CATÓLICA
FACULDADE DE DIREITO

ESCOLA DE LISBOA

MESTRADO EM DIREITO E GESTÃO

OPERAÇÕES NÃO AUTORIZADAS E REPARTIÇÃO DOS PREJUÍZOS: O *HOMEBANKING* NA JURISPRUDÊNCIA DO RSP

Orientador

PROFESSOR DOUTOR FRANCISCO MENDES CORREIA

Dissertação de

BRUNO SILVA PALHÃO

Lisboa, abril de 2018

UNIVERSIDADE CATÓLICA PORTUGUESA

FACULDADE DE DIREITO

ESCOLA DE LISBOA

MESTRADO EM DIREITO E GESTÃO

OPERAÇÕES NÃO AUTORIZADAS E REPARTIÇÃO DOS PREJUÍZOS: O *HOMEBANKING* NA JURISPRUDÊNCIA DO RSP

Orientador

PROFESSOR DOUTOR FRANCISCO MENDES CORREIA

Dissertação de

BRUNO SILVA PALHÃO

Lisboa, abril de 2018

"There are some frauds so well conducted that it would be

stupidity not to be deceived by them."

COLTON, CHARLES CALEB (1821)

AGRADECIMENTOS

A dissertação que agora se apresenta é o culminar de um percurso académico e de desenvolvimento pessoal que começou muito antes da entrada no mestrado em Direito e Gestão da UNIVERSIDADE CATÓLICA PORTUGUESA. Várias pessoas contribuíram, em maior ou menor grau, direta ou indiretamente, para as ideias presentes neste texto.

Pelo seu apoio, nas suas várias vertentes, é incontornável começar por agradecer à minha família.

Pelas semanas que me foram concedidas, em dedicação exclusiva ao presente texto, o meu obrigado à URÍA MENÉNDEZ - PROENÇA DE CARVALHO.

A nível académico, é devido um agradecimento, em particular, ao Professor Doutor FRANCISCO MENDES CORREIA, que aceitou, com entusiasmo e sem hesitações, o papel de orientador desta dissertação, tendo, ao longo dos meses, respondido a todas as solicitações com disponibilidade, rigor e solidariedade. Em segundo lugar, à UNIVERSIDADE CATÓLICA PORTUGUESA, nas várias facetas que a compõem, designadamente corpo docente e demais colaboradores, o meu obrigado por tão bem me terem acolhido. Em terceiro lugar, à FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA, e a quem dela faz uma referência, o meu obrigado por, durante largos anos, terem contribuído decisivamente para a minha formação como jurista e cidadão, proporcionando-me estímulos e desafios que se revelaram essenciais.

Por fim, por termos feito os últimos três anos do percurso juntos, e por ser a primeira pessoa com quem partilho os bons e maus momentos, agradeço à CLÁUDIA. Sem a tua ajuda, ora na forma de paciência, ora na partilha de experiências e desafios comuns, tudo teria sido mais difícil.

PALAVRAS-CHAVE

Homebanking; *phishing*; *pharming*; jurisprudência; serviços de pagamento; instrumento de pagamento; operações não autorizadas; repartição dos prejuízos; diretiva dos serviços de pagamento; regime jurídico dos serviços de pagamento e moeda eletrónica.

ABREVIATURAS

ac.	Acórdão
art(s).	artigo(s)
BCE	Banco Central Europeu
BdP	Banco de Portugal
CC	Código Civil
CE	Comissão Europeia
cit.	citado
DL	Decreto-Lei
DSP	Diretiva dos Serviços de Pagamento (Diretiva 2007/64)
DSP2	Segunda Diretiva dos Serviços de Pagamento (Diretiva 2015/2366)
EBA	Autoridade Bancária Europeia
n.º(s)	número(s)
PSP	prestador(es) de serviços de pagamento
p.	página
pp.	páginas
proc.	processo
RGICSF	Regime Geral das Instituições de Crédito e Sociedades Financeiras (DL n.º 298/92, versão consolidada, com sucessivas alterações)
RSP	Regime Jurídico dos Serviços de Pagamento e Moeda Eletrónica (Anexo I do DL n.º 317/2009, versão consolidada, com as alterações introduzidas pelo DL n.º 242/2012 e DL n.º 157/2014)
RTS	normas técnicas regulamentares
SCA	Autenticação Forte do Cliente

ss	e seguintes
STJ	Supremo Tribunal de Justiça
TRC	Tribunal da Relação de Coimbra
TRE	Tribunal da Relação de Évora
TRG	Tribunal da Relação de Guimarães
TRL	Tribunal da Relação de Lisboa
TRP	Tribunal da Relação do Porto
v.	vide

ÍNDICE

I. CONSIDERAÇÕES INICIAIS

Às operações não autorizadas, no contexto de *homebanking*, encontram-se associados uma série de fatores que lhe vêm atribuindo uma relevância crescente, nomeadamente o acesso (cada vez mais) generalizado à *internet*[1] e a modificação dos hábitos dos consumidores, progressivamente menos avessos ao uso da banca *online*, que se vem desenvolvendo, com a consequente redução dos custos fixos dos Bancos[2]. A tendencial migração do físico para o digital aumentou a exposição dos clientes bancários a comportamentos predatórios informáticos, sendo que, na última década em particular, deram-se evoluções legislativas importantes nesta área. Sem surpresa, começaram igualmente a surgir litígios, tendo os tribunais portugueses sido chamados a pronunciar-se. O labor dos nossos tribunais produziu acórdãos que ilustram a relevância da problemática, mas, também, a necessidade de olhar às fontes mediatas na concretização dos critérios legais.

Além da resposta a questões que se apresentam de forma relativamente evidente – quem, PSP[3] ou utilizador[4], e em que situações, suporta os prejuízos que decorram da utilização do *homebanking* à revelia do titular da conta –, procurar-se-á, neste trabalho, identificar tendências da jurisprudência portuguesa dos últimos cinco anos, que tem analisado uma grande variedade de casos, com um particular foco no RSP, diploma que entrou em vigor há menos de uma década e se vê, agora, novamente reformado. A identificação de casos típicos e eventuais divergências a nível jurisprudencial mostra-se fundamental para uma melhor compreensão do regime.

Cabe, neste momento, explicitar a relevância da análise jurisprudencial proposta, não só, mas também, face a trabalhos anteriores. RAQUEL LIMA[5], no trabalho que provavelmente apresenta maiores semelhanças, analisa a jurisprudência num contexto temporal mais alargado. Os quase três anos de dilação permitem, também, o acesso a novos acórdãos, com uma maior prevalência do RSP. Adicionalmente, como última diferença, nesta tese apenas será analisado o *homebanking*, e não outros instrumentos de

[1] VANHOOSE, DAVID D., *Internet Banking*, 2009, pp. 5-6. A generalização do acesso à *Internet* fez deste um novo meio para antigas realidades, como o comércio. V. SILVA, CALVÃO DA, *Banca, Bolsa e Seguros*, Almedina, Coimbra, 2013, p. 127.
[2] Entre os Bancos que lideram o movimento digital mundial conta-se, nomeadamente, o *Bank of America*.
[3] Designadamente um Banco, v. arts. 2.º/k) e 7.º do RSP.
[4] Que, geralmente, se confunde com o titular da conta bancária.
[5] LIMA, RAQUEL, *A responsabilidade pela utilização…*, FDUP, Porto, 2015.

pagamento. Entre nós encontramos outros trabalhos relacionados, designadamente a tese de MARIA CAROLINA BARREIRA[6], onde é desenvolvida a repartição dos prejuízos, mas sem um foco jurisprudencial, acrescendo o previamente referido quanto à dilação temporal e surgimento de novos acórdãos. Finalmente, na doutrina identificam-se artigos sobre o tema, frequentemente em anotação a um acórdão concreto. As evoluções legislativas da última década vêm conferindo às operações não autorizadas, e decisões que sobre estas incidam, renovada pertinência. E a DSP2, que agora será transposta para o ordenamento nacional, não dispensa a aferição dos critérios interpretativos trabalhados à luz da DSP, visto a primeira manter, no essencial, a estrutura da segunda no que à repartição dos prejuízos respeita.

Aclarada a utilidade do tema e da abordagem utilizada, no presente texto começar-se-á pela explicitação de conceitos essenciais ao trabalho, numa introdução à problemática. Subsequentemente, serão analisadas as soluções legais, nomeadamente as resultantes da DSP e do RSP. Não obstante a menor relevância da DSP2 para o que nos propomos abordar, já que à data da entrega da presente tese ainda não foi trabalhada nos nossos tribunais, esta não deixará de ser introduzida. De seguida, entraremos no núcleo do trabalho, a análise de jurisprudência, identificando-se como têm sido concretizados os conceitos legais, bem como as tendências presentes nas decisões dos tribunais portugueses, sob uma perspetiva crítica. Finalmente, sumariar-se-ão as conclusões obtidas, considerando o futuro perspetivado em face da transposição da DSP2.

A presente tese insere-se no âmbito do Direito bancário e obrigacional. Não serão, nas páginas que se seguem, abordadas as consequências penais da fraude informática, que extravasam o âmbito, necessariamente delimitado, da dissertação. O texto foi redigido ao abrigo do mais recente acordo ortográfico. Nas citações, foi respeitada a redação original adotada pelos autores.

[6] BARREIRA, MARIA CAROLINA, *Home Banking…*, FDUNL, Lisboa, 2015.

II. CONCEITOS INTRODUTÓRIOS

1. *Homebanking*[7]

1.1. A adesão ao instrumento de pagamento

O *homebanking* representa uma nova forma de prestação de serviços bancários, por oposição à banca tradicional[8], possibilitada pelo desenvolvimento tecnológico. Consistindo num serviço à distância, não exige a deslocação a balcões físicos, sendo prestado por meio de canais telemáticos[9], como o sítio de *Internet* do Banco, telefone ou outras formas de acesso remoto que possam ser desenvolvidas. Neste texto limitar-nos-emos a analisar o serviço prestado nos sítios *online* dos Bancos. Aí autenticando-se e acedendo à conta de que seja titular, o cliente bancário logo dispõe de uma panóplia de operações bancárias, em página segura, sem constrangimentos horários ou deslocações que lhe custariam tempo e dinheiro. E o Banco, operacionalizando o princípio da simplicidade[10], aproxima-se da clientela ao mesmo tempo que reduz os custos fixos.

O contrato de *homebanking* (ou de utilização do *homebanking*, um instrumento de pagamento[11]) dá-se no âmbito de uma relação fiduciária entre PSP e utilizador, o ordenante das operações de pagamento[12], uma relação bancária geral e da qual nascem deveres acessórios[13]. Esta constitui-se aquando da abertura de conta[14], um contrato quadro[15] que serve de base a outros, geralmente acompanhado de um contrato de depósito

---

[7] Alternativamente denominado Banco por *internet*, Banco *online*, entre outros. V. LEIVA, FRANCISCO MUÑOZ, *Marketing financiero*, Copicentro Editorial, Granada, 2011, p. 141.

[8] Vários estudos vêm evidenciando a crescente preferência pelo *homebanking* entre os clientes bancários. Neste sentido, v. o relatório da Accenture, intitulado *Banking Costumer 2020*, p. 6. Relatório disponível em www.accenture.com (consultado em agosto de 2017).

[9] Por meios telemáticos entenda-se as *"(...) técnicas e (...) serviços que recorrem simultaneamente à informática e às telecomunicações (...)"*. MARQUES, GARCIA, MARTINS, LOURENÇO, *Direito da Informática*, Almedina, Coimbra, 2006, p. 748.

[10] O princípio da simplicidade tem, entre as suas concretizações, o uso da informática. V. CORDEIRO, ANTÓNIO MENEZES, *Direito Bancário*, Almedina, Coimbra, 2016, pp. 238ss.

[11] V. art. 2.º/z) do RSP. De modo mais preciso, o instrumento de pagamento são os dispositivos de segurança, códigos de acesso ou numéricos, associados ao *homebanking*. GUIMARÃES, MARIA RAQUEL, *(Ainda)...*, Almedina, Coimbra, 2015, p. 118.

[12] V. art. 2.º/i) do RSP. Assim não será quando se identifiquem operações não autorizadas.

[13] Fundados na vontade das partes ou no art. 762.º/2 CC, v. CORREIA, FRANCISCO MENDES, *Moeda...*, FDL, Lisboa, 2014, pp. 537ss.

[14] A abertura de conta *"(...) constitui, com efeito, a porta de entrada do cliente (...)"*. SOARES, QUIRINO, *Contratos Bancários*, UM, Braga, 2003, p. 111. Trata-se do *"(...) contrato nuclear donde emerge a relação bancária duradoura entre a instituição de crédito e a sua contraparte."*. VASCONCELOS, PESTANA DE, *Dos contratos de depósito bancário*, Coimbra Editora, Coimbra, 2011, p. 166.

[15] Neste sentido, v. ALMEIDA, FERREIRA DE; *Contratos II*, Almedina, Coimbra, 2016, p. 146, GUIMARÃES, MARIA RAQUEL, *A repartição dos prejuízos...*, CEJUR, Braga, 2013, p. 58, SÁ, ALMENO

ou de abertura de crédito, pois são estes que possibilitam a movimentação de fundos por parte do utilizador, faculdade essencial à realização de operações de pagamento de *homebanking*. Inicia-se, então, uma relação contratual complexa e duradoura, que perdurará no tempo, tendo a aptidão de vigorar perpetuamente, e que antecede o contrato de *homebanking*[16]. A abertura de conta marca o início de grande parte das obrigações do PSP, algumas das quais, como veremos, se estendem até ao *homebanking*.

No momento da contratação, a prática demonstra que é usual o recurso a cláusulas contratuais gerais[17], sendo o conteúdo do contrato *standardizado* e pese embora o respetivo clausulado varie consoante a instituição bancária[18]. A autonomia privada manifesta-se, pois, no momento da adesão, que concede ao utilizador o acesso ao serviço de banca *online*. Em todo o caso, o pedido de envio[19] de um instrumento de pagamento cabe ao cliente do PSP, que não acede ao *homebanking* pela mera contratualização da abertura de conta[20]. Em suma, à abertura de conta, momento chave na relação entre Banco e cliente, encontra-se associada a faculdade de o cliente aderir ao contrato de *homebanking*, efetivável aquando da abertura de conta ou em momento posterior.

1.2. O contrato quadro para futuras operações de pagamento

O RSP define contrato quadro no seu art. 2.º/o). Entre estes contratos podemos incluir o *homebanking*. Sinteticamente, as operações de pagamento[21] levadas a cabo no *homebanking*, enquadráveis nos serviços de pagamento[22], e por isso dentro do âmbito de aplicação do diploma[23], podem dar-se isoladamente ou no âmbito de um contrato quadro,

---

DE, *Direito Bancário*, Coimbra Editora, Coimbra, 2008, p. 17, e MONTEIRO, ANTÓNIO PINTO, *A resposta do ordenamento…*, FDUC, Coimbra, 2014, p. 2324.

[16] Ou, no mínimo, haverá uma contemporaneidade entre a abertura de conta e a celebração do contrato de *homebanking*.

[17] Com efeito, *"(...) os bancos são hoje empresas que actuam para um universo vastíssimo de clientes, estando fora de causa negociar caso a caso o conteúdo de milhares ou mesmo milhões de contratos (...)"*. ANTUNES, JOSÉ ENGRÁCIA, *Os contratos bancários*, Almedina, Coimbra, 2011, p. 81. V., em alternativa, ANTUNES, JOSÉ ENGRÁCIA, *Direito dos Contratos Comerciais*, Almedina, Coimbra, 2014, p. 480.

