Revista Electrónica de Direito

Home banking:

A Repartição dos prejuízos decorrentes de fraude informática

Home banking: the allocation of losses due to computer fraud

Carolina França Barreira

Mestre em Ciências Jurídicas Empresariais pela Faculdade de Direito da Universidade Nova de Lisboa e Advogada Estagiária

Maio de 2015

RESUMO:

O objeto do presente texto consiste no estudo do serviço de *home banking* e de como se processa a repartição dos prejuízos decorrentes de fraude informática no âmbito deste serviço.

Na procura da resposta à questão da repartição das perdas resultantes de operações fraudulentas, importa atender, principalmente, ao comportamento do utilizador do serviço de *home banking*.

Na nossa opinião, os tribunais têm sido demasiado exigentes para com o utilizador no julgamento da sua atuação na utilização deste serviço.

Neste estudo, concluímos que, quando o utilizador "cai" num esquema de fraude informática, não deverá ser-lhe imputado um comportamento gravemente negligente, mesmo que este tenha, em virtude da fraude, revelado todos os seus códigos de acesso a um pirata informático, numa página que se assemelha à do seu banco. Em regra, tais factos não serão suficientes para merecer a qualificação da atuação do utilizador como gravemente negligente. Consequentemente, o utilizador, nos termos do Regime dos Serviços de Pagamento, deve suportar os prejuízos até ao limite máximo de € 150, arcando o banco com o remanescente das perdas.

Já se o utilizador, vítima de uma técnica fraudulenta, ignorou os avisos de segurança emitidos pela entidade bancária, deve-se considerar, sempre atendendo ao caso concreto, que contribuiu com negligência grave para a ocorrência de operações de pagamento não autorizadas. Assim, o utilizador deve suportar a totalidade dos prejuízos advindos até à comunicação ao banco do sucedido.

Compete à entidade bancária, no caso concreto, fazer prova da contribuição do cliente para as perdas ocorridas.

PALAVRAS-CHAVE: *home banking*; banco; fraude informática; *phishing*; códigos de acesso; serviços de pagamento.

ABSTRACT:

The object of this investigation is focused on the study of the home banking service and how the allocation of losses due to computer fraud is processed in the scope of this service.

When considering the questions raised by the allocation of losses associated with fraudulent operations, it is important to consider, mainly, the behaviour of the user of the home banking service.

In our opinion, courts have been too demanding towards the user when judging his action in the use of this service.

In this study, we have concluded that, when the user “falls” into a computer fraud scheme, he should not be liable for gross negligent behaviour, even if, due to the fraud, the user revealed all his access codes to a hacker on a page similar to that of his bank.

In general, such facts will not be sufficient to qualify the user’s action as grossly negligent. Therefore, the user, under the terms of the Payment Services’ System, must bear the loss up to a maximum of €150, and the bank will face the remainder of the losses.

However, if the user, victim of a fraudulent technique, ignored the safety warnings issued by the bank, one must consider, given the specific case, that he contributed to gross negligence in unauthorised payment transactions. Thus, the user must bear all the losses up to the moment when he notifies the bank about the unauthorised transactions.

It is the bank’s responsibility to, given the specific case, adduce evidence of the client’s contribution to the identified losses.

KEY WORDS: home banking; bank; computer fraud; phishing; access codes; payment services.

SUMÁRIO*:

1. Introdução

2. *Home banking*

2.1. Noção

2.2. A sua inserção num complexo contratual

2.2.1. Relação com o contrato de abertura de conta

2.2.2. Relação com o contrato de depósito bancário

2.3. Caracterização do contrato de *home banking*

2.3.1. Como contrato de adesão

2.3.2. Como contrato-quadro

2.4. Conteúdo da relação contratual

2.4.1. Os serviços abrangidos

2.4.2. Obrigações que vinculam as partes

a) Deveres do utilizador

b) Deveres do prestador de serviços de pagamento

3. A fraude e a segurança do sistema informático

3.1. O sistema bancário na sua vertente telemática

3.2. A fraude nas operações de banca eletrónica

3.2.1. *Phishing*

3.2.2. *Pharming*

3.2.3. Distinção entre as duas modalidades de fraude informática. Enquadramento legal.

3.3. A identificação do tipo de fraude informática pelos tribunais superiores

4. A repartição dos prejuízos decorrentes de fraude informática no contrato de *home banking*

4.1. Apresentação da problemática

4.2. Solução anterior à entrada em vigor do RSP

4.3. O regime vigente

4.3.1. Notas prévias

4.3.2. Atribuição do ónus da prova à entidade bancária

* Este estudo corresponde à versão revista do texto apresentado como Dissertação de Mestrado com vista à obtenção do grau de Mestre em Ciências Jurídicas Empresariais na Faculdade de Direito da Universidade Nova de Lisboa, sob orientação da Professora Doutora Margarida Lima Rego.

4.3.3. Importância da notificação e responsabilidade pelas perdas resultantes de operações não autorizadas após a comunicação da fraude

4.3.4. Dever de reembolso dos montantes indevidamente debitados

4.3.5. Responsabilidade pelos prejuízos decorrentes de operações não autorizadas antes da notificação ao banco

a) Negligência leve do utilizador

b) Negligência grave e dolo do utilizador

c) A imputação dos prejuízos ao utilizador e a fraude informática

d) A relevância dos avisos de segurança

4.4. Razão de ser da responsabilização da entidade bancária pelos prejuízos decorrentes de operações não autorizadas

5. Conclusão

Bibliografia

Jurisprudência

1. Introdução

A evolução tecnológica dos últimos anos revolucionou as relações bancárias tal como as concebemos na atualidade. Primeiro, apareceram os cartões de débito e de crédito que tornaram possível a realização de uma série de operações bancárias através de terminais de caixa automática e, mais recentemente, surgiu a possibilidade de aceder a todos esses serviços prestados à distância pelo banco através da internet – a esse serviço dá-se o nome de *home banking*.

Atendendo à sociedade da informação em que vivemos hoje, é facilmente compreensível a expansão do *home banking*. A sua vulgarização deve-se à utilidade e comodidade que proporciona aos seus utilizadores, assim como ao forte contributo do crescimento exponencial do número de utilizadores de internet[1].

Contudo, este desenvolvimento tecnológico traz novas preocupações, de entre as quais se destaca a pirataria informática. O *home banking* é um dos serviços mais atingidos por este problema uma vez que o seu acesso depende da utilização da internet. Procurando aceder às contas bancárias dos clientes e transferir fundos em proveito próprio, os piratas informáticos desenvolvem técnicas informáticas engenhosas e dissimuladas.

Com este estudo procuramos responder a algumas questões, de entre as quais: Que técnicas informáticas são estas? O que pode fazer o cliente quando se depara com o débito de quantias avultadas da sua conta bancária sem a sua autorização? Pode recuperar os montantes desviados? Como?

Numa frase, comprometemo-nos determinar quem suporta os prejuízos decorrentes da transferência fraudulenta de fundos da conta do cliente.

Assim, consideramos o *home banking* uma revelação do desenvolvimento tecnológico no que diz respeito às transferências eletrónicas de fundos mas que levanta complexos problemas de direito probatório, designadamente em matéria de distribuição do risco e de repartição do ónus da prova, dificuldades que nos empenhamos em esclarecer neste estudo[2].

Este tema, em particular no âmbito do *home banking*, nunca foi objeto de um estudo autónomo, tendo sido apenas tratado por MARIA RAQUEL GUIMARÃES numa anotação a um acórdão do Tribunal da Relação de Guimarães[3], análise essa que serviu de ponto de partida para o presente estudo[4].

---

[1] De acordo com dados de 2014, 65% das pessoas com idade entre 16 e 74 anos acedem à Internet em Portugal. Instituto Nacional de Estatística – Inquérito à utilização de tecnologias da informação e da comunicação pelas famílias 2014, novembro de 2014. In http://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=211422735&DESTAQUESmodo=2 (10/01/2015).

[2] Ac. TRL de 12/12/2013, Proc. 164/11.8TBSRT.L1-6 (Tomé Ramião) in http://www.dgsi.pt.

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

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

A relevância do trabalho que aqui apresentamos é comprovada pela abundante jurisprudência dos tribunais superiores sobre esta matéria nos últimos anos.

Este estudo é de direito civil, deixando de fora a vertente penal que a matéria suscita, nomeadamente as repercussões penais que envolvem a prática de fraude informática.

2. *Home banking*

2.1. Noção

Vulgarmente conhecido como *home banking* mas também referido como banco internético (do inglês *Internet banking*), *e-banking*, banco *online* ou banca eletrónica, é um serviço concedido pelas instituições bancárias aos seus clientes, permitindo-lhes executar uma série de operações bancárias, por telefone ou *online*, relativamente às contas de que sejam titulares[5].

Optamos pela utilização da expressão anglo-saxónica *home banking* e da expressão "banca eletrónica" na presente dissertação por serem as mais utilizadas pela doutrina e pela jurisprudência nacional para referir este serviço. Na análise das questões centrais em torno do *home banking* apenas nos vamos referir à sua execução via *online* por ser esse o âmbito em que tem surgido a maioria dos conflitos no que diz respeito a esta figura contratual.

A banca eletrónica tem apresentado uma crescente popularidade nos últimos anos dada a sua grande utilidade visto que, ao utilizar canais telemáticos que aliam meios informáticos a meios de comunicação à distância (canais de telecomunicação)[6], por via de uma página segura da entidade bancária, permite o acesso aos serviços do banco fora do horário de atendimento ou em qualquer local onde haja acesso à internet[7]. Deste modo, surge uma nova forma de relacionamento entre o banco e o cliente, proporcionando a este último todas (ou quase todas) as operações disponíveis nos balcões tradicionais da entidade bancária[8].

Através da prestação deste serviço, o banco reforça o compromisso com os seus clientes no sentido do aperfeiçoamento e desenvolvimento da atividade bancária, designadamente pela capacidade de resposta rápida e eficiente, sem prejuízo dos deveres de informação, lealdade, diligência e transparência[9] que são inerentes à confiança recíproca que existe no relacionamento banco-cliente. Mas não só. A entidade bancária também prossegue o

[5] Ac. STJ de 18/12/2013, Proc. 6479/09.8TBBRG.G1.S1 (Ana Paula Boularot) in http://www.dgsi.pt.
[6] Telemática é o nome dado ao "conjunto de técnicas e de serviços que recorrem simultaneamente à informática e às telecomunicações", cfr. GARCIA MARQUES, LOURENÇO MARTINS, Direito da Informática. 2ª edição, refundida e atualizada. Coimbra: Almedina, 2006, p. 748. Segundo ALAIN BENSOUSSAN, Informatique et télécoms. Levallois: Éditions Francis Lefebvre, 1997, p. 729, foi graças à informática que as redes de telecomunicações passaram a transportar não só voz, mas também texto e grafismos, dando origem à telemática.
[7] Ac. STJ de 18/12/2013 (Ana Paula Boularot), cit.
[8] RAMOS PEREIRA, Compêndio jurídico da sociedade da informação. Lisboa: Quid Iuris, 2004, p. 696.
[9] Art. 74º e 77º do Regime Geral das Instituições de Crédito e Sociedades Financeiras (RGICSF) – DL n.º 298/92 de 31 de dezembro com as alterações introduzidas pelo DL n.º 1/2008, de 3 de janeiro.

princípio da simplicidade através do recurso ao uso da informática[10]. Este princípio traduz-se na redução ao mínimo de qualquer diligência dispensável que apenas represente um custo de transação injustificado, de forma a diminuir os custos e a atingir o máximo lucro[11]. É através da internet que o banco encontra uma forma de simplificar a contratação e a prática de vários atos bancários que passam a ser realizados sem intervenção humana e por via informática, conseguindo libertar os seus trabalhadores para tarefas que (ainda) exigem um contacto presencial com o cliente[12].

Tendo em vista a concretização de tais objetivos, assistimos hoje à exploração de novas ferramentas bancárias, designadamente *online*, no âmbito das quais surge este serviço[13].

2.2. A sua inserção num complexo contratual

O *home banking* enquadra-se numa relação negocial complexa constituída a partir de um contrato de abertura de conta e da constituição de depósitos de montantes em conta por parte do cliente ou de abertura de crédito.

Antes de mais, importa esclarecer que o *home banking* não constitui um mero aspeto do contrato de abertura de conta.

No contrato de banca eletrónica conseguimos reconhecer uma proposta contratual e uma aceitação distintas das manifestadas na abertura de conta apesar de, muitas vezes, se sobreporem temporalmente. Nestes contratos há uma troca de declarações de vontade de conteúdo diferente, o que implica um objeto diferente, e uma vontade de vinculação distinta. Assim, no contrato de abertura de conta, as partes visam apenas estabelecer a relação bancária que se irá desenvolver, ao longo do tempo, entre o banco e o cliente, enquanto no contrato de *home banking*, os contraentes procuram estabelecer uma forma de o cliente movimentar os fundos da conta bancária recorrendo a meios informáticos.

No entanto, o facto de ser habitual o contrato de abertura de conta abranger no seu clausulado todas as relações que se possam vir a estabelecer entre as partes, incluindo uma boa parte do regime dos futuros contratos a celebrar no seu âmbito pode suscitar dúvidas quanto à sua autonomização[14]. E, de facto, hoje em dia, os clausulados dos contratos de abertura de conta dos bancos portugueses incluem grande parte das regras que regem o

[10] MENEZES CORDEIRO, Manual de Direito Bancário, 3ª edição. Coimbra: Almedina, 2006, pp. 147-150.
[11] Ibidem, loc. cit.
[12] Ibidem, loc. cit.
[13] Ac. TRG de 23/10/2012 (Filipe Caroço), cit.
[14] Como podemos observar nas Condições Gerais de Abertura de Conta e Prestação de Serviços - Pessoas Singulares da Caixa Geral de Depósitos, o contrato de abertura de conta é constituído por secções que predispõem as bases dos futuros contratos: Secção A) Disposições Comuns […], Secção B) Condições Gerais da Conta de Referência […], Secção C) Condições Gerais das Contas de Depósito com pré-aviso, a prazo e em regime especial […], Secção D) Condições Gerais do Serviço CaixaDirecta […], Secção E) Condições Gerais de Utilização da Caderneta com NIC […] e Secção F) Condições Gerais de Utilização dos Cartões […]. In www.cgd.pt (27/08/2014).

contrato de *home banking*[15]. Todavia, isto não invalida a sua autonomia contratual[16]. Corroboramos a nossa afirmação ao realizar um paralelismo com outros contratos bancários que permitem a movimentação de fundos, como o contrato de utilização de cartões de pagamento e a convenção de cheque. Ambos são tipos negociais, inegavelmente considerados como contratos autónomos, através dos quais uma instituição bancária e o titular de uma conta bancária acordam a movimentação da mesma através, respetivamente, de "cartões de plástico"[17] e de cheques.

Ainda, há que ter em conta que a iniciativa da solicitação de um instrumento de pagamento[18], como é o caso da banca eletrónica, deve partir do cliente do banco, não decorrendo o acesso a este serviço meramente da celebração do contrato de abertura de conta[19].

No contrato de banca eletrónica, além de existir uma consonância de vontades autónoma, encontramos um acordo vinculativo assente sobre duas declarações de vontade (proposta do banco, de um lado, e aceitação do cliente, do outro) contrapostas mas convergentes, articuladas na comum intenção de permitir a movimentação pelo cliente de fundos da sua conta bancária através de uma plataforma informática criada para o efeito (resultado jurídico unitário). Desta forma, podemos concluir que o contrato de *home banking* é um tipo negocial autónomo uma vez que preenche todos os requisitos para a sua qualificação como tal[20].

---

[15] A título de exemplo – Condições Gerais de Abertura de Conta e Prestação de Serviços da Caixa Geral de Depósitos, in www.cgd.pt (27/08/2014), Condições Gerais de Depósito à Ordem – Pessoas Singulares do Millennium BCP, in www.millenniumbcp.pt (27/08/2014) e Condições Gerais de Abertura de Conta do BPI, in www.bancobpi.pt (27/08/2014).

[16] Não faria sentido recusar a autonomia do contrato de *home banking* simplesmente pelo facto de este se encontrar regulado no contrato de abertura de conta pois temos de ter em conta que, quando este serviço começou a ser utilizado na prática bancária, os bancos celebraram contratos de *home banking* isolados. A título de exemplo, vide os factos assentes do Ac. TRL de 18/04/2013, Proc. 1397/10.0TVLSB.L1-6 (Anabela Calafate); Ac. TRL de 28/06/2013, Proc. 147708/12.8Y (Anabela Calafate); Ac. TRP de 29/10/2013, Proc. 1254/10.0TJP (Francisco Matos); Ac. TRG de 25/11/2013, Proc. 2869/11.4TBGMR.G1 (Espinheira Baltazar); Ac. TRL de 12/12/2013, Proc. 164/11.8TBSRT.L1-6 (Tomé Ramião), todos in www.dgsi.pt. Não é admissível aceitar a autonomia do contrato de banca eletrónica pelo simples facto de este se apresentar num clausulado isolado e recusá-la apenas porque se integra nas condições gerais de abertura de conta. Tal entendimento conduziria à perda de autonomia dos contratos de depósito e de utilização de cartões de pagamento, o que é inadmissível.

[17] MARIA RAQUEL GUIMARÃES, As transferências eletrónicas de fundos e os cartões de débito. Coimbra: Almedina, 1999, p. 13.

[18] Segundo o art. 2º, alínea z) do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RSP), constante do Anexo I do DL n.º 317/2009, de 30 de outubro, define-se como instrumento de pagamento "qualquer dispositivo personalizado ou conjunto de procedimentos acordados entre o utilizador e o prestador do serviço de pagamento e a que o utilizador de serviços de pagamento recorra para emitir uma ordem de pagamento". Assim, são considerados instrumentos de pagamento quer os cartões de débito e de crédito, quer o serviço de *home banking*.

[19] De acordo com a alínea b) do n.º 1 do artigo 68º do RSP que determina que "o prestador de serviços de pagamento que emite um instrumento de pagamento […] [deve] abster-se de enviar instrumentos de pagamento não solicitados, salvo quando um instrumento deste tipo já entregue ao utilizador de serviços de pagamento deva ser substituído". No caso da banca eletrónica, considera-se "envio" de instrumento de pagamento, a entrega dos códigos de acesso ao serviço. Contudo, isto não impede que o banco possa ter iniciativa de oferecer ao seu cliente a possibilidade de o saldo da sua conta ser movimentado através de um instrumento eletrónico. MARIA RAQUEL GUIMARÃES, O Contrato-quadro no âmbito da utilização de meios de pagamento eletrónicos. Coimbra: Coimbra Editora, 2011, p. 178.

[20] Descrevendo o contrato de utilização de cartões de pagamento – cfr. Ac. STJ de 23/11/1999 (Garcia Marques). Coletânea de Jurisprudência – Acórdãos do STJ. Coimbra: Associação de Solidariedade Social "Casa do Juiz", 1999. Tomo III (Ano VII), p. 103, [o contrato de utilização de cartão de pagamento] é "um verdadeiro contrato autónomo, querido pelas partes, em consequência do qual uma instituição bancária emite um cartão de plástico em nome de um seu cliente com o objetivo de lhe permitir a realização de um conjunto de operações automatizadas". A caracterização do contrato de *home banking* é idêntica mas, no nosso caso, à entidade bancária cabe entregar os códigos de acesso ao serviço de banca eletrónica e não um cartão de plástico.

O contrato de banca eletrónica é um contrato de prestação de serviços conferidos eletronicamente e é reconhecido como contrato autónomo tanto pela lei, designadamente pelo Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RSP), contido no Anexo I do DL n.º 317/2009, de 30 de outubro[21], com as alterações do DL n.º 242/2012, de 7 de novembro, que enquadra este tipo negocial no conceito de contrato-quadro como "contrato de prestação de serviços de pagamento que rege a execução futura de operações de pagamento individuais e sucessivas […]" (alínea o) do artigo 2º do RSP)[22], como pela doutrina[23] e pela jurisprudência dos nossos tribunais superiores[24].

A questão da autonomia do contrato de *home banking* mereceria um maior desenvolvimento teórico, contudo não seremos exaustivos nesta sede uma vez que neste ponto cabe-nos apenas apresentar o enquadramento do serviço de banca eletrónica no âmbito do complexo contratual em que se insere.

É através da celebração deste novo contrato, em simultâneo ou em momento posterior ao acordo de abertura de conta, que o cliente adere ao serviço de banca eletrónica, sendo-lhe disponibilizado pelo banco, a partir do seu *site*, uma extensão desmaterializada dos serviços que se comprometeu a prestar no exercício da sua atividade[25]. A partir do momento em que a entidade bancária entrega os códigos de acesso ao sistema *online*, o aderente passa a poder aceder à sua conta através de qualquer computador com ligação à internet, 24 horas por dia, 365 dias por ano.

2.2.1. Relação com o contrato de abertura de conta

O contrato de abertura de conta consiste num acordo estabelecido entre uma entidade bancária e um cliente "através do qual se constitui, disciplina e baliza a respetiva relação jurídica bancária"[26]. Assim, este contrato constitui o ponto de partida para o complexo contratual que compõe a relação bancária e opera como "fio condutor e integrador dos diferentes negócios concretos que as partes venham a celebrar"[27].

[21] Nº 1 do artigo 2º do DL n.º 317/2009.
[22] E como diz, e bem, MARIA RAQUEL GUIMARÃES, O Contrato-quadro…, cit., p. 133, "na medida em que o contrato-quadro compreende uma série de obrigações que se impõem às partes, é desde logo um contrato".
[23] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., pp. 58-61.
[24] A Relação de Lisboa, no Acórdão de 26/10/2010, Proc. 1943/09.1TJLSB.L1-7 (Maria Amélia Ribeiro), in www.dgsi.pt, afirmou que "Estamos no domínio de uma relação negocial complexa que necessariamente foi iniciada através de um contrato de abertura de conta, com pelo menos um depósito ou depósitos de quantias numa conta a prazo, por parte da Autora, e no âmbito da qual as partes inscreveram um novo contrato destinado a permitir a movimentação da conta "por via telefónica ou internet e por outras formas de acesso remoto que venham a ser criadas […]"; Ac. TRL de 24/05/2012, Proc. 192119/11.8YIPRT.L1-2 (Ezagüi Martins); Ac. TRG de 23/10/2012, Proc. 305/09.5TBCBT.G1 (Filipe Caroço); Ac. TRG de 30/05/2013, Proc. 6479/09.8TBBRG.G1 (Rita Romeira); Ac. TRL de 28/06/2013 (Anabela Calafate), cit.; Ac. TRP de 29/10/2013 (Francisco Matos), cit.; Ac. TRL de 5/11/2013, Proc. 9821/11.8T2SNT.L1-1 (Manuel Marques); Ac. TRG de 25/11/2013 (Espinheira Baltazar), cit.; Ac. TRL de 12/12/2013 (Tomé Ramião), cit.; Ac. STJ de 18/12/2013 (Ana Paula Boularot), cit. Todos in www.dgsi.pt.
[25] Ac. TRP de 29/10/2013 (Francisco Matos), cit.
[26] ENGRÁCIA ANTUNES, Direito dos Contratos Comerciais. Coimbra: Almedina, 2009, p. 483.
[27] MARIA RAQUEL GUIMARÃES, O Contrato-quadro…, cit., p. 347.

A abertura de conta caracteriza-se por se tratar de um contrato atípico embora correspondendo, hoje em dia, a um tipo social cuja disciplina jurídica assenta nas cláusulas contratuais gerais e nos usos bancários[28]. Este tipo negocial foi legalmente reconhecido no Aviso n.º 11/2005, de 21 de Julho, do Banco de Portugal, diploma que, hoje, já não se encontra em vigor.

Tendo em vista o início de uma relação contratual duradoura como é a relação bancária, através da abertura de conta, o banco pretende definir e determinar as suas bases gerais, deixando em aberto a celebração de ulteriores contratos bancários[29]. Por essa razão, o seu clausulado inclui regras que extravasam o contrato singular, fazendo referência a "produtos comercializados" pela entidade bancária e que dependem da vontade do cliente, apontando, desta forma, para o intuito de iniciar uma relação mais complexa[30]. Contudo, isto não significa que da abertura de conta derivam deveres de contratar no futuro, apesar de se poder identificar deveres de disponibilidade para negociar e mesmo de negociação[31]. Assim, nem o contrato de *home banking*, nem qualquer outro contrato bancário, é imposto pelo banco, antes constituindo uma faculdade de utilização do serviço pelo cliente mediante a adesão ao contrato de banca eletrónica[32].

O facto de esta figura contratual criar uma relação jurídica na qual assentarão os diferentes contratos que vão sendo sucessivamente celebrados, permite-nos classificá-la como contrato-quadro[33] uma vez que funciona como um verdadeiro "contrato de contratos"[34].

A relação contratual bancária criada entre o banco e o cliente apenas irá alcançar densidade económica e negocial através da celebração futura de vários contratos bancários especiais e renovar-se-á sucessivamente através da movimentação da conta[35]. Estes contratos bancários referidos são, por exemplo, o contrato de depósito, de abertura de crédito, de emissão de cartão e de *home banking*[36], e inserem-se no conteúdo contratual complexo do contrato de abertura de conta, qualificando-se como convenções acessórias embora mantendo a sua autonomia[37].

---

[28] ENGRÁCIA ANTUNES, op. cit., pp. 486-487; MENEZES CORDEIRO, Manual…, cit., pp. 412-415.
[29] ALMENO DE SÁ, Direito Bancário. Coimbra: Coimbra Editora, 2008, p. 17.
[30] MARIA RAQUEL GUIMARÃES, O Contrato-quadro…, cit., p. 359 e ALMENO DE SÁ, op. cit., pp. 15-16.
[31] MENEZES CORDEIRO, Manual…, cit., pp. 193-194; MARIA RAQUEL GUIMARÃES, O Contrato-quadro…, cit., p. 367.
[32] Ac. TRG de 23/10/2012 (Filipe Caroço), cit.
[33] FERREIRA DE ALMEIDA, Contratos II, 3ª edição. Coimbra: Almedina, 2012, pp. 140-142; AZEVEDO FERREIRA, A relação negocial bancária – conceito e estrutura. Lisboa: Quid Iuris, 2005, p. 684; ALMENO DE SÁ, op. cit., loc. cit. Optando pela designação "contrato normativo", temos MENEZES CORDEIRO, Da Compensação no direito civil e no direito bancário. Coimbra: Almedina, 2003, p. 193.
[34] Expressão utilizada por MARIA RAQUEL GUIMARÃES, O Contrato-quadro…, cit., p. 363.
[35] ENGRÁCIA ANTUNES, op. cit., loc. cit.
[36] A Relação de Guimarães afirma, no Acórdão de 5/11/2013 (Manuel Marques), cit., que "tendo por base o contrato de abertura de conta, as partes celebraram dois outros contratos: o de depósito e o denominado *home banking*."
[37] ENGRÁCIA ANTUNES, op. cit., p. 485; Ac. TRL de 24/05/2012 (Ezagüi Martins), cit.

