CATÓLICA

UNIVERSIDADE CATÓLICA PORTUGUESA | PORTO

Ana Rita Arsénio Cardoso

# *Phishing* e *pharming*

## (duas modalidades de fraude informática)

# Responsabilidade obrigacional do Banco

Dissertação de Mestrado em Direito das empresas e dos negócios sob a orientação da Exma. Sra. Professora Doutora Maria João Tomé.

PORTO

2016

# Índice

## Agradecimentos

A elaboração da presente dissertação de mestrado só foi possível graças ao contributo de um conjunto pessoas às quais me cabe deixar o meu agradecimento.

Agradeço ao Senhora Professora Maria João Tomé por ter aceite orientar esta dissertação, e pelo profissionalismo e rigor empregues.

À minha patrona, Senhora Dra. Carla Magalhães Campos, pela amizade e constante motivação.

Aos meus pais, que sempre incentivaram e investiram na minha formação.

À minha irmã e ao João, pela força e carinho inesgotáveis.

## Lista de abreviaturas

Ac. - Acórdão

Artº - artigo

CC - Código Civil

Cfr. - Confrontar

cit. - citado

D.L - Decreto-Lei

DSP - Diretiva relativa aos Serviços de Pagamento

n.º - número

p. - página

Proc. - Processo

RGICSF - Regime Geral das Instituições de Crédito e Sociedades Financeiras

RJCCG - Regime Jurídico das Cláusulas Contratuais Gerais

RSP - Regime Jurídico dos Serviços de Pagamento e Moeda Eletrónica

STJ - Supremo Tribunal de Justiça

TRC - Tribunal da Relação de Coimbra

TRG - Tribunal da Relação de Guimarães

TRL - Tribunal da Relação de Lisboa

TRP - Tribunal da Relação de Porto

Vol. - Volume

## Introdução

A dissertação que aqui se apresenta problematiza a (ir)responsabilidade obrigacional do banco pela ocorrência de operações fraudulentas num sistema da banca ao domicilio – *homebanking* – que, por sua vez, consiste na oferta de produtos e serviços em sistemas informáticos/computacionais, por forma a prestar um serviço mais acessível e cómodo.

Para o efeito, abordaremos no primeiro capítulo o surgimento e expansão deste serviço, a que necessidades veio dar resposta e quais as principais vantagens e desvantagens da sua utilização. Teremos ainda oportunidade de constatar que o referido serviço representou uma viragem crucial no mundo das relações bancárias com o objetivo assumido de não defraudar as graduais expetativas e exigências do consumidor "informatizado", bem como a redução de custos por transação e o aumento do volume de consumidores. Em seguida, passaremos ao enquadramento contratual do *homebanking*, enquanto contrato-quadro e contrato de adesão. Neste capítulo analisaremos ainda quais as principais obrigações que decorrem da celebração do contrato de *homebanking* para ambas as partes – utilizador e entidade bancária – , pois sem esta abordagem inicial não seria possível compreender na íntegra a fundamentação levada em diante pelos nossos tribunais superiores na decisão pela condenação (ou não) do banco e que, se compatibiliza, em parte, com a posição aqui por nós defendida.

Todavia, o *homebanking,* debate-se com a constante preocupação do possível acesso de terceiros a dados confidenciais do cliente da banca eletrónica. Este acesso de terceiros tem lugar através do recurso a pirataria informática, técnicas sofisticadas e complexas, com o intuito de aceder aos códigos pessoais do consumidor e, por sua vez, transferir os fundos em proveito próprio. Trata-se aqui de uma de duas modalidades, *phishing* ou *pharming,* abordadas e densificadas no segundo capítulo.

Esta inquietação é o que problematiza o ponto central do nosso estudo – a responsabilidade do banco pelas perdas resultantes da ocorrência de operações fraudulentas no *homebanking*.

Nesta sede, são várias as questões que se levantam, nomeadamente: como fica o cliente perante uma transferência ilícita de fundos da sua conta? Terá de arcar com a totalidade dos prejuízos causados? Ou será o banco responsabilizado pelas falhas do

sistema que disponibiliza? Quais os meios técnicos de que o banco dispõe para prevenir e/ou reparar este tipo de ataques?

Tentaremos dar resposta de forma clara a todas estas questões ao longo da presente dissertação, com o ambicioso objetivo de proporcionar uma fundamentação mais consolidada e aprofundada, tendo em conta a praticamente inexistente abordagem doutrinal deste tema, muito embora objeto de discussão atual em vários acórdãos dos nossos tribunais superiores.

## Capítulo I- *Homebanking* – Acesso a operações bancárias por via eletrónica

### 1. Breve enquadramento histórico e concetual

As expetativas dos clientes em relação aos bancos têm vindo a aumentar de forma vertiginosa ao longo dos últimos anos. Mais do que uma instituição onde se protegem e guardam as poupanças, o banco passou a ser uma instituição primordial na resolução das diversas questões financeiras relacionados com as mais variadas necessidades.

A origem deste canal de distribuição remonta à década de setenta, altura em que se registava a tentativa das entidades do sector bancário oferecerem aos seus clientes serviços processados com a ajuda de meios eletrónicos. Iniciaram com utilização apenas do telefone, para efetuar pequenas transações (como consulta de saldos e transferências de fundos) ou para apoio na venda de outros produtos ou resolução de problemas e só mais tarde envolve o computador.[1]

Somente em Outubro de 1994 surgiu o primeiro esboço do que atualmente se designa por Internet *Banking* (*Homebanking*/*e-banking*), num inovador movimento do norte-americano Stanford Federal Credit Union, instituição financeira californiana que tirou partido da expansão das telecomunicações em rede e da *World Wide Web* (WWW) para quebrar as barreiras da distância e possibilitar a alternativa de realizar *online* diversas operações.[2]

Contudo, ainda em 1999, a maioria dos bancos apenas oferecia, via internet, informação sobre os seus produtos e acesso a extratos e movimentos. Era, portanto, urgente disponibilizar novos produtos e serviços, como comprar e vender ações na internet, realizar pagamentos e transferências, ou ate mesmo abrir contas.[3]

Volvidos cerca de 4 anos, o conceito de *homebanking* estendeu-se a qualquer atividade bancária efetuada com recurso a meios tecnológicos de informação. É uma espécie de banco de acesso instantâneo a qualquer momento e em qualquer local, sendo

[1] http://bancario.pt/internet-banking-e-banking/#ixzz484RG7N7q

[2] Ibidem.

[3] Silva, Miguel Roberto Mira da/Silva, Alberto/Romão, Artur/Conde, Nuno – Comércio eletrónico na Internet, 2ª Edição Atualizada, Lisboa-Porto-Coimbra, p. 41;

já considerado por muitos dos seus utilizadores como um serviço insubstituível e indispensável.[4] Na prática, funciona como um banco *online* através do qual se pode realizar a maioria das operações disponíveis nos balcões físicos. Em Portugal, o seu verdadeiro impacto só começou há cerca de sete anos atrás.[5] Esta inovação é consequência da grande concorrência entre os bancos mas, também, das poupanças alcançadas quando se realizam estas operações na internet.

Hoje, o banco é um verdadeiro *"supermercado"* financeiro, onde o cliente procura satisfazer as mais variadas necessidades, assistindo-se, neste contexto, a um aumento significativo da utilização da banca através da internet.[6]

Esta viragem na utilização do sistema bancário deu origem a inúmeras modificações que tiveram como intuito responder de forma eficaz e célere aos estilos de vida cada vez mais dinâmicos dos consumidores.[7]

Ao ser confrontada com um crescimento exponencial e intensivo da concorrência, a atividade bancária viu-se forçada a renovar funcionalidades de forma a satisfazer as constantes e progressivas expetativas dos clientes.[8]

Com a pretensão de aproximar-se dos seus clientes, sempre que estes desejem aceder aos seus serviços, a banca viu-se forçada a adequar soluções à atual maneira de viver da sociedade, que é hoje, manifestamente, globalizada e apressada.

Estas alterações importaram a consciencialização de que os tradicionais balcões de atendimento ao público não são suficientes para responder às mais variadas carências dos diferentes clientes.[9]

---

[4] http://bancario.pt/internet-banking-e-banking/#ixzz484RG7N7q

[5] Reis, Sofia Cláudia Moreira Duarte – Os Determinantes da Adopção da Internet como Canal de Distribuição no Sector Bancário – Dissertação, Universidade de Coimbra (2005), p.122;
Raposeiro, Ana Raquel Correia - A Influência dos Valores Pessoais na Adopção da Banca pela Internet – Dissertação, Universidade de Coimbra (2007), p. 13-46;

[6] Vilela, Helena Cristina Monteiro Pinto – O serviço Caixadirecta Evolução dos Canais de Distribuição no Sector Bancário – Relatório de Estágio, Universidade do Minho (2005), p.52-58;
Reis, Sofia Cláudia Moreira Duarte – op. cit;

[7] Vilela, Helena Cristina Monteiro Pinto – op. cit;

[8] Ibidem.

[9] Vilela, Helena Cristina Monteiro Pinto – op. cit.;
Reis, Sofia Cláudia Moreira Duarte – op. cit;
Raposeiro, Ana Raquel Correia – op.cit;

A crescente evolução tecnológica permitiu o aparecimento de novas formas alternativas de prestação de serviços, aliás: "*A tecnologia tem uma influência crescente no marketing, especialmente nos sistemas de prestação de serviços bancários, não só ao modificar as relações com os clientes, mas também ao criar novas oportunidades em segmentos que anteriormente seriam pouco rentáveis…*".[10]

Assim, a disponibilização da banca no canal eletrónico tornou-se, acima de tudo, uma necessidade a que era urgente dar resposta.

De forma a poderem responder ao aumento do volume de negócios sem o correspondente aumento de custos, as empresas têm procurado, cada vez mais, a utilização intensiva das tecnologias.

Os bancos têm baseado a sua oferta de produtos e serviços em sistemas computacionais e de telecomunicações como forma de prestar melhores serviços, quer a clientes particulares quer, a clientes institucionais. [11]

Na banca eletrónica o grande desafio da entidade bancária passa pela conquista da confiança do cliente na segurança deste tipo de serviço. A solução terá de se enquadrar algures entre a qualidade e a seriedade da instituição na distribuição do serviço que oferece.

Para que se torne possível conferir maior segurança a este tipo de serviço, deverão ser desenvolvidos, frequentemente, esforços significativos, visto que a realidade virtual encontra-se em constante mutação, manifestando ter um sólido potencial enquanto canal do futuro. O desenvolvimento desses mesmos esforços deverá passar pelo cumprimento de dois pilares fundamentais: prevenir que terceiros tenham acesso ao conteúdo das transações efetuadas e garantir que quem origina a transação corresponde na realidade a quem declara ser.[12] A constante evolução e aperfeiçoamento do produto tem consubstanciado um fator elementar ao longo do processo de captação e fidelização de clientes.

[10] Vilela, Helena Cristina Monteiro Pinto – op.cit;

[11] Ibidem.

[12] Vitela, Helena Cristina Monteiro Pinto – op.cit;

Reis, Sofia Cláudia Moreira Duarte – op.cit;

Neste sentido, afigura-se como indispensável que cada um das instituições bancarias existentes em Portugal reforce a sua posição no sistema financeiro, investindo, nomeadamente, na prossecução de padrões éticos exigentes que garantam a confiança e fidelização dos clientes.[13]

## 1.1. Principais vantagens e desvantagens da sua utilização

A tecnologia permite quebrar barreiras, transformando processos tradicionalmente morosos e complexos em sistemas eficazes e céleres, de fácil acesso. A disponibilidade do serviço pelo cliente a qualquer momento e, em qualquer lugar, faz com que o surgimento do *homebanking* represente uma nova era na realidade bancária.

No entanto a par das vantagens existem uma série de perigos relacionados com a segurança do sistema, isto porque, a internet constitui uma fonte inesgotável de cruzamento e difusão de informação, o que gera, inevitavelmente, uma propensão para ataques fraudulentos.

Analisemos sucintamente os prós e contras da utilização deste serviço:

### i. A acessibilidade

A facilidade e simplicidade no acesso a este tipo de serviço consubstanciam no facto de através de uma página na Internet ser possível aceder, em qualquer lugar, a um vasto leque de operações que tradicionalmente só estão disponíveis nos balcões de uma instituição bancária, 24 horas por dia, sete dias por semana, sendo de utilização à partida simples e intuitiva, não obstante, esta variável estar fortemente relacionada com o contexto social, etário e educativo em que o indivíduo se insere.[14]

Os clientes, apenas adotarão a banca pela internet quando tiverem o conhecimento necessário para trabalhar com o computador e usar a internet. Pelo que a autoeficácia no

[13] Raposeiro, Ana Raquel Correia - op.cit;

[14] Raposeiro, Ana Raquel Correia – op.cit.p.36-46;

uso do computador ajudará a explicar a opção pela adesão ou rejeição dos utilizadores a este tipo de serviços.[15]

Desta forma, os responsáveis da banca pela internet devem, junto dos clientes, reforçar a perceção da utilidade e facilidade de uso.

