incumprimento por parte do cliente de efetuar esta comunicação o mais rapidamente possível, salvaguardando sobretudo os casos em que de facto existe uma impossibilidade legitima por parte do utilizador eu não ter tomado conhecimento mais cedo da operação não autorizada. Por outro lado, com este prazo de 13 meses não se pretende desresponsabilizar os clientes que não comunicaram ao Banco a ocorrência da operação, sobretudo quando os mesmos já tinham conhecimento da sua existência, ou tinham em sua posse todos os fatores que a permitissem identificar. A tudo isto acresce, os casos em que houve uma atuação fraudulenta por parte do utilizador e que por esse motivo a lei o leva a suportar as perdas advindas após a comunicação à entidade bancária.

A par da notificação ao Banco da ocorrência de uma operação não autorizada, no artigo 69º do RSP, encontramos regulado especificamente o direito de retificação que decorre da comunicação feita à entidade bancária acerca de tais operações. Assim e de acordo com o nº 1 do artigo 69º, o utilizador deve comunicar a situação ao banco para que este a possa retificar, o que demonstra o ónus que impende sobre o cliente, no que diz respeito à verificação das operações realizadas e se as mesmas foram ou não devidamente autorizadas e executadas. Este ónus deve-se sobretudo ao facto de ser mais fácil ao próprio cliente, conhecedor das suas contas, controlar os movimentos que nela se realizam.

[65] Conforme letra do artigo 71º nº 1 da Diretiva 2015/2366 "*O utilizador de serviços de pagamento só obtém do prestador de serviços de pagamento a retificação de uma operação de pagamento não autorizada ou incorretamente executada se comunicar ao prestador de serviços de pagamento sem demora indevida, logo que delas tiver tomado conhecimento, as operações desse tipo que deem origem a uma reclamação, nomeadamente ao abrigo do artigo 89. o , e dentro de um prazo nunca superior a 13 meses a contar da data do débito*."

4.5 Reembolso imediato dos montantes de operações de pagamento não autorizadas

Depois de o cliente tomar conhecimento de uma operação de pagamento por si não autorizada e de notificar o Banco, deverá a instituição bancária reembolsá-lo imediatamente pelo valor do montante indevidamente debitado em virtude desta operação de pagamento, veja-se para o efeito o artigo 71º nº1 do RSP, bem como o artigo 73º nº1 da DSP2 que à luz do primeiro continua a prever este dever de reembolso imediato. A Segunda Diretiva esclarece ainda que tal reembolso deverá ser cumprido o mais tarde até ao final do primeiro dia útil seguinte à tomada de conhecimento pelo Banco, sob pena deste incorrer em mora.

Como consequências civis da demora do Banco no reembolso imediato do montante da operação de pagamento não autorizada, o artigo 71º nº 2 do RSP prevê a contagem de juros moratórios desde a data em que o cliente negou ter autorizado a operação de pagamento executada, até à data do reembolso efetivo, calculados segundo a taxa legal definida no CC acrescida de dez pontos percentuais, não se afastando a possibilidade de haver lugar a indemnização suplementar.[66] [67]A isto acresce responsabilidade contraordenacional do Banco, caso se recuse a reembolsar o cliente do montante em causa, conforme dispõe o artigo 95º alínea p) do RSP.

Quanto à DSP2 cabe mencionar que a mesma exclui o dever de reembolso imediato caso o Banco tenha motivos razoáveis para suspeitar de fraude e que os comunique por escrito à autoridade nacional relevante (neste caso será o Banco de Portugal). Assim, permite-se ao banco discutir a responsabilidade do cliente antes de efetuar este dever de reembolso imediato da quantia que foi indevidamente debitada da sua conta. Estes casos de fraude referem-se sobretudo a situações[68] em que por exemplo tenha sido o próprio cliente a entregar voluntária e deliberadamente os seus códigos pessoais, nomeadamente o pin, ou o próprio instrumento de pagamento, para depois poder comunicar a sua

[66] Artigo 73º nº3 da DSP2 "*Pode ser fixada uma indemnização financeira suplementar nos termos do direito aplicável ao contrato celebrado entre o ordenante e o prestador de serviços de pagamento, ou ao contrato celebrado entre o ordenante e o prestador do serviço de iniciação do pagamento, se for caso disso."* Disponível em: https://www.bportugal.pt/sites/default/files/anexos/legislacoes/diretiva2015n2366ue.pdf

[67] O banco tem o dever não só de bloquear o instrumento de pagamento, como reembolsar o cliente, repondo a conta debitada na situação em que estaria se essa operação não tivesse acontecido (art.60º nº 1 da Diretiva 2007/64/CE; art. 71º nº 1, do DL nº 317/2009), acrescido sendo caso disso, de juros moratórios (taxa legal civil mais 10%, atualmente igual a 14% desde do dia da negação da autorização da operação executada até à data do reembolso efetivo, podendo o credor (cliente) provar que a mora lhe causou dano superior aos juros e exigir a indemnização suplementar correspondente. In: CALVÃO DA SILVA, JOÃO em "Estudos em Homenagem a Rui Manchete, Coimbra, Almedina 2015, p.363-364.

[68] CALVÃO DA SILVA, JOÃO em "Estudos em Homenagem a Rui Manchete, Coimbra, Almedina 2015. P. 359

utilização não autorizada, ou ainda o cliente e titular do instrumento de pagamento pode comunicar o roubo do cartão e de seguida realizar levantamentos não autorizados.

Ainda quanto a DSP2, já foi referido que entre outras, umas das principais preocupações aquando do seu projeto, consistiu na proteção do consumidor, facto este que se veio refletir entra outras disposições no artigo 73º nº 1, nomeadamente no dever do Banco assegurar que a data-valor do crédito na conta de pagamento do cliente não seja posterior à data em que o montante foi debitado indevidamente, isto compreende-se pelo facto do legislador pretender assegurar que os juros pagos ao cliente pelo montante que lhe foi creditado, se calculam a partir da data em que essa mesma quantia foi indevidamente debitada ao cliente, já que, se não tivesse existido tal operação não autorizada, o cliente beneficiaria desses juros sobre aquela quantia e que já seria devidos por força do seu contrato de depósito bancário.