Desta forma, e considerando a natureza autónoma do contrato de banca eletrónica, podemos verificar que este depende geneticamente de um contrato de abertura de conta celebrado anteriormente que já tenha estabelecido a relação bancária entre o banco e o cliente[38].

A abertura de conta antecede necessariamente o contrato de *home banking* que, por sua vez, deverá ter na sua base, ou, pelo menos, ser seguida de um contrato de depósito ou de abertura de crédito, como veremos no ponto *infra*[39].

2.2.2. Relação com o contrato de depósito bancário

Como já foi referido, o serviço de *home banking* surge como um instrumento de pagamento que possibilita ao cliente movimentar os fundos que estejam à sua disposição. Assim sendo, o cliente apenas terá interesse em aderir ao serviço de banca eletrónica se tiver fundos disponíveis para movimentar. Isto significa que a utilização deste serviço pressupõe o prévio acordo acerca da delimitação da disponibilidade dos fundos, ou seja, é essencial um contrato de depósito ou de abertura de crédito[40]. Doravante neste ponto, vamo-nos apenas aludir ao contrato de depósito, sem prejuízo de sempre que nos referirmos a este podermos substituir por uma menção ao contrato de abertura de crédito.

Primeiro, é importante fazer uma destrinça entre o contrato de *home banking* e o contrato de depósito bancário.

O depósito bancário[41] surge como um contrato diferente da abertura de conta mas com ele conexo[42]. Através deste acordo, o cliente ou um terceiro entregam à instituição bancária determinado montante para crédito de uma conta[43]. Por seu lado, o contrato de *home banking* também é um contrato associado à abertura de conta, integrando a relação bancária criada por este último tipo negocial.

---

[38] Referindo-se ao contrato de utilização de cartões de pagamento, MARIA RAQUEL GUIMARÃES, O Contrato-quadro…, cit., p. 379.
[39] Mais uma vez referindo-se ao contrato de utilização de cartões de pagamento, MARIA RAQUEL GUIMARÃES, O Contrato-quadro…, cit., p. 381.
[40] Entendimento de MARIA RAQUEL GUIMARÃES quanto ao contrato de utilização de cartões de pagamento. A autora defende que "a anterioridade [do contrato de depósito] é, relativamente ao contrato de utilização de um cartão de pagamento, senão cronológica, pelo menos lógica.", O Contrato-quadro…, cit., p. 179. Esta afirmação vale para o contrato de *home banking*, dada a finalidade comum deste contrato e do contrato de utilização de cartão de pagamento.
[41] Regulado pelo DL n.º 430/91, de 2 de novembro com as alterações introduzidas pelo DL n.º 88/2008, de 29 de maio.
[42] Alguns autores utilizam a expressão "depósito bancário" na aceção de contrato de abertura de conta, cfr. ANTUNES VARELA, Depósito Bancário – Depósito a prazo em regime de solidariedade. Revista da Banca. Lisboa: Associação Portuguesa de Bancos. Nº 21 (Janeiro/Março de 1992), p. 49, assim como o próprio legislador, no Decreto-Lei n.º 430/91, de 2 de Novembro, relativo ao regime geral das contas de depósito. Contudo, a maioria da doutrina distingue, e bem, os dois contratos. Cfr. ENGRÁCIA ANTUNES, op. cit, p. 484 que define o contrato de abertura de conta como "contrato bancário primogénito" em torno do qual "gravitarão usualmente os contratos de depósito, cheque…"; também MENEZES CORDEIRO, Manual…, cit., pp. 480-481; CALVÃO DA SILVA, Direito Bancário. Coimbra: Almedina, 2001, p. 344.
[43] PEDRO PAIS DE VASCONCELOS, Direito Comercial, Vol. I. Coimbra: Almedina, 2011, p. 222.

O contrato de depósito bancário e o contrato de banca eletrónica são figuras contratuais distintas[44] uma vez que nelas é possível identificar declarações de vontade de conteúdo diferente, apesar de, muitas vezes, serem proferidas pelos mesmos sujeitos e de coincidirem no mesmo momento temporal: no contrato de depósito bancário, o cliente procura entregar ao banco determinada quantia para crédito numa conta, enquanto no contrato de *home banking*, o cliente solicita à instituição bancária a utilização de um serviço informático de forma a movimentar os fundos depositados[45].

Apesar de constituírem tipos negociais diferentes, não podemos considerar que estamos perante uma multiplicidade de relações contratuais autónomas e estanques entre si.[46] As partes querem celebrar os contratos de depósito bancário e de *home banking* como um conjunto económico onde o referido nexo funcional é essencial[47] e isto porque o contrato de banca eletrónica só faz sentido se existir uma outra relação negocial subjacente, em consequência da qual o utilizador do serviço tenha fundos à sua disposição e possa movimentá-los por via eletrónica: a relação estabelecida pelo contrato de depósito bancário[48]. Por outras palavras, o contrato de *home banking* é um contrato acessório, instrumental em relação ao contrato de depósito[49].

Mais especificamente, há uma coligação de contratos[50] entre o contrato de banca eletrónica e o contrato de depósito[51] que se pode qualificar como uma coligação funcional uma vez que a influência recíproca dos dois tipos negociais manifesta-se, essencialmente, durante a execução do contrato e ao nível dos objetivos que se procuram alcançar, mantendo os dois contratos em causa, apesar do interesse económico que lhes é comum, a sua individualidade jurídica[52]. Assim, a cessação do contrato de depósito quebra o conjunto económico visado pelo cliente aquando da celebração dos diversos contratos.

Em suma, estamos perante uma verdadeira coligação de contratos que, no entanto, deixa intacta a individualidade própria de cada contrato. Logo, o contrato de *home banking* e o contrato de depósito são tipos negociais juridicamente autónomos, embora necessariamente

---

[44] Este é o entendimento dos nossos tribunais superiores. Ac. TRL de 26/10/2010 (Maria Amélia Ribeiro), cit.; Ac. TRL de 24/05/2012 (Ezagüi Martins), cit.; Ac. TRL de 5/11/2013 (Manuel Marques), cit.; Ac. TRG de 25/11/2013 (Espinheira Baltazar), cit.

[45] Adaptamos o entendimento de MARIA RAQUEL GUIMARÃES no que diz respeito ao contrato de utilização de cartões de pagamento – As transferências eletrónicas de fundos…, cit., pp. 110-111.

[46] Ac. STJ de 18/12/2013 (Ana Paula Boularot), cit.

[47] GALVÃO TELLES, Direito das Obrigações, 7ª edição (reimpressão). Coimbra: Coimbra Editora, 2010, p. 88.

[48] MARIA RAQUEL GUIMARÃES, Comércio eletrónico e transferências eletrónicas de fundos. O Comércio Eletrónico – Estudos Jurídico-Económicos. Coimbra: Almedina, 2002, p. 72.

[49] Adaptamos, mais uma vez, o raciocínio de MARIA RAQUEL GUIMARÃES relativo ao contrato de utilização de cartões de pagamento uma vez que a finalidade deste contrato e do contrato de banca eletrónica é idêntica: ambos visam a movimentação de fundos por parte do cliente – As transferências eletrónicas de fundos…, cit., p. 107. O entendimento da Autora acerca dos cartões de pagamento e do facto do contrato de utilização ser um "contrato acessório, instrumental em relação ao contrato de depósito" foi seguido pelo STJ no Acórdão de 23/11/1999 (Garcia Marques), cit.

[50] Ou "união de contratos com dependência" segundo a classificação apresentada por GALVÃO TELLES, op. cit., loc. cit.

[51] MARIA RAQUEL GUIMARÃES, As transferências eletrónicas de fundos…, cit., pp. 107-108 e GETE-ALONSO Y CALERA, Las tarjetas de crédito, Relaciones contractuales y conflictividad. Madrid: Marcial Pons, 1997, pp. 122-123 (nota 18).

[52] Fazendo um paralelismo com o entendimento de MARIA RAQUEL GUIMARÃES sobre a relação entre o contrato de utilização de cartões de pagamento e o contrato de depósito bancário – As transferências eletrónicas de fundos…, cit., pp. 108-109. O STJ seguiu o entendimento da Autora na obra *supra* citada, no Acórdão de 23/11/99 (Garcia Marques), cit., p. 103.

interdependentes[53].

2.3. Caracterização do contrato de *home banking*

O contrato de banca eletrónica é um contrato socialmente típico mas legalmente atípico uma vez que, apesar de não previsto na lei, é de tal forma solicitado pela prática que adota um figurino comum por todos conhecido[54]. Este modelo comum deriva, essencialmente, da utilização pelos bancos de cláusulas contratuais gerais muito semelhantes nos contratos de banca eletrónica.

2.3.1. Como contrato de adesão

Como se trata de um contrato bancário, acordo estabelecido entre uma instituição bancária e um cliente, segue o sistema adotado pelos bancos para a celebração dos seus contratos e que se traduz na utilização de cláusulas contratuais gerais para determinar o conteúdo da relação contratual.

O recurso a cláusulas contratuais gerais na atividade bancária é fundamental, não só devido às necessidades de rapidez inerentes à sociedade moderna e tendo em vista a racionalização de custos (de tempo e pessoal)[55] mas, também para fazer face à falta ou insuficiência de normas legais aplicáveis aos contratos bancários[56]. De facto, se atendermos à inexistência de um direito bancário positivamente unificado e à complexidade da atividade bancária, podemos verificar que as cláusulas contratuais gerais acabam por funcionar, na prática, como a principal fonte normativa[57]. Assim se confere uma maior segurança jurídica, tornando previsíveis as consequências das condutas adotadas no âmbito deste quadro contratual[58].

A subscrição do *home banking* é efetuada mediante um contrato de adesão, o seu clausulado encontra-se pré-elaborado e é imposto à parte contratualmente mais fraca (cliente) que se limita a aceitar as condições pré-estabelecidas pelo outro contraente (banco). O cliente apenas tem o direito de utilizar o serviço após a adesão ao contrato de banca eletrónica, o que implica a aceitação de todas as condições de utilização plasmadas no contrato; caso contrário, não poderá beneficiar da referida ferramenta *web*.

---

[53] MARIA RAQUEL GUIMARÃES, Comércio eletrónico…, cit., loc. cit.
[54] MENEZES CORDEIRO, Tratado de direito civil português, Tomo I. 3ª edição (reimpressão). Coimbra: Almedina, 2007, pp. 472-473.
[55] CALVÃO DA SILVA, op. cit., pp. 349-350 e Banca, Bolsa e Seguros – Direito europeu e português, Tomo I, 2ª edição (revista e aumentada). Coimbra: Almedina, 2007, p. 162.
[56] MENEZES CORDEIRO, Manual…, cit., pp. 367-368.
[57] ALMENO DE SÁ, op. cit., p. 25.
[58] AZEVEDO FERREIRA, Direito Bancário. 2ª edição. Lisboa: Quid Juris, 2009, p. 340.

Perante um contrato de adesão, o cliente, além de deter muito menos conhecimentos e informação sobre os trâmites usuais no âmbito bancário que a instituição bancária, não pode discutir e tentar negociar determinadas condições[59]. A sua única "liberdade" é a decisão de concluir ou não o contrato, daí que se mostre essencial que as cláusulas contratuais gerais sejam justas, equitativas e razoáveis[60]. Na ordem jurídica portuguesa, no que se refere à prática bancária, acresce a dificuldade decorrente da não existência de cláusulas contratuais gerais comuns aos diversos bancos, criando cada entidade bancária as suas cláusulas.[61] Face à débil posição em que se encontra o aderente nestes contratos, o ordenamento jurídico tem procurado protegê-lo através da criação de diversos mecanismos que visam o controlo das cláusulas contratuais gerais[62] e a proteção do consumidor[63].

2.3.2. Como contrato-quadro

Este contrato também pode ser qualificado como um contrato-quadro em relação às sucessivas operações de transferência eletrónica de fundos ordenadas via *online*[64]. Este entendimento decorre da Diretiva 2007/64/CE do Parlamento Europeu e do Conselho, de 13 de novembro[65], relativa aos serviços de pagamento[66] (DSP), transposta para o ordenamento jurídico português pelo RSP. A DSP introduziu o conceito de contrato-quadro no âmbito dos serviços de pagamento, distinguindo-o das operações de pagamento individuais ordenadas pelo cliente no âmbito deste[67]. Consequentemente, esta figura foi acolhida pelo RSP. De acordo com a alínea o) do artigo 2º do RSP, o contrato-quadro é um "contrato de prestação de serviços de pagamento que rege a execução futura de operações de pagamento individuais e sucessivas e que pode enunciar as obrigações e condições para a abertura de uma conta de pagamento"[68] .

Assim, cada vez que o cliente emite uma ordem de pagamento a favor de terceiro através do sistema informático posto à disposição pelo banco, é celebrado um novo contrato de

[59] CALVÃO DA SILVA, Direito Bancário…, cit., pp. 349-350.
[60] Ibidem, loc. cit.
[61] MENEZES CORDEIRO, Manual…, cit., p. 405.
[62] DL n.º 446/85, de 25 de outubro.
[63] Lei n.º 24/96, de 31 de julho.
[64] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 59.
[65] A presente Diretiva é de harmonização plena (art. 86º) e altera as Diretivas 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE e revoga a Diretiva 97/5/CE – in JOUE, n.º L 319, de 5/12/2007.
[66] De acordo com o art. 2º, alínea c) e art. 4º, alínea c) do RSP, considera-se serviços de pagamento a "execução de operações de pagamento, incluindo a transferência de fundos depositados numa conta de pagamento aberta junto do prestador de serviços de pagamento do utilizador ou de outro prestador de serviços de pagamento, tais como: i) A execução de débitos diretos, incluindo os de carácter pontual; ii) A execução de operações de pagamento através de um cartão de pagamento ou de um dispositivo semelhante; iii) A execução de transferências a crédito, incluindo ordens de domiciliação".
[67] MARIA RAQUEL GUIMARÃES, The debit and credit card frame work contract and its influence on European legislative initiatives. InDret Comparado, Revista para el Analisis del derecho. N.º 2 (2012), p. 2, in http://www.indret.com/es (04/09/2014). Reconhecendo a relevância prática desta figura, cfr. Considerando 24 da DSP, p. 4, onde se admite que "na prática, os contratos-quadro e as operações de pagamento por estes abrangidas são de longe mais comuns e importantes de um ponto de vista económico do que as operações de pagamento de caráter isolado. Se existir uma conta de pagamento ou um instrumento de pagamento específico, será necessário um contrato-quadro".
[68] Quanto às operações de pagamento abrangidas por um contrato-quadro – art. 51º e seguintes do RSP.

execução do contrato de *home banking*[69]. Podemos verificar que esta figura contratual potencia uma multiplicidade de contratos subsequentes, simplificados, na sua conclusão e execução, através do recurso a meios eletrónicos[70]. Estes contratos de execução resultam de tantos acordos de vontade quantos os contratos celebrados, não se cingindo a simples atos de execução de um contrato anterior[71].

De acordo com o que foi analisado, podemos verificar que o contrato de banca eletrónica, além de surgir no âmbito de uma relação contratual complexa, também gera uma série de contratos subsequentes. Estes, por sua vez, encontram-se intrinsecamente ligados ao contrato-quadro uma vez que a sua celebração só foi possível em virtude da adesão do cliente ao instrumento de pagamento disponibilizado pelo banco. É um "contrato que antecipa futuros contratos"[72].

2.4. Conteúdo da relação contratual

Neste ponto, vamos ingressar no núcleo do contrato de *home banking*, analisando quais os serviços incluídos, em geral, nestes contratos e, ainda, quais os deveres a que as partes se vinculam através do presente acordo.

2.4.1. Os serviços abrangidos

O *home banking* é um serviço prestado pela instituição bancária que confere ao cliente a possibilidade de efetuar consultas de saldos e de realizar operações bancárias, *maxime* pagamentos e transferências, relativamente às contas que seja titular e que possa movimentar livremente, utilizando para o efeito o telefone (serviço telefónico) ou a internet (serviço *online*).

Este serviço permite ao cliente realizar operações bancárias sem necessidade de se deslocar a uma caixa multibanco ou às sucursais do banco e sem estar sujeito aos respetivos horários de atendimento ao público, permitindo-lhe um acesso mais rápido, fácil e cómodo.

Todavia também traz vantagens indiscutíveis à instituição bancária, permitindo-lhe uma redução dos custos de funcionamento inerentes à possibilidade de o cliente efetuar operações bancárias sem intervenção do seu pessoal.[73] O banco gasta menos recursos ao transferir para o cliente a execução de atos que antes dependiam dos seus funcionários, libertando-se de meios humanos, ao mesmo tempo que se disponibiliza de forma contínua ao

[69] Referindo-se ao contrato de utilização de cartões de pagamento, cfr. MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 59.
[70] Ibidem, loc. cit.
[71] MARIA RAQUEL GUIMARÃES, O Contrato-quadro…, cit., p. 133.
[72] MARIA RAQUEL GUIMARÃES, O Contrato-quadro…, cit., p. 151.
[73] Ac. TRL de 18/04/2013 (Anabela Calafate), cit.

cliente, 24 horas por dia, 365 dias por ano, reforçando o encaminhamento das poupanças para o sistema bancário[74]. A prestação deste serviço contribui igualmente para a manutenção da clientela da entidade bancária, assim como para a sua angariação.

Pode-se concluir que estamos perante um contrato que confere benefícios recíprocos às partes[75]. Às vantagens somam-se, por outro lado, deveres que ambos os contraentes devem observar no decorrer da execução do contrato. O contexto no qual se desenrola o *home banking,* ou seja, a movimentação de uma conta bancária à distância por parte do cliente, a partir de um sistema informático que se encontra em interação com o sistema informático do banco, implica para ambas as partes a observância de procedimentos e regras de segurança[76].

2.4.2. Obrigações que vinculam as partes

Ao celebrar um contrato de execução continuada como o contrato de *home banking*[77] gera-se uma relação obrigacional complexa onde direitos subjetivos, deveres principais, acessórios e laterais se interligam tendo em vista a prossecução de um mesmo fim contratual[78] .

Atualmente, as operações de transferência eletrónica de fundos realizadas através de um sistema de banca eletrónica encontram-se reguladas no RSP. Nos artigos 67º e 68º do RSP são estabelecidos alguns deveres que devem ser observados pelo utilizador (cliente) e pelo prestador do serviço (instituição bancária) no contrato de *home banking*.

a) Deveres do utilizador

O contrato de *home banking* visa permitir ao cliente usufruir do serviço de movimentação de fundos – o que constitui a prestação principal do banco, como veremos adiante.

No que diz respeito ao cliente, o contrato de banca eletrónica não impõe a observância de qualquer dever principal[79], sem prejuízo de se considerar a utilização correta do serviço o dever mais importante do cliente no âmbito deste contrato. Contudo, não podemos classificar a utilização correta do serviço de *home banking* como um dever principal em sentido técnico-jurídico uma vez que não consubstancia qualquer prestação. Ademais, em

[74] Ac. TRL de 26/10/2010 (Maria Amélia Ribeiro), cit.
[75] Ibidem
[76] Ac. TRP de 29/10/2013 (Francisco Matos), cit.
[77] Ac. TRG de 25/11/2013 (Espinheira Baltazar), cit
[78] Fazendo um paralelismo com o contrato de utilização de cartão de pagamento – MARIA RAQUEL GUIMARÃES – O Contrato-quadro…, cit., p. 279.
[79] Num contexto obrigacional, o dever principal é o dever de prestar, ou seja, é aquele através de cuja realização cada uma das partes alcança o fim determinante da constituição do vínculo obrigacional sob cominação das sanções aplicáveis ao incumprimento. Cfr. ANTUNES VARELA, Das Obrigações em Geral, vol. I, 10ª edição (revista e atualizada: 9ª reimpressão). Coimbra: Almedina, 2012, p. 118.

caso de incumprimento, a entidade bancária não irá recorrer aos tribunais para exigir o seu cumprimento coercivo porque a utilização correta do serviço não satisfaz o interesse do banco. Com o contrato de banca eletrónica, a entidade bancária não tem como objetivo último ver os seus clientes utilizarem o serviço corretamente mas sim reduzir custos e contribuir para a manutenção e angariação de clientela. A utilização correta do serviço de *home banking* constitui um objetivo intermédio ou instrumental pois trata-se, fundamentalmente, de uma condição *sine qua non* do bom funcionamento do serviço. Logo, podemos verificar que a utilização correta do serviço é apenas uma condição que o cliente deve satisfazer para continuar a beneficiar do serviço.

Assim, a utilização correta do serviço é um dever acessório de conduta que implica a utilização do serviço dentro dos limites da provisão existente na sua conta bancária no caso de conta à ordem, não efetuando operações a descoberto, exceto se tal tiver sido acordado previamente, ou dentro dos limites do crédito concedido, no caso de abertura de crédito, e em respeito das condições gerais que regem a sua utilização, servindo-se dos códigos de acesso fornecidos pela entidade bancária (alínea a) do n.º 1 do artigo 67º do RSP).

No contrato de *home banking*, verificamos que são impostos expressamente deveres acessórios de conduta, sobretudo ao utilizador. Estes deveres são autónomos dos deveres principais e distintos dos deveres secundários, revelando-se essenciais ao correto processamento da relação contratual. [80] Os deveres acessórios de conduta podem derivar de uma cláusula contratual, de dispositivo da lei *ad hoc* ou do princípio da boa-fé (n.º 2 do artigo 762º do Código Civil, doravante, CC) que consagra genericamente esta categoria de deveres no âmbito das obrigações[81]. O seu incumprimento, apesar de constituir a violação de deveres inscritos na relação obrigacional, não dá origem a uma ação judicial de cumprimento (artigo 817º do CC), podendo apenas gerar a obrigação de indemnizar os danos dela resultantes[82].

No caso do contrato de banca eletrónica, a positivação dos deveres acessórios de conduta no RSP e no clausulado do contrato deve-se ao seu carácter duradouro e à especial relação de confiança entre as partes[83]. Assim, o utilizador do serviço tem a seu cargo um conjunto de deveres acessórios de conduta conexos com a segurança do sistema[84].

O primeiro a destacar é o dever de o utilizador tomar todas as medidas razoáveis para preservar a eficácia dos mecanismos de segurança personalizados associados ao instrumento de pagamento (n.º 2 do artigo 67º do RSP), no caso do *home banking*, os códigos de acesso a este serviço.

---

[80] ANTUNES VARELA, Das Obrigações em Geral…, cit., p. 123. O mesmo Autor acrescenta que estes deveres assumem uma especial relevância nos contratos bilaterais, onde se impõe a cada uma das partes contratuais o dever de tomar as precauções necessárias para que a obrigação que lhe incumbe satisfaça o interesse do credor na prestação, Das Obrigações em Geral…, cit., p. 125.

[81] MÁRIO JÚLIO DE ALMEIDA COSTA, Direito das Obrigações, 12ª edição (revista e atualizada). Coimbra: Almedina, 2009, p. 77; ANTUNES VARELA, Das Obrigações em Geral…, cit., loc. cit.

[82] ANTUNES VARELA, Das Obrigações em Geral…, cit., pp. 123-124, e Ac. TRC de 9/11/2004, Proc. n.º 2278/04 (Alexandrina Ferreira), in www.dgsi.pt.

[83] Quanto aos deveres laterais de conduta nos contratos de utilização de cartões de pagamento, MARIA RAQUEL GUIMARÃES, O Contrato-quadro…, cit., p. 330.

[84] Ac. TRG de 25/11/2013 (Espinheira Baltazar), cit.

As chaves de acesso conferidas pela instituição bancária, usualmente inscritas num cartão matriz[85], constituem "dispositivos de segurança personalizados" tendo uma função de autenticação, de acordo com o disposto na alínea v) do artigo 2º do RSP[86]. Assim, o conhecimento do conjunto de senhas confidenciais que, através da sua marcação no teclado do computador, permitem aceder ao serviço de *home banking* e realizar determinadas operações é o meio utilizado para identificar e imputar as operações realizadas ao seu utilizador[87]. Face à essencialidade do conhecimento dos códigos de acesso para cumprir a função de autenticação, o utilizador fica, naturalmente, vinculado ao dever de garantir a segurança desses elementos, não facultando a sua utilização a terceiros (n.º 2 do artigo 67º do RSP). Este dever de confidencialidade quanto aos dados pessoais que permitem o acesso ao serviço de banca eletrónica é fundamental visto que é impossível realizar qualquer transferência através daquele serviço sem a introdução das chaves de acesso que constam do cartão matriz e que são aleatoriamente escolhidas pelo sistema informático, além de que uma vez digitada a chave correta, o sistema valida-a e presume que está perante o seu verdadeiro portador[88]. Através destes códigos de acesso, o banco pretende verificar a coincidência entre a pessoa que pretende aceder ao serviço de *home banking* e o cliente que subscreveu o respetivo contrato, isto é, o credor do serviço eletrónico que a instituição bancária se obrigou a prestar[89]. Este dever de não divulgação dos códigos de acesso costuma constar expressamente do contrato de banca eletrónica a que o cliente aderiu, assim como decorre das regras que, segundo um padrão de normalidade, o comum utilizador da internet sabe que devem ser observadas[90].

A este, acresce um outro dever acessório de conduta do utilizador, o dever de comunicação imediata ao banco da utilização abusiva do instrumento de pagamento. Este dever é, geralmente, imposto contratualmente mas, mesmo que assim não fosse, sempre decorria da especial relação de confiança entre o banco e o cliente[91]. Este dever encontra-se plasmado na alínea b) do n.º 1 do artigo 67º do RSP e determina que, em caso de utilização não autorizada do instrumento de pagamento, o utilizador deve notificar o ocorrido ao banco, logo que tenha conhecimento e sem atrasos injustificados. A importância decisiva da notificação será explorada no ponto 3.3. do capítulo III.