### ii. A compatibilidade e/ou utilidade

A recetividade às novas tecnologias tem criado novos padrões de consumo e novas plataformas de comunicação, obrigando a uma adaptação e/ou reorganização dos modelos vigentes, de acordo com o atual e modernizado estilo de vida dos cidadãos. Apesar de o balcão continuar a ser o principal canal de distribuição da banca, o atual crescimento dos novos canais tem trazido mudanças significativas. As tecnologias permitem ao próprio cliente tratar das suas transações bancárias autonomamente sem necessitar de se dirigir ao balcão, como é o caso das ATM's (Automated Teller Machine), do telefone, da Internet, do telemóvel ou até da televisão interativa.[16]

A natureza interativa da Internet potência oportunidades para aumentar a eficiência do comportamento do consumidor pela variedade de informação disponível acerca dos produtos.

A facilidade no acesso e o grau utilidade dos serviços abrangidos são variáveis fundamentais na decisão pela utilização do sistema. Neste contexto, motivar os clientes para o uso das novas tecnologias nos serviços bancários é um grande desafio para os bancos.[17]

### iii. A (in)segurança

A segurança tem sido um dos principais obstáculos à adoção da banca eletrónica, pois a sua utilização, independentemente da operação bancária que se pretenda efetuar,

[15] Ibidem.

[16] Raposeiro, Ana Raquel Correia - op.cit.p.36-46;

[17] Ibidem.

está positivamente relacionada com a segurança do sistema, representando, assim, este vetor, a principal desvantagem na adesão a este tipo de serviço.[18]

De facto, um dos maiores obstáculos que se enfrenta na utilização da internet é o potencial acesso de terceiros a dados confidenciais, figurando-se este o verdadeiro *calcanhar de Aquiles* deste tipo de serviços. É do conhecimento comum que todo o êxito no comércio eletrónico depende da confiança que este inspire.

Assim, a (in)segurança, de per si , é o fator mais importante em toda a estrutura de um serviço *online*, isto porque, atualmente a imensidão de ataques à segurança das redes (mesmo das mais protegidas), bem como o desenvolvimento de ferramentas de *phishing* ou *pharming* que poluem o ciberespaço, têm vindo a criar receio, apreensão e desconfiança relativamente a esta inovadora ferramenta financeira.[19]

Uma das formas de prevenir a verificação de operações ilícitas é precisamente pela divulgação e explicação das políticas de segurança da rede, como a encriptação, *firewalls*, o servidor de autenticação, e *password* de proteção. Assim, a segurança, afigura-se como o fator de maior influencia na adesão/não adesão por parte dos consumidores. [20] É, pois, na repartição de responsabilidades entre o banco e os seus clientes que se situa a pedra de toque de toda esta matéria.[21] É aqui que se centra o estudo do nosso trabalho.

## 2. Enquadramento contratual do *homebanking*

A realização de operações de *homebanking* pressupõe uma relação negocial complexa, iniciada com o contrato de abertura de conta e o depósito bancário,[22] que

[18] Vilela, Helena Cristina Monteiro Pinto – op.cit;
Reis, Sofia Cláudia Moreira Duarte – op.cit;
Raposeiro, Ana Raquel Correia - op.cit.p.36-46;

[19] Ibidem;

[20] Ibidem;

[21] Cordeiro, António Menezes (2010) – Manual de Direito Bancário, 4ª Edição, Almedina.

[22] A este propósito, João Calvão da Silva refere que, apesar de andar a conta corrente bancária, normalmente associada à conta de depósito à ordem, *"trata-se de duas modalidades de convenção, perfeitamente distintas (...), A conta*

permite disciplinar, previamente, as relações entre o banco prestador do serviço e o seu cliente, simplificando os procedimentos a adotar no momento em que essas operações são concretizadas.

Todavia o *homebanking* autonomiza-se do contrato de abertura de conta, pois no contrato de banca eletrónica existe uma troca de declarações de vontade de conteúdo diverso do manifestado no contrato de abertura de conta. Tal implica um objeto diferente, bem como uma vontade de vinculação distinta.[23]

O contrato de abertura de conta representa o primeiro e o mais importante dos contratos bancários, celebrado entre o banco e o seu cliente, através do qual usualmente se constitui, disciplina e baliza a respetiva relação jurídica bancária.[24] É o contrato matriz, no sentido de estabelecer o quadro geral de regulação da maioria dos futuros negócios que venham a ser eventualmente celebrados pelas partes.[25] Por sua vez, o contrato de *homebanking* visa, essencialmente, estabelecer uma forma de o cliente realizar operações de pagamento com recurso aos meios eletrónicos.

Tanto o Tribunal da Relação de Guimarães (TRG) como o Tribunal da Relação de Lisboa (TRL), nos seus acórdãos de 26/10/2010 e de 24/05/2012, respetivamente, vieram afirmar que este contrato de *homebanking* se insere " numa relação negocial complexa iniciada 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".

---

*corrente é um contrato autónomo, com conteúdo próprio, na essência o serviço de "B", distinto do depósito e da abertura de crédito."* in Direito Bancário, Almedina, 2001, pág. 344;

[23] Barreira, Maria Carolina dos Santos Gomes Ferreira – Home Banking A repartição dos prejuízos decorrentes da fraude informática – Dissertação de mestrado (2015), Universidade Nova de Lisboa, p. 6.

[24] Cordeiro, António Menezes – Os Contratos Bancários. Separata – Estudos em homenagem ao professor doutor Carlos Ferreira de Almeida. Almedina (2011), p. 84;

Antunes, José Engrácia – Direito dos contratos comerciais. Coimbra Almedina (2009), p. 483;

[25] Ibidem;

Vide o Ac. do STJ de 19-12-2006 (Paulo Sá), in www.dgsi.pt;

## 2.1. Um contrato-quadro?

No seguimento do exposto *supra*, Maria Raquel Guimarães afirma que este contrato de abertura de conta tem a natureza de um contrato-quadro, celebrado mediante a adesão do cliente bancário a um conjunto de cláusulas contratuais gerais pré-definidas pela entidade bancária, desencadeando uma relação bancária geral, na qual assentam os diferentes contratos celebrados subsequentemente pelas partes.[26]

Por esta razão se afirma que a abertura de conta funciona como um "contrato dos contratos"[27], daí a sua classificação como contrato normativo[28] ou contrato-quadro.[29]

O anexo I do D.L 317/2009, de 30 de Outubro, do Regime dos Sistemas de Pagamento (RSP) que transpôs para o nosso ordenamento jurídico a Diretiva 2007//64/CE de 13/11 relativa aos serviços de pagamento, vem apresentar, no âmbito dos serviços de pagamento, a noção de contrato-quadro de prestação de serviços de pagamento enquanto "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" e regula as operações de pagamento abrangidas por um contrato-quadro nos artigos 51 e seguintes.[30]

O legislador partiu, assim, da ideia de que determinadas operações de pagamento não surgem de forma isolada mas antes se inserem no contexto de contrato-quadro

---

[26] Guimarães, Maria Raquel – A Repartição dos prejuízos decorrentes de operações fraudulentas de banca eletrónica (home banking), in Cadernos de Direito Privado nº 41, p. 59.

[27] Guimarães, Maria Raquel – O contrato-quadro no âmbito da utilização de meios de pagamento eletrónicos. Coimbra editora (2011), p. 363.

[28] Cordeiro, António Menezes – op.cit, p. 510.

[29] Vide Ac. do STJ de 03/04/2003 in www.dgsi.pt, que adotou a classificação de contrato-quadro; Texto preambular ao D.L. 95/2006 de 29/05 que transpôs para o direito interno a diretiva 2002/65/CE do Parlamento Europeu e do Conselho de 23/09, "relativa à comercialização à distância de serviços financeiros prestados a consumidores";
Cfr. artº 2º alínea m) do RSP;
Almeida, Carlos Ferreira de – Contratos II, Conteúdo dos contratos de troca, Almedina (2012), p. 140-143;
Ferreira, António Pedro de Azevedo - A relação negocial bancária – conceito e estrutura. Lisboa Quid Iuris (2005) p. 683-685;

[30]Guimarães, Maria Raquel – (Ainda) a responsabilidade pelo uso indevido de instrumentos de pagamento in I Congresso de Direito Bancário (2015) p. 121;
Gomes, Manuel Januário da Costa – Contratos Comerciais, Almedina (2012), p. 231-236;

anteriormente celebrado entre um utilizador do serviço de pagamento e o respetivo prestador.[31]

Por conseguinte, o contrato de *homebanking* figura, de igual forma, um contrato-quadro relativamente às sucessivas operações de transferência eletrónica de importâncias ordenadas através da internet.[32] Assim, cada vez que o cliente emite uma ordem de pagamento a favor de terceiro – mandato de pagamento - através do sistema informático colocado à disposição pelo banco, é celebrado um novo contrato de execução do contrato de *homebanking*.

Assim, as operações de pagamento eletrónico realizadas por via de um sistema de banca ao domicílio não surgem descontextualizadas correspondendo a simples atos de execução de um contrato previamente celebrado, potenciador de uma pluralidade de outros contratos subsequentes. Podemos verificar que esta figura contratual propícia uma série de contratos subsequentes, simplificados, na sua conclusão e execução, através do recurso a meios informáticos. Também estes contratos de execução correspondem individualmente, a acordos de vontade tal como o contratos-base previamente celebrados, não se reduzindo a meros atos de execução de um contrato anterior.[33]

Apesar de ser de prática comum, no contrato de abertura de conta, constar no seu clausulado, todas as possíveis relações que se possam advir entre os contraentes, abrangendo, inclusive, parte das regras que regem o contrato de *homebanking*, tal situação não obsta à sua validade enquanto contrato autónomo.[34]

Pois, no contrato de banca eletrónica, além de existir uma concertação de vontades autónoma, encontramos um acordo vinculativo assente sobre duas declarações de vontade (proposta, de um lado, e aceitação, do outro)[35] interligadas no comum objetivo de proporcionar ao cliente a realização de transferências bancária em suporte informático.

---

[31] Guimarães, Maria Raquel – (Ainda) a responsabilidade… p. 121.

[32] Guimarães, Maria Raquel – A Repartição… p. 59.

[33] Guimarães, Maria Raquel- O contrato-quadro…p. 133.

[34] Ac. TRL de 28/06/2013 (Anabela Calafate); Ac. TRP de 29/10/2013 (Francisco Matos); Ac. TRG de 25/11/2013 (Espinheira Baltazar); Ac. TRL de 12/12/2013 (Tomé Ramião), todos in www.dgsi.pt;

[35] Barreira, Maria Carolina dos Santos Gomes Ferreira – Home Banking… p. 7.

Podemos verificar que o contrato de banca eletrónica, além de surgir no âmbito de uma relação contratual complexa, também potencia uma multiplicidade de contratos subsequentes. É, pois, um "contrato que antecipa futuros contratos".[36]

### 2.2. Um contrato de adesão?

No contrato de *homebanking*, é acordada a prestação de um serviço de banca eletrónica ao domicílio por uma determinada entidade bancária a um seu cliente, ambos partes no contrato. Estes contratos assentam num conjunto de cláusulas contratuais gerais, pré-definidas de uma forma unilateral pela entidade bancária, que determinam o conteúdo da relação contratual, tendo como destinatários os seus clientes aderentes ao serviço.

Perante um contrato de adesão, a única "autonomia" que o cliente dispõe é a decisão de concluir ou não o contrato, daí que se mostre essencial que as cláusulas contratuais gerais sejam justas, equitativas e razoáveis.[37]

Face à vulnerável posição em que se encontra o aderente nestes contratos, são alguns, os mecanismos, que o nosso ordenamento jurídico prevê que visam, precisamente, o controlo das cláusulas contratuais gerais (os quais iremos densificar no capítulo III) e a inerente proteção do consumidor.[38]

## 3. Os deveres que decorrem da relação contratual complexa

Apesar de estarmos perante um serviço que confere vantagens recíprocas para os contraentes, maior facilidade e total disponibilidade de acesso, por um lado e, uma redução dos custos de funcionamento, por outro, a estas vantagens acrescem deveres, sobretudo de diligência e cuidado. Tais deveres implicam para ambas as partes a observância de procedimentos e regras de segurança.

---

[36] Guimarães, Maria Raquel – O contrato-quadro…p. 151.

[37] Silva, João Calvão da – op.cit. p. 349-350.