4.6 A apreciação da conduta do utilizador e a sua contribuição para o dano

A existência ou não de fraude, dolo, culpa grave ou culpa leve do cliente, alegada pelo Banco deverá ser apreciado *in casu*, tendo em conta todas as circunstâncias de facto do caso.

Como já vimos no ponto 4.4, é obrigação do cliente comunicar, sem atraso injustificado, ao Banco a perda, roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento. Cumprido este dever, o Banco fica em condição de impedir utilizações do instrumento de pagamento, após a comunicação ter sido recebida por si, mesmo em caso de dolo ou negligência grave do cliente.

Contudo nas operações não autorizadas e realizadas antes da comunicação ao Banco, ter-se-á que distinguir consoante o comportamento do cliente no que diz respeito ao cumprimento das obrigações que sobre ele recaem.

I. Negligência leve do cliente

Se atentarmos na letra do artigo 72º do RSP "no *caso de operações de pagamento não autorizadas resultantes da perda, de roubo ou da apropriação abusiva de instrumento de pagamento, com quebra de confidencialidade dos dispositivos de*

segurança personalizados imputável ao ordenante, este suporta as perdas relativas a essas operações dentro do limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, até ao máximo de 150 euros". O banco irá responder pelos prejuízos remanescentes que decorreram da operação de pagamento não autorizada. Esta situação justifica-se como já vimos no ponto infra sobre responsabilidade, a título de risco que corre pela instituição bancária, nomeadamente no que toca ao risco do sistema informático que suporta o serviço de *home banking*, nomeadamente quanto ao facto deste não ser seguro sendo por isso suscetível de intromissão de terceiros. É nesta disposição, nomeadamente quanto ao *quantum* suportado pelo cliente que encontramos a principal diferença naquilo que toca ao regime previsto na DSP2.

A DSP2 prevê no seu artigo 66º a responsabilidade do titular do instrumento de pagamento por operações não autorizadas onde se estabelece que o "*ordenante pode ser obrigado a suportar num montante máximo de 50 euros, as perdas relativas às operações de pagamento não autorizadas resultantes da utilização de um instrumento de pagamento perdido ou roubado ou da apropriação abusiva de um instrumento de pagamento*." A DSP2 altera assim o *quantum* da importância a suportar pelo utilizador de 150 euros para 50, por considerar que é este o montante adequado para garantir um nível elevado e harmonizado de proteção dos utilizadores na União Europeia[69], veja-se para o efeito o artigo 74º nº 2 da referida Diretiva.

Enquanto que no RSP o limite máximo era até 150 euros, exceto quando o utilizador atue com negligência grave, em incumprimento deliberado dos seus deveres, agora este limite foi reduzido para 50 euros, retirando-se da previsão da fórmula "com quebra de confidencialidade imputável ao ordenante". Assim e independentemente das circunstâncias eu que a apropriação do IP acontece, o titular responderá por perdas até 50 euros, podendo sempre assumir perdas superiores quando fique demonstrado pela instituição bancária em causa, que o mesmo agiu com culpa, negligência grave, em incumprimento deliberado dos seus deveres ou fraudulentamente.

[69] Veja-se o considerando 71º da DSP2 "*…a fim de incentivar o utilizador do serviço de pagamento a notificar o prestador, sem demora indevida, o prestador do serviço de pagamento de qualquer furto ou perda de um instrumento de pagamento, reduzindo assim o risco de operações de pagamento não autorizadas, o utilizador só deverá ser responsável por um montante muito limitado, salvo em caso de atuação fraudulenta ou de negligência grosseira da sua parte. Neste contexto, afigura-se adequado um montante de 50 euros para garantir um nível elevado e harmonizado de proteção dos utilizadores na União* (…)". Será de realçar a meu ver, que o legislador comunitário para além de realçar a importância de uma atuação preventiva por parte do utilizador do instrumento de pagamento, considera que o mesmo atua a título de negligência leve, quando não o faça.

Em suma, o cliente ao contrário do regime plasmado no atual RSP resultante da transposição da DSP1, terá que suportar perdas até ao montante de 50 euros, nos casos em que lhe seja possível detetar com antecedência a suscetibilidade de certa operação ser passível de roubo, perda, ou apropriação e assim notificar o Banco acerca dos mesmos e não o faça, chegando a ocorrer de facto a operação não autorizada, o cliente responderá até ao montante de 50 euros.

II. Negligência grave e dolo do utilizador

Nestes casos e ao contrário do que aconteceu no ponto I. quando as operações de pagamento não autorizadas resultarem de negligência grave do titular, o mesmo suporta as perdas resultantes desta operações " *até ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, ainda que superior a 150 euros, dependendo da natureza dos dispositivos de segurança personalizados do instrumento de pagamento e das circunstâncias da sua perda, roubo ou apropriação abusiva*", conforme dispõe o artigo 72 nº 3 do RSP.

Não podemos avançar sem antes descortinar o conceito de "negligência grave" no contexto que o RSP nos apresenta. Ora, à luz do raciocino apresentado pela autora CAROLINA FRANÇA BARREIRA[70], a mesma parte do conceito de negligência presente no direito civil. Assim sendo, sabemos que a negligência tal como refere o professor ANTÓNIO MENEZES CORDEIRO [71] consiste na violação de uma norma por inobservância de deveres de cuidado.

Ainda no seio do Direito Civil aparece-nos a distinção entre negligência consciente e inconsciente, distinção esta com a qual devemos fazer um paralelo com os conceitos de negligência leve e grave presentes no RSP.

Quanto à negligência grave a mesma visa uma situação em que o autor equaciona e prevê como possível determinado resultado, resultado este que se alcança não pela

[70] BARREIRA, CAROLINA FRANÇA**, "***Home Banking:* A repartição dos prejuízos decorrentes da fraude informática", Revista Eletrónica de Direito (2015)**,** disponível em: https://www.cije.up.pt/content/home-banking-repartição-dos-prejuízos-decorrentes-de-fraude-informática.

[71] Cordeiro, António Menezes em "Tratado do Direito Civil, Tomo VIII, reimpressão da 1ª edição do tomo III da parte II de 2010. Coimbra: Almedina 2014, p. 472.

violação direta da norma, mas sim pela não verificação da tomada das providências necessárias para evitar certo dano.

Na negligência leve, ao contrário da anterior referida o autor não prevê a possibilidade de ocorrência daquele resultado. O mesmo verifica-se por falta de diligência e deveres do cuidado.