---

[85] O cartão matriz consiste num cartão de coordenadas para validação de operações bancárias suscetíveis de alterar o património detido no banco.
[86] O art. 2º, alínea v) do RSP apresenta a definição de autenticação como "um procedimento que permite ao prestador de serviços de pagamento verificar a utilização de um instrumento de pagamento específico, designadamente os dispositivos de segurança personalizados".
[87] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 61.
[88] Ac. TRL de 28/06/2013 (Anabela Calafate), cit.; Ac. TRG de 25/11/2013 (Espinheira Baltar), cit. Assim, compreende-se que este dever que se impõe ao cliente "não é um capricho ou uma exigência desproporcionada ou irrazoável dos bancos, correspondendo, pelo contrário, a um meio indispensável para proteção de legítimos interesses e parte integrante do esquema de pagamentos em que se inscreve." Cfr. JOSÉ MANUEL FARIA, Acesso a contas bancárias por terceiros no âmbito de operações de pagamento. Revista da Banca. Lisboa: Associação Portuguesa de Bancos. N.º 71 (janeiro/junho 2011), p. 32.
[89] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 61.
[90] Ac. TRL de 18/04/2013 (Anabela Calafate), cit.
[91] MARIA RAQUEL GUIMARÃES, O Contrato-quadro…, cit., p. 331.

A inobservância destes deveres pelo utilizador conduz à sua responsabilização pelos prejuízos que eventualmente ocorram, nos termos do artigo 798º do Código Civil[92]. O utilizador do serviço de *home banking* responde por todos os prejuízos que lhe possam ser imputados a título de dolo ou negligência devido ao não cumprimento das suas obrigações contratuais[93].

b) Deveres do prestador de serviços de pagamento

Como já referimos, no contrato de *home banking*, só a entidade bancária tem um dever principal, cabendo-lhe aceitar os sucessivos mandatos para pagamentos emitidos mediante a correta autenticação por parte do cliente, isto nos limites do saldo disponível da conta à ordem, ou na medida em que tenha sido previsto anteriormente a possibilidade de realizar operações a descoberto, ou do crédito concedido nos casos de abertura de crédito[94].

Como dever secundário acessório da prestação principal, o banco deve entregar ao utilizador o cartão matriz e todos os códigos de acesso necessários à utilização do serviço de banca eletrónica. Esta entrega constituí um pressuposto essencial do acesso legítimo ao serviço uma vez que, sem os dispositivos de segurança personalizados na sua posse, o utilizador não consegue aceder ao serviço *online*.

Sem prejuízo dos deveres que incumbem ao utilizador e tendo em conta que o funcionamento do sistema de *home banking* depende da utilização de meios informáticos que têm inerentes riscos próprios, o que pressupõe um comportamento diligente de ambas as partes[95], ao banco cabe assegurar que os mecanismos de segurança personalizados associados ao instrumento de pagamento só sejam acessíveis ao utilizador a quem foi conferido o direito à sua utilização (alínea a) do n.º 1 do artigo 68º do RSP).

De forma a concretizar este dever acessório de conduta da entidade bancária, a lei acrescenta que cabe ao banco comunicar, como medida preventiva, "se for caso disso, uma descrição das medidas que o utilizador do serviço de pagamento deve tomar para preservar a segurança dos instrumentos de pagamento" (subalínea i) da alínea e) do artigo 53º do RSP). Assim, recai sobre a instituição bancária um reforçado dever de informação que consiste em elucidar o cliente quanto aos casos mais frequentes de fraude e aos perigos inerentes à utilização do serviço que se comprometeu a prestar, sempre tendo em consideração o tipo de utilizador e os seus conhecimentos técnicos; não sendo, por isso, suficiente que o banco permita ao seu cliente aceder ao serviço de banca eletrónica,

[92] O artigo 798º do CC estabelece que "o devedor que falta culposamente ao cumprimento da obrigação torna-se responsável pelo prejuízo que causa ao credor".
[93] Paralelismo com o contrato de utilização de cartão de pagamento – MARIA RAQUEL GUIMARÃES, As transferências eletrónicas de fundos…, cit., p. 212.
[94] Desenvolvendo os deveres principais do banco nos contratos de utilização de cartões de pagamento – MARIA RAQUEL GUIMARÃES, O Contrato-quadro…, cit., p. 282.
[95] MARIA RAQUEL GUIMARÃES, O Contrato-quadro…, cit., p. 331.

fornecendo-lhe as chaves de acesso[96]. Assim, é frequente os bancos fazerem certas recomendações aos seus clientes a fim de os prevenirem relativamente à utilização do serviço de *home banking*, designadamente no sentido de não abrir mensagens de correio eletrónico cujo remetente seja desconhecido, não executar ficheiros não solicitados, ter sempre um antivírus atualizado no computador e não aceder à página do banco através de atalhos (não aceder por um *link*[97] de uma mensagem de correio eletrónico, nem pelos "favoritos"), devendo digitar-se diretamente o *site* da entidade bancária na barra de pesquisa[98]. É ainda aconselhado pelo banco utilizar computadores de confiança para aceder ao serviço de *home banking*, nunca fornecer senhas de acesso a contas bancárias a pedido do banco por correio eletrónico ou telefone e, em caso de dúvida, contactar a entidade bancária antes de fornecer quaisquer dados[99]. Estes cuidados permitem evitar um ataque fraudulento, porém, mesmo que rigorosamente respeitados, não impedem intrusões por parte de piratas informáticos que põem o sistema permanentemente à prova. Esclarecendo este dever da instituição bancária, é significante o paralelismo feito por MARIA RAQUEL GUIMARÃES ao afirmar que "o "produto" *home banking* não é diferente, para estes efeitos, de uma qualquer máquina industrial complexa e perigosa que um fabricante de máquinas possa vender: a simples "entrega" não configura um cumprimento satisfatório"[100]. O referido dever justifica-se dada a complexidade do sistema informático que suporta o serviço de banca eletrónica e, principalmente, o risco de ocorrerem utilizações fraudulentas potenciadas pelo facto de as operações bancárias serem realizadas em "ambiente aberto", através da internet e não numa rede privativa do banco[101]. Este é um dever acessório de conduta que decorre particularmente da especial relação de confiança entre a instituição bancária e o seu cliente, tendo a sua origem no contrato de abertura de conta[102]. Desta forma, o banco procura alertar os seus clientes para o cumprimento dos deveres de segurança que devem ser observados na execução do contrato, de modo a que possam aceder às suas contas e movimentá-las em segurança, sem que terceiros desviem dinheiro das mesmas para outras[103].

Sendo a segurança do serviço uma das questões fundamentais do *home banking*, é essencial que o banco utilize uma tecnologia de encriptação (codificação) que garanta a confidencialidade das comunicações entre a entidade bancária e o seu cliente[104].

Além dos deveres que cabem ao banco em virtude do artigo 68º RSP, é necessário ter em conta que, pelo facto de disponibilizar aos clientes o serviço de banca eletrónica, recai sobre

[96] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 62.
[97] Um *link*, na internet, é "o ponto através do qual o utilizador salta (*jump*) de uma página a outra relacionada". Cfr. GARCIA MARQUES, LOURENÇO MARTINS, op. cit., p. 741.
[98] CAROLINA GONZÁLEZ e ÁNGEL TORRENCILLA, Respuestas operativas al "*phishing*". In Policía. Madrid. Nº 190 (2006), pp. 42-47, em especial p. 47.
[99] Ibidem, loc. cit.
[100] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., loc. cit.
[101] MARIA RAQUEL GUIMARÃES, As transferências eletrónicas de fundos…, cit., pp. 44-45.
[102] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., loc. cit.
[103] Ac. TRG de 25/11/2013 (Espinheira Baltazar), cit.
[104] RAMOS PEREIRA, op. cit., p. 696.

a entidade bancária o dever de prestar um serviço eficaz e seguro[105]. Este dever decorre do artigo 73º do Regime Geral das Instituições de Crédito e Sociedades Financeiras (RGICSF)[106] onde se determina que "as instituições bancárias devem assegurar, em todas as atividades que exerçam, elevados níveis de competência técnica, garantindo que a sua organização empresarial funcione com os meios humanos e materiais adequados a assegurar condições apropriadas de qualidade e segurança"[107]. Logo, o banco ao oferecer o serviço de *home banking* tem o dever de manter operacional o sistema informático que o sustenta e de garantir que não ocorrem falhas técnicas durante as operações[108]. Mais do que isso, a instituição bancária deve criar um sistema de acesso à conta bancária e respetiva movimentação no qual o utilizador possa confiar[109]. Este dever do banco é compreensível uma vez que o cliente não tem qualquer controlo sobre os sofisticados meios informáticos da entidade bancária, nem dispõe da assessoria técnica que esta tem à disposição[110].

Do dever de prestar de um serviço eficaz e seguro, decorre ainda o dever de proteção e informação por parte do banco. Segundo o Acórdão do Tribunal da Relação de Guimarães de 25 de novembro de 2013, a instituição bancária cumpre o seu dever de proteção e informação colocando no seu *site* toda a informação disponível sobre segurança, elucidando os seus clientes sobre os métodos utilizados para a captura de dados pessoais por terceiros[111]. Na nossa opinião, este não é o melhor entendimento. Apesar de considerarmos que se encontra cumprido o dever de informação, não podemos concordar que o dever de proteção por parte da entidade bancária se basta com o deixar à disposição dos avisos sobre segurança no *site*. Seguir o entendimento expresso neste acórdão implicaria permitir ao banco exonerar-se do dever de garantir um serviço seguro e eficaz pois através da simples divulgação de informação sobre o perigo da captura de dados pessoais por terceiros, considerar-se-ia que a entidade bancária cumpriu, ativamente, a sua obrigação de proteção do instrumento de pagamento.

A lei estabelece ainda no artigo 68º do RSP outros deveres acessórios de conduta a ser observados pelo banco. No que diz respeito à notificação da utilização não autorizada do instrumento de pagamento à entidade bancária, determina-se que esta deve garantir a disponibilidade, a todo o momento, de meios adequados que permitam ao utilizador comunicar ao banco o ocorrido (alínea c) do n.º 1 do artigo 68º do RSP). Na sequência da

---

[105] Ac. TRL de 12/12/2013 (Tomé Ramião), cit., Ac. TRL de 18/04/2013 (Anabela Calafate), cit., Ac. TRL de 05/11/2013 (Manuel Marques), cit.

[106] DL n.º 298/92 de 31 de dezembro com as alterações introduzidas pelo DL n.º 1/2008, de 3 de janeiro.

[107] Segundo CALVÃO DA SILVA, Direito bancário…, cit., p. 335, esta exigência de observância de padrões profissionais e éticos elevados por parte da entidade bancária resulta, também, da "relação de clientela", isto é, da "especial relação obrigacional complexa de confiança mútua e dominada pelo *intuitus personae*" que se estabelece entre as partes.

[108] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 60.

[109] Ac. TRL de 12/12/2013 (Tomé Ramião), cit.

[110] Ac. TRG de 30/05/2013 (Rita Romeira), cit.

[111] Ac. TRG de 25/11/2013 (Espinheira Baltar), cit., concluiu: "[…] julgamos que a ré [Banco] cumpriu com o seu dever de informação, dando a conhecer, no local onde os clientes […] podiam ter acesso a toda a informação, sobre os perigos de fraude a que os aderentes estavam sujeitos, só pelo facto de terem celebrado este contrato. Esta informação enquadra-se no dever de segurança que a ré [Banco] tinha de prestar na execução do contrato. Pois, com uma utilização correta dos dados fornecidos, sem que passassem para terceiros, o sistema seria seguro."

notificação, o banco deve facultar ao utilizador, a pedido deste, os meios necessários para fazer prova de que a efetuou, até dezoito meses após a notificação (alínea d) do n.º1 do artigo 68º do RSP). Consequentemente, sobre o banco recai ainda o dever de impedir qualquer utilização do instrumento de pagamento logo que a notificação da utilização não autorizada deste tenha sido efetuada (alínea e) do n.º 1 do artigo 68º do RSP). Remetemos, mais uma vez, o estudo aprofundado das referidas disposições legais para o ponto 3.3. do capítulo III.

O RSP determina ainda que corre por conta do banco o risco do envio ao utilizador de instrumento de pagamento, por exemplo, o envio de cartões de pagamento, ou dos respetivos dispositivos de segurança personalizados, como é o caso do cartão matriz com as combinações que permitem o acesso ao serviço de banca eletrónica (n.º 2 do artigo 68º do RSP). Este preceito é de fácil compreensão uma vez que o utilizador não tem qualquer controlo sobre o processo de envio do cartão matriz desde o banco até à sua entrega.

3. A fraude e a segurança do sistema informático

3.1. O sistema bancário na sua vertente telemática

A evolução tecnológica dos últimos anos revolucionou as relações bancárias como as vemos hoje. Este progresso começou com a emissão de cartões, de débito e de crédito, que permitiram aos clientes das instituições bancárias a realização de uma série de operações, utilizando para o efeito os terminais de caixa automática, conhecidos pela sigla ATM. Atualmente, através dos sistemas de *home banking*, podemos aceder a uma multiplicidade de operações bancárias, utilizando para o efeito um computador com acesso à internet.

De forma a permitir o acesso dos clientes ao serviço de banca eletrónica, o banco fornece-lhes códigos de acesso pessoais e cartões matriz compostos por uma infinidade de composições numéricas. Estas senhas de acesso são, geralmente, solicitadas no final de cada operação realizada por meios telemáticos, de modo a autenticá-la, uma vez que o cartão matriz apenas deve ser do conhecimento do aderente ao serviço.[112] Como já foi explicado no ponto 4.2.1. do capítulo I, o cliente é o único que deve utilizar os códigos pessoais e intransmissíveis conferidos pela entidade bancária, não lhe sendo permitido divulgá-los a terceiros. Este dever que vincula o utilizador é compreensível visto que, quer o protocolo do *site* do banco, quer toda a informação nela processada (incluindo as senhas de acesso) são encriptadas, tornando-se quase impossível um terceiro alcançar ou modificar os dados depois de enviados[113].

[112] Ac. STJ de 18/12/2013 (Ana Paula Boularot), cit.
[113] Ibidem.

Contudo, a criptografia[114], principal característica do sistema bancário na sua vertente telemática, não impede a possibilidade de ataques informáticos por *hackers* e a interceção dos códigos de acesso ao serviço de banca eletrónica enquanto estão a ser digitadas, vulgo *keylogging*[115].

Embora os *sites* dos bancos sejam fiáveis, temos de ter presente que a internet constitui uma fonte infindável de informação, onde os comportamentos maliciosos são potenciados pelo facto de tudo na rede ser tendencialmente anónimo[116]. Estas circunstâncias que rodeiam o sistema informático constituem um desafio para os piratas informáticos na procura de falhas.

Como podemos verificar, a internet permitiu aos clientes das entidades bancárias usufruir de uma multiplicidade de vantagens como a comodidade e celeridade inerentes ao serviço de banca eletrónica, porém, associados a estas, várias ameaças também emergiram[117].

3.2. A fraude nas operações de banca eletrónica

Uma vez que o conceito de fraude assume uma especial relevância no presente estudo, importa esclarecer qual o seu sentido técnico-jurídico e quais os seus elementos constitutivos.

Para o efeito, partimos do regime jurídico da simulação constante do CC para encontrar uma definição de fraude no âmbito do direito civil[118]. Deste modo, verificamos que, para qualificar uma atuação como fraudulenta, é necessário o preenchimento cumulativo de dois elementos psicológicos – um comportamento deliberado que o torna doloso e a intenção específica de obter uma vantagem em prejuízo de terceiros [119]. Isto significa que, para haver uma atuação fraudulenta, o sujeito deve visar, como fim imediato, retirar benefícios em prejuízo de terceiros[120].

No âmbito do contrato de *home banking*, a situação típica de uma atuação fraudulenta é a intromissão de pessoa não autorizada em determinada rede informática através de um computador, acompanhada da movimentação do saldo bancário para contas de terceiros[121].

---

[114] A criptografia é o termo utilizado para designar "qualquer técnica de mistura de dados por forma que os mesmo só possam ser compreendidos por quem possuir uma chave de descodificação própria. [...] Existem diferentes níveis de criptografia, quanto mais complexo, mais seguro". Cfr. GARCIA MARQUES, LOURENÇO MARTINS, op. cit., p. 735.
[115] Ac. STJ de 18/12/2013 (Ana Paula Boularot), cit.
[116] Ibidem; Segundo FERNÁNDEZ LÁZARO, La brigada de investigación tecnológica: la investigación policial. In Policía. Madrid. Nº 199 (2007), pp. 18-21, em especial p. 19, apesar de não se poder afirmar com veemência que tudo na internet decorre de forma anónima, certo é que, pelo menos, a sensação de anonimato existe.
[117] MARK A. FOX, Phishing, Pharming and Identity Theft in the Banking Industry. Journal of international banking law and regulation. Sweet and Maxwell (2006), Issue 9, pp. 548-552;
[118] Em especial, art. 240º/1 e 242º/1 do CC. Outra disposição legal que nos permite aferir sobre o conceito de fraude é o art. 1245º do CC relativo à nulidade do jogo e da aposta.
[119] MENEZES CORDEIRO, Tratado de Direito Civil, Tomo II. 4ª edição (reformulada e atualizada). Coimbra: Almedina, 2014, p. 888.
[120] Ibidem, loc. cit.
[121] MARIA RAQUEL GUIMARÃES, As transferências eletrónicas..., cit., p. 209.

Estamos perante um comportamento fraudulento visto que o sujeito que realizou as operações de pagamento não autorizadas pelo titular da conta agiu de forma deliberada uma vez que o seu acesso à conta do cliente via banca eletrónica exigiu a prévia criação de um esquema informático, e teve como fim imediato a obtenção de uma vantagem patrimonial, em prejuízo de terceiro (titular da conta bancária em causa).

Contudo, isto não significa que não possa haver uma utilização fraudulenta do instrumento de pagamento pelo próprio utilizador do serviço de banca eletrónica. É o que acontece quando, por exemplo, o cliente realiza transferências bancárias para uma terceira conta e notifica o banco da utilização não autorizada do instrumento de pagamento, faltando à verdade. Nesta situação, o utilizador do serviço de *home banking* também age de forma deliberada e procura obter benefícios ilegítimos à custa da entidade bancária.

Hoje em dia, a fraude informática no *home banking* constitui uma das formas mais lucrativas de cibercrime. Segundo os indicadores do APWG (Anti-Phishing Working Group)[122], o número de ataques informáticos não pára de aumentar e o setor dos serviços de pagamento é o mais afetado[123]. Este aumento deve-se, em grande parte, à evolução dos métodos utilizados nos ataques cibernautas, o que dificulta a prevenção e deteção deste tipo de fraude e permite a sua proliferação[124]. Por estas razões, a fraude continua a suscitar inseguranças nos clientes bancários, sendo apontada como o principal entrave às operações de banca eletrónica.

Neste âmbito, as modalidades de fraude informática utilizadas são o *phishing* e o *pharming*.

Estas fraudes informáticas que atingem o serviço de *home banking* supõem que o pirata informático tenha acesso à conta de um determinado cliente de um banco através do sistema de banca eletrónica, permitindo-lhe transferir os fundos aí inscritos a débito para outras contas[125]. Este acesso não autorizado é conseguido, tanto no *phishing*, como no *pharming*, através da utilização das chaves de acesso a este serviço bancário que o próprio cliente do banco forneceu, ainda que inadvertidamente, ao criminoso através da internet[126].

---

[122] O Anti-Phishing Working Group (APWG) é uma aliança a nível mundial que visa unificar a resposta global ao cibercrime. O APWG opera através de uma organização sem fins lucrativos, com sede nos EUA e do APWG.EU, fundação de pesquisa sem fins lucrativos estabelecida em Barcelona, em 2013. In https://apwg.org/about-APWG/ (14/09/2014).

[123] Segundo o Phishing Activity Trends Report, 2nd Quarter 2014 (April-June 2014) do APWG, publicado a 28/08/2014, o setor dos serviços de pagamento continua a ser o principal alvo dos piratas informáticos, representando 39,8% dos ataques cibernautas. In http://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf (14/09/2014).

[124] VAN DER MEULEN, You've been warned: Consumer liability in Internet banking fraud. Computer Law & Security Review, vol. 29 (2013), n. º 1, p. 713, in http://www.sciencedirect.com (8/09/2014).

[125] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., pp. 62-63.

[126] Ibidem, loc. cit.

3.2.1. *Phishing*

O *phishing*[127] é uma técnica fraudulenta que se traduz no envio em massa de mensagens de correio eletrónico tendo como objetivo a obtenção de dados que permitam aceder às contas bancárias das vítimas através do serviço de *home banking*[128].

Esta atividade é faticamente complexa e consiste, num primeiro momento, na remessa maciça de mensagens de correio eletrónico (*spam*)[129] que incluem uma ligação para uma página na *web*[130]. Nesta primeira fase, o pirata informático visa enganar a vítima, fazendo-a crer que está a receber um *e-mail* cujo remetente é a sua entidade bancária[131].

Em seguida, a vítima clica na hiperligação referida na mensagem de correio eletrónico. A página que lhe irá surgir no ecrã, apesar de parecer a página oficial de um banco, não o é[132]. Em regra, a página será uma reprodução aproximada do *site* oficial que se pretendeu recriar e terá um aspeto fidedigno, em tudo se assemelhando à página oficial do banco, incluindo elementos identificadores e imagens referentes à entidade que se pretende imitar; todavia, não corresponde à página oficial uma vez que foi construída e é gerida por terceiros sem autorização da entidade cujos sinais se procura reproduzir[133]. A vítima desta técnica, ao abrir o *link*, irá deparar-se com uma página semelhante ao *site* oficial do seu banco, onde lhe será solicitada a identificação através da introdução das suas palavras-passes referentes à sua conta bancária[134] ou de outras informações confidenciais como o número de conta, número de contribuinte ou outros dados pessoais[135]. Deste modo, os piratas informáticos passam a conhecer os códigos secretos relativos às contas bancárias da vítima, permitindo-lhes o acesso a estas e a realização de transferências de montantes sem conhecimento, nem consentimento do titular da conta[136].

O *phishing*, tal como a maioria dos comportamentos maliciosos que ocorrem na *web*, é uma atividade de dimensão transnacional que começou por surgir ligado à obtenção de dados de

---

[127] O termo pode derivar de uma mistura de *phreaking* (desvio de sistemas informáticos) e *fishing* (do inglês, pesca). Cfr. AMAUDRIC DU CHAUFFAUT, LIMOUZIN-LAMOTHE, Une nouvelle forme de criminalité informatique à l'épreuve de la loi: le *phishing*. In Expertises, 2005, n.º 291 apud GARCIA MARQUES, LOURENÇO MARTINS, op. cit, p. 655. Outros referem que este termo provém apenas da palavra inglesa *fishing*, fazendo alusão à tentativa de que as vítimas "mordam o anzol" e "caiam" no esquema. Cfr. FRANCISCO LUÍS, Proteger o dinheiro – *Home banking*, Conselhos aos utilizadores. Inforbanca. Lisboa: Instituto de Formação Bancária, Associação Portuguesa de Bancos. N.º 88 (abril-junho 2011), p. 12.

[128] MARIA RAQUEL GUIMARÃES, A fraude no comércio eletrónico…, cit., p. 583, nota 10.

[129] *Spam* é o "envio maciço de mensagens de correio eletrónico não solicitadas, em quantidades que podem não apenas causar incómodo como chegar ao ponto de bloquear o sistema de receção por saturação". Cfr. GARCIA MARQUES, LOURENÇO MARTINS, op. cit., p. 655.

[130] PEDRO VERDELHO, *Phishing* e outras formas de defraudação nas redes de comunicação. In Direito da Sociedade da Informação (Oliveira Ascensão, coordenação). Vol. VIII. Coimbra: Coimbra Editora, 2009, p. 413.

[131] CAROLINA GONZÁLEZ e ÁNGEL TORRENCILLA, op. cit., p. 42; MARIA RAQUEL GUIMARÃES, A fraude no comércio eletrónico…, cit., loc. cit.

[132] PEDRO VERDELHO, op. cit., p. 413; Segundo FERNÁNDEZ LÁZARO, op. cit., pp. 18-21, em especial p. 19, esta técnica fraudulenta consiste em suplantar a página web de uma entidade bancária, fazendo crer ao usuário que se encontra em face da página oficial da mesma.

[133] PEDRO VERDELHO, op. cit., loc. cit.; De acordo com CAROLINA GONZÁLEZ e ÁNGEL TORRENCILLA, op. cit., pp. 44-45, normalmente, trata-se de duplicados de páginas web de entidades bancárias.

[134] PEDRO VERDELHO, op. cit., loc. cit.

[135] CAROLINA GONZÁLEZ e ÁNGEL TORRENCILLA, op. cit., p. 42.

[136] PEDRO VERDELHO, op. cit., loc. cit.; FERNÁNDEZ LÁZARO, op. cit., loc. cit.

cartões de crédito, mas que hoje em dia tem como principal alvo o serviço de *home banking*[137].

3.2.2. *Pharming*

A par do *phishing*, tem-se desenvolvido uma técnica mais sofisticada e perigosa, o *pharming*.

Esta nova modalidade de fraude informática consiste na "difusão, via *spam*, de ficheiros ocultos, que igualmente de forma oculta se autoinstalam nos computadores ou sistemas informáticos das vítimas"[138]. Depois de instalados, são feitas alterações nos arquivos do sistema, sem conhecimento do dono do computador, nomeadamente nos ficheiros que contêm os "favoritos" e o registo de *cookies.*[139] [140] Estes ficheiros ocultos são programas que captam os códigos de pulsação do teclado, *keyloggers*, e permitem que, sempre que o utilizador digita o endereço de determinado *site*, o sistema, por via das mencionadas alterações, redirija-o para uma outra página, para além de registarem tudo o que é digitado no teclado do utilizador (nomeadamente, as palavras-passe de acesso ao serviço de *home banking*)[141]. Isto significa que estes ficheiros corrompem o IP[142] dos *sites* oficiais dos bancos no computador da vítima, redirecionando o utilizador do serviço de banca eletrónica para uma outra página sempre que digita o *site* correto da sua entidade bancária[143].

É nesta página, em tudo similar à página oficial do banco, que o cliente, acreditando que se encontra no *site* oficial, indica as suas palavras-passes de acesso ao serviço de banca eletrónica, permitindo posteriormente ao pirata informático transferir montantes para outras contas[144].