[38] Vide D.L n.º 446/85, de 25 de Outubro (Cláusulas contratuais gerais) a respeito das cláusulas absolutamente proibidas e sancionadas com nulidade (artigos 12º e 24º);
Vide Lei nº 24/96, d 31 de Julho (Lei de defesa do consumidor);

Ao celebrar-se um contrato de execução contínua, como o contrato de *homebanking*[39] cria-se uma relação obrigacional complexa que abrange os direitos subjetivos, deveres principais, acessórios e laterais de conduta, que se harmonizam na prossecução de um mesmo fim contratual.[40] São sobretudo os segundos deveres que fazem toda a diferença na conclusão perfeita do contrato de *homebanking*.

Nas palavras de Mota Pinto e Galvão Teles, a relação contratual "alimenta-se" essencialmente dos deveres laterais, deveres esses *funcionalizados em ordem ao perfeito cumprimento*. A tipificação destes deveres encontra-se dispersa em várias fontes normativas.[41]

Para Menezes Cordeiro estes deveres traduzem-se, sobretudo, em deveres de proteção, de esclarecimento e de lealdade.[42]

Por sua vez, José Carlos Proença adota uma enumeração mais extensiva, mencionando aqui os deveres de aviso/comunicação (o dever do cliente comunicar ao banco a ocorrência de uma operação fraudulenta assim que dela tenha conhecimento), os deveres de informação e esclarecimento (o banco terá de prestar todas informações e esclarecimentos necessários à correta e eficaz utilização serviço que disponibiliza), deveres cooperação (o cliente terá que colaborar com o banco na salvaguarda dos códigos de segurança), deveres de cuidado ("como a execução do contato pode comportar riscos há que evitar a criação de condições perigosas").[43]

Atualmente, as operações de pagamento realizadas através de um sistema de banca eletrónica encontram-se reguladas no RSP.[44]

---

[39] Ac. TRG de 25/11/2013 (Espinheira Baltazar) in www.dgsi.pt;

[40] Guimarães, Maria Raquel – O contrato-quadro… p. 279;

Barreira, Maria Carolina dos Santos Gomes Ferreira – Home Banking… p. 17;

[41] Proença, José Carlos Brandão – Direito das obrigações – Relatório sobre o programa, o conteúdo e os métodos de ensino da disciplina in Publicações da Universidade Católica, Porto (2007), p. 130.

[42] Ibidem.

[43] Ibidem, p. 130-131;

[44] Cfr. artigos 67º e 68º do RSP;

### 3.1. Os deveres inerentes à entidade bancária – prestador de serviços

No contrato de *homebanking*, apenas a entidade bancária tem um dever principal, que se traduz na aceitação dos sucessivos mandatos para transferências de fundos, emitidos pelo utilizador, mediante a correta autenticação da operação. Como dever secundário acessório da prestação principal, o banco deve facultar ao cliente todos os instrumentos necessários à utilização do serviço de banca ao domicílio, tais como o fornecimento do cartão matriz e todos os códigos de acesso.[45]

Ao banco compete, ainda, assegurar que os dispositivos de segurança personalizados só estejam ao alcance do utilizador a quem foi concedido o direito à sua utilização do instrumento (alínea a) do n.º 1 do artigo 68º do RSP).

A lei prevê, neste âmbito, um dever reforçado de informação a cargo do prestador de serviços que consiste em esclarecer o utilizador respetivo, quais as medidas que este deve adotar "para preservar a segurança dos instrumentos de pagamento".

Justifica-se, desta forma, um dever imposto à entidade bancária de explicar as situações mais frequentes de fraude eletrónica e alertar para os perigos decorrentes da utilização do serviço que se comprometeu a prestar, isto sempre tendo em conta o tipo de utilizador e os seus conhecimentos técnicos. Como refere MARIA RAQUEL GUIMARÃES este dever que recai sobre a entidade bancária é um dever lateral de conduta, decorrente do contrato duradouro celebrado entre as partes e, essencialmente da especial relação de confiança gerada entre o banco e o seu cliente, que tem início aquando da abertura de conta e é densificada ao longo da corrente negocial.[46]

Na execução das operações de *homebanking*, o cliente não deve abrir correio eletrónico cujo remetente seja desconhecido, não deve abrir, nem executar ficheiros que não tenham sido solicitados, ter sempre um antivírus atualizado, utilizar computadores da sua confiança entre outras. Estes são alguns exemplos de atuações pertinentes que visam evitar qualquer ataque fraudulento ao sistema, embora não garantam a cem por cento a infalibilidade do sistema.[47]

---

[45] Barreira, Maria Carolina dos Santos Gomes Ferreira – Home Banking… p. 22;

[46] Guimarães, Maria Raquel - A Repartição… p. 61.

[47] Ac. TRG de 25/11/2013 (Espinheira Baltazar), Proc. 2869/11.4TBMGR.G1 in www.dgsi.pt;

A este propósito, o TRG, no seu acórdão de 25-11-2013, entendeu que a instituição bancária cumpre o seu dever de proteção e informação colocando no seu *site* toda a informação disponível sobre segurança, elucidando os seus clientes sobre os métodos utilizados para a captura de dados pessoais por terceiros. Seguindo esta lógica do TRG, a entidade bancária liberta-se do dever de garantir um serviço seguro e eficaz através da simples explanação de informação sobre o perigo do furto de dados pessoais por terceiros. Não nos parece, no entanto, razoável que o designado dever de proteção se escasseie na mera propaganda dos deveres de segurança a ser tidos em conta pelo utilizador, no *site* do banco. Tal entendimento comprometeria gravemente a posição do cliente, deixando-o demasiado desprotegido em relação aos eventuais prejuízos causados, por não se encontrar dotado de qualquer legitimidade para exigir mais satisfações ao banco. Isto porque, a partir da referida divulgação informativa, o banco exonera-se de quaisquer responsabilidades. Somos obrigados a concordar que o banco não pode cumpre integralmente as suas obrigações constantes no contrato apenas pelo simples fato de disponibilizar ao seu cliente as condições de acesso ao serviço, fornecendo lhe para tal os códigos necessários.

Uma decisão deste teor não é sequer compatível com as obrigações decorrentes do Regime Geral das Instituições de Crédito e Sociedades Financeiras (RGICSF), que consagra, no seu artº 73º, o dever das instituições bancárias "(…) assegurarem, 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 segurança".[48] A instituição bancária deve criar um sistema de acesso às operações de pagamento via eletrónica credível no qual o utilizador possa confiar e que por sua vez garanta a não ocorrência de falhas técnicas durante a operação. Parece-nos compreensível este dever imposto à entidade bancária, uma vez que o cliente não tem qualquer controlo sobre os complexos e sofisticados meios informáticos da entidade bancária, nem tão pouco dispõe de um departamento técnico especializado.

A lei estabelece ainda no artigo 68º do RSP outros deveres acessórios de conduta a ser observados pelo banco. Quanto à notificação da utilização não autorizada do instrumento de pagamento à entidade bancária, levada a cabo pelo utilizador do sistema,

[48] D.L n.º 298/92 de 31 de Dezembro com as alterações introduzidas pelo DL n.º 1/2008, de 3 de Janeiro.

determina-se que esta deve garantir a disponibilidade, a todo o momento, de meios adequados que permitam ao utilizador comunicar ao banco o ocorrido (alínea c) do n.º 1 do artigo 68º do RSP). Consequentemente, sobre o banco recaí ainda o dever de impedir qualquer utilização do instrumento de pagamento logo que a notificação da utilização não autorizada deste tenha sido efetuada (alínea e) do n.º 1 do artigo 68º do RSP).

### 3.2. Os deveres que impendem sobre o utilizador – cliente bancário

Já no caso do utilizador do serviço de *homebanking*, este, tem a seu cargo, um conjunto de deveres acessórios de conduta relacionados essencialmente com a segurança do sistema.

Neste âmbito, o dever essencial que impende sobre o utilizador do sistema, passa pela adoção de todas as medidas razoáveis para preservar a eficácia dos mecanismos de segurança personalizados associados ao instrumento de pagamento (n.º 2 do artigo 67º do RSP). Traduz-se na salvaguarda da confidencialidade dos seus códigos pessoais de acesso ao presente serviço.

O conhecimento destes códigos de acesso é *fórmula* atualmente utilizada para se cumprirem os objetivos de identificação e de consequente associação das operações em causa ao utilizador do serviço, dando a operação como validamente autenticada.[49]

Com isto, o banco pretende verificar a coincidência entre a pessoa que pretende aceder ao serviço de *homebanking* e o cliente que subscreveu o respetivo contrato. Assim, uma vez digitada a senha correta, o sistema informático valida-a e presume que está perante o seu verdadeiro portador.[50]

Pelo exposto, o utilizador, encontra-se vinculado ao dever de garantir a segurança desses elementos, não facultando a sua utilização a terceiros (nº 2 do artigo 67º do RSP). Este dever consta de modo geral do contrato de banca eletrónica a que o cliente aderiu, assim como decorre das regras gerais de diligência (critério de um bom pai de família).

[49] Guimarães, Maria Raquel – A Repartição… p. 60.

[50] Ibidem p. 61.

Acresce ao utilizador um outro dever acessório de conduta, o dever de comunicar de imediatamente ao seu banco, assim que tenha conhecimento, a utilização inapropriada do instrumento de pagamento. Este dever encontra-se, normalmente, estabelecido no clausulado contratual mas, mesmo que assim não fosse, sempre decorria da especial relação de confiança entre o banco e o cliente.[51] Este dever tem ainda consagração legal na alínea b) do n.º 1 do artigo 67º do RSP e determina que, em caso de utilização não autorizada do instrumento de pagamento, o utilizador deve notificar o ocorrido ao banco, logo que tenha conhecimento e sem atrasos injustificados.

Os deveres supra destacados consubstanciam-se deveres acessórios de conduta que decorrem de uma relação obrigacional complexa, cuja observância revela-se essencial no correto processamento da relação contratual.[52] Importa referir que, estes deveres podem derivar de cláusulas contratuais, de dispositivos da lei *ad hoc* ou do princípio da boa-fé (n.º 2 do artigo 762º do Código Civil, doravante, CC) ou ainda da relação de especial confiança.[53]

Em caso de inobservância destes deveres pelo utilizador, como não estamos perante deveres de prestação (deveres principais), a entidade bancária, não pode recorrer em regra à ação de cumprimento (artº 817º do CC), [54] restando-lhe o direito de invocar a responsabilidade contratual e a exigir o pagamento de uma indemnização pelos prejuízos causados nos termos do 798º do Código Civil. O utilizador do serviço de *homebanking* responde pela totalidade de prejuízos que lhe possam ser imputados a título de dolo ou negligência devido ao incumprimento das suas obrigações contratuais.[55]

---

[51] Guimarães, Maria Raquel O contrato-quadro… p. 331.

[52] Varela, João Matos Antunes – Das Obrigações em Geral, Vol. I 10ª edição (revista e atualizada) Almedina (2009), p. 122-125 – De acordo com este autor estes deveres assumem uma especial relevância nos contratos bilaterais, onde se impõe a cada uma das partes contratuais o dever de tomar as precauções necessárias para que a obrigação que lhe incumbe satisfaça o interesse do credor na prestação;

[53] Costa, Mário Júlio De Almeida – Direito das obrigações, 12ª Edição (revista atualizada) Almedina (2009), p. 77;
Barreira, Maria Carolina dos Santos Gomes Ferreira – Home Banking…p. 19;
Proença, José Carlos Brandão – Direito das obrigações – Relatório sobre o programa, o conteúdo e os métodos de ensino da disciplina in Publicações da Universidade Católica, Porto (2007), p. 131.

[54] ; Varela, João Matos Antunes – Das Obrigações em Geral, Vol. I 10ª edição (revista e atualizada) Almedina (2009), p. 123-124;
Vide ac. TRC de 9/11/2004,(Alexandrina Ferreira), in www.dgsi.pt;

[55] Guimarães, Maria Raquel –As transferências eletrónicas de fundos de cartões de débito, Almedina (1999) p. 212.

Em contrapartida, o banco, poderá resolver o contrato uma vez que a observância destes deveres decorre de uma estreita relação de confiança mútua e de leal colaboração.[56]

## Capítulo II - *Phishing e pharming* – Duas modalidades de fraude eletrónica

### 1. A fraude nas operações de banca eletrónica

No capítulo anterior, consolidamos que o surgimento do *homebanking* ficou a dever-se ao gigantesco progresso tecnológico e à consequente e/ou emergente necessidade de dar respostas rápidas e eficazes às atuais exigências de um renovado e mais sofisticado consumidor.

Todavia o apanágio deste sistema, por si só, não elimina a possibilidade de eventuais ataques informáticos e a interceção de dados confidenciais do utilizador do sistema de forma encapotada.

Ainda que os *sites* bancários sejam de uma maneira geral fiáveis, não nos podemos esquecer que a internet constitui uma fonte inesgotável de cruzamento e difusão de informação, o que gera, inevitavelmente, uma propensão para este tipo de ataques maliciosos.