As situações de negligência desde sempre se revelaram causadoras de uma maior dificuldade de identificação, uma vez que e ao contrário do que se passa nas situações de dolo, a negligência suscita uma maior liberdade ao julgador no que toca à avaliação da conduta do agente.

Ora, partindo do artigo 487º do CC que nos apresenta o critério da apreciação da culpa, ou seja, *"a culpa é apreciada, na falta de outro critério legal pela diligência de um bom pai de família em face das circunstâncias de cada caso"*, o julgador terá que perante o caso concreto atender a todas as circunstâncias de facto, bem como às características pessoais do utilizador, em especial no que toca a sua profissão. Pois quanto maior for a sua competência técnica, sobretudo na área de informática, maior será a exigência de um comportamento diligente da sua parte. Todos estes fatores são cruciais para a decisão, uma vez que a falta de definição legal para o conceito de negligência no RSP pode levar à tomada de decisões arbitrarias.

Pelo exposto, será de considerar ferido de negligência grave o comportamento do utilizador/cliente que tome conhecimento de uma operação bancária não autorizada, e só notifica o banco sem qualquer justificação legitima, dias depois. Isto porque, por um lado estava ciente dos deveres que sobre ele recaem, nomeadamente a obrigação de notificar o banco, e por outro porque estava ciente do incidente ocorrido, tendo em seu conhecimento todos os elementos necessários para a tomada de uma conduta diligente, o que não se verificou. Como refere o professor ANTUNES VARELA[72] "*o grau de reprovação ou de censura será tanto maior quanto mais ampla for a possibilidade de a pessoa ter agido de outro modo, e mais forte ou intenso o dever de o ter feito",* por sua vez ANA PRATA[73] *define o conceito de negligência grave como sendo*" *negligência grosseira, erro imperdoável, desatenção inexplicável, incúria*

[72] VARELA, ANTUNES Obrigações em Geral, vol. 1. 10ª edição, Almedina, Lisboa, 2000, p.574.
[73] PRATA, ANA Clausulas de exclusão e limitação da responsabilidade Contratual, 2005, Almedina, Lisboa, p.308.

indesculpável, vistos em confronto com o comportamento do comum das pessoas, mesmo daquelas que são pouco diligentes".

Também ferido de negligência grave, será o comportamento do utilizador do instrumento de pagamento que deliberadamente incumpre os deveres que lhe são impostos por lei nomeadamente a prudência, diligência e deveres de cuidado, quando divulga a terceiros os códigos de acesso ao serviço de *home banking* violando o seu dever de segurança e confidencialidade sobre os seus dispositivos, bem como ultrapassa os avisos de segurança que vão surgindo mediante a abertura da ligação de acesso ao *home banking*, e que tem que ser por si fechados. Face a isto deverá ser o cliente a suportar todas as perdas originadas pelas operações de pagamento não autorizadas até à data da comunicação da ocorrência, art. 72º nª2 e 4 do RSP.

Ainda no âmbito daquilo que nos levará ao que é de facto o conceito de negligência grave, surge a clássica distinção entre negligência leve e grave consoante o padrão de diligência violado, ou seja, o comportamento que só seria evitado por um homem especialmente diligente em oposição ao comportamento que só seria praticado por um homem especialmente pouco cuidadoso. Neste ponto e parafraseando o professor FRANCISCO MENDES CORREIA[74], numa primeira abordagem aos factos de cada caso, o intérprete-aplicador deverá assim perguntar se a conduta em apreço teria sido praticada por um homem médio, para só depois e em caso de resposta afirmativa, perguntar se aquele comportamento apenas teria sido praticado por uma pessoa especialmente negligente.

5. Jurisprudência e análise critica

5.1 A tendência da jurisprudência nesta matéria

É sabido que a maioria dos Tribunais tem condenado a entidade prestadora do serviço a assumir a totalidade dos prejuízos decorrentes das operações bancárias não

[74] CORREIA, FRANCISCO MENDES**, "**Operações não autorizadas e o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica"**,** Revista de Direito Civil, Ano II (2017): n.º 3; p. 727.

autorizadas, para o titular, baseando-se no DL 317/2009, nomeadamente na presunção de culpa que recai sobre o Banco nesta matéria.

Podemos afirmar que se sente por parte dos tribunais, certa resistência em imputar prejuízos aos titulares de *home banking*, por motivos de quebra de confidencialidade do sistema, ou por conduta negligente, veja-se os acórdãos do TRL de 24.05.2012, de 28.06.2013, o ac. do TRP de 07.10.2014 e o ac. do TRG de 18.12.2013.

As decisões que imputam a totalidade da responsabilidade ao Banco assentam o pressuposto da sua decisão, ou na falta de prova por parte do Banco de que certo titular/ utilizador violou os deveres de segurança e confidencialidade a que estava adstrito, ou mesmo havendo certa prova por parte da entidade bancária, os tribunais superiores consideram que aquela situação não merece nenhum tipo de censura e que por isso não configura nenhuma situação de negligência, veja-se para o efeito a decisão tanto em primeira instancia, como do STJ do ac. supra referido de 18.12.2013, em que o risco da fraude aqui ocorrida corre exclusivamente por conta do Banco, em virtude de o mesmo não ter provado a culpa do cliente.

Neste sentido, cabe especialmente referir que encontramos ainda argumentos a favor de o Banco dever sempre arcar com os prejuízos provocados por intromissões fraudulentas no sistema de pagamentos baseados na desigualdade económica das partes no contrato, e que, portanto, no diferente peso desses prejuízos no orçamento do banco e do seu cliente[75].

Argumento este que vem sustentar a afirmação supra referida quando menciono uma situação de resistência no que toca a imputação da responsabilidade por parte da maioria dos Tribunais à entidade prestadora do serviço, e que deve certamente ser rejeitado, por não configurar nem assegurar a justiça das soluções.

[75] Veja-se para o efeito os argumentos apontados pelo TRL, no seu ac. de 26.10.2010 (Maria Amélia Ribeiro), cit., no sentido de que a "quantia de 16.800.00, resultado de operações fraudulentas de *home banking* é uma gota de água no oceano do volume de negócios do banco. Já no que toca à autora, que é reformada e a vive da sua reforma (…), a quantia de que esta desembolsadas foi conseguida ao longo de muitos anos de poupanças e de algumas privações (…), tratando-se de dinheiro destinado a prover necessidades inesperadas, designadamente com tratamentos médicos"; ou de que "o que está em causa para o banco está no plano das insignificâncias, mas, para a autora, não será exagero afirmar, estará no domínio da própria subsistência.