Tal como sucede no *phishing*, a página que aparece no ecrã do computador da vítima surge como um clone do *site* legítimo da entidade bancária. Quando o utilizador acredita que está a aceder a uma página escolhida por si, está, na verdade, a aceder ao IP de uma outra página *web*[145]. Assim, o *pharming* procura obter os códigos de acesso a contas bancárias através de

---

[137] PEDRO VERDELHO, op. cit., loc. cit. Esta modalidade de fraude informática teve o seu auge nos anos de 2008 e 2009, tendo vindo a decrescer significativamente deste 2010 – cfr. IBM – Relatório Semestral de Tendências e Riscos IBM x-force 2011, setembro 2011. P. 49, figura 23 in http://ftp.software.ibm.com/la/documents/imc/br/commons/Trend_Risk_report_Sept_2011_ptb.pdf (18/09/2014).

[138] PEDRO VERDELHO, op. cit., p. 415

[139] O *cookie* é "um arquivo de texto que, via de regra, é gravado no disco do computador e utilizado pela memória RAM enquanto o internauta navega na internet. Deste modo, aquando de sua primeira visita a um *website* podem ser formuladas perguntas de caráter pessoal. Tais informações serão gravadas no *cookie* colocado no sistema para que uma futura navegação seja "personalizada". Cfr. RAMOS PEREIRA, Direito da Internet e Comércio Eletrónico. Lisboa: Quid Iuris, 2001, p. 245.

[140] PEDRO VERDELHO, op. cit., loc. cit.

[141] CAROLINA GONZÁLEZ e ÁNGEL TORRENCILLA, op. cit., p. 44.

[142] O IP *(Internet Protocol)* é "o endereço específico de um equipamento na internet; define como os pacotes de dados vão da origem ao destino." Cfr. GARCIA MARQUES, LOURENÇO MARTINS, op. cit., p. 740.

[143] MARIA RAQUEL GUIMARÃES, A fraude no comércio eletrónico…, cit., pp. 583-584.

[144] Ibidem, loc. cit.

[145] Ibidem, loc. cit.

um redirecionamento para um outro *site*, de forma a, posteriormente, permitir aos piratas informáticos a movimentação dos montantes aí existentes em seu proveito[146].

Além do procedimento exposto *supra* que consiste no alojamento de um *software* malicioso no computador do utilizador do serviço de *home banking*, o *pharming* pode ser posto em prática através de outros métodos. Assim, esta modalidade também pode ocorrer quando o nome de um banco real e legítimo é escrito na barra de direções da internet com um ligeiro erro ortográfico, sendo o cliente redirecionado para um *site* falso ou quando um pirata informático "sequestra" a página legítima de uma entidade bancária, conduzindo para um site falso todas as pessoas que a ele acedam[147].

O *pharming* é uma fraude eletrónica muito mais perigosa para os utilizadores do serviço de *home banking* do que o *phishing* e muito mais eficaz para os criminosos, não sendo necessário aproveitarem-se de um momento concreto ou ultrapassarem a desconfiança dos utilizadores do serviço de banca eletrónica, bastando-lhes ultrapassar o sistema de proteção do computador[148]. Enquanto, no *phishing,* o "isco" é uma mensagem de correio eletrónico que parece provir de uma entidade bancária e que contém uma ligação para uma página forjada pelo pirata informático, no *pharming,* o utilizador do serviço é enganado sem se aperceber visto que o ficheiro oculto que vai permitir a redireção para uma página forjada autoinstalou-se, não suscitando qualquer estranheza. Por essa razão, segundo PEDRO VERDELHO, esta modalidade de fraude informática é muito difícil de reconhecer, mesmo para utilizadores experientes e alertados para a temática da segurança[149].

3.2.3. Distinção entre as duas modalidades de fraude informática. Enquadramento legal

Para distinguir, de forma clara, as duas técnicas informáticas é importante salientar os traços caracterizadores de cada uma.

Tanto no *phishing*, como no *pharming*, conseguimos destacar duas fases na sua execução, sendo que a primeira fase é distinta nas duas modalidades e a segunda fase é idêntica em ambas.

A primeira fase no *phishing* caracteriza-se pela receção de uma mensagem de correio eletrónico que parece ter como remetente um banco e que contém uma ligação para uma página *web*. Para a vítima ser apanhada no esquema tem de clicar no referido *link* e será direcionada para uma página idêntica ao *site* oficial da entidade bancária.

---

[146] PEDRO VERDELHO, op. cit., p. 416; MARK A. FOX, op. cit., loc. cit.
[147] Federal Deposit Insurance Corporation – Guidance on How Financial Institutions Can Protect against Pharming attacks. Financial Institution Letters (2005), in www.fdic.gov/news/news/financial/2005/fil6405a.html (27/07/2014).
[148] CAROLINA GONZÁLEZ e ÁNGEL TORRENCILLA, op. cit., loc. cit.
[149] PEDRO VERDELHO, op. cit., p. 415

Por outro lado, no *pharming,* esta etapa adquire pouca visibilidade uma vez que se basta com a autoinstalação de um ficheiro oculto no computador da vítima. Assim, o utilizador do computador não tem margem para desconfiar de algum indício suspeito, como no *phishing* tem a receção de um *e-mail*. A partir desse momento, sempre que a vítima queira aceder à página oficial do seu banco será redirecionado para um outro *site* construído pelo pirata informático.

A segunda fase das duas técnicas fraudulentas é idêntica. A vítima encontra-se numa página construída por um *hacker* e que é em tudo semelhante ao *site* oficial da entidade bancária. Nesta página serão solicitadas todas as palavras-passe referentes ao acesso ao serviço de banca eletrónica, permitindo aos piratas informáticos aceder e movimentar as contas bancárias das vítimas.

Em suma, estas duas modalidades de fraude informática têm em comum o facto de se manifestarem quando uma pessoa não autorizada se introduz numa rede informática e movimenta o saldo de contas bancárias de clientes através de um computador.[150] Esta intrusão não autorizada num sistema informático reconduz-se ao crime de falsidade informática, consagrado no artigo 3º da Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro), sendo punível com pena de prisão de um a cinco anos[151].

Apesar de se subsumirem a este enquadramento penal, o *phishing* e o *pharming* não surgem tipificados na lei como figuras autónomas. No entanto, estas modalidades de fraude informática, e principalmente o *phishing*, são reconhecidas dada a sua frequente ocorrência na prática e a sua sedimentação doutrinária[152] e jurisprudencial[153].

3.3. A identificação do tipo de fraude informática pelos tribunais superiores

Neste ponto, importa ter presente que, nas situações de fraude informática, é difícil obter prova documental ou pericial que permita apurar o que realmente aconteceu.

[150] MARIA RAQUEL GUIMARÃES, As transferências eletrónicas de fundos…, cit., p. 209.
[151] O n.º 1 do art. 3º da Lei do Cibercrime determina que "quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias" e o n.º 2 acrescenta que "Quando as ações descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão."
[152] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., pp. 62-64 e A fraude no comércio eletrónico…, cit., em particular nota 11 da p. 583; PEDRO VERDELHO, op. cit., pp. 413-416.
[153] Ac. TRL de 26/10/2010 (Maria Amélia Ribeiro), cit.; Ac. TRE de 7/07/2011 (Pedro Vaz Pato), Proc. 76/10.2JASTB-A.E1, in http://www.dgsi.pt; Ac. TRL de 24/05/2012 (Ezagüi Martins), cit.; Ac. TRG de 23/10/2012 (Filipe Caroço), cit.; Ac. TRG de 30/05/2013 (Rita Romeira), cit.; Ac. STJ de 18/12/2013 (Ana Paula Boularot), cit.; Ac. TRP de 29/04/2014 (Francisco Matos), proc. 225/12.6TJVNF.P1, in http://www.dgsi.pt.

Depois de analisar a jurisprudência dos nossos tribunais superiores quanto a este tema, verificamos que, na grande maioria dos casos[154], o julgador classifica as ocorrências como situações nas quais foram utilizadas técnicas de *phishing*, quando, na realidade, se examinarmos os factos dados como assentes, podemos concluir que se trata de casos de *pharming*. Aliás, os únicos acórdãos que identificam corretamente que estão perante situações de *pharming* são o Acórdão do Supremo Tribunal de Justiça de 18 de dezembro de 2013 e o Acórdão do Tribunal da Relação do Porto de 29 de abril de 2014[155].

Como podemos observar na maioria dos acórdãos, tudo parece indicar que as operações de pagamento não autorizadas tiveram origem no acesso do cliente a "uma página web falsa [criada por um terceiro] e copiada na página de abertura do *site* do serviço de banca eletrónica"[156], onde terá introduzido os dados que permitiam aceder à sua conta bancária. Apesar de a única certeza que resta, muitas vezes, ser o facto de os códigos terem sido divulgados a terceiros através da internet, não podemos ignorar que, em todos os casos que chegaram aos tribunais superiores no âmbito do serviço de banca eletrónica, não existe sequer uma referência à receção de mensagens de correio eletrónico solicitando os dados que permitem aceder ao referido serviço. A omissão da referência a um *e-mail* afasta desde logo a qualificação da fraude informática subjacente como *phishing*, uma vez que a receção de uma mensagem de correio eletrónico é um dos elementos do tipo que permite caracterizar esta técnica fraudulenta.

De acordo com o exposto neste capítulo, verifica-se que houve alguma confusão por parte dos tribunais superiores na identificação do tipo de fraude informática de que os clientes dos serviços de *home banking* foram vítimas. Isto é relevante, se tivermos em conta que a modalidade de *pharming* é muito mais difícil de detetar do que o *phishing*, sendo, por isso, muito menos censurável a conduta do cliente enganado por este esquema.

4. A repartição dos prejuízos decorrentes de fraude informática no contrato de *home banking*

4.1. Apresentação da problemática

A questão da repartição dos prejuízos decorrentes de operações fraudulentas através do serviço de *home banking* tem merecido a atenção dos nossos tribunais superiores nos últimos anos[157].

[154] Ac. TRL de 26/10/2010 (Maria Amélia Ribeiro), cit.; Ac. TRL de 24/05/2012 (Ezagüi Martins), cit.; Ac. TRG de 23/10/2012 (Filipe Caroço), cit.; Ac. TRL de 18/04/2013 (Anabela Calafate), cit.; Ac. TRG de 30/05/2013 (Rita Romeira), cit.; Ac. TRL de 28/06/2013 (Anabela Calafate), cit.; Ac. TRL de 5/11/2013 (Manuel Marques), cit.; Ac. TRG de 25/11/2013 (Espinheira Baltazar), cit.; Ac. TRL de 12/12/2013 (Tomé Ramião), cit.
[155] Ac. TRP de 29/04/2014 (Francisco Matos), cit.
[156] Ac. STJ de 18/12/2013 (Ana Paula Boularot), cit.
[157] Mais precisamente desde 2010. A primeira decisão dos tribunais superiores portugueses sobre este assunto foi proferida pelo TRL em 26/10/2010 (Maria Amélia Ribeiro), cit.

Na maioria das situações, a descrição dos factos é muito semelhante; isto permite-nos condensar os acontecimentos principais e apresentar uma breve exposição do caso típico que tem chegado aos nossos tribunais.

Regra geral, a relação contratual entre o banco e o cliente inicia-se com a celebração do contrato de abertura de conta e, em simultâneo ou em momento posterior, como forma de movimentar e consultar a sua conta, este último adere ao serviço disponibilizado pelo banco para gestão de contas e realização de operações bancárias através da internet – *home banking*. De seguida, a instituição bancária entrega-lhe as chaves de acesso ao serviço: geralmente, o número de contrato, um código secreto e um cartão matriz de coordenadas. Para aceder ao serviço, o cliente dirige-se à página do banco, seleciona a área destinada a este efeito e autentica-se, inserindo o número de contrato e a respetiva senha nos campos assinalados. Normalmente, se o aderente apenas pretender consultar informações sobre as suas contas bancárias não lhe será solicitado mais nenhum dispositivo de segurança personalizado mas, se pretender efetuar uma operação bancária, nomeadamente uma transferência de fundos para outra conta, o banco exige-lhe que indique um certo número de dígitos que constam das coordenadas do seu cartão matriz, escolhidas aleatoriamente pelo sistema informático, e/ou pede-lhe um código de confirmação que será enviado por SMS para o número de telemóvel do cliente de forma a confirmar a respetiva movimentação na sua conta bancária.

O problema surge quando são debitados montantes das contas dos clientes, sem o seu consentimento, através do sistema de banca eletrónica.

Perante esta situação colocam-se algumas questões: quem suporta os prejuízos decorrentes da transferência fraudulenta de fundos da conta do cliente? A quem incumbe provar que o débito na conta bancária do utilizador não foi realizado por este? É suficiente que o banco prove que o sistema de *home banking* funcionava normalmente antes e depois da referida operação para afastar a ocorrência de falha técnica?[158]

4.2. Solução anterior à entrada em vigor do RSP

Antes de começar o estudo do RSP no que diz respeito à repartição das perdas resultantes de operações fraudulentas, importa identificar qual a solução conferida pelo nosso ordenamento jurídico antes da sua entrada em vigor[159]. A relevância deste ponto torna-se evidente quando verificamos que, na maioria dos casos que, até hoje, foram julgados pelos

[158] Questão colocada por MARIA RAQUEL GUIMARÃES relativamente à distribuição do ónus da prova nos casos de operações fraudulentas com cartões de pagamento – As transferências eletrónicas…, cit., p. 235.
[159] Este diploma entrou em vigor em 1/11/2009, de acordo com o art. 11º do DL n.º 317/2009.

tribunais superiores[160], os factos ocorreram em momento anterior à entrada em vigor do RSP, não se encontrando ainda abrangidos pela sua disciplina.

Numa primeira hipótese, pode-se considerar que se deve contextualizar a questão à luz do seu regime jurídico, tendo presente que a Diretiva que esteve na sua base datava já de 2007 e as soluções aí plasmadas se mostram tributárias das recomendações comunitárias sobre pagamentos eletrónicos dos anos 80 e 90[161]. Porém, temos de ter presente que as diretivas antes de serem transpostas não têm caráter vinculativo na nossa ordem jurídica logo, rigorosamente, não podemos basear a solução para os problemas aqui em causa nos referidos atos jurídicos comunitários[162] .

Atente-se, também, na questão de aplicação da lei no tempo que se levanta com as disposições complementares, transitórias e finais do RSP, mais precisamente no artigo 101º. O n.º 1 deste preceito prescreve que "o regime constante do presente regime jurídico não prejudica a validade dos contratos em vigor relativos aos serviços de pagamento nele regulados, sendo-lhes desde logo aplicáveis as disposições do presente regime jurídico que se mostrem mais favoráveis aos utilizadores de serviços de pagamento". Os n.º 2 e 3 desse artigo acrescentam ainda o dever dos bancos de ajustarem os contratos vigentes antes da entrada em vigor do RSP às disposições do diploma no prazo máximo de seis meses e de remeterem aos seus clientes uma cópia integral das condições contratuais após a referida adaptação. Aqui, impõe-se esclarecer que esta disposição legal não determina a aplicação retroativa do regime jurídico dos serviços de pagamento, contrariamente ao que parece ter sido o entendimento do Supremo Tribunal de Justiça no Acórdão de 18 de dezembro de 2013[163]. O n.º 1 do artigo 101º ao estabelecer que aos contratos existentes à data da entrada em vigor do RSP se aplica o regime nele prescrito não prejudica o facto de se encontrarem ressalvados os efeitos já produzidos por factos passados (n.º 1 do artigo 12º CC)[164]. Assim, deve-se entender que uma norma com este teor visa apenas afastar o entendimento de que só os contratos novos ficarão submetidos ao regime da lei que entrou

---

[160] Ac. TRL de 26/10/2010 (Maria Amélia Ribeiro), cit.; Ac. TRL de 24/05/2012 (Ezagüi Martins), cit.; Ac. TRG de 23/10/2012 (Filipe Caroço), cit.; Ac. TRL de 18/04/2013 (Anabela Calafate), cit.; Ac. TRG de 30/05/2013 (Rita Romeira), cit.; Ac. TRL de 28/06/2013 (Anabela Calafate), cit.; Ac. TRP de 29/10/2013 (Francisco Matos), cit.; Ac. TRG de 25/11/2013 (Espinheira Baltazar), cit.; Ac. TRL de 12/12/2013 (Tomé Ramião), cit.; Ac. STJ de 18/12/2013 (Ana Paula Boularot), cit.

[161] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 57.

[162] O n.º 1 do art. 3º do DL n.º 166/95 de 15/07 relativo à emissão de cartões de crédito determinava que as entidades emitentes de cartões de crédito tivessem em conta as recomendações emanadas da União Europeia. Com este preceito surgiu a dúvida se se estaria a abrir o caminho para a aplicação direta dos princípios vertidos em recomendações comunitárias e para a aquisição de caráter vinculativo destes atos jurídicos na ordem jurídica portuguesa. O STJ foi chamado a esclarecer a questão no âmbito da decisão sobre a validade de umas cláusulas contratuais gerais inseridas em contratos de utilização de instrumentos de pagamentos eletrónicos. O STJ na sua decisão "teve em conta" as recomendações sobre a matéria mas esclareceu que estas não têm valor vinculativo pois a técnica legislativa utilizada neste artigo do DL n.º 166/95 não está a conceder à normação contidas naquelas recomendações a vinculatividade que, por si só, não dispõem. Cfr. Ac. STJ de 23/11/1999 (Garcia Marques). Coletânea de Jurisprudência, Acórdãos do STJ. Coimbra: Associação de Solidariedade Social Casa do Juiz. Ano VII, Tomo III (1999), pp. 100-108.
Temos também de ter em conta que, no caso de operações fraudulentas decorrentes de fraude informática, não existe nenhum preceito em vigor na nossa ordem jurídica que dite que temos de "ter em conta" as recomendações comunitárias.

[163] Cfr. Ac. STJ de 18/12/2013 (Ana Paula Boularot), cit., onde se declara que "[…] a aplicação do DL 317/2009 […] o qual, não obstante seja posterior aos factos em causa nesta ação, a eles é aplicável, ex vi do seu artigo 101º, n.º 1".

[164] JOÃO BAPTISTA MACHADO, Introdução ao Direito e ao Discurso Legitimador. 17ª reimpressão. Coimbra: Almedina, 2008, p. 227, nota 2.

em vigor[165]. Isto significa que as cláusulas, que estivessem a ser aplicadas em contratos relativos a serviços de pagamento, que contrariassem o disposto no RSP aquando da sua entrada em vigor, considerar-se-iam substituídas por estas porque o disposto neste regime jurídico prevalece. Por outro lado, os efeitos já produzidos por factos passados, como é o caso dos prejuízos causados por operações não autorizadas decorrentes de fraude informática, devem ser resolvidos segundo a normação que vigorava antes da entrada em vigor do RSP.

Para resolver este problema, parece que o caminho a seguir é o que decorre do incumprimento dos deveres contratuais que resultam do contrato de *home banking*. Deste contrato emerge como dever acessório de conduta do banco, o dever de prestar um serviço eficaz e seguro que permita aos seus clientes confiar no sistema de acesso à sua conta bancária e respetiva movimentação via *online*. Por outro lado, o seu utilizador deve observar uma série de deveres acessórios de conduta ligados à segurança do sistema e dos dispositivos de segurança personalizados, nomeadamente mantendo a sua confidencialidade.

A complexidade e sofisticação dos sistemas informáticos que suportam o serviço de *home banking*, criados e controlados pelas entidades bancárias, a grande exigência dos mecanismos de segurança das operações bancárias através deles realizados[166] e o facto de se tratar de uma relação contratual, justificam o funcionamento da presunção de culpa prevista pelo n.º 1 do artigo 799º do CC[167]. Esta disposição legal determina que "incumbe ao devedor provar que a falta de cumprimento ou o cumprimento defeituoso da obrigação não procede de culpa sua". Isto significa que é o banco que se encontra onerado com a prova de que o acesso de terceiros à conta do cliente não se ficou a dever a qualquer vulnerabilidade do sistema de segurança por si implementado. O facto de o risco de o sistema gerar prejuízos não imputáveis aos seus utilizadores recair sobre a entidade bancária compreende-se pois é a esta que cabe assegurar a regularidade do seu funcionamento e o controlo dos meios técnicos utilizados[168]. Assim, é pela entidade bancária que corre o risco de uma intromissão fraudulenta nas contas bancárias dos seus clientes realizada através desse sistema, ou seja, em última análise, é esta que deve arcar com os prejuízos potenciados pela debilidade dos sistemas de pagamento que comercializa[169]. Este entendimento subsume-se ao disposto no artigo 798º do CC que determina que "o devedor que falta culposamente ao cumprimento da obrigação torna-se responsável pelo prejuízo que causa ao credor".

Assim, ao utilizador basta demonstrar o não cumprimento do dever de prestar um serviço seguro que cabia ao banco e o dano que daí decorreu. Para ilidir a presunção do n.º 1 do artigo 799º do CC, a entidade bancária terá de provar que não teve culpa no ocorrido,

---

[165] Ibidem, loc. cit.
[166] Daí que a Relação de Guimarães tenha realçado, e bem, que não é legítimo ao banco invocar a sua irresponsabilidade numa situação de fraude informática com o argumento que tal ocorreu no computador do cliente e não em qualquer sistema seu ou por si dominado, quando a utilização de computadores pessoais e não do próprio banco é pressuposto do serviço de *home banking*. Cfr. Ac. TRG de 30/05/2013 (Rita Romeira), cit.
[167] Ac. TRG de 23/10/2012 (Filipe Caroço), cit.
[168] MARIA RAQUEL GUIMARÃES, As transferências eletrónicas de fundos…, cit., pp. 230-231.
[169] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 65.

mostrando que não descurou o seu dever de prestar um serviço eficaz e seguro. Caso não consiga afastar a presunção, o banco deve suportar os prejuízos derivados do acesso fraudulento à conta bancária do seu cliente. Este tem sido o entendimento dominante na nossa jurisprudência[170].

No âmbito indemnizatório, importa deixar uma nota acerca da aplicação do instituto da culpa do lesado nesta sede, apesar de tal nunca ter sido referido pela nossa jurisprudência.

De acordo com o n.º 1 do artigo 570º do CC, "quando um facto culposo do lesado tiver concorrido para a produção ou agravamento dos danos, cabe ao tribunal determinar, com base na gravidade das culpas de ambas as partes e nas consequências que delas resultaram, se a indemnização deve ser totalmente concedida, reduzida ou mesmo excluída". A existência de culpa do lesado deve ser provada por aquele que a alega, todavia esta é de conhecimento oficioso uma vez que o tribunal conhecerá dela mesmo que não seja alegada (artigo 572º do CC). Importa, desde logo, esclarecer que é de admitir a aplicação deste regime à responsabilidade contratual[171].

Para perceber o cerne do instituto da "culpa" do lesado, devemos centrar a nossa atenção no conceito de "culpa" no recorte do artigo 570º. Considera-se que o facto "culposo" do lesado deve ser entendido como uma "autorresponsabilização de uma conduta na perspetiva dos interesses próprios sacrificados e da indemnização (plena) pretendida", isto é, uma "responsabilização do lesado perante si mesmo"[172]. O pressuposto "culpa" vai conduzir a um processo de ponderação das condutas que irá delimitar o quantum indemnizatório tendo em conta a maior ou menor participação do lesado na produção do dano, em ordem à repartição justa e equilibrada do dano[173]. Assim, o lesado será privado de parte da indemnização que lhe cabia, conforme o maior ou menor relevo da sua conduta para a produção do dano, condicionando, desta forma, as consequências indemnizatórias da responsabilidade do lesante[174]. Para esta ponderação, o tribunal goza de uma ampla liberdade para encontrar as soluções que considere mais justas.

Por fim, importa não esquecer que o dano deve resultar da articulação causal das condutas do lesante e do lesado[175]. Para aferir esta articulação, é de aplicar o critério da causalidade adequada à relação causal entre o comportamento do lesado e o dano daí resultante, devendo-se, portanto, formular um juízo objetivo de probabilidade, questionando se o

---

[170] Ac. TRL de 26/10/2010 (Maria Amélia Ribeiro), cit.; Ac. TRL de 24/05/2012 (Ezagüi Martins), cit.; Ac. TRG de 23/10/2012 (Filipe Caroço), cit.; Ac. TRL de 18/04/2013 (Anabela Calafate), cit.; Ac. TRG de 30/05/2013 (Rita Romeira), cit.; Ac. TRL de 28/06/2013 (Anabela Calafate), cit.; Ac. TRG de 25/11/2013 (Espinheira Baltazar), cit.; Ac. TRL de 12/12/2013 (Tomé Ramião), cit.;

[171] BRANDÃO PROENÇA, A conduta do lesado como pressuposto e critério de imputação do dano extracontratual. Coimbra: Almedina, 1997, p. 30, e p. 49, nota 93.

[172] Ibidem, p. 74 e 123. Segundo o Autor, a exigência legal da "culpa" não tem qualquer função sancionatória, contrariamente ao que se defende para a responsabilidade do lesante, devendo-se qualificar como um ónus jurídico visto que se tratam de comportamentos cuja "inobservância não corresponde propriamente uma sanção por ausência de violação de um qualquer preceito cominatório", p. 131.

[173] Ibidem, p. 123 e 143.

[174] Ibidem, p. 394.

[175] Ibidem, p. 426.

comportamento do lesado, tendo em conta a condição colocada pelo lesante, favorecia a produção do dano ocorrido e se esse surgiu como seu efeito provável[176].

No âmbito das operações fraudulentas no *home banking*, consideramos flagrante a aplicação do instituto da culpa do lesado nos casos em que o banco consiga provar que o utilizador agiu de forma negligente.

4.3. O regime vigente

Os problemas levantados por esta problemática inserem-se no âmbito das operações de transferência eletrónica de fundos[177] e encontram-se, atualmente, regulados no RSP. Neste diploma, o legislador não distingue entre operações realizadas à distância e operações presenciais, nem entre utilização de cartões de pagamento (débito ou crédito) e utilização de outros instrumentos de pagamento (como a banca eletrónica), pelo que abrange a totalidade das operações e dos instrumentos de pagamento aqui referidos.