[18] CORDEIRO, ANTÓNIO MENEZES, *Direito Bancário*, cit., p. 532. Sobre o uso de cláusulas contratuais gerais na prática bancária, v. ainda SILVA, CALVÃO DA, *Banca, Bolsa e Seguros*, cit., pp. 173ss, SILVA, CALVÃO DA, *Direito bancário…*, Almedina, Coimbra, 2001, pp. 350ss e MONTEIRO, ANTÓNIO PINTO, *Banca e cláusulas…*, Almedina, Coimbra, 2015, pp. 101ss.

[19] No instrumento de pagamento em análise, o envio consiste tipicamente na disponibilização dos dispositivos de segurança, por parte do PSP, ao utilizador.

[20] Aliás, *"[d]o contrato geral não resulta tipicamente qualquer dever de contratar (...)."*. ALMEIDA, FERREIRA DE, *Contrato Bancário Geral…*, CEJ, Lisboa, 2015, p. 25. Tal entendimento não é incompatível com a faculdade, ao dispor do PSP, de sugerir a utilização de um instrumento de pagamento. V. GUIMARÃES, MARIA RAQUEL, *O contrato-quadro…*, Coimbra Editora, Coimbra, 2011, pp. 178-179.

[21] V. art. 2.º/g) do RSP.

[22] V. art. 4.º do RSP, pela positiva, e art. 5.º do RSP, pela negativa.

[23] V. art. 3.º do RSP.

sendo mais comuns e importantes as segundas[24]. As operações de pagamento abrangidas por contrato quadro são reguladas nos arts. 51.ºss do RSP.

A celebração de um contrato quadro agiliza acordos posteriores, na medida em que estabelece as regras base e tendencialmente diminui o tempo gasto em negociações futuras. No contrato de *homebanking* encontramos a base de vários pequenos atos, absolutamente comuns no nosso quotidiano, que se dão num contexto de execução do contrato quadro, assumindo-se como renovadas demonstrações de vontade do utilizador[25], que, aquando da celebração do contrato quadro, não previa quais as ordens que iria emitir, a favor de quem e qual o seu *quantum*.

[24] V. considerando 24 da DSP.

[25] A tal não obsta a sua natureza de ato de execução. Para maiores desenvolvimentos, v. CORREIA, FRANCISCO MENDES, *Moeda…*, cit., pp. 522ss.

2. Ameaças *online*

2.1. A fraude[26] informática

A utilização do serviço de *homebanking* não é isenta de riscos[27], embora os Bancos o disponibilizem em página segura e facultem dispositivos de segurança[28] pessoais e intransmissíveis. Divergindo, de PSP para PSP, os concretos métodos de segurança, certo é que a eliminação de todos os perigos e vulnerabilidades é uma impossibilidade. Com as vantagens surgiram, também, novos riscos[29]. Uma das maiores dificuldades que os PSP experienciam, na prevenção e mitigação dos riscos cibernéticos, é a diversidade das ameaças[30]. E a fraude afeta não só os utilizadores, mas, também, a credibilidade dos Bancos e respetivos serviços[31].

No *homebanking*, podemos encontrar situações de fraude informática. Ocupar-nos-emos desta, neste capítulo em particular, pelos efeitos nefastos na perceção de valor do *homebanking* junto dos clientes bancários[32] e pelo obstáculo que representa ao desenvolvimento do comércio eletrónico[33]. Como ponto de partida, as operações de pagamento devem ser autorizadas pelo utilizador e titular do instrumento de pagamento[34]. Todavia, nem sempre assim é. A situação típica é aquela em que um terceiro atua de modo a obter uma vantagem patrimonial, originando prejuízos para as partes da relação

[26] Abordando a simulação fraudulenta, ANTÓNIO MENEZES CORDEIRO refere que nela existe um *animus nocendi*, procurando-se retirar benefícios em prejuízo de terceiros. V. CORDEIRO, ANTÓNIO MENEZES, *Tratado de Direito Civil – Volume II*, Almedina, Coimbra, 2014, p. 888. Idêntico *animus* podemos encontrar nas operações não autorizadas. A propósito da expressão *"utilização fraudulenta"*, empregue não só, mas também, na DSP e DSP2, v. MORAIS, GRAVATO, *A utilização fraudulenta…*, Almedina, Coimbra, 2003, pp. 35ss.

[27] À semelhança do que acontece nos cartões. V. VASCONCELOS, JOANA, *Sobre a repartição entre…*, Almedina, Coimbra, 2002, pp. 487ss.

[28] É com recurso a estes dispositivos de segurança, nomeadamente o código de acesso e cartão matriz, que o utilizador se autentica, nos termos do art. 2.º/v) do RSP.

[29] Potenciados, designadamente, pelo alcance global, anonimato, remoção de barreiras sociais e automaticidade da *internet*. V., designadamente, KOOPS, BERT-JAAP, *The Internet…*, 2010, pp. 739ss.

[30] V. ROSSI, CLIFFORD, *A Risk…*, Wiley, Nova Jérsia, 2014, p. 426.

[31] Em sentido idêntico, v. GUIMARÃES, MARIA RAQUEL, *As transferências electrónicas de fundos…*, Almedina, Coimbra, 1999, p. 207.

[32] A propósito dos riscos percecionados nos pagamentos eletrónicos, com foco no *Paypal*, v. TRAUTMAN, LAWRENCE J., *E-Commerce, Cyber...*, 2016, pp. 295-296. Como refere o autor, *"[c]oncerns about fraud (…) may prompt consumers to offline channels."*.

[33] V. considerando 95 da DSP2.

[34] V. art. 65.º/1 do RSP. Admite-se a retirada do consentimento até quando, nos termos do art. 77.º/1 do RSP, a ordem de pagamento atinja a irrevogabilidade. Voltaremos a estes artigos.

bancária. Relevando, na jurisprudência dos nossos tribunais, o *phishing* e o *pharming*, torna-se indispensável analisá-los[35].

2.2. Em especial, o *phishing* e o *pharming*

Numa visão ampla dos ciberataques, tanto o *phishing* como o *pharming* conduzem à obtenção de informações privadas, ilegalmente e através do uso de sítios *online*. Embora o objetivo lhes seja comum, o método usado é distinto.

O *phishing* é, de modo simples, a prática em que alguém, um *phisher*, envia *e-mails* ou mensagens que aparentam ser de fontes fiáveis, como uma instituição bancária, com o objetivo de obter informação, dos destinatários, que lhe é vantajosa. Tipicamente[36], o *phishing* manifesta-se através de uma hiperligação para sítio *online* que represente uma ameaça a quem o visite, designadamente por ser uma representação fiel de outra página, legítima, levando o visitante a introduzir os seus dados pessoais[37]. Após os dados de acesso serem introduzidos em página falsa, o *phisher* logo obterá acesso a informação confidencial dos alvos.

Enunciado o *phishing*, vejamos o *pharming*. O *pharming* consiste num ataque informático que visa redirecionar o tráfego de um sítio *online*, legítimo, para outro, ilegítimo. Os sítios *online* têm endereços *web* (nomes, domínios) que, por sua vez, estão associados a endereços IP (números). Pelo que é possível alterar o endereço IP a que o endereço *web* está associado num dado computador e *browser* para, desse modo, redirecionar o tráfego de um determinado sítio *online* e, simultaneamente, manter a aparência e confiança suscitada pelo endereço *web* digitado. Caso ocorra, nomeadamente, o corrompimento[38] do Sistema de Nomes de Domínio[39], digitar o endereço *web* de um sítio *online* levará a vítima, nomeadamente um utilizador de serviços de *homebanking*, para página idêntica, mas ilegítima, com um endereço IP distinto, controlada por um

---

[35] O acesso, ilegítimo e *online*, à conta bancária, pode resultar da quebra dos sistemas de segurança do Banco ou, alternativamente, da obtenção dos dispositivos de segurança através do utilizador. Ambas as modalidades em análise são enquadráveis na segunda categoria. V. GUIMARÃES, MARIA RAQUEL, *A repartição dos prejuízos…,* cit., p. 63.

[36] Em concreto, o *phishing* pode apresentar-se de várias formas. V. JAKOBSSON, MARKUS, MYERS, STEVEN, *Phishing and Countermeasures*, Wiley, Nova Jérsia, 2007, p. 32.

[37] Com este intuito, *"(...) são utilizadas fórmulas combinadas de estímulos e recompensa (...)"*. GERALDES, ANA VAZ, *Phishing…*, Coimbra Editora, Coimbra, 2013, p. 91.

[38] Tal ocorrerá, tipicamente, com a *"(...) difusão, por via de spam (...), de ficheiros ocultos, que igualmente de forma oculta se auto-instalam nos computadores ou sistemas informáticos das vítimas."*. VERDELHO, PEDRO, *Phishing e outras…*, Coimbra Editora, Coimbra, 2009, p. 415.

[39] Mais conhecido pela expressão inglesa, *Domain Name System* ou DNS. Este converte endereços *web* em endereços IP.

pharmer. Aí chegado, a introdução dos dados pessoais do utilizador de *homebanking* será suficiente para estes passarem a ser conhecidos pelo *pharmer*.

Da explanação resulta que, no *phishing*, o engodo é uma página com um endereço *web* forjado. Diferentemente, no *pharming* apenas ocorre uma adulteração do endereço IP, escondido sob o endereço *web*. Enquanto o primeiro pressupõe o recebimento de um *e-mail* ou mensagem do *phisher*, onde consta o endereço *web* forjado, no segundo o utilizador digita diretamente, e sem interferência de terceiro, a página do Banco, sendo redirecionado para uma página falsa ou clone. Caso a página falsa, controlada pelo *pharmer*, seja uma reprodução fiel da original, este poderá revelar-se um esquema quiçá indetetável. E, por isso, será menos censurável a conduta do utilizador ludibriado. Tal distinção deve ser tida em conta aquando da ponderação das circunstâncias do caso concreto[40].

Por último cabe notar que, não obstante os PSP tornarem conhecidos alguns dos riscos associados ao *homebanking*, assim como os bons hábitos que levam à mitigação dos mesmos, no cumprimento das suas obrigações, seguidamente analisadas, por excessivas vezes ocorrem operações não autorizadas. Falhada a prevenção, a questão imediata passa, não surpreendentemente, por determinar quem, e em que medida, suporta os prejuízos que resultem dessas operações. É ao que se procurará responder, partindo de uma fonte imediata, a lei, para outra fonte, mediata e central ao presente texto, a jurisprudência.

[40] Neste sentido, v. GUIMARÃES, MARIA RAQUEL, *A repartição dos prejuízos…,* cit., p. 64, acompanhada por BARREIRA, MARIA CAROLINA, *Home Banking*…, cit., pp. 36-37 e LIMA, RAQUEL, *A responsabilidade pela utilização…*, cit., p. 51.

III. SOLUÇÕES LEGAIS: DA DSP E RSP À DSP2

1. O mercado único de serviços de pagamento

Foi há pouco mais de uma década que a relevância dos serviços de pagamento, cujas normas aplicáveis divergiam em função das fronteiras físicas, levou à intervenção de um legislador europeu que visava alcançar o bom funcionamento do mercado único[41]. Embora já existissem vários atos supranacionais e de base comunitária neste domínio[42], estes conseguiam apenas uma regulação parcelar, incompleta e insuficiente[43]. É neste contexto que surge a DSP, transposta para o ordenamento jurídico interno nacional pelo DL n.º 317/2009, que publicou em anexo o RSP, desde então republicado. O regime significou um importante passo de harmonização[44].

O RSP comporta uma área institucional e outra material[45], sendo que apenas nos ocuparemos da área material, de prestação e utilização do serviço, e aplica-se aos contratos em vigor sempre que daí resulte um quadro normativo mais favorável ao utilizador[46], o que pode ser relevante, nomeadamente, face às regras de distribuição do risco e ónus da prova.

2. O regime da DSP e RSP[47]

2.1. Obrigações das partes[48]

---

[41] V. considerando 1 da DSP. Sobre os antecedentes da DSP, v. CORREIA, FRANCISCO MENDES, *Moeda…*, cit., pp. 428ss.

[42] V. considerando 3 da DSP.

[43] Na verdade, *"[b]oa parte das regras consignadas no RSP, de origem europeia, eram já conhecidas e praticadas: seja na base de ccg, seja na concretização de princípios gerais."*. CORDEIRO, ANTÓNIO MENEZES, *Direito Bancário*, cit., p. 591. Contudo, *"[a]s (...) Recomendações (...) revelaram-se insuficientes para assegurar o mercado único de serviços de pagamento."*. SILVA, CALVÃO DA, *Banca, Bolsa e Seguros*, cit., p. 166.

[44] Visando a harmonização total, ou máxima, a DSP almejava a transposição para a ordem interna sem desvios, salvo quando tal faculdade se encontrasse expressamente prevista.

[45] V. CORDEIRO, ANTÓNIO MENEZES, *Direito Bancário*, cit., p. 584.

[46] V. art. 101.º do RSP.

[47] No presente texto, abordar-se-á, centralmente, o RSP, sendo as referências à DSP necessárias, mas secundárias. Analisando, em especial, a DSP, v. MAVROMATI, DESPINA, *The Law of Payment Services…*, Kluwer Law International, Alphen aan den Rijn, 2008, pp. 141ss.

[48] Da relação obrigacional complexa, entre PSP e titular do instrumento de pagamento, emergem direitos e deveres para ambas as partes. Optou-se, aqui, pelo uso da terminologia obrigação, na senda do legislador. Ainda assim, e por precisão conceitual, cabe notar que por vezes estamos perante encargos e não verdadeiros deveres: o legislador prevê uma conduta a observar, pretendendo assegurar um determinado efeito útil, designadamente a confidencialidade do instrumento de pagamento, mas, caso tal conduta seja inobservada, não pode a contraparte intentar uma ação para cumprimento, obtenção de uma indemnização ou execução judicial. Tal resulta nitidamente das obrigações do utilizador. O PSP não pode exigir que o utilizador mantenha a confidencialidade do instrumento de pagamento. A cominação, na falta de

O contrato de *homebanking* assenta num conjunto de obrigações[49], cuja disciplina consta dos arts. 62.ºss do RSP[50], que lhe conferem previsibilidade e segurança, mas também conformam a resposta a dar a final, na medida em que não sejam observadas e se identifiquem operações não autorizadas. De modo a facilitar a exposição, dividir-se-á a mesma entre as obrigações do PSP e do utilizador.

2.1.1. Obrigações do PSP[51]

i. Execução das operações de pagamento autorizadas

Escreveu-se, em momento anterior, que as operações de pagamento se dão num contexto de execução do contrato quadro de *homebanking*, não sabendo o utilizador, no momento inicial, quais as ordens que irá emitir, a favor de quem e qual o seu *quantum*. Assim, caberá ao PSP executar as operações de pagamento autorizadas pelo utilizador, que constituem mandatos para pagamento. Esta é a obrigação principal a que se encontra adstrito, por força do contrato de *homebanking*.

As operações de pagamento, ou conjuntos de operações de pagamento, só se consideram autorizadas caso o ordenante consinta na sua execução[52], geralmente em momento prévio à execução e sempre na forma acordada[53]. Caso haja consentimento, o momento da receção da ordem determina a sua irrevogabilidade: antes da receção, o consentimento pode ser retirado em qualquer momento[54]; recebida a ordem de pagamento, esta torna-se, em regra, irrevogável[55].

---

acatamento do encargo, será o titular do instrumento de pagamento perder o direito ao reembolso das quantias contra a sua vontade transferidas, no todo ou em parte. No mesmo sentido, v. CORREIA, FRANCISCO MENDES, *Operações não autorizadas…*, Almedina, Coimbra, 2017, p. 715. O regime do encargo distingue-se de um mero ónus, já que o seu não cumprimento manifesta um grau de culpa que, como veremos, conforma a repartição dos prejuízos. Para maiores desenvolvimentos, v. CORDEIRO, ANTÓNIO MENEZES, *Tratado de Direito Civil – Volume VI*, Almedina, Coimbra, 2012, pp. 525ss.