5.2 O diferente grau de censura nos casos de *phishing* e de *pharming*

Neste ponto, vamos partir de uma afirmação proferida pelo STJ de que "*quer fosse uma das técnicas (phishing) ou outra (pharming), qualquer delas consubstancia fraudes informáticas, conduzindo aos mesmos resultados em termos de responsabilidade*", para apresentar a minha discordância.

Quando se fala em responsabilidade do titular que vê a sua conta ser abusivamente movimentada, aplicar-se-á, como vimos, o regime previsto no artigo 72º do RSP. Nos casos em que existe uma quebra de confidencialidade imputável ao titular, o mesmo responderá por prejuízos ate 150, respondendo acima deste valor quando atue com negligência grave, ou responderá por todos os prejuízos se agir de forma fraudulenta, ou em incumprimento deliberado dos seus deveres[76].

O critério que deverá servir de base a estas decisões, deverá ser um critério objetivo de imputação de prejuízos, baseado na diligência da conduta das partes e na sua contribuição para os danos. A isto acresce, por um lado, que se deverá ter em conta, como refere a professora MARIA RAQUEL GUIMARÃES, o grau de "ingenuidade[77]" do utilizador ao facultar certos dados, bem como a competência técnica, conhecimento e profissão do mesmo. Por outro lado, deverá ter-se em conta, se estamos perante um caso de *phishing* ou de *pharming*, uma vez que um é mais facilmente detetável, ou passível de gerar desconfiança do que outro, fazendo por isso, no caso de se tratar de uma situação de *phishing* recair sobre o utilizador um maior grau de censura no que toca à sua conduta

Cabe ainda referir que somente o critério objetivo assegura a justiça das soluções e contribui para uma maior eficiência e segurança dos sistemas de pagamentos.

a) Nos casos de *phishing*

Nesta modalidade de fraude, como já vimos, o utilizador fornece dados confidenciais num contexto distinto dos das operações de *home banking,* em resposta a

[76] Art. 72 nº 2 e 3 do RSP

[77] GUIMARÃES, MARIA RAQUEL, "A fraude no comercio eletrónico: o problema da repartição do risco por pagamento fraudulento." Cit,p. 594

uma mensagem de correio eletrónico ou a uma chamada telefónica, acreditando ter por interlocutor o seu banco.[78]

Cada vez mais, os utilizadores da internet estão cientes dos perigos nomeadamente no que diz respeito a abrir e descarregar ficheiros de e-mails desconhecidos e de aparência duvidosa. Também a crescente necessidade de uso diário e praticamente constante da Internet pelos mais variados motivos, implica que as pessoas cada vez mais estejam informadas sobre este meio informático, o que consequentemente as torna mais capazes de reconhecer situações tidas como estranhas e de aparência duvidosa. A tudo isto acresce o facto de que cada vez mais as instituições bancárias aqui em análise se preocuparem com a segurança dos seus sites e aplicações criando para o efeito avisos e alertas de segurança cada vez mais pormenorizados e focados em travar os ataques de fraude informática, que surgem automaticamente antes do utilizador inserir os seus dados pessoais, chamando assim a sua atenção para os perigos da navegação online a que se encontra sujeito.

Sobre o assunto, será oportuno mencionar a decisão do TRG, no ac. de 25.11.2013. No momento em que a fraude ocorreu, estes alertas de segurança ainda não existiam, existiam sim informações sobre métodos de fraude e detalhes sobre a segurança num menu apresentado no site. Ainda assim, o tribunal referiu que "*apesar da aparência genuína do site, a solicitação dos dígitos do cartão matriz, em si e muito estranha, dentro do contexto e lógica do sistema de segurança implementado pela ré (...). Assim, é de concluir que o comportamento da autora foi negligente, violador das regras de segurança impostas pelo contrato, que foram causa direta da movimentação das suas contas por terceiros*". O Tribunal entendeu ainda que "*age com culpa o utente que fornece todo o conteúdo do cartão matriz perante uma solicitação numa página idêntica à do banco, uma vez que contraria toda a lógica do sistema de segurança que não pode ser desconhecida por parte do utilizador*". O mesmo acórdão chega até a referir quanto ao serviço de *homebanking*, a exigência de "*muitas cautelas devido aos perigos a que estava sujeita. É como alguém que pisa terreno minado e não se informa e toma os cuidados devidos para as circunstâncias. Corre um grande risco de ser atingido por uma mina e sofrer graves danos*".

[78] Ac. do TRL de 12.10.2017 (Pedro Martins). Disponível em: www.dgsi.pt

No mesmo sentido e pouco tempo depois pronunciou-se a Relação de Lisboa, no ac. de 12.12.2013 onde refere que em resposta a um pedido de "*atualização da matriz*" que surgia no site falso do banco, "(…) *a autora teve que inserir 192 algarismos*. *Há que considerar que a autora era uma pessoa instruída, lucida e habituada a utilizar o serviço (...) pelo que não podemos deixar de questionar como é que a mesma não estranhou que aquele mesmo sistema lhe solicitasse uma atualização que nunca antes tinha sido pedida, e que esta atualização importasse a revelação de uma quantidade enorme de algarismos (...)".*[79]

Em suma, na hora de decidir deverá ser tido em conta por um lado o cumprimento por parte da instituição bancária aos deveres a que está adstrita, nomeadamente de aviso, alerta, informação aos seus clientes e de segurança, e por outro se o pedido em causa era anormal e irregular o suficiente para chamar a atenção do utilizador no sentido de o levar a desconfiar da regularidade da operação[80], ou se, ainda assim e apesar de inabitual, era plausível, não sendo censurável ao utilizador a introdução de dados solicitados. Neste juízo terá de se ter sempre em conta o conhecimento do utilizador em questão, bem como a sua profissão, que muitas das vezes pode implicar um maior conhecimento destes ataques on-line.