Neste ponto 3, pretendemos aprofundar este regime jurídico para melhor compreender como é realizada a repartição dos prejuízos decorrentes de fraude informática no contrato de *home banking.*

4.3.1. Notas prévias

A repartição das perdas advindas de fraude informática num contrato de banca eletrónica é uma tarefa difícil pois implica encontrar resposta a várias questões para chegar à solução final. É necessário verificar o cumprimento dos deveres impostos às partes no contrato, avaliar o grau de censura da sua atuação, aplicar as regras relativas ao ónus da prova, para, finalmente, apurar como será distribuído o risco quanto aos prejuízos resultantes de operações não imputáveis a título de culpa a nenhuma das partes do contrato de *home banking*[178].

É importante deixar claro que, nestes casos que envolvem a intervenção de terceiros (piratas informáticos), não existe nenhuma relação entre o utilizador do serviço e o beneficiário da operação fraudulenta visto que este último é um terceiro face aos contratos bancários celebrados entre o cliente e o banco[179]. Tendo em conta que estamos no âmbito contratual, o que importa definir é como se fará a distribuição do risco entre as partes – a entidade

[176] Ibidem, pp. 442-443.
[177] Pode-se definir transferências eletrónicas de fundos como operações de transferência de fundos iniciadas através de terminal eletrónico, telefone, computador ou fita magnética, com o objetivo de ordenar, instruir ou autorizar uma instituição financeira a debitar ou a creditar uma conta. Definição adotada pelo *Electronic Fund Transfers Act* americano apud MARIA RAQUEL GUIMARÃES, As transferências eletrónicas de fundos…, cit., pp. 19-20 e Comércio eletrónico…, cit., p. 58.
[178] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 69.
[179] Ibidem, p. 68.

bancária e o cliente –, quem deverá suportar as perdas resultantes de operações de pagamento não autorizadas[180]. Por outro lado, verificamos que existe uma relação entre o banco e os beneficiários das operações de pagamento não autorizadas pelo utilizador do instrumento de pagamento (terceiros, piratas informáticos), tendo o primeiro legitimidade para agir contra estes de forma a reaver os montantes reembolsados ao cliente em virtude da fraude informática[181].

Devemos ainda ter presente durante a análise desta problemática que podem ser aplicadas disposições legais diferentes aos utilizadores de serviços de pagamento que sejam consumidores e aos que não o sejam pois, geralmente, estes últimos encontram-se em melhor posição para avaliar o risco de fraude e tomar medidas de salvaguarda[182]. Ressalvamos que, na nossa exposição, pretendemos centrar-nos nos casos em que os utilizadores vítimas de fraude informática são consumidores, sendo-lhes aplicável o regime dos artigos 70º a 72º do RSP (aqui provido de força imperativa), assim como a legislação de proteção do consumidor e os princípios que dela decorram.

Atualmente, a questão da distribuição do risco por operações de pagamento não autorizadas encontra-se disciplinada no artigo 72º do RSP, onde se prevê a limitação da responsabilidade patrimonial do utilizador do serviço de banca eletrónica ao valor de € 150 nos casos em que a apropriação abusiva do instrumento de pagamento não foi potenciada por culpa da sua parte[183]. Esta solução já advém da Recomendação da Comissão 97/489/CE, de 30/7/1997, relativa às transações realizadas através de um instrumento de pagamento eletrónico e, nomeadamente às relações entre o emitente e o detentor[184], depois acolhidas pela DSP, no seu artigo 61º. A relevância destas normas limitadoras da responsabilidade do cliente no caso de operações não autorizadas é manifesta, uma vez que o RSP chega mesmo a sancionar a sua inobservância com coimas elevadas, considerando a violação do previsto no artigo 72º uma infração especialmente grave (alínea q) do artigo 95º do RSP)[185].

---

[180] Uma operação não autorizada consiste numa operação de pagamento para a qual o titular [do instrumento de pagamento] não deu o seu consentimento. Cfr. definição de operação de pagamento autorizada do n.º 1 do art. 65º do RSP.

[181] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 69.

[182] Considerando 35 da DSP. Esta ideia encontra-se plasmada no nosso ordenamento jurídico no n.º 2 do art. 62º do RSP que determina que "quando o utilizador do serviço de pagamento não seja um consumidor, as partes podem afastar a aplicação, no todo ou em parte, do disposto no n.º 3 do artigo 63º, no n.º 3 do artigo 65º e nos artigos 70º, 72º, 73º, 74º, 77º, 86º e 87º e, bem assim, acordar num prazo diferente do fixado no artigo 69º." O n.º 1 do referido artigo estende ainda às microempresas o regime aplicável aos consumidores.

[183] Note-se que a letra do art. 72º do RSP (assim como a do art. 61º da DSP que esteve na sua origem), mesmo na epígrafe ("responsabilidade do ordenante por operações de pagamento não autorizadas") designa o titular do instrumento de pagamento como "ordenante" quando estamos numa situação em que este nada ordenou. Isto demonstra a confusão entre o contrato-quadro que liga o banco ao seu cliente e os contratos sucessivos (mandatos) em que são dadas ordens de pagamento ao banco em benefício de terceiro. Segundo a alínea i) do art. 2º do RSP, ordenante é "uma pessoa singular ou coletiva que detém uma conta de pagamento e que autoriza uma ordem de pagamento a partir dessa conta […]"; como é evidente, uma pessoa não pode, simultaneamente, autorizar e não autorizar uma ordem de pagamento. Era preferível utilizar a expressão do art. 70º do RSP "utilizador de serviços de pagamento que negue ter autorizado uma operação de pagamento executada", além disso, não nos esqueçamos que nos casos de operações não autorizadas, o "ordenante" é o terceiro que atua fraudulentamente! Cfr. MARIA RAQUEL GUIMARÃES, The debit and credit card frame work contract…, cit., pp. 13-16.

[184] In JOUE, n. º 208 de 2/8/1997, pp. 52-58.

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

Vamos iniciar o estudo do regime vigente começando por analisar as regras do ónus da prova aplicáveis aos casos de repartição das perdas advindas de fraude informática num contrato de *home banking* uma vez que estas têm uma forte influência na resolução do problema que aqui apresentamos, como poderemos constatar mais adiante.

4.3.2. Atribuição do ónus da prova à entidade bancária

O RSP, contrariamente ao que acontecia na Recomendação comunitária 97/489/CE, pronuncia-se sobre a questão da distribuição do ónus da prova no artigo 70º.

A necessidade de o ordenamento jurídico definir regras de repartição do ónus da prova[186] deriva, essencialmente, da incerteza gerada pela falta de prova suficiente e da proibição de *non liquet* (n.º 1 do artigo 8º do CC). No âmbito das transferências eletrónicas de fundos, onde é difícil haver certezas sobre o ocorrido "por detrás" da via informática, as regras de ónus da prova assumem uma importância fulcral.

O n.º 1 do artigo 70º consagra que "caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, ou alegue que a operação não foi corretamente efetuada, incumbe ao respetivo prestador de serviço de pagamento fornecer prova de que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência." Daqui se depreende que compete à entidade bancária provar que a operação de pagamento foi autenticada, por exemplo, provando que o instrumento de pagamento e os respetivos códigos pessoais de segurança foram, de facto, utilizados.

A opção legislativa constante do n.º 1 do artigo 70º deve-se ao simples facto de o utilizador não poder ser colocado na necessidade de fazer prova sobre o funcionamento do complexo sistema informático do banco, sistema este que não domina[187]. Uma vez feita esta prova, cabe ainda ao banco provar a culpa do seu cliente e o grau da sua contribuição para os prejuízos ocorridos[188]. Assim, o n.º 2 do mesmo artigo estabelece que, caso o utilizador negue ter autorizado determinada operação de pagamento ou alegue que esta não foi corretamente efetuada, "a utilização do instrumento de pagamento registada pelo prestador de serviços de pagamento, por si só, não é necessariamente suficiente para provar que a operação de pagamento foi autorizada pelo ordenante, que este último agiu de forma fraudulenta ou que não cumpriu, deliberadamente ou por negligência grave, uma ou mais das suas obrigações decorrentes do artigo 67º"[189].

---

[186] PEDRO MÚRIAS define normas do ónus da prova como "normas de distribuição do risco da incerteza em questões de facto", in Introdução ao ónus da prova. Texto não publicado facultado aos alunos de Teoria do Processo da Faculdade de Direito da Universidade Nova de Lisboa no ano letivo de 2013/2014, p. 4.
[187] Ac. TRL de 5/11/2013 (Manuel Marques), cit.
[188] Ibidem.
[189] Estes deveres que cabem ao utilizador do instrumento de pagamento, já referidos várias vezes ao longo da dissertação, prendem-se essencialmente com a salvaguarda da eficácia dos dispositivos de segurança

O primeiro ponto que este preceito nos indica é que o registo da operação de pagamento não pode ser entendido como um sinal inequívoco de que o titular a autorizou[190]. A autorização no *home banking*, geralmente, é concedida através da introdução de uma série de códigos pessoais e intransmissíveis no teclado de um computador, contudo não podemos ignorar os casos em que este acesso é feito por terceiros, distintos do titular do instrumento de pagamento, que conseguiram obter esses dados através de fraudes informáticas.

Mesmo que tal disposição legal não existisse no nosso ordenamento jurídico, consideraríamos igualmente que caberia ao banco a prova de que a operação de pagamento foi autorizada pelo seu cliente. Isto porque o facto de o cliente não ter procedido à ordem de pagamento consubstancia um facto negativo pois reconduz-se à alegação de um facto que não aconteceu. Como nestes casos, é muito difícil para o credor (cliente) fazer prova de que um facto não aconteceu, deve-se entender que cabe à contraparte (banco) provar o facto positivo contrário ao facto negativo invocado[191].

Assim, compete à entidade bancária provar, no caso concreto, qual o nível de participação do seu cliente na operação de pagamento não autorizada e o grau de diligência com que atuou.

Julgamos pertinente fazer aqui um paralelismo com a assinatura de um documento particular, de acordo com o artigo 374º do CC. A lei civil considera verdadeira a assinatura constante de um documento particular quando reconhecida ou não impugnada pela parte contra quem o documento é apresentado (n.º 1 do referido preceito legal). Contudo, se a parte contra quem o documento é apresentado, ou seja, se o seu alegado autor impugnar a veracidade da assinatura, incumbe à parte que apresenta o documento a prova da sua veracidade (n.º 2 do artigo 374º do CC). Isto significa que se o seu alegado autor impugnar a assinatura, o ónus da prova da sua genuinidade recai sobre quem apresenta o documento. No contrato de *home banking*, os códigos introduzidos aquando do acesso ao serviço desempenham a função de assinatura, como que substituindo-a. Num primeiro momento, os movimentos lançados na conta bancária do cliente são tidos como autorizados pelo seu titular. Todavia, se este os impugnar, negando tê-los autorizado, recai sobre o banco o ónus da prova de que foram devidamente autorizados[192]. Como podemos verificar, a nossa situação é em tudo semelhante à da assinatura de um documento particular justificando assim o lugar paralelo.

---

personalizados (palavras-passe) que supõem a confidencialidade e o uso estritamente pessoal, como decorre da alínea a) do n.º 1 do art. 67º do RSP conjugado com o n.º 2 do mesmo artigo.

[190] LÓPEZ JIMÉNEZ, Comentarios a la Ley de Servicios de Pago. Barcelona: Bosch, 2011, p. 595.

[191] PEDRO MÚRIAS, op. cit., pp. 50-51. O Autor dá o exemplo muito esclarecedor da dificuldade do credor de fazer prova de um facto negativo ao apresentar a hipótese em que o credor invoca o não pagamento de determinada mercadoria. É manifestamente complicado para este demonstrar que não recebeu qualquer pagamento mas é muito simples para o devedor provar que efetuou o referido pagamento ao apresentar o respetivo recibo.

[192] Note-se a possibilidade de, sem se impugnar a sua veracidade, se questionar a sua proveniência. Assim, MARGARIDA LIMA REGO, O *e-mail* como título executivo. Estudos em homenagem ao Prof. Doutor José Lebre de Freitas, I. Coimbra: Coimbra Editora, 2013, p. 10, no que se refere aos e-mails, "a demonstração de que um *e-mail* proveio da caixa de correio eletrónico de uma dada pessoa não garante que foi essa pessoa a enviá-lo". Também no *home banking* a demonstração de que o acesso ao serviço de banca eletrónica de determinado cliente teve origem na introdução dos códigos de acesso corretos não garante que foi essa mesma pessoa a aceder ao serviço.

Retomando a análise do regime do ónus da prova consagrado no artigo 70º do RSP, verificamos que cabe ao banco provar que a ordem de pagamento emana do seu cliente, garantindo-se, assim, a proteção do utilizador do instrumento de pagamento.[193] A mesma disposição legal atribui ao banco o ónus da prova relativo à existência de um comportamento gravemente negligente, fraudulento ou que reflita o incumprimento deliberado de deveres por parte do utilizador, que terá de provar caso queira exonerar-se do dever de suportar os prejuízos ocorridos, como veremos mais adiante.

Note-se ainda que a lei, ao atribuir o ónus da prova à entidade bancária e ao excluir a possibilidade de tal prova ser feita inteiramente com base na utilização do instrumento de pagamento e no respetivo registo, muitas vezes o único meio ao dispor do banco, dificulta a produção de prova por parte deste[194]. Na sua perspetiva, este encargo torna-se bastante pesado por dizer respeito a factos que estão fora da sua esfera de controlo, tornando-se ainda mais difícil no caso de negligência grave, onde se exige uma distinção em relação às situações em que não houve uma conduta censurável do utilizador na quebra da confidencialidade dos dispositivos de segurança personalizados (n.º 1 do artigo 72º, *in fine*), como veremos adiante[195].

Nesta sede, questiona-se se, face à letra do n.º 2 do artigo 70º RSP, será admissível uma presunção de negligência grave do utilizador do serviço de pagamento no que diz respeito a operações não autorizadas[196], como acontece na Alemanha[197]. Há quem entenda que a expressão "não é necessariamente suficiente" não impede a existência desta presunção pois se a intenção do legislador comunitário fosse impossibilitar a criação de uma presunção deste género, teria determinado que o uso do instrumento de pagamento, por si só, "não é suficiente" para provar que o utilizador agiu com negligência grave.[198] Assim, parece caber ao juiz a apreciação da existência de um comportamento gravemente negligente por parte do utilizador e a decisão se deve desvalorizar ou não a autenticação e a credibilidade dos registos informáticos da instituição bancária[199].

---

[193] A solução do n.º 2 do art. 70º era já aplicada pela jurisprudência da Cour de Cassation em matéria de cartões de pagamento, segundo a qual recaí sobre o emissor do cartão o ónus da prova em caso de negligência grave do titular e, se for utilizado o cartão por um terceiro com conhecimento do código pessoal, esse facto é, por si só, insuscetível de constituir prova de negligência grave do seu cliente – cfr. Cour de Cassation, chambre commerciale, financière et économique – arrêt n.º 1050 du 2/10/2007 (05-19.899), in http://www.courdecassation.fr (12/09/2014); Cour de Cassation, première chambre civile – arrêt n.º 354 du 28/03/2008 (07-10.186), in http://www.courdecassation.fr (12/09/2014).

[194] JOSÉ MANUEL FARIA, op. cit., p. 34.

[195] Ibidem, p. 33; JÉRÔME LASSERRE CAPDEVILLE, La contestation des opérations de paiement non autorisées. Revue de droit bancaire et financier. LexisNexis JurisClasseur. 12e année, n.º 1 (janvier-février 2011), p. 110.

[196] Questão colocada por REINHARD STEENNOT ao analisar o art. 59º da DSP que deu origem ao art. 70º do RSP – Allocation of liability in case of fraudulent use of an electronic payment instrument: The new Directive on payment services in the internal market. Computer Law & Security Review, vol. 24 (2008), in http://www.sciencedirect.com (22/07/2014), n. º 2.2.3.3., p. 558.

[197] Atualmente, na Alemanha, é utilizada uma presunção de negligência grave nestes casos. Presume-se que o utilizador do instrumento de pagamento agiu com negligência grave sempre que o banco demonstre que um terceiro teve acesso e conseguiu utilizar o instrumento de pagamento protegido por códigos pessoais de acesso. Isto significa que o utilizador terá de provar a ausência de comportamento gravemente negligente da sua parte. Já na Bélgica, o legislador proibiu expressamente a utilização de uma presunção de negligência grave, cabendo ao banco recolher elementos que provem a existência de um comportamento gravemente negligente ou fraudulento do utilizador do instrumento de pagamento.

[198] REINHARD STEENNOT, op. cit., loc. cit.

[199] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 60.

Aqui chegados, importa reter, essencialmente, que, relativamente ao ónus da prova, é ao banco que cabe demonstrar o grau de culpa subjacente ao comportamento do seu cliente e a sua contribuição para as perdas resultantes das operações fraudulentas[200].

Apesar do regime do ónus da prova fixado no RSP, tem-se verificado que as entidades bancárias incluem cláusulas contratuais gerais nos contratos de *home banking* que visam a alteração dos critérios de repartição do ónus da prova[201].

A título de exemplo, atente-se nas seguintes cláusulas inseridas nas Condições Gerais de utilização do serviço de banca eletrónica da Caixa Geral de Depósitos, cuja validade foi analisada em diferentes acórdãos dos nossos tribunais superiores[202]:

- "Sempre que uma operação seja realizada mediante os procedimentos referidos nas cláusulas anteriores e no guia do utilizador, presume-se que o foi pelo aderente."

- "Se, no entanto, se provar que a operação foi realizada por terceiro, presumir-se-á que tal foi consentido ou culposamente facilitado pelo aderente."

As cláusulas acima transcritas fazem recair sobre o aderente uma presunção de culpa caso sejam realizadas operações de pagamento, via banca eletrónica, por terceiros, mediante autenticação no sistema através da inserção dos códigos de acesso pessoais e intransmissíveis que lhe foram conferidos pela entidade bancária. Admitir a sua validade implicaria uma prova em contrário praticamente impossível pelo aderente isto porque, nas palavras da Relação de Lisboa no Acórdão de 24 de maio de 2012, o cliente "não tem qualquer controlo sobre os sofisticados meios informáticos da entidade bancária, nem dispõe da assessoria técnica de primeira água com que os departamentos respetivos daquela se apetrecham"[203]. Na defesa dos interesses das partes envolvidas, deve-se encontrar um equilíbrio assente na ponderação da especial natureza das operações eletrónicas em causa, designadamente no facto de estas serem realizadas com recurso a meios informáticos controlados pelos bancos[204]. Em última instância, fazer recair esta presunção de culpa sobre o utilizador do serviço de banca eletrónica equivale a fazer versar sobre este os prejuízos decorrentes de operações fraudulentas dada a dificuldade em afastar a presunção (o que põe em causa a aplicação prática do disposto no n.º 1 do artigo 72º do RSP)[205].

Apesar de alguns tribunais terem admitido a validade de cláusulas com conteúdo idêntico às acima transcritas no âmbito da utilização de cartões de pagamento[206], no que diz respeito

---

[200] Ibidem, p. 66.
[201] Neste ponto analisamos apenas a validade das cláusulas contratuais gerais inseridas nos contratos de *home banking*, ultrapassando a fase da inserção da cláusula no contrato uma vez esta que não assume tanto relevo nesta sede.
[202] Ac. TRL de 24/05/2012 (Ezagüi Martins), cit.; Ac. TRG de 23/10/2012 (Filipe Caroço), cit.; Ac. TRL de 28/06/2013 (Anabela Calafate), cit.; Ac. TRL de 12/12/2013 (Tomé Ramião), cit.
[203] Ac. TRL de 24/05/2012 (Ezagüi Martins), cit. Este tribunal acrescenta ainda que admitir estas cláusulas implicaria "uma prova em contrário absolutamente diabólica e na prática inalcançável pelo aderente."
[204] AZEVEDO FERREIRA, Direito bancário…, cit., p. 382; MARIA RAQUEL GUIMARÃES, As transferências eletrónicas…, cit., p. 126.
[205] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 60.
[206] Ac. TRL de 16/06/1994 (Noronha Nascimento) – CJ, III, 1994, pp. 122-124 e Ac. STJ de 15/05/2008 (Mota Miranda), Proc. 08B357, in www.dgsi.pt. Neste último afirma-se que é "ao titular do cartão [que] caberá fazer a prova de que o cartão não foi por si usado, nem que não consentiu no seu uso, fazendo a prova da factualidade

aos contratos de banca eletrónica, os tribunais superiores têm declarado a nulidade destas cláusulas contratuais gerais que estabelecem uma presunção de culpa sobre o aderente no caso de ocorrerem operações não autorizadas mediante autenticação no sistema[207]. O banco pretende modificar os critérios de repartição do ónus da prova (alínea g) do artigo 21º do DL n.º 446/85, de 25 de outubro – Regime Jurídico das Cláusulas Contratuais Gerais (RJCCG) que decorrem do artigo 70º do RSP e do n.º 1 do artigo 799º do CC. Assim, a entidade bancária seria dispensada do ónus da prova de que as operações realizadas através do serviço de *home banking,* nomeadamente a retirada de quantias das contas bancárias dos seus clientes, não resultaram do incumprimento da sua obrigação de prestar um serviço seguro[208]. Esta cláusula é absolutamente proibida e sancionada com nulidade (artigos 12º e 24º do RJCCG) quando inserida no âmbito de relações do banco com consumidores finais (artigo 20º do RJCCG).

Note-se que, mesmo que não estivéssemos perante cláusulas contratuais gerais, ainda assim, a referida cláusula seria tida como nula uma vez que esta, ao inverter o ónus da prova, estaria a agravar seriamente a dificuldade probatória para a parte que a convenção onera (n.º 1 do artigo 345º do CC)[209].

Hoje em dia, a questão da validade das cláusulas contratuais gerais inseridas em contratos de *home banking* não assume a mesma relevância face ao disposto no artigo 101º do RSP[210]. De acordo com este preceito legal, sendo as disposições legais do RSP mais favoráveis aos clientes, neste caso, em matéria de ónus da prova, devem ser aplicadas ao caso concreto, afastando as cláusulas abusivas plasmadas no contrato. Todavia, a aposição de cláusulas contratuais gerais desconformes com o disposto no RSP nos contratos de banca eletrónica continua a merecer algum destaque uma vez que a circunstância de se encontrarem nos referidos contratos pode demover os clientes de fazerem valer os seus direitos.

---

contrária; o banco não estaria em condições de provar que não foi o titular que o usou — é esta a regra que, de boa-fé, deve presidir às relações entre o Banco e o titular do cartão."

[207] Neste sentido, Ac. TRL de 24/05/2012 (Ezagüi Martins), cit.; Ac. TRL de 28/06/2013 (Anabela Calafate), cit.; Ac. TRL de 12/12/2013 (Tomé Ramião), cit. Apenas a Relação de Guimarães no acórdão de 23/10/2012 (Filipe Caroço), cit., não se pronunciou sobre a nulidade destas cláusulas, limitando-se a apontar a sua "validade duvidosa".

[208] Ac. TRL de 28/06/2013 (Anabela Calafate), cit.

[209] PEDRO MÚRIAS, op. cit., p. 55.

[210] A DSP abordou a questão das cláusulas contratuais gerais abusivas no Considerando 33, p. 6, onde estabelecia que "os termos e condições contratuais relativos ao fornecimento e à utilização de um instrumento de pagamento que tenha por efeito agravar o ónus da prova que recai sobre o consumidor ou atenuar o ónus da prova que recai sobre o emitente deverão ser considerados nulos."

4.3.3. Importância da notificação e responsabilidade pelas perdas resultantes de operações não autorizadas após a comunicação da fraude

Como já tínhamos mencionado no ponto 4.2.1 do capítulo I, a notificação do cliente dando conhecimento ao banco da ocorrência de uma operação de pagamento não autorizada na sua conta bancária joga um papel essencial na repartição dos prejuízos decorrentes de operações fraudulentas.

Visando uma exposição clara da matéria, julgamos que a melhor forma de a apresentar é tratando separadamente as perdas ocorridas após a comunicação à entidade bancária e aquelas que surgiram antes desta. A exposição do problema não atendendo à ordem cronológica dos acontecimentos justifica-se uma vez que a repartição dos prejuízos ocorridos antes da notificação assume uma complexidade que exige alguns esclarecimentos prévios.

A importância da notificação do cliente ao banco, informando-o da ocorrência de uma operação de pagamento não autorizada na sua conta bancária, é assinalável pois trata-se do momento a partir o qual o utilizador de serviços de pagamento que negue ter autorizado uma operação de pagamento executada "não suporta quaisquer consequências financeiras resultantes da utilização de um instrumento de pagamento perdido, roubado ou abusivamente apropriado, salvo em caso de atuação fraudulenta" (n.º 4 do artigo 72º)[211]. Por outras palavras, o momento relevante que define a transferência da responsabilidade do cliente para o banco é a notificação mencionada na alínea b) do n.º 1 do artigo 67º. A partir desse momento, o utilizador deixa de suportar as consequências financeiras resultantes da apropriação abusiva do seu instrumento de pagamento. A partir desta altura, e pouco importa que o banco já se mostre capaz de prevenir a utilização fraudulenta dos instrumentos de pagamento, o utilizador do serviço de *home banking* apenas sofrerá as perdas ocorridas depois da notificação se atuar de forma fraudulenta[212] [213]. A atuação fraudulenta do utilizador é a única circunstância em que este irá suportar as perdas advindas após a comunicação à entidade bancária.

Tendo em vista a redução dos riscos e das consequências das operações de pagamento não autorizadas, o cliente deve comunicar a situação ao banco sem atrasos injustificados logo que tenha conhecimento da utilização não autorizada do serviço de *home banking*. Por essa razão, não se podem aceitar cláusulas contratuais que obriguem o utilizador do instrumento de pagamento a comunicar a situação irregular de "forma imediata", "com a maior urgência" ou fórmulas análogas, nem dentro de determinado lapso de tempo (24 horas, dois dias,

[211] Esta solução contraria o n.º 2 do § 8º do Aviso n.º 11/2001 do Banco de Portugal nos casos que envolvam a utilização de cartões de débito ou de crédito pois, segundo o Aviso, o titular do cartão podia suportar prejuízos ocorridos depois da comunicação ao banco do extravio do cartão, mesmo que não lhe fosse imputável qualquer comportamento negligente, sempre que não estivesse em causa uma utilização eletrónica do cartão.
[212] Recorde-se o exemplo de atuação fraudulenta do utilizador do serviço de *home banking* apresentado no ponto 2 do Capítulo II.
[213] Uma vez notificado o banco, é sobre este que passa a recair a responsabilidade pelas perdas decorrentes de operações fraudulentas, mesmo que potenciadas por comportamento gravemente negligente do seu cliente, como veremos mais adiante.

cinco dias), uma vez que é possível que um cliente, agindo de boa-fé e adotando uma conduta diligente, não tenha conhecimento das operações não autorizadas durante várias horas ou dias[214]. Isto, nos casos em que o utilizador do instrumento de pagamento agiu de forma negligente aquando do acesso ao serviço de *home banking*, subjetiviza o momento determinante para a transferência da responsabilidade de uma parte contratual para a outra[215], do cliente para o banco, como veremos em pormenor mais adiante no ponto 3.5. deste capítulo.