[49] Sobre estas, v. igualmente CORREIA, FRANCISCO MENDES, *Moeda…*, cit., pp. 624ss.

[50] *"O RSP, nos seus artigos 62.º a 91.º, fixa os direitos e os deveres das partes, relativamente à prestação e à utilização de serviços de pagamento, bem como a sua execução. As regras são imperativas para as relações com consumidores e supletivas nos restantes casos (...)"*. CORDEIRO, ANTÓNIO MENEZES, *Direito Bancário*, cit., p. 590.

[51] Às que analisaremos aqui em particular, acrescem ainda as obrigações previstas no art. 68.º/1 do RSP, alíneas b), c), d) e e).

[52] V. art. 65.º/1 do RSP.

[53] V. art. 65.º/2 e 3 do RSP.

[54] V. art. 65.º/4 do RSP.

[55] V. arts. 65.º/4 e 77.º/1 do RSP.

Os arts. 75.ºss do RSP tratam, em particular, da execução de operações de pagamento. Do art. 76.º/1 do RSP resulta que o PSP faz um controlo formal da operação[56], o que se compreende face à massificação das operações de pagamento e a necessária previsibilidade de um serviço cuja arbitrariedade suscitaria graves inconvenientes para o utilizador, mas, também, para o comércio e economia.

Havendo fundamento para a recusa da ordem de pagamento, esta deve ser notificada ao utilizador, assim como, sempre que possível, as razões inerentes à mesma e o procedimento para retificação dos erros factuais identificados[57]. Caso o PSP recuse indevidamente uma operação de pagamento autorizada, ou a execute defeituosamente, designadamente nos montantes ou beneficiário, regem os arts. 86.ºss do RSP[58].

Pela negativa, não deve o PSP executar as operações de pagamento não autorizadas. Embora este aparente ser um dever de abstenção facilmente observável, a prática demonstra que as situações de fraude informática proliferam, de modo que, por vezes, as operações de pagamento são autorizadas por um ordenante ilegítimo e executadas à margem da vontade do titular do instrumento de pagamento.

ii. Envio dos dispositivos de segurança ao utilizador

Tal como resulta do art. 68.º/1/b) do RSP *a contrario*, bem como da efetivação do contrato de *homebanking*, após a adesão do utilizador, deve o Banco enviar os códigos que se mostrem necessários à plena utilização do serviço[59]: o envio dos dispositivos de segurança equivale a um verdadeiro envio do instrumento de pagamento. De outra forma, e sem esse envio, o utilizador ficaria impedido de cumprir as necessárias exigências de autenticação e confirmação das operações de pagamento que pretenda realizar *online*, não podendo gozar o serviço que contratou.

O risco do envio corre por conta do PSP[60], pelo que os prejuízos que decorram do extravio dos dispositivos de segurança serão necessariamente suportados pelo mesmo[61].

---

[56] Tomando em conta o perfil do utilizador, como veremos.
[57] V. art. 76.º/2 do RSP.
[58] *"As regras em jogo não prejudicam o regime geral da responsabilidade civil (88.º). Há regresso (89.º) e a força maior é exonerante (90.º)."* CORDEIRO, ANTÓNIO MENEZES, *Direito Bancário*, cit., p. 591.
[59] Tipicamente, o código de acesso e o cartão matriz.
[60] V. art. 68.º/2 do RSP.
[61] A norma em análise assumirá particular relevância quando perante envios por correio. A propósito do envio de cartões, v. GUIMARÃES, MARIA RAQUEL, *A fraude no comércio…*, Coimbra Editora, Coimbra, 2013, pp. 591-592.

iii. Manutenção da qualidade e eficiência do serviço de *homebanking*

Na relação com o cliente, o PSP que se pretenda diferenciar necessita de disponibilizar a máxima qualidade e eficiência nas suas plataformas eletrónicas. Todavia, não estamos perante um mero imperativo de boa gestão, já que se trata de uma obrigação, juridicamente sindicável[62].

Acedendo o utilizador ao serviço, frequentemente, para autorizar operações de pagamento, e cabendo ao PSP executá-las, esta apresenta uma intima conexão com a obrigação principal: a ineficiência do sistema poderá ditar a inexecução das operações autorizadas bem como a execução de operações não autorizadas.

iv. Manutenção da segurança do serviço de *homebanking*

A segurança é um dos elementos prioritários aquando da escolha de um Banco, na perspetiva do cliente bancário médio, seja na banca tradicional ou *online*[63]. Numa primeira aproximação, e apenas como faceta negativa da obrigação que se acaba de referir, não deve o PSP disponibilizar os dispositivos de segurança a um terceiro. Mas a lei não se fica pela exigência de um comportamento negativo[64]. Com efeito, encontramos uma exigência de atuação, na manutenção da segurança na sua plataforma eletrónica. O PSP não deve disponibilizar o código de acesso, cartão matriz ou outro dispositivo de segurança, mas encontra-se obrigado, igualmente, a tomar as medidas necessárias para que um terceiro não obtenha acesso às credenciais de segurança do utilizador pelos seus próprios meios[65].

Estreitamente ligada à obrigação de manutenção da segurança do serviço de *homebanking*, e por isso aqui não individualizada, encontra-se a obrigação de informação, perante o utilizador, das medidas de segurança que este deva adotar, já que conscientizar o utilizador, num esforço de prevenção, constitui obstáculo relevante à interceção dos dispositivos de segurança por terceiros[66].

---

[62] Do art. 73.º do RGICSF decorre uma obrigação que vincula o Banco, na letra do legislador, em todas as atividades, incluindo, portanto, a prestação do serviço de *homebanking*.
[63] Trata-se de um fator crítico de sucesso.
[64] V. art. 68.º/1/a) do RSP.
[65] E nesse sentido, deve, nomeadamente, encriptar a sua plataforma eletrónica. V. PEREIRA, JOEL, *Compêndio…*, Quid Juris - Sociedade Editora, Lisboa, 2004, p. 696.
[66] Estamos perante *"(…) um dever imposto à entidade bancária de explicar as situações mais comuns de fraude e os perigos específicos dos diferentes serviços que fornece, em função do tipo de utilizador*

No âmbito das informações gerais pré-contratuais[67], encontramos a exigência, no art. 53.º/e)/i do RSP, quanto às medidas preventivas e retificativas, de o PSP fornecer,*"[s]e for caso disso, uma descrição das medidas que o utilizador do serviço de pagamento deve tomar para preservar a segurança dos instrumentos de pagamento (...)"*. Dificilmente se vislumbram, no contexto do *homebanking*, situações em que, na expressão legal, *"não seja caso disso"*; porventura quando o utilizador tenha particulares conhecimentos técnicos na área da prevenção da fraude informática, nomeadamente por aí atuar profissionalmente, o que constituirão casos residuais. E esta obrigação não vincula o Banco apenas antes de celebração do contrato quadro, mas, também, durante o decurso da relação contratual[68]. Com o constante desenvolvimento de novas modalidades de fraude informática, que se mutam diariamente, tornando-se progressivamente mais engenhosas e difíceis de detetar, o PSP deve adotar uma postura continuamente preventiva e proactiva durante a execução do contrato de *homebanking*, alertando os seus clientes para os perigos que existem e como os podem mitigar[69]. Existe, no *homebanking*, um dever de informação alargado, que abrange o antes, durante e pós-contrato[70].

v. Monitorização

O utilizador do serviço de *homebanking* nem sempre deteta as operações de pagamento não autorizadas imediatamente, razão pela qual a vigilância, ou monitorização, das operações que lhe são atribuídas, tendo em conta o seu perfil e padrão de normalidade, não é de somenos importância. Embora aqui a tónica seja já reativa, e não estritamente preventiva, assumirá um caráter preventivo face a operações não autorizadas futuras, evitando prejuízos que ocorreriam sem essa mesma monitorização.

Não se encontra expressamente, na letra da lei, uma obrigação de monitorização. Contudo, alguns dos enunciados normativos fornecem pistas para uma solução. Nos termos do art. 66.º/2 do RSP, suscitando-nos particular atenção as alíneas a) e b), o bloqueio do instrumento de pagamento deve ser alvo de estipulação expressa no contrato

envolvido e dos seus conhecimentos técnicos.". GUIMARÃES, MARIA RAQUEL, *A repartição dos prejuízos…,* cit., p. 62.

[67] V. arts. 52.º e 53.º do RSP.

[68] Embora tal já resultasse dos deveres acessórios em que o Banco incorre pela celebração do contrato, o art. 54.º do RSP parece igualmente apontar neste sentido.

[69] Dificilmente se compreenderia que o PSP se eximisse desta obrigação apenas por, no momento zero de uma relação que se pode sedimentar ao longo de décadas, alertar o utilizador para os perigos então existentes.

[70] No mesmo sentido, v. LIMA, RAQUEL, *A responsabilidade pela utilização…*, cit., p. 16.

quadro. Por sua vez, o art. 73.º/1/b) do RSP estatui o reembolso das operações de pagamento, iniciadas pelo beneficiário ou através deste[71], quando uma das condições preenchidas seja *"[o] montante da operação de pagamento exceder o montante que o ordenante poderia razoavelmente esperar com base no seu perfil de despesas anterior, nos termos do seu contrato quadro e nas circunstâncias específicas do caso."*.

Assim, e salvo melhor entendimento, o perfil do utilizador não é despiciendo no enquadramento do RSP[72-73]. Todavia, tal nunca poderá servir de base a um bloqueio do instrumento de pagamento, na ausência de acordo expresso nesse sentido[74]. Ao PSP caberá, no cumprimento da sua prestação principal, solicitar uma confirmação reforçada, designadamente através de *hard token* ou *sms token*, ou recusar a ordem de pagamento e informar o utilizador dos motivos, nomeadamente as suspeitas de se tratar de fraude informática, tendo em conta o perfil do utilizador[75]. O art. 76.º/1 do RSP alude às condições previstas no contrato quadro celebrado com o ordenante, mas não exige estipulação expressa que permita a recusa de ordens de pagamento, pelo que este entendimento da norma não se mostra incompatível com o enunciado normativo. Com efeito, do contrato quadro de abertura de conta, e posteriormente de *homebanking*, resultam deveres fiduciários na relação entre o Banco e o utilizador[76], cuja inobservância no momento em que mais são necessários – o da execução das operações de pagamento – não se compreenderia. Pelo que existe, efetivamente, uma obrigação de monitorização por parte do PSP. Esta constitui um corolário da obrigação de proteção a cargo do PSP[77].

---

[71] Os pagamentos através de débito direto.
[72] Neste sentido, v. LIMA, RAQUEL, *A responsabilidade pela utilização…*, cit., pp. 28-30.
[73] Os tribunais vêm igualmente apontando a importância do perfil do utilizador de *homebanking*, como adiante se verá.
[74] Sob pena de se inutilizar o art. 66.º/2 do RSP, por força de um entendimento *contra legem*.
[75] A segunda opção é preferível. Embora os Bancos exijam a confirmação, nomeadamente via *sms*, das operações de pagamento de montante relevante, a prática demonstra que não raras vezes também os telemóveis associados à conta de *homebanking* são comprometidos, conseguindo o terceiro ordenante confirmar a operação à revelia do titular do instrumento de pagamento.
[76] *"Esta especial relação obrigacional complexa, de confiança mútua e dominada pelo intuitus personae, impõe à instituição financeira (...) deveres de protecção dos legítimos interesses do cliente (...), em consonância com os ditames da boa fé (...)."* SILVA, CALVÃO DA, *Conta corrente bancária…*, Coimbra Editora, Coimbra, 2015, p. 310.
[77] Pela boa solução, que merece concordância no essencial, a propósito da obrigação de monitorização, v. SANTOS, HUGO LUZ DOS, *Plaidoyer…*, Almedina, Coimbra, 2015, em especial pp. 729-732. Em sentido idêntico, v. LIMA, RAQUEL, *A responsabilidade pela utilização…*, cit., pp. 28-30 e CAMPOS, DIANA, CARMO, MARIA, *Home Banking: Consequências jurídicas*, Governance Lab, 2017, p. 17.

Quando identifique operações que se desviem do perfil do utilizador, e dentro de um padrão de razoabilidade, deverá o PSP atuar[78].

2.1.2. Obrigações do utilizador

i. Utilização do *homebanking* de acordo com as condições que o regem

Dita o art. 67.º/1/a) do RSP, no âmbito das obrigações do utilizador, que este obriga-se a *"[u]tilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização"*[79]. Como concretização, encontramos uma obrigação de diligência do utilizador[80] na preservação da eficácia dos dispositivos de segurança. O utilizador deve tomar, nesse sentido, todas as medidas razoáveis[81]. Inclui-se neste âmbito, designadamente, a obrigatoriedade de sigilo e não transmissão dos seus códigos pessoais e intransmissíveis a terceiros, algo que não só seria já exigível segundo o padrão do homem médio como, frequentemente, se encontra expressamente previsto no clausulado a que o cliente bancário adere.

ii. Comunicação ao PSP da quebra de confidencialidade dos dispositivos de segurança ou qualquer utilização não autorizada

Como catalisador de algumas das obrigações do PSP[82], encontramos no art. 67.º/1/b) a obrigação de comunicação[83], *"sem atrasos injustificados"*[84], de todas as situações de vulnerabilidade dos dispositivos de segurança. Embora, como se defendeu, exista uma obrigação de monitorização por parte do PSP, o legislador não deixa de exigir um comportamento diligente por parte do utilizador. Pois se é verdade que a plataforma de *homebanking* é controlada pelo Banco, os dispositivos de segurança, pessoais e

[78] A obrigação de atuação surge *"(...) sempre que o Banco se aperceba de operações inabituais pelos seus montantes, periodicidade ou volume, ou de operações originadas em países suspeitos, e, portanto, passíveis de esconderem situações de fraude."*. GUIMARÃES, MARIA RAQUEL, *O contrato-quadro…*, cit., p. 317.
[79] O utilizador deverá, designadamente, *"(...) pagar o preço correspectivo à emissão do IP. (...) Este preço tem, em geral, um carácter anual (...)"*. GUIMARÃES, MARIA RAQUEL, *Os Contratos-Quadro...*, Almedina, Coimbra, 2016, p. 182.
[80] V. art. 67.º/2 do RSP. Um utilizador diligente não responderá pelos prejuízos que resultem das operações não autorizadas, como se verá adiante. É a inobservância desta obrigação que originará perdas na sua esfera jurídica. V. GUIMARÃES, MARIA RAQUEL, *A fraude no comércio…*, cit., p. 590.
[81] Tal obrigação já se encontrava prevista no art. 5.º/a) da Recomendação 97/489/CE.
[82] Nomeadamente as previstas no art. 68.º/1 do RSP, alíneas c), d) e e).
[83] Ou notificação, na expressão do art. 68.º/1/c) do RSP.
[84] O uso de um conceito indeterminado, embora determinável e necessário à equidade, introduz necessariamente alguma imprevisibilidade. Sobre a concretização que foi sendo feita na jurisprudência, v. LIMA, RAQUEL, *A responsabilidade pela utilização…*, cit., pp. 24-26. Resumidamente, deve ser concedido um lapso temporal que considere todas as circunstâncias, podendo ser maior ou menor em função do caso concreto.

intransmissíveis, estão sob o controlo do utilizador. Como se verá, esta comunicação assume considerável relevância na repartição dos prejuízos resultantes de operações não autorizadas.

2.2. Operações não autorizadas e repartição dos prejuízos

As operações não autorizadas nascem habitualmente, embora não necessariamente, da inobservância das obrigações que recaem sobre as partes do contrato de *homebanking*. Isto é, ainda que as obrigações das partes sejam devidamente observadas, podem verificar-se operações de pagamento não autorizadas, nomeadamente por, através das formas de fraude informática anteriormente enunciadas, um terceiro obter os dispositivos de segurança do utilizador de *homebanking*. Os arts. 70.º a 72.º[85] do RSP versam, em particular, sobre a repartição dos prejuízos nas operações de pagamento não autorizadas e assumem especial relevância para o presente trabalho[86].