Ao banco competirá fazer prova sobretudo de que cumpriu os seus deveres de informação quanto a este tipo de perigos. É a existência destes avisos, logo na página inicial do site do banco, que tornarão a conduta do titular do IP especialmente censurável. O utilizador é constantemente alertado para os indícios de fraude, o que o permite estar consciente de que os pedidos feitos nestas páginas falsas não são legítimos.

É precisamente esta lógica que serve de pressuposto à sentença do Ac. do TRE de 25.06.2015[81] quando condena as utilizadoras, referindo que *"... A Autora não podia*

[79] Ac. do TRL de 12.12.2013 (Tomé Ramião), disponível em www.dgsi.pt
[80] Ac. do TRL de 12.10.2017 (Pedro Martins), disponível em www.dgsi.pt

[81] Ac. do TRE de 26.06.2015 (Cristina Cerdeira), Disponível em: www.dgsi.pt, referindo entre outras coisas que : "*Ao divulgar na internet a totalidade dos dados do seu cartão matriz – apesar dos vários alertas de segurança no site da Ré na internet, advertindo os utilizadores para não reproduzirem os elementos do cartão matriz, e de ter tomado conhecimento das Recomendações de Segurança constantes do "guia de utilizador" que lhe foi entregue e que também se encontram acessíveis no mencionado site - a Autora actuou ao arrepio do contrato de home banking a que aderiu e em violação de regras básicas de segurança nele previstas para a utilização do serviço "Caixadirecta Online", o que permitiu que terceiros se apoderassem dos seus elementos de segurança e assim lograssem aceder às contas bancárias tituladas pelas Autoras e efectuar operações fraudulentas*".

ignorar que não podia reproduzir integralmente a matriz, sendo esse o aviso de segurança mais frequente. Ao ser-lhe solicitado, o que aliás configurou com certeza uma operação demorada, o utilizador medianamente diligente recorria às linhas de apoio ou ao atendimento presencial".

No pressuposto do que aqui foi referido, o acórdão[82] em questão assenta a sua decisão sobretudo na informação prestada pela instituição bancária ao cliente / utilizador "*Age com culpa o utente que fornece todo o conteúdo do cartão matriz perante uma solicitação numa página idêntica à do Banco, uma vez que contraria toda a lógica do sistema de segurança que não pode ser desconhecida por parte do utilizador". "Por força da subscrição do serviço "Caixadirecta Online", o cliente do Banco obriga-se a manter a confidencialidade do número do contrato, do código de acesso (vulgo, password) e ainda do seu cartão matriz, respeitando, assim, regras básicas de segurança que se encontram disponíveis aos utilizadores quer através do* ***guia de utilizador****, quer das* ***Condições Gerais*** *do serviço, quer dos* ***alertas*** *e* ***Recomendações de Segurança*** *disponibilizadas logo aquando do acesso ao serviço onde são anunciadas/publicitadas tais regras de segurança."*

Também o professor CALVÃO DA SILVA, na anotação ao acórdão de 18 de dezembro de 2013 em que o STJ na linha das instâncias condena a entidade prestadora do serviço, fazendo correr exclusivamente por conta do Banco a responsabilidade, por entender que o mesmo não ilidiu a presunção por não ter provado a culpa do cliente, questiona-se sobre três dos factos dados como provados por estes demonstrarem uma conduta por parte do utilizador merecedora de censura.

Vejamos: no acórdão de 18 de dezembro de 2013 foram dados entre outros, como provados os seguintes factos: "O *pedido de coordenadas no acesso ao Banco Net é uma situação anormal e irregular*", "Na *área de segurança do site da Ré (banco), consta o link.*"; "*Nos sites Banco Net e do Banco, a Ré publicou noticias sobre ataques mediante o envio de um e-mail com o objetivo de obter códigos de acesso e dados financeiros*" e por fim que o cliente utilizou o serviço de *home banking* " *sempre em conformidade com a recomendação do banco e sem qualquer incidente durante quatro anos*..". Aqui o autor questiona e a meu ver bem se tal situação anormal e irregular não

[82] Ac. do TRE de 26.06.2015 (Cristina Cerdeira), disponível em: www.dgsi.pt

deveria ter causado estranheza e desconfiança, uma campainha de alarme, a impelir o cliente a usar o link disponível na área de segurança do site do Banco, e certificar-se da alteração da boa e reiterada pratica que o cliente/utilizador realizou durante estes quatro anos de utilização do serviço.

O professor questiona ainda se não seria este comportamento próprio da prudência e cautela exigíveis de um utilizador normal colocado nas circunstâncias do caso concreto, tanto mais quando o Banco publicou no seu site geral e no site do Banco Net notícias sobre o envio de e-mail com o objetivo de obter códigos de acesso e dados financeiros, o que apresenta a minha total concordância.

É aqui que surge a relevância do tipo de fraude com a qual nos deparamos, isto porque caso estivéssemos perante uma situação de *phishing* em que o ordenante tivesse fornecido os seus códigos ou coordenadas pessoais de acesso em resposta a um e-mail, verificar-se ia uma comportamento culposo, o mesmo será dizer que o utilizador teria atuado com negligência grosseira, uma vez que se constatou e se deu como provado que a entidade bancaria tinha prestado todas as advertências necessárias, nomeadamente alertando o cliente para este tipo concreto de fraude.

Situação diferente será a de estarmos perante um caso de *pharming*, em que a página do banco foi clonada, dificultando por isso a perceção do cliente quando à estranheza da situação.

Ainda na esteira do entendimento do professor CALVÃO DA SILVA, na hipótese em apreço apesar de estarmos perante uma situação de *pharming* e o cliente não ter atuado com negligência grosseira, a sua conduta será na mesma censurável por falta de precaução e pelo facto do mesmo ter contribuído para o dano, o que na solução do professor não elimina nem exclui o dever de indemnizar por parte da instituição bancária, mas pondera uma redução da indemnização com o fim de sinalizar a função preventiva e sancionatória da autorresponsabilidade do cliente, vitima.