No que diz respeito ao meio pelo qual se deve proceder à notificação, pode-se verificar que o RSP não nos dá nenhuma resposta; todavia, se atendermos às necessidades de prontidão no que concerne a estas operações, entendemos que a via telefónica é o meio mais célere e capaz de impedir futuras operações fraudulentas[216].

Tendo em conta a sua importância, o RSP impõe à entidade bancária o dever de garantir a disponibilidade, a todo o momento, de meios adequados que permitam ao cliente proceder à notificação (alínea c) do n.º 1 do artigo 68º), ou seja, o utilizador do instrumento de pagamento deve ter a faculdade de comunicar a ocorrência de uma operação não autorizada 24 horas por dia e 7 dias por semana. Caso o banco não cumpra este dever, o utilizador do serviço de *home banking* deixa de ficar obrigado a suportar as consequências financeiras resultantes da utilização deste instrumento de pagamento, salvo nos casos em que tenha agido de modo fraudulento (n.º 5 do artigo 72º). É manifesto que, em caso de incumprimento, a entidade bancária, além de violar uma obrigação imposta pela lei[217], estaria a atuar de má-fé, em *venire contra factum proprium*, ao tentar imputar o risco ao seu cliente[218]. Perante estas circunstâncias, o banco terá de suportar a totalidade das perdas advindas das operações fraudulentas, inclusive das que ocorreram antes de o utilizador do instrumento de pagamento ter tentado proceder à notificação da alínea b) do n.º 1 do artigo 67[219]. Consequentemente, o cliente não suportará nenhum prejuízo decorrente da intromissão de terceiro na sua conta bancária.

A instituição bancária deve, ainda, facultar ao cliente, a seu pedido, os meios necessários para fazer prova de que efetuou a notificação, até 18 meses após a referida comunicação (alínea d) do n.º 1 do artigo 68º).

Uma vez feita a notificação, sobre o banco passa a incidir o dever de proteger a conta bancária do seu cliente, nomeadamente através do respetivo bloqueio, de forma a impedir a ocorrência de mais operações não autorizadas (alínea e) do n.º 1 do artigo 68º.[220] A obrigação de proteção da conta por parte do banco é compreensível pois esta é a parte

[214] LÓPEZ JIMÉNEZ, op. cit., p. 586.
[215] Ibidem, loc. cit.
[216] Neste sentido, REINHARD STEENNOT, op. cit., n.º 2.2.2., p. 556
[217] Pela alínea c) do n.º 1 do art. 68º do RSP. Além de corresponder a uma contraordenação especialmente grave prevista na alínea o) do art. 95º do RSP.
[218] JANUÁRIO DA COSTA GOMES, op. cit., p. 247.
[219] REINHARD STEENNOT, op. cit., n. º 2.2.2., p. 557.
[220] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 67.

contratual que se encontra em melhores condições de controlar o sistema de pagamentos e evitar novos prejuízos[221].

Note-se que, a par da notificação ao banco da ocorrência de operações de pagamento não autorizadas, o RSP regula especificamente no artigo 69º o direito de retificação decorrente da comunicação à entidade bancária de operações de pagamento não autorizadas ou incorretamente executadas.

Segundo o n.º 1 do referido artigo, quando o utilizador do instrumento de pagamento verifica que ocorreu uma operação de pagamento não autorizada ou incorretamente executada, deve comunicar ao banco esta situação, para que este último possa proceder à sua retificação. Esta imposição ao utilizador do ónus de verificar se as operações de pagamento foram autorizadas e executadas corretamente deve-se ao facto de ser manifestamente mais simples que cada cliente controle os movimentos das suas contas bancárias do que seja o banco a seguir, diariamente, as operações bancárias de todos os seus clientes[222]. Porém, isto não obsta a que, se a entidade bancária tiver conhecimento da existência de operações de pagamento não autorizadas ou executadas incorretamente, proceda imediatamente à sua retificação, sem necessidade de aguardar por uma indicação do seu cliente[223].

Por motivos de segurança jurídica, o RSP fixou um prazo que satisfizesse tanto os interesses do utilizador do instrumento de pagamento, como os da entidade bancária, tendo determinado que a comunicação deverá ser feita sem atraso justificado e dentro de um prazo nunca superior a treze meses a contar da data do débito (n.º 1 do artigo 69º*, in fine*). A conciliação destes dois momentos temporais – "sem atraso justificado" e o prazo de treze meses – pode parecer confusa à primeira vista. Passamos a explicar. Em regra, o cliente deverá realizar a comunicação ao banco sem atraso injustificado após ter tomado conhecimento da operação não autorizada; considerando-se, geralmente, que está em posição de proceder à referida comunicação quando consulta os movimentos da sua conta bancária, onde consta a tal operação de pagamento não autorizada. Mas, é praticamente impossível o banco ter a certeza que o cliente está, de facto, ao corrente da situação.

Por esta razão, o legislador comunitário previu o prazo máximo de treze meses a contar da data do débito[224]. Assim, o banco não poderá afastar a sua responsabilidade invocando o incumprimento que impende sobre o cliente de agir o mais brevemente possível, quando este prove que estava em situação de impossibilidade material de ter conhecimento do ocorrido[225]. Por exemplo, o cliente pode ter acesso aos movimentos da sua conta bancária mas só ter tido efetivamente conhecimento da operação não autorizada semanas depois porque se encontrava internado no hospital. Nestes casos, faz sentido que o cliente beneficie

[221] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., loc. cit.
[222] LÓPEZ JIMÉNEZ, op. cit., p. 592.
[223] Ibidem, loc. cit.
[224] JÉRÔME LASSERRE CAPDEVILLE, op. cit., p. 110.
[225] Ibidem, loc. cit. Porém, também não se pode considerar legítimo que o cliente deixe perdurar a utilização fraudulenta do instrumento de pagamento por vários meses. Em sentido contrário entendeu a Cour de Cassation, chambre commerciale, financière et économique – arrêt n.º 1183 du 12/11/2008 (07-19.324), in http://www.courdecassation.fr (12/09/2014).

de prazo até treze meses a contar da data do débito para proceder à comunicação da operação de pagamento não autorizada e pedir a respetiva retificação.

Todavia, este limite máximo de prazo não deve ser uma via que permita desresponsabilizar o cliente nos casos em que este não comunicou ao banco a ocorrência de operações de pagamento não autorizadas, sem atraso injustificado, quando já as tinha detetado ou quando já dispunha de todos os elementos que as permitia identificar[226].

Por fim, o n.º 2 do artigo 69º ainda acrescenta que, relativamente à operação de pagamento em causa, quando o banco não tenha prestado ou disponibilizado as informações a que está obrigado nos termos do capítulo I do título III (transparência das condições e dos requisitos de informação aplicáveis aos serviços de pagamento), o cliente poderá proceder à referida comunicação sem ter de observar os prazos estabelecidos no n.º 1 do mesmo preceito.

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

4.3.4. Dever de reembolso dos montantes indevidamente debitados

Depois de o cliente verificar que ocorreu uma operação de pagamento não autorizada na sua conta bancária e de ter notificado o banco, a entidade bancária deve reembolsá-lo imediatamente do montante indevidamente debitado em virtude dessa operação de pagamento e deve repor a conta de pagamento debitada na situação em que estaria se essa transferência não tivesse sido executada, isto sem prejuízo do direito de retificação do artigo 69º (n.º 1 do artigo 71º)[227].

A partir deste momento e quando pertinente, iremos fazer referência, ao longo da apresentação do regime atual da repartição dos prejuízos decorrentes de operações

[226] Ibidem, loc. cit. Ainda no que diz respeito aos prazos, pergunta-se se quando o cliente fez a comunicação do n.º 1 do art. 69º tempestivamente e não obteve o imediato reembolso por parte do banco, se aquele terá o direito de agir judicialmente depois de decorrerem esses 13 meses. Segundo o Autor, cabe ao julgador clarificar esta questão. Todavia, parece-nos que o prazo de treze meses apenas respeita à comunicação do artigo acima referido e, esta, uma vez realizada tempestivamente, permitirá ao cliente recorrer às vias judiciais dentro do prazo de prescrição ordinário (art. 309º CC).

[227] Mais uma vez, verificamos a confusão do legislador ao referir no n.º 1 do art. 71º que o "[…] prestador de serviços de pagamento do ordenante deve reembolsá-lo imediatamente do montante da operação de pagamento não autorizada […]" quando devia designar o titular do instrumento de pagamento que se encontre na situação descrita como "utilizador de serviços de pagamento que negue ter autorizado uma operação de pagamento executada". Ver nota de rodapé 183, p. 45. LÓPEZ JIMÉNEZ, op. cit., pp. 598-602, ao analisar o art. 32º da Ley de Servicios de Pago, equivalente ao nosso art. 72º do RSP, também utiliza os termos "ordenante" e "usuario", aparentemente de forma indistinta, não fazendo qualquer crítica à letra da lei.

fraudulentas, à Proposta de Diretiva do Parlamento Europeu e do Conselho relativa aos serviços de pagamento no mercado interno (PDSP) que visa substituir a, atualmente em vigor, DSP[228]. Tais esclarecimentos justificam-se dadas as alterações introduzidas no âmbito da responsabilidade do banco aquando da ocorrência de operações fraudulentas na conta bancária do seu cliente.

No que diz respeito ao dever de reembolso que recaí sobre a entidade bancária, a PDSP procura reforçar a proteção dos consumidores de serviços de pagamento deixando expresso que o banco, ao reembolsar o cliente da quantia desviada devido a uma operação de pagamento não autorizada, deve-se assegurar que a data-valor[229] do crédito reembolsado não seja posterior à data em que o montante respetivo foi debitado, ou seja, os juros pagos ao cliente devem ser calculados a partir da data de débito da quantia desviada e não a partir de qualquer outra data (n.º 1 do artigo 65º da PDSP que corresponde ao n.º 1 do artigo 60º da DSP).

Se o dever de reembolso e pagamento por parte do banco não for cumprido, o RSP prevê a aplicação de uma coima de € 10 000 a € 5 000 000 ou de € 4 000 a € 2 000 000, consoante seja aplicada a ente coletivo ou a pessoa singular, correspondente à infração especialmente grave prevista na alínea p) do artigo 95º do RSP. O n.º 2 do artigo 71º acrescenta ainda que, caso o reembolso não seja imediato, à quantia devida somam-se juros moratórios, contados dia a dia desde a data em que o utilizador de serviços de pagamento haja negado ter autorizado a operação de pagamento executada até à data do reembolso efetivo, calculado à taxa legal, fixada nos termos do Código Civil, acrescida de 10 pontos percentuais, sem prejuízo do direito à indemnização suplementar a que haja lugar. Note-se que este n.º 2 limita a contagem dos juros moratórios visto que estes são contados a partir da data em que o cliente negou ter autorizado a operação de pagamento, e não a partir da data em que a tal operação ocorreu[230].

No entanto, ao analisar este artigo, surge-nos uma questão: como se compatibiliza a obrigação de reembolso imediato pelo banco com a distribuição dos prejuízos resultantes de operações fraudulentas?[231] Segundo o regime jurídico que deriva da DSP, quando o utilizador do instrumento de pagamento notifica a entidade bancária que ocorreram operações de pagamento não autorizadas na sua conta bancária e exige o reembolso dos montantes em falta, o banco não pode recusar a devolução das quantias até o conflito ser resolvido. A discórdia nascerá, geralmente, quando o banco alegar que as operações de pagamento que ocorreram antes da notificação foram potenciadas pela negligência grave do utilizador do serviço de *home banking*[232]. Contudo, o que a lei prescreve é que o banco está obrigado a

[228] Visa alterar as Diretivas 2002/65/CE, 2013/36/CE e 2009/110/CE e revogar a Diretiva 2007/64/CE – COM (2013) 547 final, Bruxelas, 24/07/2013, in http:// http://eur-lex.europa.eu.
[229] Data-valor é a data de referência utilizada por um prestador de serviços de pagamento para o cálculo de juros sobre os fundos debitados ou creditados numa conta de pagamento (n.º 19 do art. 4º da PDSP).
[230] JANUÁRIO DA COSTA GOMES, op. cit., p. 245.
[231] Questão colocada e apresentação da explicação da resposta por REINHARD STEENNOT, op. cit., n.º 2.3.4., p. 559.
[232] JÉRÔME LASSERRE CAPDEVILLE, op. cit., p. 111, levanta a questão se poderá o banco verificar a legitimidade da refutação da execução da operação de pagamento do seu cliente, permitindo-o, antes de

reembolsar o seu cliente, de imediato, pelo valor dos montantes subtraídos devido a operações fraudulentas. Assim, este reembolso assemelha-se, no seu efeito, à cláusula *solve et repete* segundo a qual "paga-se primeiro e discute-se depois".

Será consoante a apreciação, pelo tribunal, do comportamento do utilizador do instrumento de pagamento e das circunstâncias do caso concreto que se vai determinar como se vão repartir estes prejuízos. Adiantando um pouco o que será melhor desenvolvido nos pontos seguintes, após intervenção judicial, se o julgador decidir que a operação de pagamento não autorizada não se deveu a qualquer comportamento gravemente negligente ou doloso, o cliente deve suportar as perdas até ao valor de € 150 (valor determinado para os casos em que o utilizador atuou com negligência leve, como veremos *infra*); já se chegar à conclusão que o cliente agiu com negligência grave, este será declarado responsável pelas perdas ocorridas até à notificação da entidade bancária e terá de devolver ao banco as quantias entregues a título de reembolso.

4.3.5. Responsabilidade pelos prejuízos decorrentes de operações não autorizadas antes da notificação ao banco

Neste ponto, a apreciação do comportamento do utilizador do serviço de *home banking* revela-se um fator da maior importância uma vez que é a partir dele que descobrimos quem irá suportar as perdas resultantes de operações fraudulentas antes da notificação da ocorrência à entidade bancária.

a) Negligência leve do utilizador

De acordo com o n.º 1 do artigo 72º, "no caso de operações de pagamento não autorizadas resultantes de perda, de roubo ou da apropriação abusiva de instrumento de pagamento, com quebra da confidencialidade dos dispositivos de segurança personalizados imputável ao ordenante, este suporta as perdas relativas a essas operações dentro do limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, até ao máximo de € 150"[233] [234]. Assim, sempre que se verifiquem operações de pagamento não

proceder ao reembolso, assegurar-se que está realmente perante uma operação de pagamento não autorizada pelo seu cliente e não perante uma fraude do mesmo. O Autor defende que o banco deve ter a possibilidade de o fazer e defende o regresso da solução que vigorava em França no art. L. 132-4 do Code monétaire et financier até ser revogada pela lei que transpôs a DSP (Ordonnance n.º 2009-866 de 15/07/2009) que dispunha que o reembolso deveria ser feito o mais tardar até um mês após a notificação ao banco da ocorrência de uma operação não autorizada.

[233] O disposto no n.º 1 deste artigo já resultava, como foi referido *supra*, do disposto na Recomendação da Comissão 97/489/CE, nomeadamente do n.º 1 do art. 6º e do n.º 1 do art. 8º, adotado depois no n.º 1 do art. 61º da DSP. Todavia, esta solução contradiz, mais uma vez, o disposto no Aviso n.º 11/2001 do Banco de Portugal, de 20 de novembro, relativo à emissão e utilização de cartões de crédito e de débito, nomeadamente o n.º 6 do § 8º, nos casos que envolvam a utilização deste tipo de cartões de pagamento pois neste não eram

autorizadas que não sejam imputáveis ao titular do instrumento de pagamento a título de negligência grave ou dolo, o cliente vê a sua responsabilidade limitada até ao *plafond* máximo de 150 euros[235]. Considera-se, então, que esta limitação da responsabilidade deve-se aplicar em caso de quebra de confidencialidade dos dispositivos de segurança personalizados pelo utilizador do instrumento de pagamento a título de negligência leve. Portanto, é o banco que deve arcar com os prejuízos excedentes decorrentes de operações de pagamento não autorizadas uma vez que é a este que cabe suportar o risco do sistema informático que sustenta o serviço de *home banking* não ser seguro e permitir a intromissão de terceiros.

Não nos podemos esquecer que o n.º 1 do artigo 72º regula situações nas quais houve quebra de confidencialidade dos códigos pessoais que permitem aceder ao instrumento de pagamento. Isto significa que, numa interpretação *a contrario* do referido artigo, se o utilizador do serviço de pagamento atuou de forma diligente, preservando a confidencialidade e eficácia dos dispositivos de segurança que lhe foram entregues (ou o contrário não se conseguir provar), e, ainda assim, um terceiro conseguiu obter os seus dados de acesso e infiltrar-se na sua conta bancária, o utilizador não deve responder pelos prejuízos resultantes das operações fraudulentas ocorridas antes da notificação ao banco, nem sequer até ao montante de € 150[236]. Este é também o entendimento de LÓPEZ JIMÉNEZ que, referindo-se especificamente ao caso da fraude relacionada com cartões de pagamento, defende que nos casos que conduzam a uma ordem de pagamento não autorizada através da prévia captação dos elementos que constam nos cartões, como é o caso do *phishing*, se o cliente for diligente no cumprimento das suas obrigações de guarda e notificação, não deve suportar nenhum prejuízo decorrente da operação fraudulenta[237].

Cabe-nos fazer de novo referência à PDSP uma vez que a sua alteração mais significativa surgiu no âmbito da repartição dos prejuízos resultantes de operações de pagamento não autorizadas. Esta alteração é introduzida pelo seu artigo 66º, correspondente ao artigo 61º da DSP (que deu origem ao artigo 72º do RSP), que disciplina a responsabilidade do titular do instrumento de pagamento por operações não autorizadas e que estabelece, na primeira

definidos quaisquer limites para as perdas a suportar pelo cliente antes da notificação do extravio do cartão em função do grau de negligência que lhe era imputável.

[234] Note-se, ainda, que o n.º 1 do art. 61º da DSP que deu origem ao n.º1 deste artigo refere-se a "perdas relativas às operações de pagamento não autorizadas resultantes da utilização de um instrumento de pagamento perdido ou roubado ou, caso o ordenante não tenha assegurado a confidencialidade dos dispositivos de segurança personalizados da apropriação abusiva de um instrumento de pagamento" e não a "[perdas relativas às] operações de pagamento não autorizadas resultantes de perda, de roubo ou da apropriação abusiva de instrumento de pagamento, com quebra da confidencialidade dos dispositivos de segurança personalizados imputável ao ordenante". A diferença pode parecer insignificante pois reduz-se à colocação de uma vírgula, mas o sentido muda radicalmente: na redação atual do n.º 1 do art. 72º, a ideia que permanece é que tanto a perda, como o roubo e a apropriação abusiva do instrumento de pagamento foram potenciados pela quebra da confidencialidade dos dispositivos de segurança personalizados pelo ordenante.

[235] Ao responsabilizar o cliente apenas por um montante limitado nestas situações, pretende-se incentivar a comunicação ao banco, sem atrasos justificados, da utilização não autorizada do instrumento de pagamento. Cfr. Considerando 32 da DSP, p. 6.

[236] Cfr. Ac. TRL de 5/11/2013 (Manuel Marques), cit.

[237] LÓPEZ JIMÉNEZ, op. cit., p. 602.

parte do n.º 1 do referido artigo, que "[…] o ordenante[238] pode ser obrigado a suportar, num montante máximo de 50 euros, as perdas relativas às operações de pagamento não autorizadas resultantes da utilização de um instrumento de pagamento perdido ou roubado ou da apropriação abusiva de um instrumento de pagamento".

Verificamos que o utilizador continua a ser responsável por um montante limitado dos prejuízos decorrentes de operações não autorizadas, salvo em caso de atuação fraudulenta ou negligência grave da sua parte, a fim de incentivá-lo a comunicar sem atraso injustificado a operação não autorizada, reduzindo assim os riscos que desta podem decorrer. Contudo, a PDSP altera a importância a suportar pelo utilizador-consumidor de 150 euros (como decorria da DSP) para 50 euros, considerando-se este montante como "adequado para garantir um nível elevado e harmonizado de proteção dos utilizadores na União"[239]. De acordo com a Proposta, um consumidor nunca deverá ser obrigado a pagar mais do que 50 euros na ocorrência de uma operação não autorizada a partir da sua conta, exceto em caso de fraude ou de negligência grave. Note-se ainda que este artigo não faz qualquer referência à quebra de confidencialidade dos dispositivos de segurança personalizados (como fazia o n.º 1 do artigo 61º da DSP). Isto significa que, com a PDSP, o cliente deverá suportar, sempre e independentemente das circunstâncias, um montante até 50 euros dos prejuízos relativos a operações não autorizadas decorrentes da utilização de um instrumento de pagamento perdido ou roubado ou da apropriação abusiva do instrumento.

b) Negligência grave e dolo do utilizador

Já se as operações de pagamento não autorizadas resultarem de negligência grave do titular do instrumento de pagamento, este suporta "as perdas resultantes de operações de pagamento não autorizadas até ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, ainda que superiores a € 150, dependendo da natureza dos dispositivos de segurança personalizados do instrumento de pagamento e das circunstâncias da sua perda, roubo ou apropriação abusiva" (n.º 3 do artigo 72º). Esta foi a solução encontrada pelo legislador nacional para disciplinar a situação intermédia entre os casos em que o utilizador do serviço de *home banking* não teve uma conduta censurável e os casos em que este atuou de forma fraudulenta ou em claro incumprimento das obrigações que decorrem do contrato[240]. Todavia, pode-se adivinhar que nos casos em que o cliente

[238] O legislador comunitário continua a designar o titular do instrumento de pagamento como "ordenante" no âmbito das operações de pagamento não autorizadas quando estamos numa situação em que este nada ordenou. Ver nota de rodapé 183, p. 45.
[239] Considerando 54 da PDSP, p. 27.
[240] Apesar da DSP se tratar de uma diretiva de harmonização plena, o legislador comunitário concedeu uma margem de manobra em determinados artigos, um deles é o n.º 3 do art. 61º da DSP que foi transposto pelo RSP para o n.º 3 do art. 72º (n.º 1 do art. 86º da DSP).

tenha um saldo disponível bastante superior a € 150, a ausência de consenso sobre os factos ocorridos irá gerar, certamente, um litígio entre as partes[241].

Para perceber a aplicação prática deste preceito legal, é necessário compreender qual o alcance do conceito de "negligência grave" no contexto do RSP uma vez que este não nos deixou qualquer definição[242]. Antes de mais, importa aqui ter presente a disciplina geral da negligência em direito civil. Como sabemos, a negligência consiste na "violação (objetiva) de uma norma por inobservância de deveres de cuidado"[243]. Neste âmbito, distinguem-se dois graus de negligência: a negligência consciente e a inconsciente. O RSP, apesar de não utilizar estas designações, parece referir-se a esta mesma distinção ao diferenciar os casos de negligência grave e leve, mas, neste caso, refletindo em especial a violação de deveres contratuais. Na primeira situação, o autor prevê como possível a violação de uma norma mas "por leviandade, precipitação, desleixo ou incúria na sua não verificação, e só por isso não toma as providências necessárias para o evitar"[244]. Já na negligência inconsciente/leve, o autor não chega a prever a possibilidade de a violação ocorrer, porém deveria tê-lo feito se fizesse uso da diligência exigida[245]. Para enquadrar se, em determinado caso, estamos perante uma situação de negligência consciente/grave ou inconsciente/leve é necessário ter em conta que o grau de censura será tanto maior quanto maior a possibilidade de a pessoa ter agido de outra forma e mais intenso o dever de o ter feito[246].

O facto de a violação não decorrer de um comportamento diretamente prevaricador, contrariamente ao que acontece no dolo, suscita algumas dificuldades de apreciação da existência ou não de um comportamento negligente[247]. No que diz respeito à responsabilidade contratual, âmbito que releva para o nosso tema, o n.º 2 do artigo 799º do CC dispõe que "a culpa é apreciada nos termos aplicáveis à responsabilidade civil", remetendo assim para o n.º 2 do artigo 487º do CC que determina que "a culpa é apreciada, na falta de outro critério legal, pela diligência de um bom pai de família, em face das circunstâncias de cada caso".

Assim, parece caber ao juiz decidir, no caso concreto e atendendo às circunstâncias relevantes, se determinado comportamento constituí negligência grave. Contudo, importa ter em consideração que o facto de a qualificação de negligência grave estar aberto a diferentes interpretações pode conduzir à falta de clareza que, por sua vez, pode conduzir à falta de consistência, deixando o processo de decisão vulnerável a decisões arbitrárias baseadas na fluidez dos conceitos[248]. Sempre tendo em conta a necessidade de atender ao caso concreto,

---

[241] JANUÁRIO DA COSTA GOMES, op. cit., p. 246, nota 828.
[242] SYLVIA MERCADO-KIERKEGAARD ao analisar o processo legislativo que antecedeu a aprovação da DSP apontou para a necessidade de uma definição ou descrição do conceito de negligência grave para os casos em que se discuta a autorização da operação de pagamento. Cfr. o texto da autora – Harmonising the regulatory regime for cross-border payment services. In Computer Law and Security Review, vol. 23 (2007), p. 183, in http://www.sciencedirect.com (22/07/2014).
[243] MENEZES CORDEIRO, Tratado de Direito Civil, Tomo VIII, reimpressão da 1ª edição do tomo III da parte II de 2010. Coimbra: Almedina, 2014, p. 472.
[244] ANTUNES VARELA, Das Obrigações em Geral…, cit., p. 573.
[245] Ibidem, loc. cit.
[246] Ibidem, pp. 573-574.
[247] MENEZES CORDEIRO, Tratado de Direito Civil, Tomo VIII…, cit., loc. cit.
[248] NICOLE VAN DER MEULEN, op. cit., n. º 2.1., p. 714.

note-se, por exemplo, que o facto de o não cumprimento do dever de proteger os dispositivos de segurança personalizados poder constituir negligência grave, confere ao julgador um amplo poder discricionário[249].