A utilização fraudulenta do serviço de *homebanking* consiste na realização de operações dolosas, em que o autor da fraude consegue aceder, *online*, a uma conta de determinado cliente de certo banco, levando a cabo transferências de quantias nela (conta) existentes para contas de terceiros. Este acesso não autorizado poderá ser logrado através de programas informáticos – "quebrando" os mecanismos de segurança do sistema – ou, mais comummente, utilizando os códigos de acesso de um cliente: falamos aqui do *phishing* e o *pharming*.[57]

[56] Machado, João Baptista – Pressupostos da resolução por incumprimento in Obra dispersa I (1991), p. 41;
[57] Guimarães, Maria Raquel - *A Repartição…* p. 63;

### 1.1.Phishing

O *phishing* consiste na aquisição de dados pessoais, isto é, no envio de mensagens de correio eletrónico com vista à obtenção de dados intransmissíveis tais como número de conta, número de contrato, número fiscal, códigos de acesso, ou qualquer outra informação dos destinatários que permita o acesso às contas bancarias destes.[58] Estas mensagens surgem com uma aparência fidedigna, "camufladas", bastas vezes, como mensagens da própria entidade bancária da qual o destinatário é cliente.[59]

O destinatário, ao abrir as referidas mensagens e ao fornecer as informações solicitadas, e/ou ao acionar *links* para outras paginas, ou ao descarregar possíveis arquivos ali contidos, poderá estar a proporcionar o furto de informações bancarias e sua subsequente utilização.[60]

Daqui podemos depreender que o *phishing* se consubstancia numa espécie de "furto de identidade", praticado em ambientes de redes informáticas (Internet), traduzido na subtração de informações específicas (dados bancários), para finalidades também determinadas (transferência de quantias existentes em contas bancárias).[61]

A este propósito, PEDRO VERDELHO refere que: *"esta atividade é faticamente complexa e traduz-se na remessa massiva de mensagens de correio eletrónico (utiliza portanto a técnica de spam). Tais mensagens incluem um link para uma página na WWW. Esta página será normalmente a reprodução aproximada de uma outra (esta autêntica), por exemplo de um banco ou de uma entidade emissora de cartões de crédito. Conterá elementos identificadores da entidade autêntica e imagens a ela referentes. Porém, será falsa, por ser construída e gerida por terceiros, sem autorização da entidade cujos sinais pretende imitar. Se a vítima usar o link para aceder à página falsa deparar-se-á com uma página parecida com a do seu banco, ou da entidade gestora do seu cartão de crédito (ou de qualquer outro sítio na Internet que permita a realização de pagamentos online).*

---

[58] Guimarães, Maria Raquel - A Fraude no Comércio Eletrónico: O Problema da Repartição do Risco por Pagamentos Fraudulentos in Infrações Económicas e Financeiras, Estudos de Criminologia e Direito (J. Cruz, C. Cardoso, A. L. Leite, R. Faria, coordenação). Coimbra Editora (2013).

[59] Ibidem.

[60] Guimarães, Maria Raquel – As operações fraudulentas de homebanking na jurisprudência recente in Cadernos De Direito Privado Nº 49 (2015) - ISSN: 1645-7242, p. 25 e 26;

[61] Silva, Flávio Manuel Carneiro – A usurpação da ciberidentidade (2014), dissertação – Universidade Católica Portuguesa, p. 31.

*Será pedido à vítima que se identifique, introduzindo os seus códigos confidenciais, referentes às sua conta bancária ou ao seu cartão, que permitirão aceder às contas bancárias das vítimas, transferindo o dinheiro que aí houver para contas suas. Ou utilizar os respetivos cartões de crédito em seu proveito".*[62]

### 1.2.Pharming

O *pharming*, por sua vez, é uma técnica mais sofisticada e, consequentemente mais perigosa, na medida em que é adulterado o próprio nome de domínio de uma entidade financeira, redirecionando o utilizador para um *site* falso, que constitui uma espécie de "*colonagem"* da real página da entidade visada. Isto é, sempre que o utilizador digita no teclado o endereço correto da sua entidade bancária, é conduzido de forma automática para a página forjada, com as mesmas características gráficas e estéticas da verdadeira. Crendo o utilizador, desta forma, estar efetivamente perante o *site* do seu banco, este "colabora" com o infrator ao disponibilizar as suas informações confidenciais, procedendo o infrator, de imediato, à recolha dos dados, para posteriormente ingressar na real página do banco e proceder ao levamento ilícito das quantias.[63]

PEDRO VERDELHO reflete igualmente sobre esta modalidade caracterizando-a como uma *"técnica que utiliza os métodos de difusão de vírus que têm formato de verme – os worms. Passa pela difusão, por via de spam – portanto de correio eletrónico. – de ficheiros ocultos, que igualmente de forma oculta se auto-instalam nos computadores ou sistemas informáticos das vítimas. Uma vez alojados, estes ficheiros alteram de forma oculta, sem o conhecimento do dono do computador, os arquivos do sistema, designamente os ficheiros contendo os populares favoritos e o registo de cookies. Por via desta alteração, quando o dono do computador acede ao seu habitual site bancário, o sistema, ardilosamente alterado, redirige-o para um outro site, construído e disponibilizado online com métodos idênticos aos do phishing. Nestes casos torna-se muito difícil reconhecer a fraude, mesmo para utilizadores avançados".*[64]

---

[62] Pedro Verdelho, Phishing e outras formas de defraudação nas redes de comunicação, in Direito da Sociedade de Informação, p. 413;

[63] Guimarães, Maria Raquel - *A Repartição*… p.

[64] Pedro Verdelho, Phishing e… p. 413.

1.3.*Phishing* e *pharming* duas modalidades distintas?

Não podemos, inevitavelmente, deixar de colocar a questão de se saber se o *pharming* representa, de facto, uma modalidade autónoma de fraude eletrónica, ou se se reconduz a um mero aprimoramento e renovação do *phishing*.

Na verdade, no *pharming*, o utilizador não recebe um *e-mail* fraudulento como passo inicial da execução da operação ilícita, nem precisa de acionar um *link* para ser conduzido ao *site* "clonado", uma vez que basta o seu computador estar infetado pelo vírus para que seja diretamente reencaminhado para o *site* falso assim que digita o endereço eletrónico correto. O *pharming* representa, portanto, a nova geração de ataque via *phishing*, apenas sem o recurso à assim denominada "isca" (o *e-mail* com a mensagem enganosa).[65]

O nosso ordenamento jurídico-penal prevê e pune o crime de burla informática e nas comunicações (art. 221.º do Código Penal).

No entanto, a doutrina salienta o difícil enquadramento do *phishing* num determinado tipo legal de crime, atendendo às múltiplas formas de execução do crime, uma vez que este constitui, simultaneamente, um meio de obtenção de dados pessoais e uma conduta em si subsumível à usurpação da ciberidentidade.[66]

## Capítulo III - Repartição das perdas decorrentes das operações de pagamento fraudulentas

1. Distribuição do ónus da prova e do risco contratual

Toda a complexidade e sofisticação inerentes ao serviço de *homebanking* (criado e controlado pela entidade bancária), bem como a crescente necessidade de mecanismos rigorosos de segurança das operações bancárias através daquele serviço realizadas, sem esquecer o facto de estarmos perante uma relação contratual [complexa], justificam o funcionamento da presunção de culpa prevista pelo n.º 1 do artigo 799º do CC.[67] Este

[65] Silva, Flávio Manuel Carneiro – A usurpação… p. 30.

[66] Ibidem, p. 31.

[67] Ac. TRG de 23-10-2012 (Filipe Caroço) in www.dgsi.com;

normativo legal determina o seguinte: "incumbe ao devedor provar que a falta de cumprimento ou o cumprimento defeituoso da obrigação não procede de culpa sua". Tal significa que é ao banco que incumbe o ónus de provar que o acesso por parte de terceiros à conta do seu cliente não se ficou a dever a qualquer fragilidade do sistema de segurança por si implementado.

Parece-nos de fácil asserção que sobre a entidade bancária recaiam os prejuízos decorrentes das vulnerabilidades do seu sistema, dado que é a esta que compete assegurar a regularidade do seu funcionamento e o controlo dos meios técnicos utilizados.[68] Assim sendo, é a entidade bancária que corre o risco de uma intromissão fraudulenta nas contas bancárias dos seus clientes realizada através desse sistema, ou seja, em última análise, é esta que deve arcar com os prejuízos potenciados pela debilidade dos sistemas de pagamento que comercializa.[69] Este entendimento reconduz-se ao teor legal disposto no artigo 798º do CC que determina que "o devedor que falta culposamente ao cumprimento da obrigação torna-se responsável pelo prejuízo que causa ao credor".

Para ilidir a presunção do n.º 1 do artigo 799º do CC, a entidade bancária terá de provar que não teve culpa no sucedido, demonstrando, para o efeito, que não descurou o seu dever de prestar um serviço eficaz e seguro[70], mas que, por sua vez, foi o utilizador do sistema que atuou de forma fraudulenta. Caso não lhe seja possível afastar a presunção, o banco deve suportar os prejuízos derivados do acesso fraudulento à conta bancária do seu cliente. De facto, em linhas gerais, como as que acabamos de traçar, tem sido este o entendimento predominante na nossa jurisprudência.

Certo é que a distribuição do risco contratual dependerá necessariamente do grau de censurabilidade inerente às condutas das partes, – cliente e entidade bancária - ou seja, quanto mais reprovável for o comportamento de uma das partes, maior é a probabilidade de ser essa mesma parte a suportar o risco da operação não autorizada.[71]

Barreira, Maria Carolina dos Santos Gomes Ferreira – Home Banking…p. 41;

[68] Guimarães, Maria Raquel – As transferências... p. 230-231.

[69] Guimarães, Maria Raquel – A Repartição… p. 65.

[70] Barreira, Carolina França – *Home banking…* p. 41.

[71] Guimarães, Maria Raquel – A Repartição... p. 69.

Tendo em conta que estamos na esfera contratual, a distribuição do risco entre as partes torna-se crucial para posteriormente apurar qual das partes será responsável por suportar os prejuízos resultantes das operações não autorizadas.

Atualmente, a questão da distribuição do risco por operações de pagamento não autorizadas encontra-se regulada no artº 72º do RSP, onde se prevê a limitação da responsabilidade patrimonial do utilizador do serviço de banca eletrónica ao valor de € 150,00 nos casos em que a apropriação abusiva do instrumento de pagamento não foi potenciada por culpa da sua parte.[72] O desrespeito por estas normas limitadoras de responsabilidade é sancionado com a aplicação de coimas consideráveis, consubstanciando uma infração especialmente grave.[73]

Sendo o risco o perigo de um prejuízo que alguém suporta como titular de uma posição jurídica, pode dizer-se que o *risco de prestação* é inerente à posição do devedor, (banco), ou seja quando a falha, no plano obrigacional, se deteta na prestação em si. Por sua vez o *risco de cooperação*, assim como *risco de utilização* são inerentes à posição do credor (do cliente), isto é, quando o plano se fruste por contingências relacionadas com o uso/finalidade da prestação pelo credor.[74]

Desta forma, na distribuição do risco contratual pelas partes há que distinguir dois tipos de contingências perturbadoras do programa obrigacional: a contingência que afeta a prestação ou o objeto desta que é um risco suportado pelo devedor, e a contingência atinente à utilização da prestação ou à participação/colaboração do credor na efetivação da prestação estará mesmo relacionada a um obstáculo à utilização da prestação procedente da esfera do mesmo credor.[75]

Quanto à questão da distribuição do ónus da prova, o RSP estabelece, igualmente, uma posição muito clara e vincada, patente no seu artigo 70º.

---

[72] Guimarães, Maria Raquel – The debit and credit card frame work contract and its influence on European legislative initiatives. InDret Comparado, Revista para el Analisis del derecho. N.º 2 (2012), p. 2 in http://www.indret.com/es, p. 13-16;

[73] Cfr. alínea q) do artigo 95º do RSP;

A competência para o processamento destas contraordenações e aplicação das respetivas sanções pertence ao Banco de Portugal, de acordo com o artigo n.º1 do art. 213.º do RGICSF *ex vi* do artigo 99º do RSP;

[74] Machado, João Baptista – Risco contratual e a mora do credor in Obra Dispersa, p.274-275;

[75] Ibidem.