O professor assenta a sua tese no instituto legal da culpa do lesado previsto no artigo 570º do CC, defendo uma interpretação evolutiva e atualista do mesmo.

b) Nos casos de *pharming*

Como vimos no ponto 3.2 da presente dissertação, esta técnica é mais difícil de ser detetada, o que nos leva de imediato a um menor grau de censura sobre o utilizador. Isto porque, quando o mesmo se depara com uma página web falsa para a qual foi direcionado quando escreveu a morada do seu banco com recurso ao teclado de um computador, e aqui introduz os códigos que lhe são solicitados, dificilmente será passível de culpa, uma vez que este procedimento em nada difere do procedimento dito normal e esperado. Solução diferente existiria caso o procedimento que o utilizador tenha que levar a cabo para aceder a uma operação através do *home banking*, seja muito distinto do habitual e o seu banco o tenha alertado para este tipo de fraudes, aqui já seria passível de um juízo de censura.

Nestes casos devemos ter presente que as páginas falsas são na maioria das vezes iguais às páginas dos bancos e identificadas como ligações seguras, veja-se o ac. do TRG de 30.05.2013 que defendeu não existir uma conduta imprudente, descuidada ou negligente, do utilizador vítima deste tipo de fraude.

Na mesma linha o ac. de 7.10.2014 do TRP[83] quando refere que, ao contrário do *phishing*, *o qual uma pessoa mais atenta pode evitar simplesmente não respondendo ao e-mail fraudulento, o pharming é, por sua vez praticamente impossível de ser detetado por um utilizador comum da Internet, por aqui se vê a sofisticação da técnica em causa que não permite sequer que o utilizador desconfie que esta perante uma página web falsa. Ainda no mesmo acórdão o Tribunal entendeu afastar sem qualquer hesitação, o dolo ou intencionalidade no comportamento do apelado e mesmo uma negligencia consciente ou culpa grave. Resta apurar se atuou com negligência ou culpa leve (...) era necessário que o apelado fosse uma pessoa muito experiente e muito conhecedora do meio de navegação em ambiente eletrónico para que pudesse desconfiar do isco que lhe foi lançado nas circunstâncias mencionadas*.

A par destas decisões encontramos outras[84] em que apesar do facto de já existirem alertas da instituição bancária na página de acesso ao serviço, nomeadamente alertas

[83] Acórdão do TRP de 7.10.2014, Proc n.º 747/12.9TJPRT.P1, Relator Ana Lucinda Cabral;

[84] Veja-se o ac. de 22.05.2014 do TRE, Relator Mata Ribeiro, em que o Tribunal considerou que o utilizador que cede informações sobre o seu telemóvel numa página falsa não tem um comportamento menos cuidadoso do que qualquer outro utilizador que tenha baixos conhecimentos informáticos. Deu-se como provado que o utilizador, num acesso anterior tinha-se deparado com uma página fraudulenta e forneceu inadvertidamente, a informação referente as

específicos sobre o facto do Banco nunca solicitar o número de telemóvel, o Tribunal considerou não existir sequer negligência leve por parte do utilizador, quando o mesmo faculte o seu número de telemóvel, bem como a sua senha de acesso, decisão da qual apresento a minha discordância tendo em conta os avisos específicos existentes à data na página do branco sobre o assunto, o que o deveria exonerar de responsabilidade ou limitar, uma vez que cumpriu os deveres a que estava adstrito, nomeadamente os de informação, sob pena de todas as situações em termos de responsabilidade serem imputadas, sem mais, à entidade prestadora do serviço.

Apesar do exposto e em números mais reduzidos, têm surgido decisões[85] em sentido contrário, tendo por base os alertas colocados pela instituição bancária na página de *home banking*. Nestas decisões defende-se sobretudo a não responsabilização do banco, uma vez que o titular ao disponibilizar a terceiros, neste caso, hackers, o seu código de acesso, bem como os dados do seu equipamento telefónico agiu de forma negligente e descuidada, revelando até, na minha opinião desinteresse por tais alertas, e por que por isso levará a responder por todas as perdas.

Foi neste mesmo sentido que se pronunciou o TRG, no seu ac. de 25 de novembro de 2013[86], em que perante um caso de *pharming*, entendeu que o comportamento do utilizador quando digitou numa página clonada do Banco todos as coordenadas do seu cartão matriz, perante a solicitação da página nesse sentido, era censurável a título de negligência. O Tribunal justifica a sua posição afirmando que "*para um utilizador informático minimamente diligente, cuidadoso, e minimamente informado no uso desta tecnologia, sabendo ou tendo o dever de saber dos perigos que assolavam o sistema (através da informação prestada pela ré sobre o assunto e colocada no site onde as pessoas eram logo alertadas e podiam informar-se melhor acedendo ao menu segurança) e a Web em geral, tinha que se questionar perante tal solicitação. E, perante esta dúvida, tinha um de dois caminhos a seguir, ou contactava rapidamente com a ré, via telefone, ou ignorava a solicitação e comunicava o acontecimento à ré. E só em face da solução que lhe fosse dada, é que continuaria a*

---

suas chaves de acesso e telemóvel associado à autorização por SMS (facto provado 20), numa altura em que o banco já publicava alertas na página de acesso ao serviço. Disponível em: www.dgsi.pt

[85] Sentença de 21.09.2012 dos Julgados de Paz, a mesma refere que: "foi *a negligência no sentido de não ter tido as necessárias cautelas, de não ter prestado mais atenção ao que lhe estava sendo solicitado, precavendo-se das fraudes que eram já anunciadas no próprio site do banco, com alertas e informações para que os consumidores se tivessem habilitado a se prevenir e as pudessem evitar, não cometendo a imprudência de informar terceiros dos seus dados pessoais e sigilosos".*

[86] Proc. Nº 2869/11.4TBGMR.G1, Relator Espinheira Baltar, disponível em www.dgsi.pt

usar o programa. Tinha de ter a consciência que estava numa situação que não era normal e tinha de sanar a dúvida".

Por aqui se vê a importância dos alertas que vão surgindo na página do banco ao longo da navegação do utilizador e a consequente tomada de atenção e de consciencialização que deveria existir por parte de todos os clientes, aqui utilizadores do instrumento de pagamento. Se por um lado, existe uma exigência a nível comunitário da prestação de informações cada vez mais claras e qualificadas, em vários momentos ao longo de toda a execução do contrato celebrado entre a instituição bancaria e o cliente, por outro também deveria ser exigido aos clientes uma maior exigência no cumprimento dos seus deveres, nomeadamente em ser diligente, cuidadoso bem como preservar com segurança os seus dispositivos e elementos pessoais.