2.2.1. O ónus da prova

Quando o utilizador de *homebanking* negue ter autorizado uma operação de pagamento, ou alegue a sua deficiente execução por parte do PSP, caberá a este último *"(...) 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."*[87]. O ónus da prova é, portanto, do PSP[88], que não o pode atenuar[89]. Trata-se de um desvio ao regime geral, e apresenta-se como mais favorável ao utilizador[90]. Acresce ainda que o registo da utilização do *homebanking*, ou dos códigos de acesso, *"não é necessariamente suficiente"*[91] para provar a autorização, a existência de fraude ou

[85] Sobre o art. 69.º do RSP, que prevê o direito de retificação, não nos debruçaremos de modo central, até porque a comunicação é uma obrigação do utilizador aqui já previamente abordada. Cabe apenas sublinhar que o utilizador vê reforçado o encargo de controlar os movimentos que lhe são atribuídos e que o prazo máximo de 13 meses, constante do n.º 1, é cumulativo com a celeridade imposta pelo uso da expressão *"sem atraso injustificado"*. Para maiores desenvolvimentos, v. BARREIRA, MARIA CAROLINA, *Home Banking*…, cit., pp. 56-58.

[86] Cabe recordar que o regime é imperativo apenas para os consumidores, tal como resulta do art. 62.º/2 do RSP. Pela conveniência de o analisar numa perspetiva abstrata e geral, centrar-nos-emos no quadro normativo sempre aplicável aos consumidores.

[87] V. art. 70.º/1 do RSP. Trata-se de uma presunção de ilicitude, a favor do utilizador, relativamente a três vetores do incumprimento, v. CORREIA, FRANCISCO MENDES, *Operações não autorizadas…*, cit., p. 722.

[88] V. CORDEIRO, ANTÓNIO MENEZES, *Direito Bancário*, cit., p. 590.

[89] V. considerando 33 da DSP.

[90] Nos termos gerais, o titular do instrumento de pagamento teria de provar o cumprimento defeituoso, art. 342.º/1 do CC, presumindo-se a culpa, art. 799.º/1 do CC. Aqui, o legislador bastou-se com a alegação de falta de autorização da operação. V., CORREIA, FRANCISCO MENDES, *Moeda…*, cit., p. 643.

[91] Face ao uso da expressão, discute-se se são admissíveis as presunções sobre o utilizador que é afetado pela operação não autorizada e devidamente registada. *"(...) [T]em sido entendido que a expressão (...)*

a inobservância de obrigações por parte do utilizador[92]. Em suma, e como regra geral, caberá ao PSP provar o grau de culpa do utilizador, titular do instrumento de pagamento, e a sua contribuição para os prejuízos ocorridos[93].

2.2.2. O imediato reembolso

Identificada uma operação não autorizada, o utilizador deve ser imediatamente reembolsado pelo PSP, no montante da operação não autorizada *"(…) e, se for caso disso, repor a conta de pagamento debitada na situação em que estaria se a operação de pagamento não autorizada não tivesse sido executada."*[94]. Na medida em que o reembolso deve ser imediato, dando-se o apuramento das concretas perdas a suportar em momento posterior, a solução legal passa por uma medida provisória que onera o PSP, conduzindo o atraso no reembolso a juros moratórios calculados à taxa do CC acrescida de 10 pontos percentuais[95]. Os juros serão calculados desde o momento em que o cliente bancário negue ter autorizado a operação e até à data do reembolso efetivo. *"A indemnização moratória assim calculada não impede o utilizador de exigir uma eventual indemnização suplementar a que haja lugar, nos termos gerais do direito."*[96].

2.2.3. A imputação dos prejuízos

---

não condena definitivamente uma presunção nesse sentido, deixando espaço ao julgador para a sua apreciação.". GUIMARÃES, MARIA RAQUEL, *A repartição dos prejuízos…,* cit., p. 60. Um argumento prático, embora quiçá excessivamente literal, neste sentido, é que o legislador que procurasse proibir a presunção teria usado a expressão *"não é suficiente"*, v. STEENNOT, REINHARD, *Allocating liability in case of fraudulent use…*, Financial Law Institute, Gante, 2010, pp. 8-9. Em sentido aparentemente distinto, v. FARIA, JOSÉ MANUEL, *Acesso a contas…*, Associação Portuguesa de Bancos, Lisboa, 2011, p. 33 e CORREIA, FRANCISCO MENDES, *Moeda…*, cit., pp. 643-644. Salvo melhor opinião, uma operação ser ordenada com recurso aos códigos pessoais e intransmissíveis do utilizador não é suficiente para operar qualquer presunção, já que a fraude informática tem como efeito prático a obtenção dos ditos códigos e o operar de tal presunção obrigaria o utilizador a fazer prova de factos relacionados com sistemas informáticos que não domina.

[92] V. art. 70.º/2 do RSP. O legislador faz referência ao ordenante, mas deve entender-se este como o titular do instrumento de pagamento, fruto de uma interpretação corretiva. Nas operações não autorizadas, o ordenante é o terceiro com intuitos fraudulentos. Idêntica interpretação deverá ser feita nos artigos seguintes.

[93] Solução que facilmente se compreende, desde logo, pela operatividade do ónus da prova: o utilizador médio, se onerado com um ónus de prova sobre um sistema informático que não domina, veria recair sobre si uma prova diabólica.

[94] V. art. 71.º/1 do RSP. A solução é igual à que resultaria do art. 562.º CC. Esta regra *"(...) resulta claramente do âmbito da presunção de incumprimento que rege toda a responsabilidade não aquiliana."*. BARBOSA, MAFALDA MIRANDA, *Serviços de pagamentos…*, 2017, p. 595.

[95] V. art. 71.º/2 do RSP. Soma-se-lhe ainda uma coima, prevista no art. 95.º/p) do RSP, de € 10.000,00 a € 5.000.000,00. O incumprimento da obrigação de reembolso é qualificado, no regime contraordenacional dos arts. 94.ºss do RSP, como uma infração especialmente grave.

[96] GOMES, JANUÁRIO DA COSTA, *Contratos Comerciais*, Almedina, Coimbra, 2012, p. 245. Tal resulta do art. 71.º/2 *in fine* do RSP. Como bem aponta o autor, o legislador nacional, na transposição da DSP, fez uso da faculdade prevista no respetivo art. 60.º/2.

O PSP, que num primeiro momento é chamado ao reembolso, tem todo o interesse em, num segundo momento, discutir qual o *quantum* que o onera, tendo em conta a conduta das partes e, particularmente, a culpa imputável ao utilizador, ficando com direito de crédito sobre o cliente bancário e utilizador de *homebanking* na medida em que o montante reembolsado tenha sido superior ao efetivamente devido. Assim, o PSP poderá eximir-se de eventuais perdas, total ou parcialmente, *"(...) revertendo essa responsabilidade para o ordenante, quando a falha lhe seja imputável, em certos termos."*[97]. Vejamos em que termos.

Em caso de *"(...) apropriação abusiva (...), com quebra da confidencialidade dos dispositivos de segurança personalizados imputável ao ordenante (...)"*[98], as perdas serão suportadas por este, no limite do saldo disponível ou da linha de crédito associada à conta e nunca em mais de € 150,00[99]. Tratam-se dos casos de culpa, ou negligência, adotando a terminologia do legislador comunitário, leve[100].

Alternativamente, havendo atuação fraudulenta ou incumprimento deliberado das obrigações plasmadas no art. 67.º do RSP, o utilizador suporta todas as perdas resultantes das operações não autorizadas[101]. Caso consiga demonstrar a fraude ou dolo do utilizador, o PSP verá ser-lhe restituído, integralmente, o montante despendido no reembolso. A

[97] CORDEIRO, ANTÓNIO MENEZES, *Direito Bancário*, cit., p. 591. Salvo melhor opinião, idêntica lógica se encontraria no Direito comum, onde sempre poderia concorrer a culpa do utilizador lesado.
[98] MARIA RAQUEL GUIMARÃES enquadra nesta disposição, por entender que são imputáveis ao utilizador, a grande maioria dos casos de *phishing*. V. GUIMARÃES, MARIA RAQUEL, *A fraude no comércio…*, cit., p. 594.
[99] V. art. 72.º/1 do RSP. Neste enunciado normativo é omitida referência ao art. 71.º do RSP, sendo a redação incongruente com a adotada pelo legislador europeu nos equivalentes arts. 60.º e 61.º da DSP. Com efeito, o art. 61.º/1 da DSP, equivalente ao art. 72.º/1 do RSP, começa por dispor *"[e]m derrogação do disposto no artigo 60.º (...)"*. Assim, e numa interpretação de acordo com a DSP, quando a quebra de confidencialidade seja imputável ao utilizador, o PSP deverá subtrair o montante a suportar pelo utilizador, nunca em mais de € 150,00, ao montante a reembolsar de imediato. Neste sentido, v. GUIMARÃES, MARIA RAQUEL, *(Ainda)…*, cit., p. 130.
[100] No mesmo sentido, v. CORREIA, FRANCISCO MENDES, *Operações não autorizadas…*, cit., pp. 715-716. Como resulta do considerando 32 da DSP, a atuação fraudulenta ou negligência grave requer um enquadramento diverso, devendo o utilizador suportar prejuízos num montante superior. Certo é que, caso a conduta do utilizador não seja qualificável, no mínimo, como negligência leve, o PSP suportará todos os prejuízos. Sobre a distinção entre negligência e dolo, e modalidades possíveis, v. VARELA, ANTUNES, *Das Obrigações…*, Almedina, Coimbra, 2003, pp. 566ss, COSTA, ALMEIDA, *Direito das Obrigações*, Almedina, Coimbra, 2012, pp. 582-583, CORDEIRO, ANTÓNIO MENEZES, *Tratado de Direito Civil – Volume II, Tomo III*, Almedina, Coimbra, 2010, pp. 470ss e LEITÃO, LUÍS MENEZES, *Direito das Obrigações…*, Almedina, Coimbra, 2013, pp. 283ss. Na medida em que os conceitos não foram densificados, e nem teriam de ser, os contributos doutrinários e jurisprudenciais assumem particular relevância.
[101] V. art. 72.º/2 do RSP.

solução compreende-se, visto a operação não autorizada resultar da vontade manifestada pela conduta do utilizador.

Num cenário intermédio entre os dois anteriores, encontramos os casos de negligência grave do utilizador[102]. A principal particularidade a apontar, por contraposição à negligência leve, é o alargar do teto máximo, que passa dos € 150,00 para *"(...) até ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento (...)"*. Desta forma, o PSP consegue reduzir significativamente, ou até excluir, a sua contribuição para o ressarcimento dos prejuízos.

Por fim, os n.os 4 e 5 do art. 72.º preveem os efeitos jurídicos associados à notificação a que se refere o art. 67.º/1/b) do RSP. Feita a notificação pelo utilizador, e inexistindo fraude, o PSP suporta todas as perdas resultantes de operações não autorizadas que ocorram desde esse momento em diante. Caso o PSP não disponibilize os meios para a notificação ocorrer, e na ausência de fraude, as consequências serão as mesmas[103].

2.2.4. A obrigação de manutenção da segurança do serviço de *homebanking* como conformadora dos prejuízos suportados pelo PSP

O esquema de imputação de prejuízos ao PSP, entidade que é chamada imediatamente ao reembolso, apresenta uma íntima ligação com a distribuição do risco, aproximando-se de uma responsabilidade objetiva[104]. No regime resultante da DSP[105], o PSP responderá pelos prejuízos resultantes de operações não autorizadas sempre que não

---

[102] V. art. 72.º/3 do RSP. No Direito interno, o uso da terminologia negligência grave não é habitual. Estará em causa a conhecida culpa grave, ou culpa lata, que corresponde a uma negligência grosseira. Sobre esta, v. PRATA, ANA, *Cláusulas…*, Almedina, Coimbra, 1985, pp. 306ss e TELLES, INOCÊNCIO GALVÃO, *Direito das obrigações*, Coimbra Editora, Coimbra, 1997, pp. 354ss.

[103] Pois *"(...) em caso de incumprimento, a entidade bancária (...) estaria a atuar de má-fé (...) ao tentar imputar o risco ao seu cliente"*. BARREIRA, MARIA CAROLINA, *Home Banking*…, cit., p. 55. Note-se, contudo, *"(...) que os casos previstos nos n.os 4 e 5 do artigo 72.º (...) apenas ilustram instâncias de incumprimento, e que a regra geral da imputação obrigacional de danos prevista no artigo 798.º do Código Civil se aplica a todos os casos em que a perturbação no cumprimento seja imputável ao prestador de serviços de pagamento."*. CORREIA, FRANCISCO MENDES, *Operações não autorizadas…*, cit., p. 710. Assim, e imputando-se ao PSP uma operação não autorizada, teremos como potencialmente aplicável o regime geral da responsabilidade contratual. A previsão do legislador em sede de RSP não prejudica, naturalmente, a aplicação das regrais gerais.

[104] *"Em rigor, o artigo 72 regula amplamente as questões de risco e respetiva distribuição (...)"*. GOMES, JANUÁRIO DA COSTA, *Contratos Comerciais*, cit., p. 245. No mesmo sentido, v. CORREIA, FRANCISCO MENDES, *Moeda…*, cit., p. 642 e *Operações não autorizadas…*, cit., pp. 718-720 e FONSECA, GISELA, *Utilização…*, FDL, Lisboa, 2011, p. 204.

[105] E também na DSP2, como veremos.

os possa imputar ao utilizador e independentemente de culpa[106]. Estamos perante uma imputação objetiva, ainda que mitigável, em parte reconduzível às soluções que resultariam da aplicação do regime geral da responsabilidade contratual, designadamente quando a conduta do PSP seja censurável, mas que, na maioria das vezes, destas nitidamente se afasta. Em síntese, dir-se-á que *"[h]á zonas (...) em que a imputação dos danos deve (...) obedecer a outros princípios, repousar sobre outros fundamentos."*[107]. Os serviços de pagamento constituem uma destas zonas.

Segundo a teoria do risco, as consequências nefastas que resultem de uma atividade ou fonte de perigo devem ser assumidas por quem primariamente a controla e colhe os seus benefícios[108]. Haveria, pois, *"(...) como que uma contrapartida das vantagens que aufere (...)"*[109] o Banco, enquanto PSP. No RSP, e importa frisá-lo, a *ratio* do esquema de repartição de prejuízos não passa pela associação dos benefícios aos prejuízos[110]. O PSP suporta os prejuízos pois é sobre este que incumbe a obrigação de assegurar um serviço eficiente e seguro[111]. Tal ideia sai reforçada na DSP2. Nesta, como veremos, o PSP suporta todos os prejuízos que ocorram, exceto quando haja fraude do utilizador, sempre que não imponha a SCA. Daqui resulta claro que a ideia subjacente não é que deve suportar os prejuízos quem mais tem a ganhar com a plataforma, mas antes que deve suportar os prejuízos quem, devendo assegurar a segurança do serviço[112], não o faz. Quando não imponha a SCA, o PSP, que não colhe mais benefícios por isso, omite parte da sua obrigação de manutenção da segurança do serviço. E, assim sendo, entendeu o legislador que deve arcar, em medida adicional, com os prejuízos que decorram de condutas negligentes do titular do instrumento de pagamento. A maior fragilidade do utilizador médio – não profissional – e a capacidade do PSP para lidar com a progressiva sofisticação da fraude informática legitimam, salvo melhor opinião, as

---

[106] *"Esta imputação objetiva de perdas (...) vai perdendo força, à medida que cresce a censurabilidade subjacente à vicissitude que motivou a operação não autorizada."*. CORREIA, FRANCISCO MENDES, *Moeda…*, cit., p. 642.