O n.º 1 do artigo 70º estipula que *"caso um utilizador (...) negue ter autorizado uma operação de pagamento executada (...) incumbe ao respetivo prestador de serviço de pagamento fornecer prova de que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência."* Deste preceito retira-se que compete à entidade bancária provar que a operação de pagamento foi autenticada, ou seja, provar que o instrumento de pagamento e os respetivos códigos pessoais de segurança foram, de facto, utilizados. Acrescenta o nº 2 do mesmo artigo que: "*(...) a utilização do instrumento de pagamento registada pelo prestador de serviços de pagamento, por si só, não é necessariamente suficiente para provar que a operação de pagamento foi autorizada pelo ordenante, que este último agiu de forma fraudulenta ou que não cumpriu, deliberadamente ou por negligência grave, uma ou mais das suas obrigações decorrentes do artigo 67.º*" ou seja, uma vez feita a prova da autenticação da operação de pagamento, cabe ainda ao banco provar a culpa do seu cliente bem como o seu grau de contribuição para os prejuízos apurados.[76]

Esta norma encontra justificação no simples facto de o utilizador não poder ser colocado numa posição tão ingrata como a da necessidade de produzir prova sobre o funcionamento de um sistema informático complexo do banco, que não domina.[77]

A autorização no *homebanking*, geralmente, é concedida através da introdução de uma série de códigos pessoais e intransmissíveis no teclado de um computador. Assim, o conhecimento desse conjunto de códigos secretos é a fórmula utilizada para se observarem os objetivos de identificação e de consequente imputação das operações em causa ao mesmo utilizador. O fornecimento destes códigos visa cumprir uma função de "autenticação", nos da alínea t) do art 2º do RSP.[78]

A função de autenticação cumprida por estes dispositivos de segurança personalizados leva a que lei obrigue o utilizador respetivo a "tomar todas as medidas razoáveis, em especial ao receber um instrumento de pagamento, para preservar a eficácia dos seus dispositivos de segurança personalizados".[79]

---

[76] Guimarães, Maria Raquel – A Repartição… p. 60.

[77] Ac. TRL de 5-11-2013 (Manuel Marques) in www.dgsi.com;

[78] Guimarães, Maria Raquel – A Repartição… p. 61.

[79] Cfr. artº 67 nº 2 do RSP.

Contudo não podemos ignorar os casos em que este acesso é feito por terceiros, distintos do titular do instrumento de pagamento, que conseguiram obter esses dados através de fraudes informáticas, daí o legislador não admitir que seja prova bastante a autenticação da operação de pagamento, sendo igualmente exigível que prove a conduta negligente e/ou dolosa do utilizador do sistema (artº 70º nº 2).

Verificamos, assim, no que concerne ao ónus da prova que, compete à entidade bancária provar, no caso concreto, qual a quota-parte de culpa do seu cliente na operação de pagamento não autorizada e o grau de diligência com que atuou, garantindo-se, desta forma, a proteção do utilizador do sistema de pagamento, ou seja, a proteção do consumidor.[80] Para além disso, compete ao banco a prova da existência de um comportamento gravemente negligente/doloso ou que revele um incumprimento deliberado de deveres por parte do utilizador, sob pena de não poder exonerar-se do dever de suportar os prejuízos ocorridos.

O banco insurge-se, alegando que tal encargo lhe é demasiado penoso por não se encontrar diretamente relacionado com factos internos, mas sim com factos fora da sua esfera de domínio, tornando-se muito difícil no caso de prova de negligência grave, onde se exige uma distinção em relação às situações em que não houve uma conduta censurável do utilizador na quebra da confidencialidade dos dispositivos de segurança personalizados (n.º 1 do artigo 72º, in fine).[81]

Aqui chegados, importa reter, essencialmente, que, relativamente ao ónus da prova, é ao banco que cabe demonstrar o grau de culpa subjacente ao comportamento do seu cliente e a sua contribuição para as perdas resultantes das operações fraudulentas.

Recomendação da Comissão 97/489/CE, de 30/7/1997, relativa às transações realizadas através de um instrumento de pagamento eletrónico.

[80] Cfr. artº 70º do RSP;

[81] Barreira, Carolina França – *Home banking*… p. 49;

Faria José Manuel – Acesso a contas bancárias por terceiros no âmbito de operações de pagamento. Revista da Banca. Lisboa: Associação Portuguesa de Bancos. N.º 71 (janeiro/junho 2011), p. 34.

### 1.1. Cláusulas contratuais gerais

Não obstante o regime do ónus da prova estar devidamente disciplinado no RSP (artigo 70º nºs 1 e 2, do RSP), as entidades bancárias têm procurado inserir nos contratos de *homebanking* cláusulas contratuais gerais com vista à alteração dos critérios de repartição do ónus da prova, cuja validade é duvidosa.

Estas cláusulas fazem recair o risco do mau funcionamento dos terminais eletrónicos sobre o utilizador, ou seja, fazem recair sobre o cliente uma presunção de culpa caso sejam realizadas operações de pagamento, via banca eletrónica, por terceiros, mediante autenticação no sistema através da inserção dos códigos de acesso pessoais e intransmissíveis que lhe foram conferidos pela entidade bancária. A sua validade permitiria à entidade bancária a dispensa do ónus da prova em relação operações não autorizadas realizadas através do serviço de *homebanking*, por estas não resultarem do incumprimento da sua obrigação de prestar um serviço seguro.[82]

Esta situação acarretaria uma prova em sentido contrário por parte do utilizador do sistema praticamente impossível de realizar e isto porque, não é de todo equitativo uma solução que coloque o utilizador, que já se encontra de *per si* em desvantagem desde o início da relação contratual, na posição e/ou necessidade de produzir prova perante o mau funcionamento de um sofisticado sistema informático da entidade bancária sobre o qual não tem qualquer controlo. A este propósito, refere o TRL, no Acórdão de 24-05-2012, que o cliente "não tem qualquer controlo sobre os sofisticados meios informáticos da entidade bancária, nem dispõe da assessoria técnica de primeira água com que os departamentos respetivos daquela se apetrecham". [83]

Fazer recair esta presunção de culpa sobre o utilizador do serviço de banca eletrónica equivale a fazer versar sobre este os prejuízos decorrentes de operações fraudulentas dada a dificuldade em afastar a presunção, colocando em causa a aplicação prática do disposto no n.º 1 do artigo 72º do RSP.[84]

---

[82] Ac. TRL de 28/06/2013 (Anabela Calafate) in www.dgsi.com.

[83] Ac. TRL de 24/05/2012 (Ezagüi Martins): "(…) uma prova em contrario [seria] absolutamente diabólica e na prática inalcançável pelo aderente", in www.dgsi.com.

[84] Guimarães, Maria Raquel – A Repartição… p. 60.

Por essa razão, os tribunais superiores têm entendido pela nulidade destas cláusulas contratuais gerais que estabelecem uma presunção de culpa sobre o utilizador no caso de ocorrerem operações não autorizadas mediante autenticação no sistema.[85] O banco pretende, com as referidas cláusulas, modificar os critérios de distribuição do ónus da prova (alínea g) do artigo 21º do DL n.º 446/85, de 25 de outubro – Regime Jurídico das Cláusulas Contratuais Gerais (RJCCG) que decorrem do artigo 70º do RSP e do n.º 1 do artigo 799º do CC.

Todavia estas cláusulas são absolutamente proibidas e sancionadas com nulidade (artigos 12º e 24º do RJCCG) quando inserida no âmbito de relações do banco com consumidores finais (artigo 20º do RJCCG).

Ainda que não estivéssemos perante cláusulas contratuais gerais, a referida cláusula seria tida como nula uma vez que esta, ao inverter o ónus da prova, estaria a agravar seriamente a dificuldade probatória para a parte que a convenção onera (n.º 1 do artigo 345º do CC).[86]

### 1.2. Análise à luz do Acórdão do Supremo Tribunal de Justiça de 18/12/2013

Uma das decisões jurisprudenciais que nos pode auxiliar na melhor compreensão, sentido e alcance desta temática é a vertida no Acórdão do Supremo Tribunal de Justiça (STJ), de 18/12/2013, que incide, precisamente, sobre a *mobilização da teoria da distribuição dinâmica do ónus da prova*[87] para os quadros do *homebanking*, motivada, justamente pela perspetiva da diminuição do ónus probatório a cargo do consumidor e correspetivo aumento do ónus da prova da entidade bancária (prestador do serviço de *homebanking*).

---

[85] Ac. TRL de 24/05/2012 (Ezagüi Martins); Ac. TRL de 28/06/2013 (Anabela Calafate); Ac. TRL de 12/12/2013 (Tomé Ramião), todos in www.dgsi.com.

[86] Barreira, Carolina França – *Home banking…*, p.52;

Tal nulidade decorre igualmente da aplicação do artigo 101º do RSP;

[87] W. Peyrano, Jorge - La prueba difícil in Civil Procedure Review, Vol.2, n.º 1, January/April, 2011, (2011), p. 86-96. Santos, Hugo Luz - Plaidoyer por uma "distribuição dinâmica do ónus da prova" e pela "teoria das esferas de risco" in O Direito, Ano 145.º (2013), Volume III, Director: Jorge Miranda, Almedina,Coimbra, (2014), p. 717

Este aumento do ónus da prova a cargo da entidade bancária justifica-se atenta a implícita assimetria informativa que separa um consumidor de uma entidade bancária.

O referido acórdão preceitua uma clara diminuição do ónus da prova a cargo do consumidor e, inerentemente, um correspetivo e simétrico aumento do ónus probatório que impende sobre a entidade bancária e predisponente do serviço de *homebanking*.[88]

A questão aqui discutida, tal como refere o STJ, é a " *(...) de saber se sobre o Réu/Recorrente impende a responsabilidade pela transferência fraudulenta dos fundos da conta da Autora*".

Na tese do banco: "inexistiu qualquer quebra de segurança, na criação, manutenção e execução de operações no *site* do Banco, tendo verificado antes uma quebra de segurança por parte da Recorrida no acesso ao referido site, o que, de forma casual, determinou que um terceiro se tenha apropriado das credenciais da mesma recorrida para realização de operações, via *homebanking*, não podendo o Recorrente ser responsabilizado, por qualquer intromissão fraudulenta no computador do cliente".

Por sua vez, de acordo com a versão da Autora, esta, ao aceder à página que pensava ser do réu para efetuar as suas operações, disponibilizou as coordenadas aí solicitadas, sem se dar conta que estava afinal numa página "clonada" (o designado *pharming* caraterizado no capítulo II).[89]

O STJ entendeu que da factualidade apurada pelas instâncias não resulta que tenha havido por parte da Autora qualquer comportamento indiciador de quebra de segurança no acesso à página do banco e que, por sua vez, tivesse proporcionado a um terceiro as coordenadas para a realização das operações bancárias via *homebanking*.[90]

Neste sentido o Tribunal conclui que os riscos da falha do sistema informático utilizado, bem como dos ataques cibernautas ao mesmo, têm de correr por conta do Réu, por a tal conduzir o disposto no artigo 796º, nº 1 do CC, não se tendo provado, como não se provou, que tivesse havido culpa da Autora.

---

[88] Ibidem.

[89] Ao contrário do *phishing*, o *pharmin*g não se faz valer de uma mensagem de correio eletrónico como isco para "sacar" os códigos pessoais do utilizador, consistindo antes num plágio integral da página do banco que surge no computador do utilizador assim que este digita o correto endereço eletrónico do seu banco através da instalação de um vírus.

[90] Santos, Hugo Luz – Plaidoyer…p. 717.

De acordo com o artigo 68º nº 1 alínea a) do Anexo I do RSP *"O prestador de serviços de pagamento que emite um instrumento de pagamento tem as seguintes obrigações: a) Assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento, sem prejuízo das obrigações do utilizador do serviço de pagamento estabelecidas no antigo anterior "*. Daqui depreende-se, acompanhando o entendimento do STJ, que os riscos pela utilização normal do sistema correm por conta do prestador de serviços.

O mesmo regime, como já analisámos, faz impender ónus da prova sobre a entidade bancária (artigo 70º nºs 1 e 2, do RSP).

Tal entendimento não prejudica e/ou diminui o facto de, sobre o cliente, enquanto utilizador daqueles meios, recair a especial obrigação de os utilizar de acordo com as condições que regem a sua emissão e utilização, e nos termos do artigo 67º nº 1 alínea a), do RSP, não devendo o Tribunal desconsiderar a avaliação da diligência do utilizador.

Desta forma, o STJ deu como assente que a Autora não violou nenhuma das suas obrigações contratuais por não ter sido a mesma a autorizar a ordem de pagamento.

Assim, na ótica do STJ, *a responsabilidade pelo reembolso das quantias objeto de transferências não autorizadas, posto que se não venha a apurar que o ordenante tenha tido qualquer culpa na sua efetivação*, impende sobre o prestador de serviços, por força do artigo 72º nº 1 do RSP (responsabilidade essa que, provinha já da responsabilidade contratual geral, por via do disposto no artigo 796º nº 1 do CC).

Acresce que, se no âmbito do direito material - Direito bancário- assiste um especial dever de proteção do consumidor e, sendo o direito processual civil instrumental em relação ao direito material, não será de todo coerente uma solução que coloque o consumidor, no plano processual, na posição e/ou necessidade de produzir prova, pois tal encadeamento conduziria a uma manifesta desconsideração de um primordial objetivo legalmente estabelecido em sede de direito material (especial dever de proteção do consumidor).[91]

[91] Santos, Hugo Luz – Plaidoyer… p. 737;
Oliveira, Madalena Perestrelo de - "A "inexigibilidade" na relação contratual: interpretação do contrato e heteronomia", in O Direito, Ano 145.º (2013), Volume III, Director: Jorge Miranda, Almedina, Coimbra, (2014), p. 539.