A tudo isto, e a meu ver, saliento que deveria ser exigido ao cliente e consequentemente utilizador do serviço de banca eletrónica que apreenda o conteúdo dos avisos que constam da página do Banco, designados de *banners*, assimilando-os de tal modo que quando confrontado com certo indício de fraude os reconheça, e que assim evite a fraude, nomeadamente não facultado a terceiros os seus dados pessoais de acesso ao serviço (aqui as coordenadas do cartão matriz). Caso contrário, tal conduta deverá revelar uma enorme imprudência e descuido por parte do cliente/utilizador que apenas teria ocorrido caso estivesse em causa uma pessoa especialmente descuidada e incauta, devendo por isto ser o mesmo punido a título de negligência grave[87].

Atualmente, considero que o Banco apresenta três níveis de informação que presta ao cliente sendo o I) assente em toda a informação que é devida para a realização do contrato, o II) consiste na informação que se encontra explicada no menu da página oficial do banca na secção que diz respeito à segurança, em que alerta o cliente para os ataques informáticos que mais acontecem neste setor (*phishing* e *pharming*) , e por fim o III) que visam todos os alertas criados pelo Banco e que vou surgindo ao longo da navegação, em que para avançar há hiperligação, o cliente terá obrigatoriamente de fechar o aviso, o que leva à uma quase obrigatoriedade quanto à leitura dos mesmos.

[87] No mesmo sentido, CAMPOS, DIANA BEATRIZ CARRASCO e CARMO, MARIA DO MAR PATRICIO, em "Home Banking: Consequências Jurídicas, disponível em: www.governancelab.org; BARREIRA, CAROLINA FRANÇA, p. 79; GUIMARÃES, MARIA RAQUEL, As operações fraudulentas…p.32; Lima, Raquel Sofia Ribeiro de, A responsabilidade pela utilização abusiva...,p.50 e 51

Ora, se a exigência é maior naquilo que diz respeito à informação prestada, o mesmo deveria se refletir quanto à informação retida, tendo assim os Tribunais face ao caso concreto, avaliar todos os elementos circunstanciais do caso, bem como profissão e competência técnica do utilizador, tendo sempre em conta a existência ou não da prestação ao cliente destes três referidos níveis de informação e se os mesmos foram ou não por ele tomados em consideração.

6. Conclusão

É hoje inegável, a comodidade e facilidade geradas pelo serviço de *home banking*, este permite aos seus clientes realizarem uma serie de operações bancárias através de páginas seguras da Internet, acabando com o fator físico ou presencial adaptando assim a banca tradicional à nova era digital. Tornou- se assim imprescindível adequar os serviços bancários às exigências e necessidades dos seus clientes, nomeadamente quanto à realização de diferentes transações realizadas à distância, permitindo-lhes agora a possibilidade de gerirem a sua vida *on-line.*

Todavia, e se toda esta revolução tecnológica trouxe inúmeras vantagens, também a ela estão associados vários perigos, nomeadamente no que toca a suscesptibilidade que o serviço de *home banking* apresenta pela possibilidade de sofrer ataques informáticos, que se consubstanciam na intromissão não autorizada de terceiro e a realização de uma operação bancária sem a prévia autorização e conhecimento do titular da conta em causa e utilizador do instrumento de pagamento, quer devido a um ataque que afeta toda a estrutura técnica do sistema em causa, quer pela obtenção das coordenadas do cartão matriz que permitem o seu acesso.

É no seio da responsabilidade de casos de operações bancárias não autorizadas e que protagonizou a presente dissertação, que concluo o presente trabalho pela atenuação da responsabilidade da entidade bancária prestadora do serviço e a consequente chamada de atenção para a intensidade dos deveres impostos ao utilizador do instrumento de pagamento, nomeadamente o seu dever de confidencialidade e sigilo.

Assim, ao longo de toda a execução do contrato, o cliente deverá exercer de forma ativa todos os deveres a que está adstrito bem como absorver e assimilar os avisos se segurança (*bunners*) existentes na página da respetiva instituição bancária, com o fim de prevenir situações de fraude.

A meu ver, e apesar do regime plasmado na DSP2 e no atual RSP, ou seja, quanto ao facto do risco correr por conta do Banco, deverá o juiz perante o caso concreto, avaliar fortemente a conduta do cliente bancário, percebendo sobretudo se

o mesmo dotado de toda a informação por parte do Banco quanto às questões de segurança, apesar disso, adotou uma postura de indiferença perante os riscos informáticos a que estava sujeito, ignorando para o efeito toda a informação prévia, bem como a que foi prestada ao longo de toda a execução do contrato.

Em suma, no momento da decisão deverão ser tidos em conta fatores como a profissão e competência técnica do utilizador, tendo sempre em conta a existência ou não da prestação ao cliente de toda a informação necessária à execução saudável e segura do contrato, o que a meu ver, na maioria dos casos se verificará uma vez que hoje, as instituições bancárias, devido também a toda a exigência comunitária nesse sentido prestam cada vez mais, informação clara, assertiva e adequada, ou seja, aquilo a que apresentei como sendo os três níveis de informação: I) assente em toda a informação que é devida para a realização do contrato, o II) consiste na informação que se encontra explicada no menu da página oficial do banca na secção que diz respeito à segurança, em que alerta o cliente para os ataques informáticos que mais acontecem neste setor (*phishing* e *pharming*) , e por fim o III) que visam todos os alertas criados pelo Banco (*bunners*) e que vão surgindo ao longo da navegação, em que para avançar há hiperligação, o cliente terá obrigatoriamente de fechar o aviso, o que leva à uma quase obrigatoriedade quanto à leitura dos mesmos.

Em muitos dos casos é o cliente bancário que com a sua conduta imprudente e indiferente face à informação prestada, que concorre para a concretização da operação bancária por si não autorizada e com a intromissão de terceiro alheio ao sistema, através do fornecimento dos seus códigos pessoais de acesso, bem como das coordenadas do seu cartão matriz, elementos estes pessoais e intransmissíveis.

Para tal, revela-se crucial a análise como referi, da conduta do utilizador antes da sua notificação ao Banco da existência de uma operação de pagamento não autorizada.