[107] MONTEIRO, JORGE SINDE, *Responsabilidade civil*, UC, Coimbra, 1978, p. 329.

[108] *"(...) [Q]uem cria ou mantém um risco em proveito próprio, deve suportar as consequências prejudiciais do seu emprego, já que deles colhe o principal benefício (ubi emolumentum, ibi onus; ubi commodum, ibi incommodum)."*. VARELA, ANTUNES, *Das Obrigações…*, cit., p. 633.

[109] COSTA, ALMEIDA, *Direito das Obrigações*, cit., p. 613.

[110] Defendendo que o Banco suporta os prejuízos pois é quem colhe os maiores benefícios, v. ac. do STJ, de 18 de dezembro de 2013 (processo 6479/09.8TBBRG.G1.S1) e ac. do TRL, de 16 de abril de 2015 (processo 971/13.7TJLSB.L1-8), acompanhados por CAMPOS, DIANA, CARMO, MARIA, *Home Banking: Consequências jurídicas*, cit., p. 23.

[111] Neste sentido, v. BARREIRA, MARIA CAROLINA, *Home Banking*…, cit., pp. 80-81.

[112] Constituindo a implementação da SCA uma medida relevante para tal objetivo.

soluções legais[113]. Contudo, e para operacionalizar o regime, há que evitar a excessiva oneração do PSP: a fronteira entre os comportamentos negligentes do utilizador e os comportamentos desculpáveis em resultado de fraude informática deverá ser corajosamente traçada.

3. Alterações introduzidas pela DSP2

O regime analisado, resultante da DSP, foi alvo de uma revisão que esta, em maior ou menor medida, já previa[114]. No seguimento do Livro Verde para um mercado europeu integrado de pagamentos eletrónicos[115], lançado pela CE em 2012, surgiu, em 2013, a proposta de Diretiva que visava revogar a DSP[116]. Dois anos depois, em 2015, foi aprovada a DSP2, ainda não transposta para a ordem jurídica interna nacional. Estamos, portanto, perante um novo regime dos serviços de pagamento, ainda não trabalhado pelos tribunais, mas que mantém, no essencial, a estrutura de repartição dos prejuízos que acabamos de percorrer[117]. Cabe referir as alterações mais pertinentes na matéria[118].

Em matéria de ónus de prova[119], este, sem surpresa, continua a pertencer ao PSP, prevendo-se agora também a possibilidade de existir um prestador de serviços de iniciação de pagamentos, igualmente onerado com um ónus da prova nas suas competências. O legislador optou, neste âmbito, por manter a expressão *"não é necessariamente suficiente"*[120], acrescentando que o PSP deverá apresentar elementos que fundamentem a negligência grave ou dolo do utilizador.

No tocante ao reembolso[121], o legislador definiu o prazo em que deve operar, e, com maior pertinência, previu a possibilidade de o PSP, caso tenha *"motivos razoáveis"*

---

[113] Com interesse, v. o estudo citado no ac. do TRP, de 07 de outubro de 2014 (processo 747/12.9TJPRT.P1).
[114] V. art. 87.º da DSP. Sobre a revisão da DSP, v. CORREIA, FRANCISCO MENDES, *Moeda…*, cit., pp. 481ss.
[115] V. Bruxelas, 11.1.2012, COM(2011) 941 final.
[116] V. GUIMARÃES, MARIA RAQUEL, *(Ainda)…*, cit., pp. 119-120.
[117] No mesmo sentido, v. BARBOSA, MAFALDA MIRANDA, *Serviços de pagamentos…*, cit., p. 599.
[118] Os arts. 70.º a 72.º do RSP, tal como transpõe a DSP, correspondem aos arts. 72.º a 74.º da DSP2. Apenas o art. 74.º/1 da DSP2 constava da Consulta Pública do BdP n.º 1/2017, referente à transposição da DSP2, já que, tal como a DSP, esta é de harmonização total e confere poucas opções aos Estados. Assim, as soluções da DSP2 serão quase integralmente transpostas para a nossa ordem jurídica interna.
[119] V. art. 72.º/1 da DSP2.
[120] V. art. 72.º/2 da DSP2.
[121] V. art. 73.º/1 da DSP2.

para suspeitar de fraude do utilizador, não o reembolsar imediatamente[122]. Também aqui é prevista a possibilidade de a operação ser iniciada por um prestador de serviços de iniciação de pagamentos[123].

No que respeita à repartição dos prejuízos[124], o esquema reproduzido na DSP2 é, em grande medida, similar ao da DSP. Em caso de negligência leve[125], o utilizador suportará agora € 50,00 ou menos. Caso os prejuízos resultem de uma atuação fraudulenta que lhe seja imputável, ou incumpra as suas obrigações[126] com dolo ou negligência grosseira, suportará todas as perdas[127]. Na transposição da DSP, o Estado português exerceu a opção conferida e criou um regime diferenciado, consoante o PSP consiga demonstrar o dolo ou somente a negligência grave do utilizador[128]. Afigura-se pertinente perceber se, na transposição da DSP2, a opção também será exercida.

Uma das grandes novidades da DSP2 passa pela introdução de um novo mecanismo de segurança, a SCA[129], com um extenso âmbito de aplicação[130], que representa um obstáculo adicional às técnicas de fraude informática. Pese embora o PSP não tenha de impor a SCA aos seus clientes e utilizadores de *homebanking*, caso não o faça estes apenas responderão pelos prejuízos resultantes de operações não autorizadas quando atuem de modo fraudulento. Curiosa é a possibilidade de os prejuízos serem suportados pelo beneficiário ou pelo seu PSP, não aceitando estes a SCA[131].

---

[122] Comunicando as suas suspeitas à autoridade nacional competente e levando a cabo uma investigação, v. considerando 71 da DSP2. *A contrario*, não poderá o reembolso ser adiado perante a suspeita de negligência grave do utilizador.
[123] V. art. 73.º/2 da DSP2.
[124] V. art. 74.º da DSP2.
[125] Embora tenha sido eliminada a referência expressa à quebra de confidencialidade imputável ao utilizador, o art. 74.º/1 da DSP2 introduz uma cláusula de exclusão para aqueles casos em que a perda, o furto ou a apropriação abusiva não pudesse por este ser detetada. Assim, um utilizador diligente não responderá pelos prejuízos, à semelhança da solução da DSP.
[126] V. art. 69.º da DSP2.
[127] V. art. 74.º/1 da DSP2.
[128] Criticando o exercício da opção, v. SILVA, CALVÃO DA, *Serviços de pagamento…*, Almedina, Coimbra, 2015, pp. 367-368. Não só este tratamento diferenciado – nas consequências jurídicas – não é habitual no nosso ordenamento jurídico, como o combate às operações não autorizadas não exige que o utilizador que age com negligência grave responda em menor medida do que aquele que age com dolo. É, pois, de rejeitar, no plano do Direito a constituir, a diferenciação e consequente teto máximo para as situações de negligência grave.
[129] V. art. 4.º/30 da DSP2. Esta constitui o segundo de quatro princípios elencados pelo BCE para a segurança dos pagamentos *online*. V. ECB, *Recommendations for the security of internet payments*, January 2013, p. 3.
[130] V. art. 97.º/1 da DSP2.
[131] V. art. 74.º/2 da DSP2.

E, sem surpresa, a comunicação do utilizador continua a ser fundamental, marcando o momento em que apenas responde por atuações fraudulentas[132].

Importa destacar o papel da EBA na concretização da DSP2[133], designadamente em matéria de SCA, através de *Guidelines*[134] e de RTS[135] submetidas à CE. As RTS criam requisitos específicos de conformidade para os PSP, com o objetivo de assegurar a proteção do consumidor e o reforço da concorrência, efetivando a SCA como o padrão na autenticação e realização de pagamentos *online*, bem como estabelecendo os requisitos que essa mesma SCA deve observar. A 27 de novembro de 2017, a CE anunciou[136] ter feito pequenas alterações às RTS propostas pela EBA. E já em 2018, no dia 13 de março, as RTS foram publicadas no Jornal Oficial da União Europeia[137]. Ao abrigo da SCA, os utilizadores provarão a sua identidade através de dois ou mais dos seguintes elementos: *(i)* conhecimento: algo que conhecem (nomeadamente uma palavra chave ou um PIN); *(ii)* posse: algo que possuem (nomeadamente um cartão ou um telemóvel); e *(iii)* inerência: algo que são (nomeadamente as respetivas informações biométricas). A SCA tornar-se-á obrigatória 18 meses após a publicação, a partir de 14 de setembro de 2019. Esta dilação temporal dará oportunidade aos PSP de adaptarem os seus procedimentos às novas medidas de segurança.

Em suma, e considerando a delimitação realizada, as maiores novidades da DSP2 reconduzem-se à possibilidade, excecional, de recusa do reembolso imediato e à introdução da SCA. É de prever que esta última reduza significativamente os prejuízos dos utilizadores, em consequência de operações não autorizadas, ora por diminuir as situações de fraude informática, quando adotada, ora por, nos cenários em que o PSP não a imponha, o cliente deixar de suportar prejuízos que resultem das suas condutas negligentes. O incentivo à adoção generalizada da SCA afigura-se evidente.

---

[132] V. art. 74.º/3 da DSP2.
[133] V. arts 15.º e 95.º/3 da DSP2.
[134] Ainda no final de 2014, a EBA publicou um bloco de Orientações onde, na antecâmara da DSP2, já era abordada a SCA. São Orientações *"(...) na acepção do artigo 16º do Regulamento que instituiu a EBA – Regulamento (UE) nº 1093/2010 – (...) esperando-se que o Banco de Portugal, na sua qualidade de autoridade competente na matéria, fiscalize o seu cumprimento, exigindo explicações para eventuais situações de inobservância (possivelmente na linha do procedimento conhecido por comply or explain) as quais poderão vir a influenciar a avaliação do risco (operacional) a que está exposta a instituição no âmbito da supervisão prudencial"*. FARIA, JOSÉ MANUEL, *Evolução recente…*, Almedina, Coimbra, 2016, p. 610.
[135] Disponíveis em eba.europa.eu (consultado em fevereiro de 2018).
[136] Através de um comunicado, disponível em europa.eu (consultado em fevereiro de 2018).
[137] V. Regulamento Delegado (UE) 2018/389.

IV. ANÁLISE DE JURISPRUDÊNCIA

Vejamos, aqui chegados, se e como tem sido aplicado o RSP na jurisprudência portuguesa. Este constitui, aliás, o núcleo da análise proposta. O foco no RSP justifica-se pela delimitação da abordagem, mas, também, pela relevância do mesmo no passado recente e futuro perspetivado com a DSP2. O método que seguiremos reconduzir-se-á a um percurso pelos acórdãos, com conclusões intercalares, seguido de uma apreciação global a final.

1. Percurso cronológico

1.1. Ac. de 05 de novembro de 2013 (Processo 9821/11.8T2SNT.L1-1) - TRL

Começamos o percurso pela jurisprudência do RSP num acórdão do TRL, datado de 05 de novembro de 2013.

Das cláusulas contratuais gerais do Banco resultava que *"[o] Cliente é o único responsável por todos os prejuízos resultantes da utilização indevida do Serviço do Banco (...) por parte de terceiros"*, desonerando-se este apenas com a comunicação da perda, extravio, furto ou falsificação das credenciais de autenticação ao Banco. Embora já ao abrigo do regime das cláusulas contratuais gerais esta estipulação pudesse ser qualificada como nula, por absolutamente proibida ao alterar a distribuição do risco e onerar desproporcionadamente um utilizador que agisse de boa fé, o tribunal decide aplicar o então novo regime por *in casu* ser mais favorável ao utilizador do serviço de *homebanking*, operacionalizando o art. 101.º do RSP. Assim, o ónus da prova deveria recair sobre o Banco, na demonstração da contribuição da conduta do utilizador para os prejuízos ocorridos. Ora, tal ficou por demonstrar, desconhecendo-se o modo pelo qual um terceiro obteve acesso aos códigos confidenciais associados ao instrumento de pagamento.

Concluiu, pois, o tribunal que, embora as transferências tenham sido realizadas com as credenciais do utilizador, não se demonstrou sequer a negligência leve do mesmo, devendo o Banco suportar a totalidade dos prejuízos.

1.2. Ac. de 18 de dezembro de 2013 (Processo 6479/09.8TBBRG.G1.S1) - STJ

No dia 18 de dezembro de 2013, o RSP chegava pela primeira vez ao STJ.

Embora do enquadramento factual não conste, em concreto, de que modo foi facilitada a operação não autorizada, por presunção, e tendo em conta os factos provados, o tribunal entendeu estar-se provavelmente perante uma situação de *pharming*[138]. Com efeito, a autora terá introduzido as suas credenciais numa página clonada, julgando estar em página segura.

O tribunal entendeu que tal comportamento não deveria merecer censura, correndo por conta do Banco qualquer risco resultante do ataque informático. Ficando por demonstrar culpa imputável ao titular do instrumento de pagamento, também aqui seria o Banco a suportar a totalidade dos prejuízos resultantes da operação não autorizada[139].

1.3. Ac. de 29 de abril de 2014 (Processo 225/12.6TJVNF.P1) - TRP

No acórdão em análise, do TRP, datado de 29 de abril de 2014, encontramos uma combinação de *phishing*[140] e *pharming*[141].

A operação não autorizada deu-se após o autor receber uma mensagem no telemóvel, alegadamente enviada pelo Banco, instruindo-o a descarregar uma aplicação para realizar operações de *homebanking*. O autor atuou em conformidade com as instruções. Provou-se, também, que o utilizador havia acedido a uma página fraudulenta, onde partilhou informações que possibilitaram a operação não autorizada.

No seguimento das decisões anteriores, e identificada a fraude informática, foi excluída a censura da conduta utilizador, imputando-se a quebra de segurança ao PSP.

1.4. Ac. de 22 de maio de 2014 (Processo 11/13.6T2ASL.E1) - TRE

[138] Embora seja de concordar com a qualificação, já é de rejeitar que, tal como se pode ler no acórdão, esta qualificação como *pharming*, e não *phishing*, não tenha *"(...) quaisquer implicações (...)"*. A censurabilidade da conduta do utilizador deverá entender-se menor na primeira modalidade.

[139] Defendendo que, *in casu*, *"(...) seria de ponderar uma redução da indemnização, que sinalizasse a função preventiva e sancionatória da auto-responsabilidade do cliente, vítima (também) da sua negligência no contributo razoavelmente exigível nas circunstâncias concretas (...)"*, v. SILVA, CALVÃO DA, *Conta corrente bancária…*, cit., p. 319.

[140] Manifestado através de uma mensagem, recebida no telemóvel do utilizador.

[141] Sensivelmente um mês antes de receber a referida mensagem, o utilizador facultou os códigos pessoais e o número de telemóvel, bem como a respetiva marca e o modelo, em página falsa, quando procurava aceder à página do Banco.

Em acórdão do TRE, datado de 22 de maio de 2014, encontramos evidências de *pharming*[142].

Da matéria de facto resulta que o autor tentou consultar o seu saldo, *online*, tendo-lhe surgido uma página fraudulenta onde partilhou, inadvertidamente, o número de telemóvel associado à confirmação por *sms*. No mesmo dia, e com recurso aos códigos confidenciais, foi ordenada a operação não autorizada. A transferência foi confirmada através de um código enviado por *sms*, embora o utilizador nunca o haja recebido ou reencaminhado para terceiros. Autor que, aliás, até então havia utilizado o serviço de *homebanking* apenas para consulta de saldos.