Será que o cliente ao proceder à notificação tardia da apropriação abusiva do instrumento de pagamento está a revelar um comportamento gravemente negligente? Como já vimos, a comunicação ao banco informando-o da utilização não autorizada do serviço de *home banking* constitui um dever do utilizador que o vincula a realizar a notificação imediatamente após ter conhecimento do sucedido. Como é difícil demonstrar que o utilizador tem efetivamente conhecimento da ocorrência, considera-se que basta que este se encontre numa situação em que seja impossível ignorar o incidente, por exemplo, a partir do momento em que o cliente verifica os movimentos da sua conta bancária, onde figurarão as operações fraudulentas[250]. Numa situação em que se prove que o utilizador teve conhecimento da ocorrência e só notificou o banco dias depois, não apresentando nenhuma justificação válida para o sucedido, o julgador provavelmente irá considerar que este agiu com negligência grave. Consequentemente, o cliente irá suportar os prejuízos que ocorreram antes do momento da notificação, até ao limite do saldo disponível (n.º 3 do artigo 72º).

O cliente pode ainda contribuir para os prejuízos resultantes de operações não autorizadas se, de forma deliberada, incumprir os deveres que lhe foram impostos por lei, pelo artigo 67º do RSP, designadamente os deveres de cuidado e diligência. Considera-se que o cliente incumpre deliberadamente estes deveres quando, por exemplo, divulga a terceiros os códigos de acesso ao *home banking*, incumprindo o seu dever de preservar a eficácia dos seus dispositivos de segurança personalizados. Perante estas circunstâncias, é o próprio que deve suportar todas as perdas originadas pelas operações de pagamento não autorizadas até à comunicação da ocorrência (n.º 2 e 4 do artigo 72º).

Ainda neste âmbito, atente-se no clausulado do contrato de *home banking* analisado pela Relação de Lisboa no Acórdão de 5 de novembro de 2013:

"4.2. O Cliente compromete-se, igualmente, a guardar sob segredo as suas Credenciais de Autenticação, bem como a prevenir adequadamente a sua utilização abusiva por parte de terceiros. O Cliente é o único responsável por todos os prejuízos resultantes da utilização indevida do Serviço do Banco M. por parte de terceiros, com exceção do estabelecido no ponto 5.3.

5.1. No caso de perda, extravio, furto, roubo ou falsificação de credenciais de autenticação, o cliente deverá comunicar imediatamente ao Banco M. tal facto, através do serviço do Banco M., via *phone* 24.

5.3. A responsabilidade do cliente por todas as operações irregulares efetuadas utilizando as credenciais de autenticação, ou através da utilização abusiva das mesmas, motivadas por perda, extravio, furto, roubo ou falsificação cessa no momento em que seja efetuada a

[249] REINHARD STEENNOT , op. cit., n. º 2.2.3.1., p. 557.
[250] Ibidem, n. º 2.2.3.2., p. 557.

comunicação acima referida, salvo se forem devidas a dolo e/ou negligência grosseira do cliente."

Esta cláusula 5.3. faz impender inteiramente sobre o titular do instrumento de pagamento o risco da sua utilização abusiva até ao momento da notificação ao banco e mesmo depois desta em caso de dolo ou negligência grosseira da sua parte. O banco pretende afastar a sua responsabilidade ao fazer recair o risco das operações realizadas por terceiros sobre o utilizador do serviço de *home banking*. É comum as entidades bancárias argumentarem que, com este tipo de cláusulas, pretendem repor o equilíbrio contratual uma vez que estas não têm possibilidade de "adivinhar" que quem introduz os códigos de segurança é o verdadeiro titular da conta[251]. Contudo, este é um risco inerente ao serviço de banca eletrónica que propôs aos seus clientes. A matéria da alteração das regras relativas à distribuição do risco encontra-se intimamente ligada à questão do ónus da prova uma vez que o risco ao recair exclusivamente sobre o aderente implica um ónus da prova praticamente inalcançável da sua parte. Neste caso, o conteúdo da cláusula 4.2. 2ª parte, quando conjugada com o disposto na cláusula 5.1. e 5.3., é nula por absolutamente proibida quando inserida no âmbito de relações do banco com consumidores porque altera as regras respeitantes à distribuição do risco consagradas no artigo 72º do RSP (alínea f) do artigo 21º, artigo 20º e artigos 12º e 24º do RJCCG)[252]. Mesmo à luz das regras da boa-fé não seria concebível que o utilizador do serviço de banca eletrónica pudesse ser responsabilizado por utilizações abusivas após a comunicação da ocorrência ao banco que, a partir desse momento, passa a reunir todas as condições para impedir novas intromissões[253]. E mesmo até à notificação à entidade bancária, a não repartição dos riscos ignora o facto de a utilização do serviço ser do interesse de ambas as partes[254].

Como já dissemos *supra* relativamente às cláusulas proibidas que visam alterar as regras do ónus da prova, o artigo 101º do RSP vem dispor que os preceitos legais deste regime jurídico que sejam mais favoráveis aos clientes devem ser aplicados ao caso concreto, afastando as cláusulas abusivas plasmadas no contrato de banca eletrónica.

Por outro lado, se o que esteve na origem dos prejuízos foi um comportamento fraudulento do utilizador, deve ser ele a responder pelas perdas causadas até à comunicação do incidente ao banco, mas também por aquelas que advierem após a notificação (n.º 2 e 4 do artigo 72º). Podemos verificar que a limitação da responsabilidade do cliente no que diz respeito às operações de pagamento não autorizadas não se aplica quando estamos perante uma atuação fraudulenta do aderente ao serviço de *home banking,* exonerando, assim, o banco da obrigação de suportar os prejuízos causados por essas operações.

[251] Ac. TRL de 12/12/2013 (Tomé Ramião), cit.
[252] Ac. TRL de 5/11/2013 (Manuel Marques), cit.
[253] AZEVEDO FERREIRA, Direito bancário…, cit., p. 389.
[254] Ibidem, loc. cit.

Uma vez que nos encontramos a analisar o cerne do artigo 72º do RSP, parece pertinente retomar aqui o estudo do regime jurídico relativo à repartição dos prejuízos resultantes de operações não autorizadas constante da PDSP.

De acordo com a segunda parte do n.º 1 do artigo 66º da PDSP, correspondente ao artigo 61º da DSP (que por sua vez esteve na base do artigo 72º do RSP), "o ordenante suporta todas as perdas resultantes de operações de pagamento não autorizadas se aquelas tiverem sido incorridas devido a atuação fraudulenta ou ao incumprimento deliberado ou por negligência grave de uma ou mais das obrigações decorrentes do artigo 61º. Nestes casos, não é aplicável o montante máximo referido no nº 1 do presente artigo [os € 50 a suportar pelo utilizador no caso de não ter agido com negligência grave ou dolo]. Em relação aos pagamentos efetuados através de uma comunicação à distância em que o prestador de serviço de pagamento não exige uma sólida autenticação dos clientes, o ordenante deve apenas suportar eventuais consequências financeiras em caso de atuação fraudulenta. Se o beneficiário ou o seu prestador de serviços de pagamento não aceitar uma sólida autenticação do cliente, deve reembolsar os prejuízos financeiros causados ao prestador de serviços de pagamento do ordenante".

Verificamos que, em caso de atuação fraudulenta ou de incumprimento deliberado das obrigações que impendem sobre o cliente, a solução continua a ser a mesma que provinha do DSP (n.º 2 do artigo 61º da DSP), devendo este suportar a totalidade das perdas provocadas pelo seu comportamento doloso. Foi ainda retirada a possibilidade dos Estados-Membros criarem um regime intermédio para as situações que se situem entre os casos de negligência leve e os de fraude ou incumprimento deliberado das obrigações do cliente (como no n.º 3 do artigo 61º da DSP), estabelecendo a Proposta que as situações em que o utilizador agiu de forma gravemente negligente devem ser resolvidas da mesma forma que os casos em que este agiu de forma fraudulenta ou em incumprimento deliberado das suas obrigações.

A PDSP reforça ainda a proteção dos interesses dos utilizadores dos serviços de pagamento ao ressalvar que, no caso de pagamentos efetuados através de comunicação à distância como acontece no *home banking*, se o banco não exigir uma sólida autenticação dos clientes será ele a suportar as perdas resultantes de operações de pagamento não autorizadas, exceto em caso de atuação fraudulenta do utilizador do serviço de pagamento. O conceito de autenticação sólida do cliente é-nos conferido pelo legislador comunitário no n.º 22 do artigo 4º da PDSP onde se define como "um procedimento de validação da identificação de uma pessoa singular ou coletiva, baseado na utilização de dois ou mais elementos pertencentes às categorias conhecimento, posse e inerência que são independentes, na medida em que a violação de um destes elementos não compromete a fiabilidade dos demais, sendo concebido de forma a proteger a confidencialidade dos dados de autenticação". Assim, de acordo com a PDSP, para se verificar, com um elevado grau de certeza, se a pessoa em questão é realmente quem diz ser deve-se conjugar dois ou mais elementos dos métodos existentes que permitem autenticar pessoas num sistema de informação – prova por conhecimento,

prova de posse e prova biométrica. Podemos prever que os sistemas de autenticação multifator serão implementados pela totalidade das entidades bancárias pois, se estes não adaptarem os seus sistemas de pagamento convertendo-os à autenticação multifator, irão suportar as consequências da ocorrência de operações não autorizadas nas contas dos seus clientes, salvo em caso de atuação fraudulenta destes últimos. Esta última parte do n.º 1 do artigo 66º da PDSP visa, claramente, o reforço do dever que impende sobre os bancos de prestarem um serviço eficaz e seguro.

Já quanto às consequências financeiras ocorridas após a notificação, a PDSP mantém *ipsis verbis* o regime que consta da DSP.

Após uma análise sumária das principais alterações apresentadas pela PDSP podemos confirmar que a Proposta vem simplificar a disciplina da repartição das perdas resultantes de operações não autorizadas, nomeadamente no que diz respeito à responsabilidade do titular. Este regime jurídico passa a explicar-se em poucas linhas. Assim, se o utilizador do serviço de pagamento potenciou a ocorrência de uma operação de pagamento não autorizada ao agir de modo fraudulento ou incumprindo deliberadamente ou com negligência grave uma ou mais obrigações que lhe competia observar, deve suportar a totalidade das perdas causadas até à notificação do banco. Em qualquer dos restantes casos, se se verificar uma operação de pagamento não autorizada, o utilizador irá suportar sempre até 50 euros dos prejuízos que dela resultaram.

Retomando o estudo do regime em vigor e tendo presente tudo o que foi exposto até aqui, podemos concluir que as consequências das operações fraudulentas realizadas via banca eletrónica tornam-se mais desvantajosas para o cliente à medida que a sua atuação se revela mais censurável[255]. Assim, à medida que a atuação do utilizador se mostra mais repreensível, este vai suportando, de forma mais extensa, os prejuízos por si potenciados até ao limite máximo da desresponsabilização total do banco pelas perdas causadas, mesmo após a notificação à entidade bancária da utilização do instrumento de pagamento abusivamente apropriado nos casos de comportamento fraudulento do utilizador (n.º 4 do artigo 72º *in fine*).

Em suma, a repartição dos prejuízos decorrentes de fraude informática no *home banking* antes da notificação ao banco rege-se pela ideia da distribuição equitativa das perdas causadas pela utilização abusiva do instrumento de pagamento, por terceiros. Desta forma, assume grande relevância o cumprimento das obrigações contratuais de ambas as partes – a comunicação da ocorrência ao banco pelo utilizador do serviço de pagamentos e a salvaguarda do sistema informático pela entidade bancária – reforçando-se ainda a segurança do serviço e a diligência dos contraentes[256]. A lei, ao conferir um critério objetivo de imputação das perdas sofridas baseado na diligência do utilizador do serviço de banca

[255] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 66.
[256] AZEVEDO FERREIRA, Direito bancário…, cit., p. 388; MARIA RAQUEL GUIMARÃES, As transferências eletrónicas…, cit., p. 216.

eletrónica e na sua contribuição para os prejuízos, está a conceder uma solução justa e promotora de uma maior eficiência e segurança dos sistemas de pagamento[257].

c) A imputação dos prejuízos ao utilizador e a fraude informática

Ao analisar a jurisprudência dos nossos tribunais superiores, podemos verificar que a prova da existência ou não de negligência por parte do cliente tem um papel crucial no desfecho dos casos de repartição dos prejuízos decorrentes de fraude informática no *home banking*.

A identificação de uma situação como denunciadora de negligência leve ou grosseira é complexa, principalmente quando estamos no âmbito de uma fraude informática. Um caso particularmente intrincado é aquele em que o cliente fornece todos os algarismos do seu cartão matriz, por tal lhe ter sido pedido na internet, numa página idêntica à do banco, ou seja, é complicado avaliar o grau de negligência presente quando o cliente "caí" num esquema de *pharming*. Nesta sede, a pergunta que se impõe é a seguinte: podemos considerar a conduta do cliente censurável, quando numa página parecida com a do banco que não cria qualquer dúvida sobre a sua genuinidade, digitou todas as combinações possíveis do cartão matriz, perante uma solicitação nesse sentido?

Apesar de a larga maioria das decisões dos tribunais superiores ter concluído pela condenação do banco e respetivo reembolso ao cliente da totalidade dos prejuízos[258] devido à ausência de prova da existência de um comportamento especialmente censurável do cliente, temos alguns acórdãos que terminaram em absolvição da entidade bancária[259]. Vejamos.

A Relação de Guimarães, no Acórdão de 25 de novembro de 2013, considerou a conduta do utilizador do serviço de *home banking* gravemente negligente uma vez que a entrega de todos os dados do cartão matriz contraria toda a lógica do sistema de segurança que não lhe pode ser desconhecida, destacando ainda que seria incongruente da parte do banco pedir a totalidade dos dígitos do cartão quando este deve ter na sua posse uma cópia para confirmar e validar os movimentos da conta bancária do seu cliente através do serviço de banca eletrónica[260]. Este Tribunal colocou a tónica no comportamento distraído e desinteressado do cliente, desvalorizando, completamente, o facto de a página a que acedeu ser idêntica à página oficial da sua entidade bancária. Considera que um utilizador informático minimamente diligente e informado no uso deste serviço devia explorar a página do banco e tinha a obrigação de conhecer os perigos que o sistema implica, logo, perante a solicitação

[257] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos..., cit., p. 66.
[258] Ac. TRL de 26/10/2010 (Maria Amélia Ribeiro), cit.; Ac. TRL de 24/05/2012 (Ezagüi Martins), cit.; Ac. TRG de 23/10/2012 (Filipe Caroço), cit.; Ac. TRL de 18/04/2013 (Anabela Calafate), cit.; Ac. TRG de 30/05/2013 (Rita Romeira), cit.; Ac. TRL de 28/06/2013 (Anabela Calafate), cit.; Ac. TRL de 5/11/2013 (Manuel Marques), cit.; Ac. STJ 18/12/2013 (Ana Paula Boularot), cit.; Ac. TRP de 29/04/2014 (Francisco Matos), cit.
[259] Ac. TRG de 25/11/2013 (Espinheira Baltazar), cit.; Ac. TRL de 12/12/2013 (Tomé Ramião), cit.
[260] Ac. TRG de 25/11/2013 (Espinheira Baltazar), cit.

anormal desses dados, devia ter desconfiado e contactado o banco por telefone, agindo de acordo com as indicações que lhe fossem dadas[261]. Este acórdão concluiu que o cliente foi negligente ao violar as regras de segurança impostas pelo contrato, permitindo a intromissão de terceiros na sua conta bancária.

A Relação de Lisboa, no Acórdão de 12 de dezembro de 2013, num caso idêntico ao da Relação de Guimarães, também considerou o comportamento do utilizador do serviço de banca eletrónica gravemente negligente com base no facto de este não ter estranhado a solicitação da atualização da matriz, pedido nunca dantes feito e que comportava a revelação de uma quantidade enorme de números do cartão matriz[262] que sabia que era a única garantia de segurança que as operações eram por si realizadas, para além de ter ignorado os avisos de segurança divulgados na página do banco. Este Tribunal desvalorizou o facto de o computador do cliente estar "infetado" por um *software* malicioso que permitiu a terceiros aceder ao sistema e desviar quantias da sua conta, tendo concluído que ficou provado que o cliente divulgou a terceiros os seus dados de acesso ao serviço de *home banking*, descurando os deveres de cuidado que sobre si impendiam, o que demonstra uma utilização imprudente do serviço.

Na nossa opinião, o entendimento seguido pela Relação de Guimarães e de Lisboa nos acórdãos *supra* referidos é demasiado intransigente para o utilizador do serviço de banca eletrónica. A imputação de um comportamento de negligência grave ao utilizador parece-nos exagerado tendo em consideração que o que conduziu à apropriação abusiva do instrumento de pagamento foi uma fraude informática. Já uma imputação a título de negligência leve seria de se considerar, como veremos *infra*.

Todavia, na grande maioria dos casos que chegaram aos tribunais superiores, o banco foi condenado a suportar a totalidade das perdas porque não conseguiu provar que houve um comportamento do cliente revelador de menor cuidado relativamente aos seus deveres de preservação da eficácia e confidencialidade das palavras-passe. E, não conseguindo a entidade bancária provar que o cliente fez uma utilização imprudente do serviço de *home banking*, nem que divulgou as suas credenciais acesso a este a terceiros, o banco não pode imputar a quebra da confidencialidade dos dispositivos de segurança personalizados ao seu cliente.

Para perceber melhor a essencialidade da prova neste âmbito, importa aqui retomar o que foi explicitado no ponto 3.2. deste capítulo, dedicado ao ónus da prova. Como já vimos, o artigo 70º do RSP atribui ao banco o ónus da prova de que a operação de pagamento alegadamente não autorizada pelo utilizador foi autenticada, devidamente registada e contabilizada e não afetada por qualquer problema técnico, assim como lhe cabe provar que a operação de pagamento foi autorizada pelo seu cliente e que este agiu de forma

[261] Idem.

[262] Da matéria de facto consta que o cliente divulgou todas as combinações possíveis do cartão matriz e que o terceiro que acedeu à sua conta bancária só o pôde fazer porque conhecia o número de contrato, o número do código de acesso (sem os quais não consegue sequer fazer o login) e ainda todos ou parte das 64 combinações de 3 algarismos cada uma que compõem o cartão matriz. Isto significa que o cliente teve de inserir 192 algarismos. Cfr. TRL de 12/12/2013 (Tomé Ramião), cit.

negligente, fraudulenta ou em claro incumprimento das obrigações decorrentes do artigo 67º do RSP. Estas normas de distribuição do ónus da prova são muito penalizadoras para a entidade bancária pois exigem uma prova muito complexa e rigorosa. No âmago das normas de distribuição do ónus da prova constantes do RSP encontram-se os deveres gerais dos bancos que derivam do RGICSF, nomeadamente a competência técnica e o critério de diligência (artigos 73º e 75º do RGICSF, respetivamente). Especialmente nos casos de operações bancárias ordenadas à distância pelos clientes, é exigida uma especial diligência e cuidado uma vez que o risco de fraude é mais elevado devido à inexistência de contacto direto entre o banco e o cliente[263]. Foi com base nos deveres acima referidos que o Supremo Tribunal de Justiça, no Acórdão de 16 de setembro de 2014, decidiu que o banco é responsável pelas transferências efetuadas aparentemente por ordem do seu cliente (depositante), sendo a sua responsabilidade apenas excluída caso este justifique a diminuição do saldo da conta bancária do seu cliente[264]. O Supremo Tribunal de Justiça continua o seu raciocínio afirmando que é sobre o banco que recai o ónus da prova de que a movimentação da conta do seu cliente só ocorreu por motivo justificado, nomeadamente porque tinha autorização para o fazer[265]. Assim, não será considerado justificado o facto de as transferências não terem sido ordenadas pelo depositante (cliente) e terem sido realizadas pela entidade bancária sem a diligência exigível para a confirmação da legitimidade da ordem e da aparente autoria[266]. Revelando o entendimento unânime do Supremo Tribunal de Justiça quanto a esta questão, vejam-se ainda os Acórdãos de 18 de fevereiro de 2008, Proc. 08B2688 (Santos Bernardino) e de 8 de fevereiro de 2012, Proc. 500/08.4TBESP.G1.S1 (Bettencourt de Faria)[267] onde se defende que "a movimentação fraudulenta por terceiro de um depósito bancário não é oponível ao depositante, que a ela foi alheio, independentemente de culpa do banco depositário nessa movimentação"[268].

Note-se que, na falta de disposição especial do RSP, o mesmo resultado decorreria da aplicação do n.º 1 do artigo 799º do CC que faz recair sobre o devedor (banco) a prova de que a falta de cumprimento da obrigação não procede de culpa sua.

É preciso ainda ter em consideração que, na altura em que os factos ocorreram, este tipo de fraude informática não era do conhecimento comum como acontece hoje em dia. O cliente, ignorando a existência de ataques à segurança do sistema informático da entidade bancária, forneceu os dispositivos de segurança personalizados que foram solicitados aquando do acesso ao serviço de *home banking* porque acreditou que esses dados lhe estavam a ser solicitados pelo banco[269]. Não podemos ignorar que o esquema do *pharming* é muito mais complexo e ardiloso que o *phishing*. Todavia, mesmo nos casos de *phishing* deve-se apurar, no caso concreto, se a conduta do utilizador é censurável tendo em conta a aparência fidedigna ou não da mensagem de correio eletrónico (e a ingenuidade manifestada pelo

[263] Ac. STJ de 16/09/2014, Proc. 333/09.0TVLSB.L2.S1 (Paulo Sá), in www.dgsi.pt.
[264] Ac. STJ de 16/09/2014 (Paulo Sá), cit.
[265] Ac. STJ de 16/09/2014 (Paulo Sá), cit.
[266] Ac. STJ de 16/09/2014 (Paulo Sá), cit.
[267] Ambos disponíveis em www.dgsi.pt.
[268] Ac. STJ de 8/03/2012 (Bettencourt de Faria), cit.
[269] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 64.

utilizador), assim como o cumprimento pelo banco das obrigações de informação e esclarecimento dos clientes impostas pela lei[270].

Na nossa opinião, a melhor solução para a questão se existe ou não negligência grave quando o cliente divulga todas as combinações do cartão matriz é a que decorre do entendimento da Relação do Porto no Acórdão de 29 de abril de 2014. A Relação do Porto considerou que o facto de o cliente ter divulgado os dispositivos de segurança personalizados não permite que lhe seja imputado um comportamento gravemente negligente porque a intromissão de terceiros não se deveu a qualquer violação grave dos deveres de sigilo quanto aos códigos de acesso que o cliente estava obrigado a observar, mas a um esquema de *pharming* – uma fraude informática que, ao clonar a página da internet do banco, fez crer ao cliente que estava no *site* de acesso ao *home banking* da sua entidade bancária[271]. Portanto, não se evidencia qualquer incumprimento por parte do cliente dos deveres de confidencialidade dos códigos de acesso na utilização do sistema de banca eletrónica, mas sim uma quebra de segurança nos meios de acesso ao sistema informático do banco cuja responsabilidade lhe é imputável pois a ele lhe cabe prestar um serviço eficaz e seguro e assegurar que os códigos de acesso só sejam acessíveis ao utilizador do serviço de pagamento que tem direito a utilizá-lo (alínea a) do n.º 1 do artigo 68º do RSP)[272]. Nestes casos de operações fraudulentas, há uma contribuição do banco para o sucedido uma vez que, se o esquema fraudulento criado por terceiros deu frutos, foi, em parte, porque a entidade bancária não desenvolveu todas as ações que se impunham em ordem a garantir a segurança do sistema informático que permite o acesso à conta bancária do seu cliente[273]. Assim, tendo a fraude informática ocorrido nos meios de acesso ao serviço de banca eletrónica cuja segurança é da responsabilidade do banco, é ele que deve suportar os prejuízos resultantes das operações de pagamento não autorizadas decorrentes desta.

Pelas razões apresentadas, não podemos considerar que o cliente atuou com negligência grave pois apenas observamos um comportamento de negligência leve da sua parte ao divulgar os seus dados de acesso nas circunstâncias descritas.

Concluímos que, nos casos de fraude informática e, particularmente nos esquemas de *pharming*, não existe um comportamento doloso por parte do utilizador do serviço de banca eletrónica, exceto quando existam alertas de segurança suscetíveis de ser apreendidos e estes sejam negligentemente ignorados[274].

---

[270] Ibidem, loc. cit.
[271] Ac. TRP de 29/04/2014 (Francisco Matos), cit.
[272] Idem.
[273] Ac. TRG de 30/05/2013 (Rita Romeira), cit. E não nos esqueçamos que os bancos têm técnicos especializados que se dedicam exclusivamente à segurança dos sistemas informáticos.
[274] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., loc. cit.

d) A relevância dos avisos de segurança

De modo a prevenir os seus clientes da existência de fraudes informáticas que atingem o serviço de banca eletrónica, os bancos têm procurado divulgar alertas de segurança na página de acesso ao serviço de *home banking*. O exemplo mais frequente é aquele que avisa que o banco nunca pede a confirmação dos dados do cartão matriz e que as combinações que aí constam nunca deverão ser facultadas a terceiros uma vez que este é o principal método utilizado pelos piratas informáticos para aceder às contas bancárias das vítimas.

Estas recomendações, geralmente, derivam do contrato de banca eletrónica que contém uma cláusula que vincula o cliente a observar as regras de segurança que forem, ao longo do tempo, divulgadas pelo banco, dando assim cumprimento ao reforçado dever de informação que recai sobre a entidade bancária, como referido no ponto 4.2.2. do capítulo I.