Bibliografia

AL.KHATIB, Adnan M., "Electronic Payment Fraud Detection Techniques" in World of computer Science and Information Tecnology Journal (WCSIT), Vol. 2, N.º 4, 2012, pp. 137-141**;**

ALMEIDA, Carlos Ferreira de "Contrato bancário geral e depósito bancário", Coleção de Formação Continua – Direito Bancário, Lisboa: Centro de Estudos Judiciários (2015, disponível em: **http://www.cej.mj.pt/cej/recursos/ebooks/civil/Direito_Bancario.pdf;**

CAMPOS, Diana Beatriz Carrasco Campos e CARMO, Maria do Mar Patricio " HOME BANKING: Consequências Jurídicas", Working Paper Nº. 3/2017, fevereiro, disponível em: www.governancelab.org;

COSTA, Mário Júlio de Almeida, "Direito das Obrigações", 17ª edição, Almedina, Coimbra (2009)**;**

BARREIRA, Carolina França, "*Home Banking:* A repartição dos prejuízos decorrentes da fraude informática", Revista Eletrónica de Direito (2015)**,** disponível em: https://www.cije.up.pt/content/home-banking-repartição-dos-prejuízos-decorrentes-de-fraude-informática;

CORDEIRO, António Menezes, "Direito Bancário", Almedina, Coimbra (2014);

- "Tratado do Direito Civil, Tomo VIII, reimpressão da 1ª edição do tomo III da parte II de 2010. Coimbra: Almedina 2014**;**

CORREIA, Francisco Mendes, "Operações não autorizadas e o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica"**,** Revista de Direito Civil, Ano II (2017): n.º 3;

GOMES, Januário da Costa, "Contratos Comerciais", Coimbra: Almedina (2012);

GUIMARÃES, Maria Raquel, "As operações fraudulentas de *homebanking* na jurisprudência recente: Acordão do Supremo Tribunal de Justiça de 18.12.2013", Proc.6479/09, Cadernos de Direito Privado, nº 49, CEJUR, Braga;

- "A fraude no comércio eletrónico: o problema da repartição do risco por pagamentos fraudulentos, Infrações económicas e financeiras: estudos de criminologia e direito", Coimbra Editora (2013);

- "A repartição dos prejuízos decorrentes de operações fraudulentas de banca eletrónica (*home banking*): Acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09", Cadernos de Direito Privado, n.º 41, CEJUR, Braga, janeiro - março (2013);

- "Contrato-quadro no âmbito da utilização de meios de pagamento eletrónicos", Coimbra Editora, Coimbra (2011);

- "Algumas considerações sobre o aviso nº 11/2001 do Banco de Portugal de 20 de novembro relativo aos cartões de crédito e de débito", Revista da Faculdade de Direito da Universidade do Porto (2004);

- " As transferências eletrónicas de fundos e os cartões de débito. Alguns problemas jurídicos relacionados com as operações de levantamento de numerário por meio eletrónico", Coimbra, Livraria Almedina 1999;

LEITÃO, Luís Menezes, "Direito das Obrigações", Vol. III, 9ª edição, Almedina, Coimbra, 2014;

LIMA, Sofia Ribeiro de "A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na jurisprudência portuguesa"; Dissertação de Mestrado, Faculdade de Direito da Universidade do Porto;

OLIVEIRA, Luiz Gustavo Caratti de, "Responsabilidade civil dos bancos nos casos de fraudes pela internet que lesam as contas de seus clientes" - Monografia de conclusão de curso apresentada ao curso de Pós-Graduação em Direito Civil e Processo Civil da Universidade Castelo Branco, disponível in http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=9110:

ROCHA, Maria Vitória, "Novos meios de pagamento no comércio eletrónico (e-commerce)", Direito da sociedade de informação/ Alberto de Sá e Mello… [et al.] – Coimbra: Coimbra Editora, 2004. – Vol. 5;

SANTOS, Hugo Luz, "Plaidoyer por uma "distribuição dinâmica do ónus da prova" e pela "teoria das esferas de risco" à luz do recente acórdão do Tribunal de Justiça, de

18/12/2013: o (admirável) "mundo novo" no *homebanking*?" Revista Eletrónica de Direito (Abril de 2014), Disponível em: https://www.cije.up.pt/content/plaidoyer-por-uma-"distribuição-dinâmica-do-ónus-da-prova"-e-pela-"teoria-das-esferas-de-ris;

SILVA, João Calvão da, "Serviços de pagamento e responsabilidade civil", Estudos em homenagem a Rui Manchete (2015), Almedina;

- "Conta corrente bancária: operação não autorizada e responsabilidade civil", in Revista de Legislação e de Jurisprudência, Ano 144, n.º 3991, março/abril de 2015, Coimbra Editora, pp. 290-326

VARELA, João Antunes, "Das obrigações em geral", Vol., 10ª edição, Coimbra, Almedina, março 2010;

VASCONCELOS, Miguel Pestana, "Dos contratos de depósito bancário", Revista da Faculdade de Direito da Universidade do Porto, ano VIII, Coimbra, Coimbra Editora, 2011;

VERDELHO, Pedro, "*Phishing* e outras formas de defraudação nas redes de comunicação", em: Direito da sociedade da informação / Alberto de Sá e Mello... [et al.]. - Coimbra: Coimbra Editora, 1999-2006. - vol. 8;

Lista de Jurisprudência

Toda a jurisprudência citada pode ser consultada em: www.dgsi.pt

- Acórdão do STJ de 18.12.2013, Proc. n.º 6479/09.8TBBRG.G1.S, Relator Ana Paula Boularot;
- Acórdão do STJ, de 9.06.2010, Proc. n.º 579/09.1YFLSB, Relator Sousa Grandão;
- Acórdão do TRE de 22.05.2014, Proc. n.º 11/13.6T2ASL.E1, Relator Mata Ribeiro;
- Acórdão do TRG de 25.11.2013 Proc.n.º 2869/11.4TBGMR.G1, Relator Espinheira Baltar;
- Acórdão do TRL de 26.10.2010, Proc. n.º 1943/09.1TJLSB.L1-7, Relator Maria Amélia Ribeiro;
- Acórdão do TRG de 17.12.2014, Proc. n.º1910/12.8TBVCT.G1, Relator Fernando Fernandes Freitas;
- Acórdão do TRL de 5.11.2013, Proc. n.º 9821/11.8T2SNT.L1-1;
- Acórdão do TRP de 7.10.2014, Proc n.º 747/12.9TJPRT.P1, Relator Ana Lucinda Cabral;

.