É, assim, compreensível que nos casos de manifesta dificuldade na prova de determinados factos, compreende-se a razão pela qual a doutrina advogue a inversão do ónus da prova (artigo 344º nºs 1 e 2 do CC) ou, pelo menos, uma redistribuição mais equilibrada do ónus da prova[92] e, no âmbito desta, a mobilização da teoria da distribuição dinâmica do ónus da prova.[93]

De acordo com a teoria da distribuição da dinâmica do ónus da prova, *cujo precursor, no seu desenho atual, foi o processualista Jorge W. Peyrano, o ónus probatório deveria ser distribuído não por causa da função que os factos desempenham no processo, mas, antes, em função do conceito de prova mais fácil, atribuindo-o, especificamente, à parte que está casuisticamente em posição mais favorável de o demonstrar.*[94]

Deste forma, "se estimula a efetiva produção de prova e a procura da verdade material, onerando a parte com maior facilidade probatória, bem como se promove a igualdade material entre as partes, dando a ambos maior igualdade na possibilidade de fazerem valer a posição em juízo. Isto porque a parte com maior facilidade probatória pode efetivamente demonstrar a versão do facto que lhe aproveita e a parte contraria, apesar de ter menor facilidade em provar, pode sempre beneficiar de uma decisão de ónus da prova, caso a outra parte não consiga realizar a prova*".*[95]

No caso concreto relatado pelo referido Acórdão, a teoria da distribuição da dinâmica do ónus da prova seria aplicada, na perspetiva da inadmissibilidade de ónus da prova a cargo do consumidor quanto ao mau funcionamento do sistema informático de *homebanking*, pois é o prestador de serviços de *homebanking* quem tem maior facilidade em demonstrar a versão fatual que lhe aproveita, ou seja, a de que a utilização fraudulenta do serviço de *homebanking* por parte de terceiros não se deveu ao mau funcionamento do

[92]Fernandez, Elizabeth -Desvio de poder: mito ou realidade? in Cadernos de Justiça Administrativa p. 25.

[93] Santos, Hugo Luz – Plaidoyer… p. 740;

Teixeira, Micael, Por uma distribuição dinâmica do ónus da prova, Dissertação de Mestrado –

Faculdade de Direito da Universidade Nova de Lisboa, Lisboa, (2012), p. 49 e ss.

[94] W. Peyrano, Jorge – op. cit. 86-96.

[95] Carvalho, Jorge Morais/Teixeira, Micael - Crédito ao consumo-ónus da prova da entrega de exemplar do contrato e abuso do direito de invocar a nulidade, in Cadernos de Direito Privado, n.º 42, Abril/Junho 2013, cejur, Coimbra Editora, (2013), Coimbra, p. 47

sistema informático, como bem decidiu, aliás, ainda que com fundamentação diferente, o STJ.[96]

## Capítulo IV - A responsabilidade do banco por operações de pagamento não autorizadas

A regulação da responsabilidade civil dos prestadores de serviços deve ter em conta interesses distintos. Por um lado, os interesses dos próprios prestadores de serviços (a industria das telecomunicações, por exemplo) e, por outro, os interesses dos consumidores, que podem ser gravemente lesados pela difusão de conteúdos ilícitos na Internet.[97]

A atribuição de responsabilidades ao banco pelas perdas resultantes das operações de pagamento irregulares dependerá do juízo de censurabilidade do comportamento do cliente.[98]

A responsabilidade do banco pelas operações de pagamento não autorizadas deve ser analisada em duas fases distintas que ora adiante nos vamos debruçar.

### 1. A responsabilidade do banco por operações de pagamento não autorizadas antes da comunicação do cliente

O nº 1 do artigo 72º do RSP, no âmbito da repartição dos prejuízos pelas partes no contrato de *homebanking*, no caso das operações não autorizadas levadas a cabo antes da comunicação do cliente ao prestador de serviços, imputa ao utilizador do instrumento de pagamento o valor de € 150,00,[99] sempre que ocorra uma "apropriação abusiva com quebra de confidencialidade dos dispositivos de segurança personalizados imputável ao ordenante", mas também em caso de perda ou roubo de um cartão.[100]

[96] Santos, Hugo Luz – Plaidoyer…p. 741.

[97] Alves, Hugo Ramos – Da responsabilidade dos prestadores de serviços em rede in O Direito 145 (2013), III, 553-640, p. 558.

[98] Guimarães, Maria Raquel – A repartição… p. 66;

[99] Cfr. artº 72º nº 1 do RSP;

[100] Guimarães, Maria Raquel – (Ainda) a responsabilidade… p. 129;

Desta forma, sempre que se confirmem operações de pagamento desconformes e que não sejam imputáveis ao utilizador do instrumento de pagamento a título de negligência grave/grosseira ou dolo, o cliente vê a sua responsabilidade limitada até ao valor máximo de 150 euros.[101] Esta limitação de responsabilidade apenas se aplica nos casos de negligência leve do consumidor, ou seja, quando se verifique uma quebra de confidencialidade dos códigos de segurança não intencional ou uma atuação gravemente negligente por parte cliente. Com efeito, corre por conta do banco a responsabilidade quanto ao remanescente das perdas resultantes das operações de pagamento não autorizadas.[102]

Deste modo, nas situações em que não se apura tal falha, tendo sido o cliente diligente no cumprimento das suas obrigações de guarda e notificação, não deve suportar qualquer prejuízo decorrente da operação fraudulenta.[103]

Porém, o presente Regime não densifica o conceito da designada "negligência leve", sendo complexo, por um lado e, arbitrário por outro, determinar os casos em que o cliente atuou com mera culpa.

Assim, o utilizador é responsável por um montante limitado dos prejuízos decorrentes de operações não autorizadas, salvo em caso de incumprimento deliberado ou de atuação fraudulenta ou se verifique negligência grave da sua parte.[104] Esta limitação visa incentivar a comunicação sem atraso injustificado da operação não autorizada, prevista na al. b) do nº 1 do artº 67 do RSP.

Solução distinta da prevista para os casos de negligência leve ou de inexistência de negligência, é aquela pensada para as operações de pagamento não autorizadas que resultam de negligência grave ou atuação dolosa do titular do instrumento de pagamento.[105] Naturalmente que, neste tipo de casos, suporta o cliente "as perdas resultantes de operações de pagamento não autorizadas até ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, ainda que

[101] Com isto pretende-se incentivar a comunicação ao banco sem atrasos injustificados da ocorrência da operação de pagamento não autorizada. – Cfr. considerando 32 da DSP.

[102] Barreira, Maria Carolina dos Santos Gomes Ferreira – Home Banking… p. 62.

[103] Vide ac. do TRL de 5-11-2013.

[104] Guimarães, Maria Raquel – (Ainda) a responsabilidade… p. 132.

É o que resultas do disposto no nº 4 do artº 72 do RSP.

[105] Barreira, Maria Carolina dos Santos Gomes Ferreira – Home Banking… p. 64

superiores a € 150, dependendo da natureza dos dispositivos de segurança personalizados do instrumento de pagamento e das circunstâncias da sua perda, roubo ou apropriação abusiva" (n.º 3 do artigo 72º).

É, pois, necessário prever duas soluções diferentes para dois padrões de conduta claramente distinguíveis (os casos em que o utilizador do serviço de *homebanking* não teve uma conduta censurável e os casos em que este atuou de forma fraudulenta ou em claro incumprimento das obrigações que decorrem do contrato).

Nas palavras de Menezes Cordeiro, a negligência consiste na "violação (objetiva) de uma norma por inobservância dos deveres de cuidado".[106]

Em vista a aplicação prática do disposto no RSP, importa distinguir as duas modalidades de negligência: a negligência consciente e a negligência inconsciente. No primeiro caso o agente representa o resultado juridicamente desvalioso como uma consequência possível da sua conduta, ou seja, o autor prevê como possível a ocorrência daquele desfecho (ilícito), mas ainda assim, ou por leviandade ou desleixo, não toma as precauções necessárias para a sua não verificação. Já no segundo caso, o agente nem sequer representa o resultado juridicamente desvalioso como uma consequência possível da sua conduta, ainda que pudesse e devesse tê-lo previsto, isto é, o autor não chega a prever a possibilidade da verificação desse desfecho ilícito, porém deveria tê-lo feito se atuasse nos termos da diligência exigida.[107]

Estabelecendo a conexão entre estes dois graus de negligência (consciente e inconsciente) com as expressões utilizadas pelo RSP – negligência grave e negligência leve – a negligência consciente corresponde à designada negligência grave e por conseguinte, a negligência inconsciente corresponde à assinalada negligência leve. A primeira modalidade é a que está mais próxima do dolo, encontrando-se paredes-meias com o dolo eventual.[108]

Embora o nosso código não estabeleça essa diferenciação, é pertinente considerar neste âmbito os chamados três graus de mera culpa, isto é, a culpa grave, a culpa leve e a

[106] Cordeiro, António Menezes – Tratado de direito civil, Tomo VIII. Almedina 2014, p. 472.

[107] Oliveira, Nuno Manuel Pinto Oliveira – Princípios de Direito dos Contratos. Coimbra editora, p. 434 e 435.

[108] Telles, Incêncio Galvão – direito das obrigações 6ª Edição – Revista e Atualizada, Coimbra editora, p. 344

culpa levíssima.[109] De acordo com Manuel de Andrade a "culpa grave lata é a negligência grosseira, escandalosa, intolerável (…) aquela em que só cai um homem extraordinariamente desleixado; Culpa leve é a negligência em que não incorreria um *bonus pater famílias*; Culpa levíssima é a negligencia em que só não incorreria um homem excecionalmente zeloso (um *diligentissimus pater famílias*)…". [110]

A valoração da culpa pode ser feita segundo o modelo concreto (tendo em consideração a conduta usual do agente), ou de acordo com um modelo abstrato (analisada à luz do critério de um bom pai de família), de conteúdo ético e não estatístico que não despreze as circunstâncias concretas do caso.[111]

O nosso Código Civil no artº 487º, nº 2, do CC (aplicável à responsabilidade contratual ex vi artº 799º, nº 2), acolhe como critério da culpa o cuidado ou a diligência de um homem médio ou de um homem normal – o cuidado ou diligência de um bom pai de família, é não só um padrão de um homem cuidadoso e zeloso (perspetiva da culpa como deficiência da vontade), mas também competente, informado, bem preparado e apto (perspetiva da culpa como conduta deficiente).[112] Ou seja, o padrão valorativo para o juízo de censura é aquilo que ética e/ou deontologicamente é exigível ao homem médio, ao homem que não se basta com a diligência comum ou habitual mas que emprega o cuidado eticamente reclamado.[113]

Atendendo à dificuldade em fazer corresponder os mais variados comportamentos do utilizador às situações de negligência grave (consciente) ou de negligência leve (inconsciente), parece permitir-se ao juiz um amplo poder discricionário na tomada de decisão. Compete-lhe, tendo em conta as circunstâncias de cada caso, decidir se determinado comportamento se consubstancia negligência grave ou negligência leve. Esta falta de densificação dos dois conceitos atendendo aos casos em concreto de fraude informática, pode conduzir a diferentes interpretações deixando o processo de decisão vulnerável a decisões arbitrárias baseadas na fluidez dos conceitos.[114]

---

[109] Proença, José Carlos Brandão – Direito das Obrigações – Relatório sobre o programa, o conteúdo e os métodos de ensino da disciplina, Publicações universidade Católica (2007), p. 186.

[110] Ibidem.

[111] Proença, José Carlos Brandão – Direito das Obrigações… p. 186.

[112] Ibidem, p. 187.

[113] Faria, Jorge Leite Areias Ribeiro de – Direito das Obrigações Vol. I, Almedina. Coimbra.

[114] Barreira, Maria Carolina dos Santos Gomes Ferreira – Home Banking… p. 64

Como vimos supra, no âmbito da distribuição do ónus da prova, o artº 70º do RSP atribui ao banco o ónus da prova de que a operação de pagamento alegadamente não autorizada foi corretamente autenticada e que o seu cliente agiu de forma negligente ou fraudulenta ou em claro incumprimento das obrigações decorrentes do artº 67º do RSP. Estas normas de repartição do ónus da prova são muito penalizadoras para a entidade bancária, pois exigem uma prova muito complexa e rigorosa.[115]

O mesmo resultado decorre da aplicação do n.º 1 do artº 799º do CC que faz recair sobre o devedor (banco) a prova de que a falta de cumprimento da obrigação não procede de culpa sua.