Dos factos provados consta, também, que o Banco frequentemente publicava recomendações de segurança, sob a forma de *banners* ou notícias, em vários dos *sites* por si geridos. Ainda antes de entrarem no serviço de *homebanking*, os clientes podiam ler, nomeadamente, que o Banco *"(...) nunca solicita a introdução do seu nº de telemóvel."*[143]. Em primeira instância, e na sequência deste quadro factual, entendeu-se que o réu cumpriu o seu dever de informação, sendo censurável, na forma negligente, o comportamento do utilizador de *homebanking* vítima de *pharming*.

O TRE, na linha jurisprudencial que vinha a ser seguida pelos tribunais superiores, entendeu que a existência de fraude informática exclui a culpa do utilizador, não sendo a partilha do número de telemóvel em página clone uma causa adequada para a operação não autorizada. De forma inovadora face aos casos anteriores, defendeu-se igualmente a existência de uma obrigação de monitorização, a cargo do Banco: o autor apenas usava o serviço de *homebanking* para consulta de saldos e nunca pretendeu um cartão matriz, necessário à realização de certas operações. Nas suas cláusulas gerais o Banco salvaguardava até a possibilidade de não executar determinadas ordens, se e quando se colocassem dúvidas sobre a identidade do ordenante. Tal, defende o tribunal, *"(...) leva a concluir que a entidade bancária tem consciência de que existe um padrão de utilização que pode fazer suspeitar sobre a identidade da pessoa que a transmite, pelo que no caso concreto impunham as regras de segurança que pusesse reservas à operação recolhendo elementos adicionais com vista à autorização, já que estava em causa uma transferência da quase totalidade dos fundos da conta bancária, por parte de um cliente, que ao longo*

[142] Que o tribunal assim bem qualifica.
[143] Tais avisos, cada vez mais frequentes, são adotados de forma generalizada pelos Bancos.

de vários anos nunca tinha realizado qualquer operação (…) que não fosse de simples consulta de saldos bancários.". Pelo que, concluiu, os prejuízos resultantes da operação não autorizada não deveriam ser imputados ao utilizador.

1.5. Ac. de 07 de outubro de 2014 (Processo 747/12.9TJPRT.P1) - TRP

O presente acórdão do TRP, datado de 07 de outubro de 2014, assenta numa factualidade, em grande medida, semelhante à dos anteriores.

Em síntese, o autor tentou aceder à página do Banco, tendo-lhe aí surgido uma mensagem que instruía o *download* de uma aplicação para o telemóvel, faltando apenas preencher a marca e modelo do mesmo. Após preencher estes campos, descarregou a aplicação. Dias depois, a operação não autorizada foi confirmada com recurso às credenciais e confirmação por *sms* associados à conta do utilizador. Uma vez mais, os códigos pessoais e intransmissíveis foram obtidos por terceiro, que, concomitantemente, instruiu a instalação de *software* malicioso no telemóvel usado para confirmar as operações. E, igualmente sem surpresa, em sua defesa o Banco alegou que regularmente divulgava avisos de segurança e nunca havia sido alvo de pirataria, devendo as falhas de segurança ser imputadas ao utilizador.

Após enquadrar este caso numa situação de fraude informática[144], o tribunal refere desde logo que não se identifica dolo ou culpa grave do utilizador. A verdadeira questão passaria por saber se a factualidade era, ou não, subsumível a negligência leve, qualificação que os tribunais superiores, até então, ainda não haviam adotado em sede de RSP.

A final, proferiu-se decisão onde, por ser comum a confirmação das operações de *homebanking* via *sms*, se defendeu que não é censurável o comportamento do utilizador que descarrega uma aplicação para o telemóvel. Os tribunais portugueses recusavam, novamente, a qualificação da conduta do utilizador alvo de fraude informática como negligente, ainda que na respetiva modalidade leve[145].

1.6. Ac. de 17 de dezembro de 2014 (Processo 1910/12.8TBVCT.G1) - TRG

[144] O tribunal qualifica-o como um caso de *phishing*. É de discordar. No acórdão, pode ler-se que o utilizador acedeu autonomamente à página do Banco. Trata-se, indiciam os factos, de *pharming*.
[145] Criticando esta corrente jurisprudencial, v. CORREIA, FRANCISCO MENDES, *Operações não autorizadas…*, cit., p. 726, acompanhado por LIMA, RAQUEL, *A responsabilidade pela utilização…*, cit., pp. 49-52 e CAMPOS, DIANA, CARMO, MARIA, *Home Banking: Consequências jurídicas*, cit., p. 27.

O acórdão em análise, do TRG, datado de 17 de dezembro de 2014, constitui um bom exemplo de como a dificuldade de prova pode ditar o desfecho do mesmo *ab initio*[146].

Dos factos consta que foram movimentadas várias contas bancárias do autor, não se provando que este tenha facultado quaisquer códigos pessoais a um terceiro ordenante. Foi por *"(...) introdução de um vírus (...)"* que este terceiro obteve acesso aos ditos códigos, não obstante ter o autor demonstrado que mantinha um antivírus atualizado no seu computador.

Similarmente a acórdão anterior[147], o tribunal defendeu a relevância do perfil do utilizador[148], embora não retirando consequências práticas em concreto. Não se tendo demonstrado que, e de que forma, o utilizador do serviço de *homebanking* forneceu elementos confidenciais a terceiros, decidiu-se, sem surpresa, que os prejuízos resultantes das várias operações não autorizadas deveriam ser suportados pela instituição de crédito.

1.7. Ac. de 03 de março de 2015 (Processo 1727/13.2TJLSB.L1-1) - TRL

No presente acórdão do TRL, datado de 03 de março de 2015, a matéria de facto e análise de direito subsequente são idênticas às que temos vindo a encontrar, de tal modo que não se as desenvolverão: ocorreu uma operação não autorizada, ordenada com recurso aos códigos do utilizador, mas à sua revelia, tendo o tribunal concluído que os prejuízos deveriam ser suportados pelo PSP.

Por outro lado, e com maior interesse, pode ler-se que *"[n]as semanas seguintes ao sucedido, o Autor teve dificuldade em dormir e andou muito nervoso, angustiado e preocupado."*. Tendo ficado demonstrado que estes danos não patrimoniais resultaram não apenas da operação não autorizada, mas, também, do incumprimento da obrigação de

[146] Faltando factos para se concluir, nomeadamente, pela modalidade de fraude informática no caso em apreço.
[147] V. ac. do TRE, de 22 de maio de 2014 (processo 11/13.6T2ASL.E1).
[148] *"(...) [C]om os meios informáticos de que dispõe e o conhecimento das pessoas que são seus clientes habituais, fácil será aos Bancos traçar o perfil do utilizador (como o faz a Google em relação aos titulares das contas de correio electrónico), barrando as operações a quem, v.g. pela hora tardia e inusitada, tenta fazer "transferências" para terceiros, ou, pela repetição de transferências inusitada num curto lapso de tempo, enfim, tudo o que saia da normalidade que o cliente vem revelando, contribuindo assim para uma maior segurança do sistema, que se quer, até onde for possível, blindado."*.

reembolso imediato[149], foi o Banco condenado numa indemnização por danos não patrimoniais[150].

1.8. Ac. de 16 de abril de 2015 (Processo 971/13.7TJLSB.L1-8) - TRL

Em acórdão do TRL, datado de 16 de abril de 2015, encontramos a primeira decisão dos nossos tribunais, ao abrigo do RSP, em que os prejuízos decorrentes de uma operação não autorizada foram suportados pelo utilizador e não pelo Banco.

Da prova produzida resulta que, com grande probabilidade, os autores foram vítimas de *pharming*[151]. Estes, com a ajuda da filha[152], procuraram aceder à página do Banco, tendo sido redirecionados para uma página falsa onde divulgaram os códigos de segurança, bem como quase todas as combinações de números constantes do cartão matriz. Ora, refere o tribunal que nunca são solicitados, no ato de *login*, *"(...) os dígitos do cartão matriz, muito menos a totalidade dos mesmos (...)"*, constando tais avisos da página do Banco. Os dígitos do cartão matriz são pedidos aquando da confirmação da operação, e, mesmo aí, deve o ordenante introduzir somente uma das 64 combinações possíveis. Assim, apenas após esta quebra das regras de segurança por parte dos autores, e consequente partilha de quase todas as combinações do cartão matriz, o terceiro obteve os elementos que lhe permitiram realizar a operação não autorizada. *"Por isso, (...) fica provado que (...) fizeram uma utilização imprudente, negligente e descuidada desse serviço (...)"*, sendo excluída a imputação ao Banco dos prejuízos resultantes da operação não autorizada.

Após várias decisões que recusaram qualificar a conduta do utilizador como sequer levemente negligente, designadamente até em situações de *phishing*, o TRL decidiu-se pela censurabilidade da conduta do titular do instrumento de pagamento num caso de *pharming*, suportando este as perdas que resultaram da operação não autorizada[153]. Um acórdão em contramão naquela que vinha sendo a corrente jurisprudencial.

---

[149] Que onera o PSP, como vimos, por força do art. 71.º do RSP.
[150] Sobre a ressarcibilidade destes no âmbito da compensação pelos danos sofridos, em favor do utilizador e para além do respetivo direito ao reembolso, v. BARBOSA, MAFALDA MIRANDA, *Serviços de pagamentos…*, cit., pp. 607-611.
[151] E não *phishing*, como mal qualifica o Ministério Público em despacho reproduzido no acórdão.
[152] O tribunal entendeu que a comunicação dos códigos de segurança à filha não é apta a causar uma quebra de segurança, visto esta última atuar de acordo com os interesses dos autores.
[153] Aparentemente, a título de negligência grave.

1.9. Ac. de 21 de maio de 2015 (Processo 337/14.1YXLSB.L1-2) - TRL

Cerca de um mês mais tarde, surge nova decisão do TRL, datada de 21 de maio de 2015.

No acórdão em apreciação, a conta da autora foi movimentada com recurso ao código pessoal e três coordenadas do cartão matriz. Logo que tomou conhecimento da operação, a autora contactou o Banco com o intuito de bloquear o acesso à mesma. Pediu ainda a reposição dos montantes transferidos.

Não conseguido ilidir a presunção de culpa, e por ter recusado o imediato reembolso, o Banco não só suportou a totalidade dos prejuízos como incorreu, adicionalmente, em responsabilidade por danos não patrimoniais[154], à semelhança do que já se havia decidido no Ac. de 03 de março de 2015 (Processo 1727/13.2TJLSB.L1-1), do TRL.

1.10. Ac. de 25 de junho de 2015 (Processo 3052/11.4TBSTR.E1) – TRE

O acórdão em análise, do TRE, datado de 25 de junho de 2015, é o segundo em que, no âmbito do RSP, se imputaram os prejuízos resultantes de uma operação não autorizada ao utilizador.

Do enquadramento factual resulta que as autoras foram alvo de fraude informática[155], tendo a reprodução integral dos respetivos códigos numa página clonada, quando tentavam aceder à pagina do Banco, possibilitado a operação não autorizada. Entendeu o tribunal que a reprodução integral dos códigos de utilizador[156], apesar dos vários avisos divulgados pelo Banco, violou as regras de segurança básicas do contrato de *homebanking*. Tal divulgação, escreve-se, contraria a lógica do sistema de segurança. *"Assim sendo, não é a Ré responsável pela movimentação das contas de forma fraudulenta, porquanto a mesma se deveu a culpa exclusiva da A. BB, que não teve o cuidado devido ao executar o contrato a que estava vinculada, traduzida no fornecimento da totalidade dos dados do cartão matriz a terceiros."*.

[154] Em consequência da falta de reembolso das quantias transferidas, a autora viu-se impossibilitada de fazer pagamentos a credores. Com repercussões no seu bom nome.
[155] Mais concretamente, de *pharming*.
[156] Nomeadamente dos dígitos do cartão matriz, que são pelo PSP pedidos apenas parcialmente, operação a operação, em conjuntos de três algarismos.

Esta decisão, se enquadrada no panorama mais vasto da jurisprudência do RSP, tem vários pontos de interesse, concretamente: *(i)* após vários acórdãos, aqui passados em revista, em que se via excluída qualquer imputação dos prejuízos resultantes de uma operação não autorizada ao utilizador do serviço de *homebanking*, mesmo que a título de negligência leve, em 2015 os tribunais passam a adotar uma perspetiva tendencialmente mais crítica do comportamento do utilizador[157]; *(ii)* curiosamente, os dois primeiros casos em que os tribunais portugueses, ao abrigo do RSP, imputam ao utilizador os prejuízos resultantes de operações não autorizadas, envolvem fraude informática qualificável como *pharming*[158]; e *(iii)* até este momento temporal, os tribunais portugueses vinham abordando a repartição dos prejuízos resultantes de operações não autorizadas como um jogo de tudo ou nada: ora suportava o PSP todos os prejuízos, o que, ao abrigo do RSP, significa a inexistência de qualquer censura à conduta do utilizador, ora suportava o utilizador todos os prejuízos, estatuição reservada para quando se identifique negligência grave[159] ou dolo. A negligência leve continuava fora da jurisprudência nacional.

1.11. Ac. de 02 de fevereiro de 2016 (Processo 902/13.4TBCNT.C1) – TRC

No presente acórdão do TRC, datado de 02 de fevereiro de 2016, a autora é uma pessoa coletiva.

Sucintamente, da conta mantida pelos representantes da autora foram transferidas determinadas quantias, contra a vontade e sem autorização da mesma, não se tendo demonstrado que qualquer um dos representantes ou funcionários da autora tenha facultado o acesso a terceiros exteriores à pessoa coletiva e ficando igualmente por demonstrar, no entendimento sufragado pelo tribunal, qualquer conduta imprudente imputável à autora[160].

---

[157] Deixando este de ser visto como um utilizador incapaz, a que tudo se lhe perdoa.
[158] Onde, pelas razões atrás expostas, o comportamento do utilizador alvo deveria ser, em média, e sempre considerando todas as circunstâncias do caso concreto, merecedor de um menor grau de censura.
[159] Recorde-se que, nestes casos, o utilizador suporta os prejuízos até ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento. O que pode muito bem cobrir todos os prejuízos.
[160] Ficou ainda assim demonstrado que um dos sócios gerentes, que se assumia como utilizador autorizado perante o Banco, entregou os códigos de acesso a outro dos sócios gerentes que, por sua vez, os entregou a uma funcionária para efetuar diversos pagamentos, sem que tenha ocorrido qualquer comunicação ou registo de novos utilizadores perante o Banco. Das condições gerais do contrato de *homebanking* constava que a autora poderia proceder à adesão de novos utilizadores, desde que fosse preenchido um anexo para esse efeito, posteriormente enviado ao Banco. Embora, como refere o tribunal, esta cadeia de transmissões não retire os códigos da esfera de domínio da autora, e seja até necessário à atividade empresarial da autora que mais de uma pessoa tenha acesso à conta bancária, é igualmente verdade que tal partilha exponencia o

Decidiu o tribunal que fosse, pois, o Banco a assumir a totalidade dos prejuízos sofridos pela autora em resultado da operação não autorizada.

1.12. Ac. de 15 de março de 2016 (Processo 1063/12.1TVLSB.L1-1) – TRL

Em acórdão do TRL, datado de 15 de março de 2016, encontramos uma situação factual similar à do acórdão imediatamente anterior.

Neste, uma pessoa coletiva indicou como utilizador o respetivo sócio e gerente, que, por sua vez, partilhou as credenciais da conta de *homebanking* da pessoa coletiva com um terceiro, contabilista, que, embora agindo no interesse da mesma, não se encontrava designado como utilizador autorizado perante o Banco[161]. Ficou igualmente demonstrado, sem surpresa, que as operações não autorizadas foram concluídas com as credenciais do utilizador.