Os bancos têm-se mostrado preocupados em garantir que os seus clientes conheçam efetivamente estes alertas. Num primeiro momento, estas mensagens surgiam na página inicial do serviço de banca eletrónica da entidade bancária ou num menu onde se encontravam reunidos todos os conselhos para um acesso e utilização segura deste instrumento de pagamento. Mais tarde, a esta divulgação das informações de segurança sobre o sistema de banca eletrónica acresce a que passa a ser feita no local e no momento em que qualquer cliente acede ao serviço na página do banco através dos *banners* – avisos que aparecem ao abrir a ligação de acesso ao *home banking* e que têm de ser fechados pelo cliente para conseguir aceder ao serviço, introduzindo o seu número de adesão ou de conta e o código secreto[275]. Estes são uma forma de difundir as recomendações de segurança do banco no acesso e na utilização da banca eletrónica, ao mesmo tempo que "obrigam" qualquer cliente que queira aceder ao serviço a ler tais avisos. Assim, o cliente deve ter um comportamento diligente, apreendendo efetivamente os conteúdo dos avisos se tiver sido colocado em posição de os conhecer, sob pena de a sua atuação se qualificar como negligente. Este foi o entendimento da Relação de Guimarães, no Acórdão de 25 de novembro de 2013, onde censura o comportamento dos utilizadores do serviço de banca eletrónica que apenas se concentram em entrar rapidamente no sistema para aceder às suas contas, desinteressando-se dos avisos, uma vez que o contrato de *home banking* impõe-lhes regras de segurança cujo desenvolvimento é contínuo. Afirma ainda que uma página da internet com alertas de segurança cujo desenvolvimento está num menu, é um sinal de alerta para o cliente se informar, de modo a não correr riscos desnecessários[276]. Esta exposição permite-nos concluir que os bancos têm evoluído na forma de divulgar os alertas de segurança procurando torná-los facilmente apreensíveis aos seus clientes, de forma a proteger os seus legítimos interesses.

[275] Ac. TRP de 29/04/2014 (Francisco Matos), cit.
[276] Ac. TRG de 25/11/2013 (Espinheira Baltazar), cit.

Todavia, não podemos esquecer que a função primordial destes avisos de segurança é dar cumprimento à especial obrigação de informação que impende sobre a entidade bancária. Este dever lateral de conduta decorre do princípio geral da boa-fé (n.º 2 do artigo 762º do CC) e assenta, essencialmente, na especial relação de confiança que caracteriza a relação entre bancos e clientes, justificando-se pela complexidade do sistema informático que suporta o serviço de *home banking* e pelos riscos que lhe são inerentes. Tendo em vista o regular funcionamento do serviço de banca eletrónica, a obrigação de informação mantém os laços de confiança em que a relação assenta, relação esta que, não esqueçamos, se insere na moldura mais vasta do contrato de abertura de conta. Assim, o banco deve alertar para os perigos inerentes ao *home banking* pois desta informação pode depender a correta execução das ordens recebidas e a salvaguarda dos interesses dos seus clientes[277]. Este dever encontra-se estritamente associado à esfera contratual em que se insere, logo, em caso de violação, o banco será imediatamente responsabilizado devido à não prestação de informação ao cliente, nos termos da presunção de culpa prevista no n.º 1 do artigo 799º do CC.[278] Isto significa que a ausência de avisos de segurança faz versar o risco de operações abusivas sobre o banco visto que foi este que potenciou a situação ao não cumprir a obrigação contratual de informação[279]. Mas, e se a entidade bancária cumpriu essa obrigação? Devemos considerar que a divulgação de avisos de segurança afasta a responsabilidade da entidade bancária em caso de operações não autorizadas?

Na nossa opinião, se se provar que o banco, na altura dos acontecimentos, divulga mensagens a alertar para os perigos inerentes ao *home banking,* nomeadamente dá conhecimento da existência de esquemas fraudulentos, e mais tarde, ocorre uma operação não autorizada na conta bancária do seu cliente tendo na origem a divulgação dos dispositivos de segurança personalizados para aceder ao serviço, é legítimo considerar que o cliente incumpriu com negligência grave os seus deveres, designadamente a do n.º 2 do artigo 67º do RSP. Apesar de, tanto no caso dos avisos de segurança deixados num menu na página do banco, como nos *banners,* se considerar que a mensagem foi devidamente comunicada, é manifesto que a ignorância de uma mensagem que aparece ao abrir a ligação de acesso ao *home banking* e que tem de ser fechada pelo cliente para conseguir aceder ao serviço (*banner*) será alvo de um maior grau de censura. Caberá ao julgador decidir se deverá ser feita uma distinção quanto à intensidade de negligência incorrida consoante a forma pela qual foi realizada a divulgação dos alertas. Podemos concluir que a divulgação destes alertas exonera o banco de suportar as perdas resultantes de operações fraudulentas antes da notificação da sua ocorrência[280].

---

[277] AZEVEDO FERREIRA, Direito Bancário…, cit., p. 464.
[278] Ibidem, loc. cit., p. 461.
[279] Neste sentido, MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 64. Concordamos com a autora que se afasta do entendimento acolhido no Ac. TRG de 23/10/2012 (Filipe Caroço), cit., onde se declara que a divulgação de mensagens de segurança na página do banco prestador do serviço não corresponde a uma obrigação contratual assumida.
[280] Não podemos concordar com o entendimento da Relação de Guimarães, no Acórdão de 23/10/2012 (Filipe Caroço), cit., ao desvalorizar a necessidade de tais avisos, considerando-os um simples meio de prevenir a fraude através da informação da utilização do serviço, logo se esta ocorrer, a responsabilidade não será do cliente.

4.4. Razão de ser da responsabilização da entidade bancária pelos prejuízos decorrentes de operações não autorizadas

Como podemos verificar do estudo do artigo 72º do RSP, é a instituição bancária que suporta os prejuízos causados pelas debilidades dos sistemas de pagamento que disponibiliza aos seus clientes sempre que as perdas não tenham sido potenciadas por estes[281]. Isto decorre da alínea a) do n.º 1 do artigo 68º do RSP que impõe ao banco a obrigação de assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao seu utilizador. Consequentemente, se um terceiro consegue aceder ao sistema informático que suporta o serviço de *home banking* e esta intromissão não foi potenciada pelo comportamento do cliente, é evidente que será o banco a suportar os prejuízos ocorridos. Isto significa que os riscos da utilização normal do sistema de pagamentos disponibilizado recaem sobre a entidade bancária. Este entendimento tem, fundamentalmente, por base a obrigação que recai sobre o banco de prestar um serviço seguro e eficaz.

Assim, não podemos aceitar que a desigualdade económica das partes e a dimensão que as perdas resultantes de operações fraudulentas possam assumir na esfera de cada uma sejam tomadas como argumento a favor da responsabilidade do banco no caso de intromissões por terceiros no sistema de *home banking*[282]. Logo, são de rejeitar as afirmações da Relação de Lisboa no Acórdão de 26 de outubro de 2010 onde assevera que "a quantia [de 16 800,00€, resultado de operações fraudulentas ocorridas via banca eletrónica] é uma gota de água no oceano do volume de negócios do banco. […] O que está em causa para o banco está no plano das insignificâncias mas, para o cliente, não será exagero afirmar, estará no domínio da própria subsistência", assim como o comentário do Supremo Tribunal de Justiça, no Acórdão de 18 de dezembro de 2013, quando afirma que o risco da utilização normal do sistema de banca eletrónica é "uma obrigação perfeitamente normal já que é o Banco que vai retirar os maiores benefícios económicos do seu bom funcionamento". O facto de a entidade bancária ser a parte contratual que "tem mais a ganhar" com o funcionamento do sistema que sustenta o *home banking* não pode servir de critério para agravar a sua responsabilidade na repartição dos prejuízos decorrentes de operações fraudulentas nas contas bancárias dos seus clientes. Além disso, temos de ter em conta que os bancos dispõem serviços de segurança compostos por técnicos especializados que acompanham os movimentos suspeitos efetuados via *home banking*, contrariamente aos seus clientes que

[281] Ibidem, p. 65. No mesmo sentido, LUIZ GUSTAVO CARATTI DE OLIVEIRA, Responsabilidade civil dos bancos em casos de fraude pela internet que lesam as contas de seus clientes (Monografia de conclusão de curso apresentada ao curso de Pós Graduação em Direito Civil e Processo Civil da Universidade Castelo Branco), in http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=9110 (2/09/2014) acrescenta que "o cliente ao se sentir lesado por ser vítima de terceiro que movimente sua conta ao ponto de lhe causar prejuízo financeiro, deve ser ressarcido pelo banco, pois este tem o dever de manter seu serviço em segurança".

[282] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 66.

não têm possibilidade de acompanhar ininterruptamente as suas contas[283]. É manifesto que as entidades bancárias estão cientes da vulnerabilidade do sistema informático que sustenta a banca eletrónica e da responsabilidade que dela pode advir em caso de fraude informática.

No que diz respeito ao cumprimento do dever de prestar um serviço seguro e eficaz no qual se funda a responsabilidade das entidades bancárias pelo sistema, os bancos têm sido desafiados pela sofisticação e atualização permanentes observadas nos acessos fraudulentos às contas bancárias dos seus clientes, exigindo um esforço continuado da sua parte no que diz respeito à segurança, pelo menos enquanto se apresentarem como guardiãs confiáveis dos montantes que lhes foram entregues[284].

5. Conclusão

Aqui chegados, importa expor as principais conclusões a que chegamos no presente estudo.

O contrato de *home banking* é um tipo negocial autónomo, através do qual o banco permite ao cliente usufruir de um serviço de movimentação de fundos recorrendo a meios informáticos.

Da utilização do serviço decorre a necessidade de o seu utilizador cumprir uma série de deveres acessórios de conduta, muitos deles conexos com a segurança do sistema de banca eletrónica, de entre os quais se destaca o dever de preservar a eficácia dos códigos de acesso ao serviço entregues pela entidade bancária. Por outro lado, ao banco cabe, principalmente, assegurar que o serviço é eficaz e seguro.

No que diz respeito à fraude informática, verificamos que o *phishing* e o *pharming* são as técnicas fraudulentas que atingem o sistema de *home banking*. Enquanto o *phishing* utiliza como "isco" uma mensagem de correio eletrónico, no *pharming*, modalidade mais perigosa que a anterior por surgir de forma quase impercetível, o utilizador do serviço é enganado sem se aperceber uma vez que esta técnica passa pela autoinstalação de um ficheiro oculto que, por sua vez, vai permitir a redireção para uma página forjada sempre que o utilizador digite o *site* do seu banco. Estas duas modalidades de fraude informática caracterizam-se pela introdução de uma pessoa não autorizada numa rede informática e consequente movimentação de fundos das contas bancárias dos clientes para contas de terceiros.

O tema da repartição dos prejuízos decorrentes de fraude informática encontra-se hoje regulado pelo RSP e implica encontrar resposta a diferentes questões prévias para se chegar a uma resposta final.

A primeira questão está relacionada com o ónus da prova. Neste âmbito, cabe ao banco provar que a operação de pagamento foi devidamente autenticada e, uma vez feita esta

[283] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 65.
[284] Ac. TRL de 24/05/2012 (Ezagüi Martins), cit.

prova, compete-lhe ainda provar, no caso concreto, a contribuição do cliente para os prejuízos ocorridos e o grau de culpa subjacente ao seu comportamento.

O comportamento do utilizador do serviço de *home banking* é decisivo para a definição de quem irá suportar as perdas resultantes de operações fraudulentas antes da notificação da ocorrência à entidade bancária. Com o nosso estudo, verificamos que as consequências das operações fraudulentas realizadas via banca eletrónica tornam-se mais desvantajosas para o cliente à medida que a sua atuação se revela mais censurável.[285] Assim, à medida que a atuação do utilizador se revela mais censurável, este vai arcando, de forma mais extensa, os prejuízos por si potenciados até ao limite máximo da desresponsabilização total do banco pelas perdas causadas, mesmo após a notificação à entidade bancária da utilização do instrumento de pagamento abusivamente apropriado, nos casos de comportamento fraudulento do utilizador.

Assim, confirmamos que a prova da existência de negligência por parte do utilizador é essencial para resolver os casos de repartição dos prejuízos decorrentes da realização de operações de pagamento não autorizadas. E a complexidade da prova da existência de negligência do utilizador manifesta-se de forma ainda mais intensa quando estamos perante um caso de fraude informática.

Na nossa opinião, o utilizador do serviço de *home banking* que "caia" num esquema de *pharming*, divulgando todas as combinações do cartão matriz, não incumpriu os seus deveres de preservação da eficácia dos códigos de acesso ao sistema de banca eletrónica, logo não deve suportar os prejuízos ocorridos até à notificação do sucedido. As operações de pagamento não autorizadas não se deveram à violação dos deveres de confidencialidade que recaiam sobre o cliente, mas deveram-se a uma fraude informática. O que, de facto, ocorre é uma quebra de segurança nos meios de acesso ao sistema informático do banco. Deste modo, uma vez que é à entidade bancária que compete assegurar um serviço eficaz e seguro e garantir que os códigos de acesso só são acessíveis ao seu utilizador, compreende-se que seja sobre o banco que recai o dever de suportar as perdas decorrentes de fraude informática. Assim, consideramos que o cliente agiu meramente com negligência leve ao divulgar os seus códigos de acesso no âmbito de um esquema de *pharming*. Concluímos que, nos casos de fraude informática e, particularmente nos esquemas de *pharming*, não existe um comportamento doloso por parte do utilizador do serviço de banca eletrónica, exceto quando existam alertas de segurança suscetíveis de ser apreendidos e estes sejam negligentemente ignorados.

Após a verificação da ocorrência de uma operação de pagamento não autorizada, o cliente deve notificar o banco do sucedido. Esta notificação determina o momento em que o utilizador deixa de suportar os prejuízos decorrentes da operação fraudulenta, salvo em caso de comportamento fraudulento da sua parte. A partir desse momento, o banco deve

[285] MARIA RAQUEL GUIMARÃES, A repartição dos prejuízos…, cit., p. 66.

reembolsar imediatamente o cliente da quantia indevidamente debitada da sua conta, assemelhando-se, no seu efeito, este mecanismo de reembolso à cláusula *solve et repete*.

Bibliografia

ALMEIDA, CARLOS FERREIRA DE, Contratos II, 3ª edição. Coimbra: Almedina, 2012.

ANTUNES, JOSÉ ENGRÁCIA, Direito dos Contratos Comerciais. Coimbra: Almedina, 2009.

BENSOUSSAN, ALAIN, Informatique et télécoms. Levallois: Éditions Francis Lefebvre, 1997.

CAPDEVILLE, JEROME LASSERRE, La contestation des opérations de paiement non autorisées. Revue de droit bancaire et financier. LexisNexis JurisClasseur. 12e année, n.º 1 (janvier-février 2011), pp. 109-113.

CORDEIRO, ANTÓNIO MENEZES, Da Compensação no direito civil e no direito bancário. Coimbra: Almedina, 2003.

CORDEIRO, ANTÓNIO MENEZES, Manual de Direito Bancário, 3ª edição. Coimbra: Almedina, 2006.

CORDEIRO, ANTÓNIO MENEZES, Tratado de Direito Civil, Tomo I. 3ª edição (reimpressão). Coimbra: Almedina, 2007.

CORDEIRO, ANTÓNIO MENEZES, Tratado de Direito Civil, Tomo II. 4ª edição (reformulada e atualizada). Coimbra: Almedina, 2014.

CORDEIRO, ANTÓNIO MENEZES, Tratado de Direito Civil, Tomo VIII, reimpressão da 1ª edição do tomo III da parte II de 2010. Coimbra: Almedina, 2014

COSTA, MÁRIO JÚLIO DE ALMEIDA, Direito das Obrigações, 12ª edição (revista e atualizada). Coimbra: Almedina, 2009.

FARIA, JOSÉ MANUEL, Acesso a contas bancárias por terceiros no âmbito de operações de pagamento. Revista da Banca. Lisboa: Associação Portuguesa de Bancos. N.º 71 (janeiro/junho 2011), pp. 25-39.

FEDERAL DEPOSIT INSURANCE CORPORATION, Guidance on How Financial Institutions Can Protect against Pharming attacks. Financial Institution Letters (2005), in www.fdic.gov/news/news/financial/2005/fil6405a.html, consultado a 27/07/2014.

FERNÁNDEZ LÁZARO, FERNANDO, La brigada de investigación tecnológica: la investigación policial. In Policía. Madrid. Nº 199 (2007), pp. 18-21.

FERREIRA, ANTÓNIO PEDRO DE AZEVEDO, A relação negocial bancária – conceito e estrutura. Lisboa: Quid Iuris, 2005.

FERREIRA, ANTÓNIO PEDRO DE AZEVEDO, Direito Bancário. 2ª edição. Lisboa: Quid Juris, 2009.

FOX, MARK A., Phishing, Pharming and Identity Theft in the Banking Industry. Journal of international banking law and regulation. Sweet and Maxwell (2006), Issue 9, pp. 548-552.

GETE-ALONSO Y CALERA, MARÍA DEL CARMEN, Las tarjetas de crédito, Relaciones contractuales y conflictividad. Madrid: Marcial Pons, 1997.

GOMES, JANUÁRIO DA COSTA, Contratos Comerciais. Coimbra: Almedina, 2012.

GONZÁLEZ, Carolina e TORRENCILLA, Ángel, Respuestas operativas al "phishing". In Policía. Madrid. Nº 190 (2006), pp. 42-47.

GUIMARÃES, MARIA RAQUEL, As transferências eletrónicas de fundos e os cartões de débito. Coimbra: Almedina, 1999.

GUIMARÃES, MARIA RAQUEL, Comércio eletrónico e transferências eletrónicas de fundos. O Comércio Eletrónico – Estudos Jurídico-Económicos. Coimbra: Almedina, 2002, pp. 57-80.

GUIMARÃES, MARIA RAQUEL, O Contrato-quadro no âmbito da utilização de meios de pagamento eletrónicos. Coimbra: Coimbra Editora, 2011.

GUIMARÃES, MARIA RAQUEL, The debit and credit card frame work contract and its influence on European legislative initiatives. InDret Comparado, Revista para el Analisis del derecho. N.º 2 (2012), in http://www.indret.com/es, consultado a 4/09/2014, pp. 1-19.

GUIMARÃES, MARIA RAQUEL, A repartição dos prejuízos decorrentes de operações fraudulentas de banca eletrónica *(home banking)*: anotação ao Acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09. Cadernos de Direito Privado. Braga: CEJUR. Nº 41 (janeiro/março 2013), pp. 45-69.

GUIMARÃES, MARIA RAQUEL, A fraude no comércio eletrónico: o problema da repartição do risco por pagamentos fraudulentos. In Infrações Económicas e Financeiras: Estudos de Criminologia e Direito (J. Cruz, C. Cardoso, A. L. Leite, R. Faria*, coordenação*). Coimbra: Coimbra Editora, 2013, pp. 581-597.

IBM, Relatório Semestral de Tendências e Riscos IBM x-force 2011, setembro 2011.In http://ftp.software.ibm.com/la/documents/imc/br/commons/Trend_Risk_report_Sept_2011_ptb.pdf, consultado a 18/09/2014.

INSTITUTO NACIONAL DE ESTATÍSTICA, Inquérito à utilização de tecnologias da informação e da comunicação pelas famílias 2014, novembro de 2014. In http://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=211422735&DESTAQUESmodo=2, consultado a 10/01/2015.

LÓPEZ JIMÉNEZ, JOSÉ MARÍA, Comentarios a la Ley de Servicios de Pago. Barcelona: Bosch, 2011.

LUÍS, FRANCISCO, Proteger o dinheiro – *Home banking*, Conselhos aos utilizadores. Inforbanca. Lisboa: Instituto de Formação Bancária, Associação Portuguesa de Bancos. N.º 88 (abril-junho 2011), pp. 10-12.

MACHADO, JOÃO BAPTISTA, Introdução ao Direito e ao Discurso Legitimador. 17ª reimpressão. Coimbra: Almedina, 2008.

MARQUES, GARCIA E MARTINS, LOURENÇO, Direito da Informática. 2ª edição, refundida e atualizada. Coimbra: Almedina, 2006.

MERCADO-KIERKEGAARD, SYLVIA, Harmonising the regulatory regime for cross-border payment services. In Computer Law and Security Review, vol. 23 (2007), in http://www.sciencedirect.com, consultado a 22/07/2014, pp. 177-187.

MÚRIAS, PEDRO, Introdução ao ónus da prova. Texto não publicado facultado aos alunos de Teoria do Processo da Faculdade de Direito da Universidade Nova de Lisboa no ano letivo de 2013/2014.

OLIVEIRA, LUIZ GUSTAVO CARATTI DE, Responsabilidade civil dos bancos em casos de fraude pela internet que lesam as contas de seus clientes (Monografia de conclusão de curso apresentada ao curso de Pós Graduação em Direito Civil e Processo Civil da Universidade Castelo Branco), in http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=9110, consultado a 2/09/2014.

PEREIRA, JOEL TIMÓTEO RAMOS, Direito da Internet e Comércio Eletrónico. Lisboa: Quid Iuris, 2001.

PEREIRA, JOEL TIMÓTEO RAMOS, Compêndio jurídico da sociedade da informação. Lisboa: Quid Iuris, 2004.

PHISHING ACTIVITY TRENDS REPORT, 2nd Quarter 2014 (April-June 2014). In http://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf, consultado a 14/09/2014.

PROENÇA, JOSÉ CARLOS BRANDÃO, A conduta do lesado como pressuposto e critério de imputação do dano extracontratual. Coimbra: Almedina, 1997.

REGO, MARGARIDA LIMA, O *e-mail* como título executivo. Estudos em homenagem ao Prof. Doutor José Lebre de Freitas, I. Coimbra: Coimbra Editora, 2013, pp. 1021-1043.

SÁ, ALMENO DE, Direito Bancário. Coimbra: Coimbra Editora, 2008.

SILVA, JOÃO CALVÃO DA, Direito Bancário. Coimbra: Almedina, 2001.

SILVA, JOÃO CALVÃO DA, Banca, Bolsa e Seguros – Direito europeu e português, Tomo I, 2ª edição (revista e aumentada). Coimbra: Almedina, 2007.

STEENNOT, REINHARD, Allocation of liability in case of fraudulent use of an electronic payment instrument: The new Directive on payment services in the internal market. Computer Law &

Security Review, vol. 24 (2008), in http://www.sciencedirect.com, consultado a 22/07/2014, pp. 555-561.

TELLES, INOCÊNCIO GALVÃO, Direito das Obrigações, 7ª edição (reimpressão). Coimbra: Coimbra Editora, 2010.

VAN DER MEULEN, NICOLE, You've been warned: Consumer liability in Internet banking fraud. Computer Law & Security Review, vol. 29 (2013), in http://www.sciencedirect.com, consultado a 8/09/2014, pp. 713-718.

VARELA, JOÃO DE MATOS ANTUNES, Depósito Bancário – Depósito a prazo em regime de solidariedade. Revista da Banca. Lisboa: Associação Portuguesa de Bancos. Nº 21 (Janeiro/Março de 1992), pp. 41-75.

VARELA, JOÃO DE MATOS ANTUNES, Das Obrigações em Geral, vol. I, 10ª edição (revista e atualizada: 9ª reimpressão). Coimbra: Almedina, 2012.

VASCONCELOS, PEDRO PAIS, Direito Comercial, Vol. I. Coimbra: Almedina, 2011.

VERDELHO, PEDRO, Phishing e outras formas de defraudação nas redes de comunicação. In Direito da Sociedade da Informação (Oliveira Ascensão, coordenação). Vol. VIII. Coimbra: Coimbra Editora, 2009, pp. 407-419.

Jurisprudência

Ac. TRL de 16/06/1994 (Noronha Nascimento), CJ, III, 1994, pp. 122-124.

Ac. STJ de 23/11/1999 (Garcia Marques) in Coletânea de Jurisprudência – Acórdãos do STJ. Coimbra: Associação de Solidariedade Social "Casa do Juiz", 1999. Tomo III (Ano VII), pp. 100-108.

Ac. TRC de 9/11/2004, Proc. n.º 2278/04 (Alexandrina Ferreira), in www.dgsi.pt.

Cour de Cassation, chambre commerciale, financière et économique – arrêt n.º 1050 du 2/10/2007 (05-19.899), in http://www.courdecassation.fr.

Ac. STJ de 18 de fevereiro de 2008, Proc. 08B2688 (Santos Bernardino), in www.dgsi.pt.

Cour de Cassation, première chambre civile – arrêt n.º 354 du 28/03/2008 (07-10.186), in http://www.courdecassation.fr.

Ac. STJ de 15/05/2008, Proc. 08B357 (Mota Miranda), in www.dgsi.pt.

Ac. TRL de 26/10/2010, Proc. 1943/09.1TJLSB.L1-7 (Maria Amélia Ribeiro), in www.dgsi.pt.

Ac. TRE de 7/07/2011, Proc. 76/10.2JASTB-A.E1 (Pedro Vaz Pato), in http://www.dgsi.pt.

Ac. STJ de 8 de fevereiro de 2012, Proc. 500/08.4TBESP.G1.S1 (Bettencourt de Faria), in www.dgsi.pt.

Ac. TRL de 24/05/2012, Proc. 192119/11.8YIPRT.L1-2 (Ezagüi Martins), in www.dgsi.pt.

Ac. TRG de 23/10/2012, Proc. 305/09.5TBCBT.G1 (Filipe Caroço), in www.dgsi.pt.

Ac. TRL de 18/04/2013, Proc. 1397/10.0TVLSB.L1-6 (Anabela Calafate), in http://www.dgsi.pt.

Ac. TRG de 30/05/2013, Proc. 6479/09.8TBBRG.G1 (Rita Romeira), in www.dgsi.pt.

Ac. TRL de 28/06/2013, Proc. 147708/12.8Y (Anabela Calafate), in http://www.dgsi.pt.

Ac. TRP de 29/10/2013, Proc. 1254/10.0TJP (Francisco Matos), in http://www.dgsi.pt.

Ac. TRL de 5/11/2013, Proc. 9821/11.8T2SNT.L1-1 (Manuel Marques), in www.dgsi.pt.

Ac. TRG de 25/11/2013, Proc. 2869/11.4TBGMR.G1 (Espinheira Baltazar), in http://www.dgsi.pt.

Ac. TRL de 12/12/2013, Proc. 164/11.8TBSRT.L1-6 (Tomé Ramião), in http://www.dgsi.pt.

Ac. STJ de 18/12/2013, Proc. 6479/09.8TBBRG.G1.S1 (Ana Paula Boularot), in http://www.dgsi.pt.

Ac. TRP de 29/04/2014 (Francisco Matos), proc. 225/12.6TJVNF.P1, in http://www.dgsi.pt.

Cour de Cassation, chambre commerciale, financière et économique – arrêt n.º 1183 du 12/11/2008 (07-19.324), in http://www.courdecassation.fr (12/09/2014).

Ac. STJ de 16/09/2014, Proc. 333/09.0TVLSB.L2.S1 (Paulo Sá), in www.dgsi.pt.