Analisando a jurisprudência dos nossos tribunais superiores, verifica-se que a prova da existência ou não de negligência por parte do cliente tem um papel decisivo no desfecho dos casos de fraude informática no *homebanking*.

Um caso que merece aqui particular destaque é aquele em que o cliente, perante solicitação feita numa página similar a do banco (*pharming*), fornece todos os algarismos do seu cartão matriz. A questão a que se impõe dar resposta é a de saber se podemos considerar este comportamento do cliente como censurável à luz dos critérios mínimos de diligência ou não.

Um Acórdão que decidiu em sentido oposto à grande maioria das decisões jurisprudenciais neste contexto, foi o da TRG (Acórdão de 25-11-2013), que considerou a conduta do utilizador do serviço de *homebanking* como gravemente negligente. Com efeito, a entrega de todos os dados do cartão matriz *contraria toda a lógica do sistema de segurança que não lhe pode ser desconhecida*, não sendo de todo coerente aceitar que o banco solicitasse a totalidade dos dígitos do cartão matriz, uma vez que o banco deve ter na sua posse uma cópia do mesmo para poder confirmar e validar os movimentos da conta bancária do seu cliente. O TRG considerou, assim, que um aderente ao serviço de *homebanking*, minimamente cuidadoso e informado devia ter uma noção geral do procedimento habitual no recurso a este serviço, sendo, portanto, de desconfiar qualquer solicitação anómala e contrária à lógica de um sistema que lhe foi previamente explicado. É, pois, necessariamente exigível ao cliente que, perante tal incongruência, contactasse o banco a fim de clarificar tal situação antes de assumir qualquer operação.[116] Este acórdão

[115] Ibidem, p. 65

[116] Cfr. Ac. do TRG de 25-11-2013.

concluiu que o cliente foi negligente ao violar as regras de segurança impostas pelo contrato, permitindo a intromissão de terceiros na sua conta bancária.

Também o TRL, no Acórdão de 12-12-2013, num caso idêntico, considerou o comportamento do utilizador do serviço de banca eletrónica gravemente negligente, pois não desconfiou nem tão pouco estranhou a solicitação da atualização da matriz, pedido esse nunca dantes feito e que implicava a revelação de uma quantidade enorme de números do cartão matriz que como sabia (ou deveria saber) essa era a única garantia de segurança de que as operações eram por si e não por terceiro realizadas.[117]

Contudo, a esmagadora maioria das decisões dos tribunais superiores tem concluído pela condenação do banco e respetivo reembolso ao cliente da totalidade dos prejuízos. Com base na ausência de prova da existência de um comportamento especialmente censurável por parte do cliente, o banco foi condenado a suportar a totalidade das perdas porque não conseguiu provar que houve um comportamento do cliente revelador de menor cuidado relativamente aos seus deveres de preservação da eficácia e confidencialidade das palavras-passe. E, assim sendo, o banco está inibido de imputar a quebra da confidencialidade dos dispositivos de segurança ao seu cliente.

Uma decisão que exemplifica este entendimento é a do Tribunal da Relação do Porto (TRP), no Acórdão de 29-04-2014. Considerou que o facto de o cliente ter divulgado os dispositivos de segurança não permite que lhe seja imputado um comportamento gravemente negligente porque a intromissão de terceiros não se deveu a qualquer violação grave dos deveres de sigilo quanto aos códigos de acesso que o cliente estava obrigado a observar.[118] Afirma o TRP que, compete ao banco prestar um serviço eficaz e seguro e assegurar que os códigos de acesso só estejam ao alcance do utilizador do serviço de pagamento que tem direito a utilizá-lo (alínea a) do n.º 1 do artigo 68º do RSP).[119] Alguma jurisprudência defende que, nestes casos, se verifica uma contribuição do banco para o sucedido uma vez que, o sucesso dessa operação fraudulenta, se deve, em parte, à entidade bancária que não desenvolveu todas as ações que se impunham em

[117] Cfr. Ac. TRL de 12-12-2013.

[118] Cfr. Ac. TRP de 29-04-2014.

[119] Ibidem.

ordem a garantir a segurança do sistema informático que permite o acesso à conta bancária do seu cliente.[120]

Há ainda que ter em conta, que consubstanciando-se o *pharming* numa modalidade de fraude eletrónica muito mais complexa e sofisticada do que o *phishing*, o cliente é mais facilmente exonerado de qualquer responsabilidade. Assim sendo, nos casos de *phishing*, revela-se particularmente crucial apurar, no caso concreto, se a conduta do utilizador é censurável, tendo em conta a aparência fidedigna ou não da mensagem de correio eletrónico, bem como a observância do banco pelos deveres de informação e esclarecimento dos clientes.[121]

Porém, consideramos que seria importante procurar uma solução mais equilibrada ou intermedia na responsabilização das partes envolvidas, tendo em conta que, com o decurso do tempo e a consequente vulgarização desta problemática, será mais exigível, por um lado, ao consumidor que adote uma conduta cada vez mais diligente e preventiva uma vez que dispõe de mais informação e, por outro lado ao banco que desenvolva regularmente mecanismos de proteção progressivamente mais sofisticados.

Sendo certo que o juízo de censurabilidade do comportamento do cliente dependerá sempre dos avanços técnicos alcançados no que concerne à segurança do sistema, da maior divulgação dos métodos fraudulentos, mas também da crescente sofisticação dos esquemas utilizados, que "*ciclicamente transformará os esclarecidos de hoje nos ingénuos de amanha*". [122]

Em síntese, a repartição dos prejuízos decorrentes de fraude informática no *homebanking* antes da notificação ao banco rege-se pela ideia da distribuição equitativa dos prejuízos decorrentes da utilização imprópria do instrumento de pagamento, por terceiros. Releva aqui, para auxílio e fundamentação da boa decisão da causa, a avaliação do cumprimento das obrigações contratuais assumidas por ambas as partes, nomeadamente, a comunicação do incidente ao banco pelo utilizador do serviço de

[120] Cfr. Ac. do TRG de 30-05-2013 (Rita Romeiro) in www.dgsi.com;

[121] Guimarães, Maria Raquel – A repartição… p. 63.

[122] Guimarães, Maria Raquel – As operações…p. 33.

pagamentos e a proteção do sistema informático pela entidade bancária, tal como a diligência dos contraentes.[123]

Ao consagrar um critério objetivo de imputação das perdas sofridas baseado na diligência do utilizador do serviço de banca eletrónica e na sua contribuição para os prejuízos, a lei estabelece uma solução justa e promotora de uma maior eficiência e segurança dos sistemas de pagamento.[124]

Nesta sede, o problema fundamental e que, por sua vez, carece de maior disciplina é, precisamente, os termos e critérios específicos em que o Tribunal se deverá basear na identificação e determinação da negligência grave ou leve por parte utilizador, ou mesmo a sua inexistência.

## 2. Responsabilidade pelas perdas resultantes de operações não autorizadas após a comunicação da fraude

Como vimos anteriormente, a distribuição dos prejuízos pelas partes – cliente/utilizador e prestador do serviço – imputa ao utilizador um valor até ao limite máximo de € 150,00, apenas quando estamos perante a verificação de operações de pagamento não autorizadas antes da comunicação do cliente ao prestador de serviços.[125]

No entanto, é necessário tutelar a posição do cliente após a sua comunicação ao banco da operação de pagamento não autorizada.

A comunicação do cliente dando conhecimento ao banco da ocorrência de uma operação de pagamento não autorizada na sua conta bancária assume um papel essencial na repartição dos prejuízos decorrentes de operações fraudulentas.[126]

Esta comunicação está contemplada na alínea b) do n.º 1 do artigo 67º do RSP.

A partir do momento em que o cliente dá conhecimento da ocorrência de uma operação de pagamento para a qual não prestou o seu consentimento, exonera-se de

[123] Ferreira, António Pedro de Azevedo – A relação negocial bancária – conceito e estrutura. Lisboa: Quid Iuris (2015), p. 388.

Guimarães, Maria Raquel – As transferências eletrónicas de fundos de cartões de débito, Almedina (1999) p. 216.

[124] Guimarães, Maria Raquel – A repartição… p. 63.

[125] Guimarães, Maria Raquel – A repartição… p. 66.

[126] Guimarães, Maria Raquel – (Ainda) a responsabilidade… p. 128.

suportar quaisquer prejuízos decorrentes dessa utilização indevida do sistema de pagamento por parte de terceiros. Tal entendimento é o que decorre da aplicação do RSP: "não suporta quaisquer consequências financeiras resultantes da utilização de um instrumento de pagamento perdido, roubado ou abusivamente apropriado, salvo em caso de atuação fraudulenta" (nº 4 do artigo 72º).[127] Passando a recair sobre o banco a obrigação de proteger a conta do seu cliente, por forma a evitar a repetição de tais operações.

Assim, a comunicação levada a cabo pelo cliente das perdas resultantes de operações não autorizadas traduz-se na transferência da responsabilidade do cliente para o banco das operações não autorizadas posteriores a essa comunicação. Na verdade, após a referida comunicação, é indiferente do ponto de vista do cliente, que o banco seja capaz de prevenir ou não a utilização fraudulenta dos instrumentos de pagamento, uma vez que, o cliente está isento de qualquer responsabilidade, cabendo ao banco o ressarcimento de todos os prejuízos apurados. Neste caso, resta ao banco a prova da atuação fraudulenta do utilizador.

Quanto ao prazo estabelecido para proceder à referente comunicação a lei esclarece que o cliente deve proceder à comunicação sem atrasos injustificados ao prestador de serviços logo que tenha conhecimento, da apropriação abusiva do instrumento de pagamento.[128] A presente redação legal ao consagrar um dever de comunicação do cliente "sem atrasos injustificados" pretende dirimir os riscos e consequências das operações de pagamento não autorizadas.[129]

Por essa razão, não se podem consentir cláusulas contratuais que obriguem o cliente a comunicar a situação irregular de "forma imediata" ou dentro de determinado limite de tempo[130], uma vez que é aceitável que um cliente, agindo de boa-fé e sendo

[127] Esta solução contraria o n.º 2 do § 8º do Aviso n.º 11/2001 do Banco de Portugal nos casos que envolvam a utilização de cartões de débito ou de crédito pois, segundo o Aviso, o titular do cartão podia suportar prejuízos ocorridos depois da comunicação ao banco do extravio do cartão, mesmo que não lhe fosse imputável qualquer comportamento negligente, sempre que não estivesse em causa uma utilização eletrónica do cartão.

[128] Cfr. alínea b) do artigo 67 do RSP.

[129] Barreira, Maria Carolina dos Santos Gomes Ferreira – Home Banking… p. 55.

[130] Ibidem p. 54

diligente na sua conduta, não tenha conhecimento das operações não autorizadas durante várias horas ou dias.[131]

No entanto, por razões de segurança e certeza jurídicas, o RSP fixa um prazo que visa tutelar os interesses de ambas as partes,[132] concretizando a expressão "sem atrasos injustificados" ao estipular um prazo máximo de treze meses a contar da data do débito.[133]

Note-se que este prazo de treze meses se conta a partir da data da verificação da operação de pagamento desconforme, e não a partir do momento em que o cliente tenha, ou deveria ter, conhecimento do débito irregular. Considera-se que o cliente tem ou deveria ter conhecimento do débito irregular, por exemplo, aquando da consulta dos movimentos bancários.

Quanto aos termos em que a referida comunicação/notificação deve ser procedida, o RSP não fornece qualquer indicação. Todavia, tendo em conta a urgência de atuação, o cliente deverá optar ou pelo contato telefónico.[134]

O RSP impõe à entidade bancária o dever de garantir a disponibilidade, a todo o momento, de meios adequados que permitam ao cliente proceder à comunicação/notificação nos termos da alínea c) do n.º 1 do artigo 68º). Caso o banco não cumpra este dever, o utilizador do serviço de *homebanking* fica desonerado de suportar quaisquer consequências financeiras, salvo nos casos em que tenha agido de forma fraudulenta (n.º 5 do artigo 72º). Sendo certo que, nos casos em que se verifique este incumprimento, a entidade bancária, para além de violar uma obrigação legal,[135] estaria a atuar de má-fé, em abuso do direito, - *venire contra factum proprium* - ao tentar imputar o risco ao seu cliente.[136] Na constatação destas circunstâncias, a totalidade das perdas advindas das operações fraudulentas, inclusive das que ocorreram antes de o

[131] López Jiménez, José Maria- Comentarios a la ley de servicios de pago (2011), p. 586.

[132] Ibidem.

[133] Com exceção dos casos em que o Banco não tenha cumprido os seus deveres de informação - Cfr. nº 2 do artº 69º do RSP;

[134] Barreira, Maria Carolina dos Santos Gomes Ferreira – Home Banking… p. 55.