Decidiu o tribunal que, e contrariamente ao entendimento sufragado na sentença recorrida, o ato de cedência das credenciais de segurança a um contabilista não pode ser qualificado como negligência grave, pois: *(i)* não foi demonstrado o nexo de causalidade entre a operação não autorizada e o cedência das credenciais, ficando por provar de que modo o terceiro obteve acesso ao instrumento de pagamento; e *(ii) "[m]as também, e fundamentalmente, porque a apontada actuação (e ainda que tivesse dado causa à obtenção das credenciais de segurança) não pode ser qualificada como negligência grave"*. Na ausência de demonstração de uma quebra de segurança imputável ao utilizador, foi o Banco condenado a reembolsar a totalidade das quantias transferidas à revelia do titular do instrumento de pagamento, acrescidas de juros de mora e do ressarcimento de outros prejuízos que resultaram da recusa do imediato reembolso.

Estes dois últimos acórdãos são representativos de uma tendência já aqui explicitada: os tribunais portugueses continuavam a abordar a repartição dos prejuízos resultantes de operações não autorizadas como um jogo de tudo ou nada, sendo a conduta

risco de apropriação abusiva do instrumento de pagamento por parte de terceiros. Os códigos do utilizador, pessoais e intransmissíveis, conhecidos por uma pessoa singular, passaram, por via de transmissões não comunicadas ao Banco, a ser conhecidos por mais duas pessoas singulares. Parece no mínimo discutível que o comportamento da autora (isto é, dos seus representantes) não seja qualificável como negligente na forma leve, devendo o instrumento de pagamento ser utilizado de acordo com as condições acordadas e assumindo-se a obrigação de manutenção da confidencialidade, assim como a de comunicação, ainda que para situações distintas, como uma trave mestra das obrigações do utilizador ao abrigo da DSP e do RSP.

[161] É de notar que o tribunal de primeira instância considerou que tal partilha é reveladora de culpa grosseira – um *plus* face à negligência leve por nós sugerida na análise do acórdão anterior – e absolveu o réu do pedido.

do utilizador de *homebanking* ora qualificada como negligente na forma grave ou grosseira[162], ora qualificada como irrepreensível segundo o padrão de diligência do homem médio. A problematização da negligência leve, enquanto modalidade de culpa potencialmente subsumível a alguns dos comportamentos que chegavam aos tribunais nacionais, não ocorria, pois, tampouco nos casos de partilha dos códigos de acesso no interesse e dentro da esfera de controlo de uma determinada pessoa coletiva.

1.13. Ac. de 13 de outubro de 2016 (Processo 2513/14.8TBVFR.P1) – TRP

Em acórdão do TRP, datado de 13 de outubro de 2016, encontramos a primeira decisão, em sede de RSP, em que a conduta do utilizador e titular do instrumento de pagamento é qualificada como negligente na forma leve.

Aproximadamente duas semanas antes da ocorrência das operações não autorizadas, quando o utilizador tentava realizar uma transferência na página do Banco, foi-lhe solicitada a indicação do número e modelo do seu telemóvel. Tendo preenchido esses mesmos dados, o utilizador, inadvertidamente, facultou informações essenciais à realização das operações não autorizadas[163]. As duas operações não autorizadas foram realizadas com um dia de dilação entre as mesmas, e após algumas tentativas falhadas, pelo que o Banco poderia ter impedido a ordem, ou pelo menos rejeitado a execução. Todavia, e em vez de impedir qualquer execução, preventivamente, limitou-se a telefonar ao titular do instrumento de pagamento no dia seguinte.

Entendeu o tribunal que *"[a] falta de cuidado usada pelo A. não vai além da culpa leve ou mesmo levíssima, já que se prevê que os deveres de cuidado omitidos poderiam sê-lo por grande número de utilizadores, porventura a maior parte face ao modo como lhe surgiu o pedido de simples e vulgares dados, se não tivessem tido a oportunidade de ler, em tempo útil, informação detalhada sobre o dever de não serem fornecidos aqueles dados do telemóvel (...)"*. Porquanto decidiu que o utilizador deveria suportar € 300,00 dos prejuízos globais, num máximo de € 150,00 por operação.

O racional usado nesta decisão é, salvo melhor opinião, de aplaudir. O utilizador, de forma descuidada, ainda que não especialmente descuidada e certamente não intencional, acabou por viabilizar as duas operações não autorizadas subsequentes.

[162] V. a sentença recorrida a que se fez referência.
[163] Trata-se, pois, de um caso de *pharming*, como bem qualifica o tribunal.

Justifica-se, dentro do espírito e letra da DSP e RSP, que suporte danos até ao montante de € 150,00 por operação[164].

1.14. Ac. de 14 de dezembro de 2016 (Processo 1063/12.1TVLSB.L1.S1) – STJ

Em acórdão do STJ, datado de 14 de dezembro de 2016, encontramos o recurso de um outro anteriormente analisado[165].

Defende-se no acórdão em análise, sumariamente, que a obrigação do utilizador é tomar todas as medidas razoáveis para que os dispositivos de segurança não cheguem ao conhecimento de terceiros que os possam usar abusivamente, não violando tal obrigação quando partilha o instrumento de pagamento com um contabilista. Citando, *"[a] entrega (...) à referida contabilista do código de acesso e do cartão matriz não era, assim, por si só, idónea a comprometer a segurança do sistema. Tudo se passou (e passaria) como se fosse o autor a aceder às contas, não se saindo da esfera de actuação deste. A quebra de segurança resultou antes da intromissão abusiva de terceiros, que lograram, por meio desconhecido, obter os dispositivos de segurança que permitiram o acesso às aludidas contas."*.

A corrente jurisprudencial, nesta matéria, encontra-se clara e inequivocamente identificada: a partilha de um instrumento de pagamento com, e na falta de melhor expressão, um utilizador não autorizado, desde que ocorra dentro da esfera de controlo do titular da conta bancária, não merece censura.

1.15. Ac. de 12 de outubro de 2017 (Processo 4761/15.4T8VNG-2) – TRL

No presente acórdão do TRL, datado de 12 de outubro de 2017, a autora, pessoa coletiva, procurava ser ressarcida na sequência de um conjunto de operações não autorizadas.

Entendeu o tribunal que ficou por demonstrar o concreto modo pelo qual o terceiro obteve acesso ao instrumento de pagamento, bem como a censurabilidade da conduta da autora, nomeadamente por inobservância das regras de cuidado a que o utilizador de

[164] As maiores dúvidas podem resultar de estarmos perante fraude informática qualificável como *pharming*. Tal qualificação não tem sido, contudo, devidamente ponderada na jurisprudência nacional.
[165] V. ac. do TRL, de 15 de março de 2016 (processo 1063/12.1TVLSB.L1-1).

homebanking se obrigou por força da adesão ao serviço[166]. Assim, suportou o Banco todos os prejuízos decorrentes da intromissão por parte de terceiro.

1.16. Ac. de 21 de dezembro de 2017 (Processo 1318/09.2TBTNV.L1-6) – TRL

No acórdão em análise, do TRL, datado de 21 de dezembro de 2017, encontramos um exemplo adicional das dificuldades que o PSP enfrenta no momento da prova.

Em síntese, o PSP não provou o modo pelo qual os terceiros levaram a cabo as operações não autorizadas, à revelia dos autores, *"(...) apenas se sabendo que foram introduzidos os seus dados pessoais (credenciais de segurança) para utilização do sistema de pagamento, não se tendo apurado por quem e em que circunstâncias."*.

Ficando por demonstrar a quebra de segurança, e, designadamente, se e em que medida poderia esta ser imputada ao titular do instrumento de pagamento, suportou o Banco todos os prejuízos emergentes das operações não autorizadas.

2. Apreciação crítica

A jurisprudência do RSP leva, sensivelmente, cinco anos. Contudo, cabe notar que o RSP chegou aos nossos tribunais após várias decisões onde se discutiam as consequências da fraude informática e operações não autorizadas ao abrigo do CC e da lei que regula as cláusulas contratuais gerais. Pensar-se-ia, portanto, que alguns dos critérios jurídicos pudessem encontrar-se devidamente maturados.

Em primeiro lugar, identificam-se confusões aquando da identificação da modalidade de fraude informática em causa[167], não sendo, por vezes, tampouco devidamente ponderadas as consequências que tal qualificação pode assumir na censurabilidade da conduta do utilizador[168]. Embora sejam significativamente mais numerosas as situações de *pharming* que chegam aos tribunais superiores, e não se possa subsumir, automática e acriticamente, a conduta do utilizador a um grau de culpa em função da modalidade de fraude informática de que este seja vítima, já que devem ser ponderadas todas as circunstâncias do caso concreto, é surpreendente que, na jurisprudência do RSP dos nossos tribunais superiores, as poucas situações em que o

[166] Não se criou o convencimento, sequer, que o utilizador tenha divulgado as credenciais de segurança em resultado de fraude informática.
[167] V. ac. do TRP, de 07 de outubro de 2014 (processo 747/12.9TJPRT.P1).
[168] V. ac. do STJ, de 18 de dezembro de 2013 (processo 6479/09.8TBBRG.G1.S1), onde se pode ler que a distinção não tem implicações.

utilizador assumiu os prejuízos decorrentes de uma operação não autorizada envolvam *pharming*[169], não merecendo reprovação condutas análogas do utilizador vítima de *phishing*[170].

Em segundo lugar, suscitam dúvidas aquelas situações em que um utilizador, atuando no interesse de uma pessoa coletiva, partilha as credenciais de segurança com outrem, nomeadamente um funcionário da mesma, que não se encontra devidamente registado como utilizador perante o PSP. A jurisprudência dos tribunais superiores tem sido unânime: desde que tal partilha não retire os códigos da esfera de domínio da pessoa coletiva, não merece censura[171]. Salvo melhor entendimento, essa não aparenta ser a solução do legislador, que no art. 72.º/1 do RSP refere a mera *"(...) quebra da confidencialidade dos dispositivos de segurança personalizados imputável ao utilizador (...)"*, e tornaria o ónus da prova do PSP, já de si bastante dificultado[172], potencialmente impossível de operar. Levado ao extremo, o argumento possibilitaria que centenas de colaboradores de uma grande empresa tivessem acesso às credenciais de um único utilizador autorizado. Com o devido respeito, parece também de difícil sustentação a tese de que a partilha, desde que dentro da esfera de controlo da pessoa coletiva, não constitui um comportamento suscetível de comprometer a segurança do sistema. Tal partilha aumenta a esfera de risco e o número de potenciais alvos de fraude informática. Adicionalmente, a obrigatoriedade de sigilo e não transmissão dos códigos pessoais e intransmissíveis a terceiros é, como vimos, um dos principais encargos que incide sobre o utilizador de *homebanking*[173].

Em terceiro lugar, observa-se que, mesmo quando a quebra de confidencialidade é imputável ao utilizador, os tribunais são tendencialmente benevolentes para com este. Nem mesmo os avisos e recomendações publicados pelos Bancos, procurando

[169] V. ac. do TRL, de 16 de abril de 2015 (processo 971/13.7TJLSB.L1-8), ac. do TRE, de 25 de junho de 2015 (processo 3052/11.4TBSTR.E1) e ac. do TRP, de 13 de outubro de 2016 (processo 2513/14.8TBVFR.P1).
[170] V. ac. do TRP, de 29 de abril de 2014 (processo 225/12.6TJVNF.P1).
[171] V. ac. do TRC, de 02 de fevereiro de 2016 (processo 902/13.4TBCNT.C1), ac. do TRL, de 15 de março de 2016 (processo 1063/12.1TVLSB.L1-1) e ac. do STJ, de 14 de dezembro de 2016 (processo 1063/12.1TVLSB.L1.S1).
[172] Recorde-se que o PSP é várias vezes malsucedido na sua tentativa de demonstração do modo pelo qual o terceiro obteve acesso às credenciais de segurança e ordenou a operação não autorizada, v. ac. do TRL, de 05 de novembro de 2013 (processo 9821/11.8T2SNT.L1-1), ac. do TRG, de 17 de dezembro de 2014 (processo 1910/12.8TBVCT.G1), ac. do TRL, de 12 de outubro de 2017 (processo 4761/15.4T8VNG-2) e ac. do TRL, de 21 de dezembro de 2017 (processo 1318/09.2TBTNV.L1-6).
[173] Resultando da lei, e sendo, geralmente, repetido nas cláusulas contratuais gerais a que o utilizador adere.

conscientizar os utilizadores do seu serviço de *homebanking* para os perigos associados à utilização do instrumento de pagamento, parecem convencer os nossos tribunais de que o comportamento do utilizador que divulga, involuntariamente, as suas credenciais de segurança a um terceiro é censurável[174]. Poderá admitir-se que esta negação da imputação dos prejuízos na esfera jurídica do utilizador resulte de, à data da prática dos factos, os riscos associados à fraude informática não se encontrarem devidamente divulgados junto do utilizador comum. Certo é que, com o esforço de conscientização que tem sido feito, desde logo por parte dos Bancos, esperar-se-á que em novos acórdãos se adote um crivo mais exigente aquando da análise da conduta do titular do instrumento de pagamento. Parece existir uma ligeira tendência de inversão, nesse sentido, tendo sido parcialmente quebrada a corrente jurisprudencial, em sede do RSP, que vinha imputando os prejuízos decorrentes de operações não autorizada exclusivamente ao PSP.

Em quarto lugar, e analisando os acórdãos que decidiram pela imputação dos prejuízos ao utilizador a título de negligência grave[175], o critério para a imputação merece inteiro acolhimento: ainda que perante fraude informática qualificável como *pharming*, age de modo censurável, potencialmente com especial descuidado, o utilizador que não se limita a inserir as credenciais de segurança que habitualmente lhe são solicitadas pelo seu Banco mas, antes, divulga a quase totalidade das combinações do cartão matriz ou outras informações que o PSP não tenha por hábito solicitar aquando da confirmação da ordem de pagamento, nomeadamente a marca, modelo e número de telemóvel, desde que de tal facto se tenha dado conhecimento ao utilizador[176].

Por último, resulta das várias decisões analisadas que a negligência leve não tem sido adequadamente equacionada na aferição da culpa do utilizador[177], tendo a primeira e única decisão nesse sentido ocorrido no último trimestre de 2016[178] e repetindo-se os acórdãos que imputam os prejuízos inteiramente na esfera jurídica do PSP ou, menos frequentemente, do utilizador. Uma correta ponderação da negligência leve, enquanto alternativa imediata à imputação a título de negligência grosseira, afigura-se como um

[174] V. ac. do TRE, de 22 de maio de 2014 (processo 11/13.6T2ASL.E1) e ac. do TRP, de 07 de outubro de 2014 (processo 747/12.9TJPRT.P1).
[175] V. ac. do TRL, de 16 de abril de 2015 (processo 971/13.7TJLSB.L1-8) e ac. do TRE, de 25 de junho de 2015 (processo 3052/11.4TBSTR.E1).
[176] Em concordância, v. GUIMARÃES, MARIA RAQUEL, *As operações fraudulentas...*, CEJUR, Braga, 2015, p. 26.
[177] No mesmo sentido, v. CORREIA, FRANCISCO MENDES, *Operações não autorizadas…*, cit., pp. 725-727.
[178] V. ac. do TRP, de 13 de outubro de 2016 (processo 2513/14.8TBVFR.P1).

passo necessário para uma maior equidade nas decisões. Dado o teto máximo aplicável aos prejuízos que o utilizador pode suportar nesses casos, presente tanto na DSP como na DSP2, nem se poderá concluir que tal qualificação desoneraria o PSP de suportar a maior fatia dos prejuízos.

V. CONCLUSÕES

I. O *homebanking* apresenta-se como um canal de prestação de serviços bancários, possibilitado pelo desenvolvimento tecnológico, surgindo no âmbito de uma relação entre Banco e cliente bancário que se inicia aquando da abertura de conta.

II. O conteúdo do contrato de utilização de instrumento de pagamento é *standardizado*, encontrando-se geralmente vedado a negociação e sendo a autonomia privada do cliente bancário manifestada aquando da adesão. Tratando-se de um contrato quadro, facilita operações bancárias futuras.