[135] Cfr. alínea c) do n.º 1 do art. 68º do RSP. Sendo ainda considerada uma contraordenação especialmente grave prevista na alínea o) do art. 95º do RSP

[136] Gomes, Januário da Costa – op. cit. p. 247.

utilizador do instrumento de pagamento ter tentado proceder à notificação da alínea b) do n.º 1 do artigo 67, será suportada pelo Banco.[137]

Uma vez realizada a comunicação, o banco fica investido na obrigação de proteger a conta bancária do seu cliente, nomeadamente através do respetivo bloqueio, de forma a impedir a ocorrência de novas operações não autorizadas (alínea e) do n.º 1 do artigo 68º. [138] Esta obrigação é compreensível pois o banco figura como parte contratualmente mais forte, isto é, aquela que se encontra em melhores condições de controlar o sistema de pagamentos e evitar novas perdas.[139]

Concluindo, o artigo 69º do RSP dispõe que incumbe ao cliente o ónus de controlar as operações de pagamento da sua conta bancária, verificando se foram autorizadas e executadas corretamente. Mal seja comunicada ao banco a falta de autorização de determinada operação de pagamento dentro dos prazos previstos ("sem atraso injustificado e dentro de um prazo nunca superior a treze meses a contar da data do débito"), passa a ser a entidade bancária que deverá verificar que a referida operação foi autenticada, devidamente registada e contabilizada e que não foi afetada por qualquer avaria técnica (n.º 1 do artigo 70º do RSP), como já vimos supra.

[137] Barreira, Maria Carolina dos Santos Gomes Ferreira – Home Banking…, p. 56.

[138] Guimarães, Maria Raquel – A Repartição… p. 67.

[139] López Jiménez, José Maria- Comentarios… p. 592.

## Conclusão

Ao longo deste trabalho procuramos evidenciar a enorme importância da densificação legal e doutrinal da presente temática.

Importa agora tecer as principais conclusões do presente estudo.

O serviço de *homebanking* é fruto do impacto ascendente e abrupto do fenómeno virtual, quer em termos de difusão e rapidez de informação, quer em termos de variedade de produtos. Neste campo, o grande desafio da entidade bancária consiste na conquista da confiança do cliente na segurança deste tipo de serviço. Estão em causa a qualidade e a seriedade da instituição na distribuição do serviço que oferece.

Pode dizer-se que o *homebanking*, tal como o contrato de abertura de conta, figura num contrato-quadro celebrado mediante a adesão do cliente bancário a um conjunto de cláusulas contratuais gerais predefinidas pela entidade bancária, desencadeando uma relação bancária geral, na qual assentam os diferentes contratos celebrados subsequentemente pelas partes. Neste tipo contratual conseguimos identificar declarações de vontade independentes que permitem sustentar a sua validade enquanto contrato autónomo.

Da celebração do presente contrato decorre um leque de deveres acessórios, na sua maioria relacionados com a segurança e eficácia do sistema de pagamento eletrónico. Na verdade, os inúmeros ataques à segurança das redes (mesmo das mais protegidas), assim como o desenvolvimento de técnicas de *phishing* e *pharming* que poluem o ciberespaço, têm vindo a gerar, junto da clientela, um clima de receio, apreensão e desconfiança relativamente a este sistema de pagamentos. São já algumas as ferramentas que o banco tem vindo a disponibilizar em vista da prevenção deste tipo de ataques, nomeadamente a divulgação, no seu *site*, do aumento dos ataques informáticos e dos cuidados destinados a evitar a sua concretização.

Todavia, como não estamos perante uma realidade estanque, são necessários esforços contínuos no aperfeiçoamento das medidas de segurança do sistema eletrónico com vista a acompanhar a progressiva sofisticação das técnicas informáticas fraudulentas.

Perante a ocorrência de uma dessas operações irregulares, coloca-se a questão do ónus da prova e do inerente risco contratual. Procuramos, nesta sede, esclarecer que é

sobre a entidade bancária que recai o ónus de provar que a operação de pagamento foi corretamente autenticada e que a "invasão informática" ficou a dever-se a negligência grosseira ou incumprimento deliberado por parte do utilizador. É, portanto, sobre a entidade bancária que impende o risco de uma intromissão fraudulenta nas contas bancárias dos seus clientes. Com efeito, é ao banco que naturalmente compete assegurar a regularidade do funcionamento do sistema que comercializa e o controlo dos meios técnicos por si disponibilizados. Este entendimento encontra plena aderência nos vários normativos legais (artº 799º, artº 798 do CC e artº 72º do RSP, regime esse que praticamente serve de base a toda a fundamentação elaborada pelos Tribunais Superiores).

A responsabilização de uma das partes pelos prejuízos causados deve ser analisada em duas fases distintas (antes e após da comunicação ao banco da operação fraudulenta). No capítulo III, assume particular relevância o comportamento do utilizador, demonstrando-se pertinente estabelecer aqui um paralelismo com o capítulo I no que concerne aos deveres que impendem sobre o utilizador do serviço. Importa, pois, ter em conta as obrigações que vinculam o utilizador do sistema, de forma a poder imputar-lhe (ou não) uma atuação ilícita, negligente ou dolosa. De acordo com o RSP e a jurisprudência, apenas dessa forma o banco se poderá exonerar de qualquer responsabilidade.

À medida que o comportamento do utilizador se revelar mais censurável aumenta a probabilidade de ser este a suportar a totalidade das perdas decorrentes de uma operação de pagamento ilícita.

Entendemos, no entanto, que tanto a regulamentação legal como a jurisprudência são parcas no que toca à densificação do conceito de negligência por parte do consumidor. Deste modo, cabe ao juiz formar a sua "livre", embora sempre vinculada, convicção. Desta forma, sentimos a necessidade de desbravar doutrina no âmbito das modalidades da negligência em ordem a estabelecer a correspondência com as expressões utilizadas pelo RSP (negligência leve e negligência grave). Tentámos, igualmente, identificar, na prática, os casos em que se verifica uma conduta totalmente reprovável do consumidor. A esmagadora maioria dos Tribunais tem decidido no sentido da não verificação de uma conduta gravemente negligente do cliente e, por conseguinte, da responsabilização do banco pelos prejuízos apurados. De facto, o cliente não deverá ser prejudicado pelo (mau) funcionamento de um complexo sistema informático que não domina.

Em nossa opinião, este juízo de censura deverá moldar-se à evolução sofrida por estas práticas e pela divulgação da respetiva informação. Isto é, a apreciação da conduta do utilizador, no que respeita à observância das obrigações que sobre si recaem, terá de ser mais rigorosa, tendo em conta que, com o decurso do tempo e a consequente difusão de informação, este deverá estar mais precavido e devidamente informado quanto ao combate aos ataques informáticos. Será, pois, fundamental analisar o tipo de perfil do utilizador (se é um utilizador experiente ou amador), bem como o tipo de fraude em causa e o seu nível de sofisticação. Trata-se de determinar até que ponto é exigível ao utilizador adotar determinado comportamento face à sua experiência no meio informático e ao grau de complexidade da fraude de que foi vitima. Só assim é possível a aplicação de um critério de justiça material e personalizada.

## Bibliografia


Almeida, Carlos Ferreira de – Contratos II, Conteúdo dos contratos de troca, Almedina (2012);

Alves, Hugo Ramos – Da responsabilidade dos prestadores de serviços em rede in O Direito 145 (2013), III, 553-640;

Antunes, José Engrácia – Direito dos contratos comerciais. Coimbra Almedina (2009);

Barreira, Maria Carolina dos Santos Gomes Ferreira – Home Banking A repartição dos prejuízos decorrentes da fraude informática – Dissertação de mestrado (2015);

Carvalho, Jorge Morais/Teixeira, Micael - Crédito ao consumo-ónus da prova da entrega de exemplar do contrato e abuso do direito de invocar a nulidade, in Cadernos de Direito Privado, n.º 42, Abril/Junho 2013, cejur, Coimbra Editora, (2013);

Cordeiro, António Menezes – Os Contratos Bancários. Separata – Estudos em homenagem ao professor doutor Carlos Ferreira de Almeida. Almedina (2011);

Cordeiro, António Menezes – Tratado de direito civil, Tomo VIII. Almedina (2014);

Cordeiro, António Menezes (2010) – Manual de Direito Bancário, 4ª Edição, Almedina;

Costa, Mário Júlio De Almeida – Direito das obrigações, 12ª Edição (revista atualizada) Almedina (2009);

Faria José Manuel – Acesso a contas bancárias por terceiros no âmbito de operações de pagamento. Revista da Banca. Lisboa: Associação Portuguesa de Bancos. N.º 71 (janeiro/junho 2011);

Faria, Jorge Leite Areias Ribeiro de – Direito das Obrigações Vol. I, Almedina. Coimbra;

Fernandez, Elizabeth -Desvio de poder: mito ou realidade? in Cadernos de Justiça

Administrativa (CJA), n.º 93, Maio/Junho 2012, cejur, Coimbra Editora (2012);

Ferreira, António Pedro de Azevedo - A relação negocial bancária – conceito e estrutura. Lisboa Quid Iuris (2005);

Ferreira, António Pedro de Azevedo – A relação negocial bancária – conceito e estrutura. Lisboa: Quid Iuris (2005);

Gomes, Manuel Januário da Costa – Contratos Comerciais, Almedina (2012);

Guimarães, Maria Raquel – (Ainda) a responsabilidade pelo uso indevido de instrumentos de pagamento in I Congresso de Direito Bancário (2015) p.121;

Guimarães, Maria Raquel - A Fraude no Comércio Eletrónico: O Problema da Repartição do Risco por Pagamentos Fraudulentos in Infrações Económicas e Financeiras, Estudos de Criminologia e Direito (J. Cruz, C. Cardoso, A. L. Leite, R. Faria, coordenação). Coimbra Editora (2013);

Guimarães, Maria Raquel – A Repartição dos prejuízos decorrentes de operações fraudulentas de banca eletrónica (home banking), in Cadernos de Direito Privado Nº 41 (2013);

Guimarães, Maria Raquel – As operações fraudulentas de homebanking na jurisprudência recente in Cadernos De Direito Privado Nº 49 (2015);

Guimarães, Maria Raquel – O contrato-quadro no âmbito da utilização de meios de pagamento eletrónicos. Coimbra editora (2011);

López Jiménez, José Maria- Comentarios a la ley de servicios de pago (2011);

Machado, João Baptista – Pressupostos da resolução por incumprimento in Obra dispersa I (1991);

Machado, João Baptista – Risco contratual e a mora do credor in Obra Dispersa;

Maria Raquel Guimarães –As transferências eletrónicas de fundos de cartões de débito, Almedina (1999);

Oliveira, Madalena Perestrelo de - "A "inexigibilidade" na relação contratual: interpretação do contrato e heteronomia", in O Direito, Ano 145.º (2013), Volume III, Director: Jorge Miranda, Almedina, Coimbra, (2014);

Oliveira, Nuno Manuel Pinto Oliveira – Princípios de Direito dos Contratos. Coimbra editora;

Pedro Verdelho, Phishing e outras formas de defraudação nas redes de comunicação, in Direito da Sociedade de Informação;

Proença, José Carlos Brandão – Direito das obrigações – Relatório sobre o programa, o conteúdo e os métodos de ensino da disciplina in Publicações da Universidade Católica, Porto (2007);

Raposeiro, Ana Raquel Correia - A Influência dos Valores Pessoais na Adopção da Banca pela Internet – Dissertação, Universidade de Coimbra (2007);

Reis, Sofia Cláudia Moreira Duarte – Os Determinantes da Adopção da Internet como Canal de Distribuição no Sector Bancário – Dissertação, Universidade de Coimbra (2005);

Santos, Hugo Luz - Plaidoyer por uma "distribuição dinâmica do ónus da prova" e pela "teoria das esferas de risco" in O Direito, Ano 145.º (2013), Volume III, Director: Jorge Miranda, Almedina,Coimbra, (2014);

Silva, Flávio Manuel Carneiro – A usurpação da ciberidentidade (2014), dissertação – Universidade Católica Portuguesa;

Silva, Miguel Roberto Mira da/Silva, Alberto/Romão, Artur/Conde, Nuno – Comércio eletrónico na Internet, 2ª Edição Atualizada, Lisboa-Porto-Coimbra;

Teixeira, Micael, Por uma distribuição dinâmica do ónus da prova, Dissertação de Mestrado – Faculdade de Direito da Universidade Nova de Lisboa, Lisboa, (2012)

Telles, Inocêncio Galvão – direito das obrigações 6ª Edição – Revista e Atualizada, Coimbra editora;

Varela, João Matos Antunes – Das Obrigações em Geral, Vol. I 10ª edição (revista e atualizada) Almedina (2009);

Vilela, Helena Cristina Monteiro Pinto – O serviço Caixadirecta Evolução dos Canais de Distribuição no Sector Bancário – Relatório de Estágio, Universidade do Minho (2005);

W. Peyrano, Jorge - La prueba difícil in Civil Procedure Review, Vol.2, n.º 1, January/April, 2011, (2011).