III. Da utilização do instrumento de pagamento em análise advêm riscos distintos dos presentes na banca tradicional. Fruto da relevância que assumem nas operações não autorizadas, destacámos o *phishing* e o *pharming*, modalidades de fraude informática presentes na jurisprudência dos tribunais nacionais.

IV. No *phishing*, existe uma manifestação externa do intuito fraudulento de um terceiro, concretizada num *e-mail* ou mensagem. Por outro lado, no *pharming*, apenas ocorre uma adulteração de endereço IP, sendo o utilizador redirecionado para página falsa quando procura, autonomamente, aceder a um determinado sítio *online*.

V. Os serviços de pagamento têm merecido uma regulação de base comunitária. A DSP significou um importante passo de harmonização neste domínio, visando a harmonização total.

VI. Transposta para o ordenamento jurídico interno pelo RSP, comporta um conjunto de obrigações orientadas para o PSP e para o utilizador. As operações não autorizadas nascem, habitualmente, do incumprimento de alguma das obrigações que vinculam as partes, embora não seja necessariamente assim.

VII. Identificada uma operação não autorizada, o PSP tem o ónus da prova. Num primeiro momento, incide sobre este a obrigação de reembolsar imediatamente o titular do instrumento de pagamento. Num segundo momento, interessará ao PSP discutir a repartição dos prejuízos em função da culpa imputável ao utilizador.

VIII. Ocorrendo a comunicação, por parte do utilizador ao PSP, da perda, do roubo, da apropriação abusiva ou de qualquer utilização não autorizada do instrumento de pagamento, e inexistindo fraude do utilizador, o PSP suportará todas as perdas resultantes

de operações não autorizadas que se produzam desde esse momento em diante. O PSP assumirá, igualmente, todos os prejuízos que resultem de operações não autorizadas sempre que não os possa imputar ao utilizador a título de culpa.

IX. O PSP responde objetivamente pelos prejuízos, independentemente de culpa, por ser sobre este que recai a obrigação de assegurar um serviço eficiente e seguro. Na DSP2, a *ratio* do esquema de repartição de prejuízos emerge particularmente nítida, suportando o PSP todos os prejuízos que ocorram, exceto quando haja fraude do utilizador, caso não imponha a SCA.

X. A DSP2, ainda não transposta para o ordenamento jurídico interno aquando da entrega do presente texto, mantém, no essencial, o esquema de repartição de prejuízos estabelecido pela DSP.

XI. As maiores novidades, neste âmbito, prendem-se com a possibilidade, excecional, de recusa do reembolso imediato por parte do PSP, bem como pela introdução da SCA. A EBA vem assumindo um papel relevante na concretização destas matérias.

XII. Em sede da jurisprudência do RSP – e sem prejuízo da apreciação crítica realizada no ponto IV.2, para a qual se remete –, concluiu-se que as modalidades da fraude informática, bem como a sua importância aquando da aferição da culpa do utilizador, ainda não aparentam encontrar-se devidamente assimiladas.

XIII. Uma tendência dos nossos tribunais passa pela consideração de que a partilha das credenciais de segurança, desde que dentro da esfera de controlo de uma pessoa coletiva, não preenche o conceito de quebra de confidencialidade imputável ao utilizador. Argumentou-se que tal interpretação não parece coadunar-se com o espírito da DSP e do RSP. Casuisticamente, poderá também impossibilitar a prova do PSP.

XIV. Ademais, e embora com uma suavização, que se saúda, em várias das decisões analisadas parece adotar-se um padrão de ingenuidade do utilizador médio que, salvo melhor opinião, não se justifica. Uma adequada utilização da negligência leve, que aparenta estar subjacente a algumas das condutas identificadas, afigura-se tão necessária quanto útil à equidade da jurisprudência do RSP, ainda frequentemente de tudo ou nada, no trilho de uma corrente jurisprudencial que fomente a autorresponsabilidade do titular do instrumento de pagamento.

XV. Em sentido oposto, é de acolher a tese que age com negligência, porventura grosseira, o utilizador que, sendo alvo de fraude informática, divulga a totalidade das combinações do cartão matriz ou outras informações que o PSP não tenha por hábito solicitar aquando da confirmação da ordem de pagamento, na medida em que tal divulgação contraria a lógica do sistema.

XVI. Por fim, a DSP2 não deverá comportar alterações substanciais às decisões em matéria de repartição dos prejuízos resultantes de operações não autorizadas. Fruto da implementação da SCA, a maior expetativa prende-se com a diminuição do número de operações não autorizadas, e, consequentemente, com a redução da frequência de decisões dos nossos tribunais nesta matéria. Contudo, o aguçar do engenho fraudulento, e a sua capacidade de mutação, poderão trazer novos desafios.

VI. ÍNDICE BIBLIOGRÁFICO

ALMEIDA, FERREIRA DE

– *Contrato Bancário Geral e Deposito Bancário* in *Direito Bancário*, Centro de Estudos Judiciários (CEJ), Lisboa, 2015;

– *Contratos II*, 4.ª edição, Almedina, Coimbra, 2016;

ANTUNES, JOSÉ ENGRÁCIA

– *Direito dos Contratos Comerciais*, 3.ª reimpressão da edição de 2009, Almedina, Coimbra, 2014;

– *Os contratos bancários* in *Estudos em Homenagem ao Professor Doutor Carlos Ferreira de Almeida – Volume II*, Almedina, Coimbra, 2011;

BARBOSA, MAFALDA MIRANDA, *Serviços de pagamentos, repartição do risco e responsabilidade civil – algumas reflexões a propósito da nova diretiva dos serviços de pagamentos (DSP2)* in *Revista de Direito Comercial*, 2017;
Disponível em revistadedireitocomercial.com (consultado em fevereiro de 2018)

BARREIRA, MARIA CAROLINA, *Home Banking – A repartição dos prejuízos decorrentes de fraude informática*, Dissertação de Mestrado em Direito – Ciências Jurídicas Empresariais, Faculdade de Direito da Universidade Nova de Lisboa (FDUNL), Lisboa, 2015;

CAMPOS, DIANA, CARMO, MARIA, *Home Banking: Consequências jurídicas*, Governance Lab, 2017;
Disponível em governancelab.org (consultado em agosto de 2017)

CORDEIRO, ANTÓNIO MENEZES

– *Direito Bancário*, 6.ª edição, Almedina, Coimbra, 2016;

– *Tratado de Direito Civil – Volume II*, 4.ª edição, Almedina, Coimbra, 2014;

– *Tratado de Direito Civil – Volume II, Tomo III*, Almedina, Coimbra, 2010;

– *Tratado de Direito Civil – Volume VI*, 2.ª edição, Almedina, Coimbra, 2012;

CORREIA, FRANCISCO MENDES

– *Moeda bancária e cumprimento: o cumprimento das obrigações pecuniárias através de serviços de pagamento*, Dissertação de Doutoramento em Direito – Ciências Jurídicas, Faculdade de Direito da Universidade de Lisboa (FDL), Lisboa, 2014;

– *Operações não autorizadas e o Regime Jurídico dos Serviços de Pagamento e da Moeda Electrónica* in *Revista de Direito Civil, ano II, n.º 3*, Almedina, Coimbra, 2017;

COSTA, ALMEIDA, *Direito das Obrigações*, 12.ª edição, Almedina, Coimbra, 2012;

FARIA, JOSÉ MANUEL

– *Acesso a contas bancárias por terceiros no âmbito de operações de pagamento* in *Revista da banca, n.º 71*, Associação Portuguesa de Bancos, Lisboa, 2011;

– *Evolução recente da regulação dos serviços de pagamento da União Europeia* in *Estudos em Homenagem ao Professor Doutor Carlos Pamplona Corte-Real*, Almedina, Coimbra, 2016;

FONSECA, GISELA, *Utilização abusiva de cartão bancário – A repartição do risco entre emitente e titular*, Dissertação de Mestrado em Direito – Ciências Jurídico-Bancárias, Faculdade de Direito da Universidade de Lisboa (FDL), Lisboa, 2011;

GERALDES, ANA VAZ, *Phishing: fraude on line* in *Revista da Faculdade de Direito da Universidade de Lisboa, Volume 54, n.os 1 e 2*, Coimbra Editora, Coimbra, 2013;

GOMES, JANUÁRIO DA COSTA, *Contratos Comerciais*, Almedina, Coimbra, 2012;

GUIMARÃES, MARIA RAQUEL

– *A fraude no comércio electrónico: o problema da repartição do risco por pagamentos fraudulentos* in *Infrações económicas e financeiras: estudos de criminologia e direito*, Coimbra Editora, Coimbra, 2013;

– *A repartição dos prejuízos decorrentes de operações fraudulentas de banca electrónica (home banking): acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09* in *Cadernos de Direito Privado n.º 41*, Centro de Estudos Jurídicos do Minho (CEJUR), Braga, 2013;

– *As operações fraudulentas de homebanking na jurisprudência recente – Ac. do STJ de 18.12.2013, Proc. 6479/09* in *Cadernos de Direito Privado, n.º 49*, CEJUR, Braga, 2015;

– *As transferências electrónicas de fundos e os cartões de débito*, Almedina, Coimbra, 1999;

– *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos*, Coimbra Editora, Coimbra, 2011;

– *Os Contratos-Quadro de Prestação de Serviços de Pagamento* in *I Congresso de Direito do Consumo*, Almedina, Coimbra, 2016;

– *(Ainda) a responsabilidade pelo uso indevido de instrumentos de pagamento electrónicos em operações presenciais e à distância* in *I Congresso de Direito Bancário*, Almedina, Coimbra, 2015;

JAKOBSSON, MARKUS, MYERS, STEVEN, *Phishing and Countermeasures*, Wiley, Nova Jérsia, 2007;

KOOPS, BERT-JAAP, *The Internet and its Opportunities for Cybercrime*, 2010;
Disponível em papers.ssrn.com (consultado em agosto de 2017)

LEITÃO, LUÍS MENEZES, *Direito das Obrigações – Volume I*, 10.ª edição, Almedina, Coimbra, 2013;

LEIVA, FRANCISCO MUÑOZ, *Marketing financiero*, Copicentro Editorial, Granada, 2011;

LIMA, RAQUEL, *A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na jurisprudência portuguesa*, Dissertação de Mestrado em Direito – Ciências Jurídico-Privatísticas, Faculdade de Direito da Universidade do Porto (FDUP), Porto, 2015;

MARQUES, GARCIA, MARTINS, LOURENÇO, *Direito da Informática*, 2.ª edição, Almedina, Coimbra, 2006;

MAVROMATI, DESPINA, *The Law of Payment Services in the EU: The EC Directive on Payment Services in the Internal Market*, Kluwer Law International, Alphen aan den Rijn, 2008;

MONTEIRO, ANTÓNIO PINTO

– *A resposta do ordenamento jurídico português à contratação bancária pelo consumidor* in *Boletim de Ciências Económicas – Volume LVII, Tomo II*, Faculdade de Direito da Universidade de Coimbra (FDUC), Coimbra, 2014;

– *Banca e cláusulas contratuais gerais (Breve apontamento)* in *I Congresso de Direito Bancário*, Almedina, Coimbra, 2015;

MONTEIRO, JORGE SINDE, *Responsabilidade civil* in *Revista de Direito e Economia*, *n.º 2*, Universidade de Coimbra (UC), Coimbra, 1978;

MORAIS, GRAVATO, *A utilização fraudulenta de cartões de crédito na contratação à distância* in *Estudos em comemoração do 10.º aniversário da licenciatura em direito da Universidade do Minho*, Almedina, Coimbra, 2003;

PEREIRA, JOEL, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris - Sociedade Editora, Lisboa, 2004;

PRATA, ANA, *Cláusulas de exclusão e limitação da responsabilidade contratual*, Almedina, Coimbra, 1985;

ROSSI, CLIFFORD, *A Risk Professional's Survival Guide: Applied Best Practices in Risk Management*, Wiley, Nova Jérsia, 2014;

SANTOS, HUGO LUZ DOS, *Plaidoyer por uma "distribuição dinâmica do ónus da prova" e pela "teoria das esferas de risco" à luz do recente Acórdão do Supremo Tribunal de Justiça, de 18/12/2013: o (admirável) "mundo novo" no homebanking?* In *O Direito, A. 147, n.º 3*, Almedina, Coimbra, 2015;

SÁ, ALMENO DE, *Direito Bancário*, Coimbra Editora, Coimbra, 2008;

SILVA, CALVÃO DA

– *Banca, Bolsa e Seguros*, 4.ª edição, Almedina, Coimbra, 2013;

– *Conta corrente bancária: operação não autorizada e responsabilidade civil* in *Revista de Legislação e Jurisprudência a. 144, n.º 3991*, Coimbra Editora, Coimbra, 2015;

– *Direito bancário: Relatório apresentado para a prestação de provas de Agregação (Ciências Jurídicas), na Faculdade de Direito da Universidade de Coimbra*, Almedina, Coimbra, 2001;

– *Serviços de pagamento e responsabilidade civil* in *Estudos em Homenagem a Rui Machete*, Almedina, Coimbra, 2015;

SOARES, QUIRINO, *Contratos Bancários* in *Scientia Iuridica, Tomo 52, n.º 295*, Universidade do Minho (UM), Braga, 2003;

STEENNOT, REINHARD, *Allocating liability in case of fraudulent use of electronic payment instruments and the Belgian mobile payment instrument pingping*, Financial Law Institute, Gante, 2010;
Disponível em biblio.ugent.be (consultado em agosto de 2017)

TELLES, INOCÊNCIO GALVÃO, *Direito das obrigações*, 7.ª edição, Coimbra Editora, Coimbra, 1997;

TRAUTMAN, LAWRENCE J., *E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from PayPal*, 2016;
Disponível em papers.ssrn.com (consultado em setembro de 2017)

VANHOOSE, DAVID D., *Internet Banking*, 2009;
Disponível em papers.ssrn.com (consultado em setembro de 2017)

VARELA, ANTUNES, *Das Obrigações em Geral – Volume I*, 10.ª edição, Almedina, Coimbra, 2003;

VASCONCELOS, Joana, *Sobre a repartição entre titular e emitente do risco de utilização abusiva do cartão de crédito no direito português* in *Estudos em homenagem ao Prof. Doutor Inocêncio Galvão Telles – Volume II*, Almedina, Coimbra, 2002;

VASCONCELOS, PESTANA DE, *Dos contratos de depósito bancário* in *Revista da FDUP - A. 8*, Coimbra Editora, Coimbra, 2011;

VERDELHO, PEDRO, *Phishing e outras formas de defraudação nas redes de comunicação* in *Direito da sociedade da informação – Volume 8*, Coimbra Editora, Coimbra, 2009.

VII. ÍNDICE DE JURISPRUDÊNCIA

– proc. n.º 4761/15.4T8VNG-2, de 12/10/2017. Relator MARTINS, PEDRO;
Disponível em dgsi.pt (consultado em fevereiro de 2018)
– proc. n.º 1318/09.2TBTNV.L1-6, de 21/12/2017. Relator RODRIGUES, MANUEL;
Disponível em dgsi.pt (consultado em fevereiro de 2018)

TRIBUNAL DA RELAÇÃO DO PORTO
– proc. n.º 225/12.6TJVNF.P1, de 29/04/2014. Relator MATOS, FRANCISCO;
Disponível em dgsi.pt (consultado em fevereiro de 2018)
– proc. n.º 747/12.9TJPRT.P1, de 07/10/2014. Relatora CABRAL, ANA LUCINDA;
Disponível em dgsi.pt (consultado em fevereiro de 2018)
– proc. n.º 2513/14.8TBVFR.P1, de 13/10/2016. Relator CAROÇO, FILIPE.
Disponível em dgsi.pt (consultado em fevereiro de 2018)