Revista Electrónica de Direito

A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na jurisprudência portuguesa

Responsibility for the on-line misuse of electronic payment instruments in Portuguese case law

Raquel Sofia Ribeiro de Lima

Advogada

Outubro de 2016

RESUMO: O problema da fraude nos pagamentos *on-line* continua, em muitas situações, a ser o principal obstáculo no momento de finalizar compras na internet. A utilização fraudulenta de um instrumento de pagamento e a consequente repartição dos prejuízos é a questão que mais litígios cria entre o utilizador do instrumento e o prestador desse serviço, tendo os tribunais, nos últimos anos, sido chamados a resolver muitos desses conflitos. Com o presente trabalho pretendemos abordar o contrato que permite a utilização do instrumento de pagamento eletrónico, a fraude e a repartição dos prejuízos entre as partes, essencialmente, pelo Regime dos Serviços de Pagamento, introduzido no Decreto-Lei n.º 317/2009, de 30 de outubro, analisando parte da jurisprudência publicada sobre a matéria. Por fim, colocaremos em evidência algumas das alterações previstas na nova Diretiva relativa aos serviços de pagamento.

PALAVRAS-CHAVE: Instrumento de pagamento eletrónico; Contrato de utilização; Internet; Homebanking; Fraude; Repartição dos prejuízos.

ABSTRACT: The issue of online payments fraud, in many cases, continues to be the main obstacle when making purchases on the internet. The fraudulent use of payment instruments, and the consequent allocation of losses, is the subject that creates more litigation between the user of the instrument and the provider of the said service, which, in the last years, has led to many of this issues being settled in Court. With this paper we aim to explore the contract that allows the use of electronic payments instruments, as well as the fraud and allocation of losses between the parties, essentially analyzing the solutions provided by the Payment Services, introduced in our national legal system by the Decree-Law nº 317/2009, 30th of October, taking into consideration some of the jurisprudence that has been published about the subject. Finally, we will highlight some of the predicted changes of the New Payment Services Directive.

KEY WORDS: Electronic Payments Instrument; Framework Contract for Payment Services; Internet; Homebankig; Fraud; Allocation of losses.

SUMÁRIO*:

* Este estudo corresponde à versão revista do texto apresentado como Dissertação de Mestrado com vista à obtenção do Grau de Mestre em Ciências Jurídico-Privatísticas na Faculdade de Direito da Universidade do Porto, sob a orientação da Professora Doutora Maria Raquel Guimarães.

Introdução

O progresso tecnológico, principalmente nos meios de comunicação à distância, como destaca o nosso Supremo Tribunal, "veio revolucionar todo o comércio jurídico, nomeadamente a nível das relações bancárias, pois começamos com a emissão de cartões, de crédito e de débito, sendo que estes podem realizar uma infinidade de operações utilizando-se para o efeito os terminais de caixas automáticas, vulgo ATM, e podemos agora, através dos sistemas de *homebanking*, aceder a uma variedade de operações bancárias*, on-line*, utilizando para o efeito um computador pessoal"[1].

A internet permitiu, de facto, alargar o comércio eletrónico[2/3], registando também uma particular evolução dos meios de pagamento[4]. Progressivamente, a distância deixou de constituir um obstáculo à celebração de contratos – a contratação não se prende, hoje, a um *paradigma de espaço*. É fácil aceder a vários mercados, é igualmente simples e rápido pagar o serviço ou bem adquirido[5].

Este desenvolvimento do comércio eletrónico e dos meios de pagamento exigiu a atenção do Direito para a matéria. Depois de várias recomendações que tratavam alguns dos aspetos dos pagamentos eletrónicos, surge em 2007 o primeiro regime comunitário[6]: a Diretiva 2007/64/CE, de 11 de novembro, relativa aos serviços de pagamento no mercado interno, conhecida como *Payment Systems Directive* – PSD. Esta foi transposta para a ordem jurídica

*Este estudo corresponde à versão revista do texto apresentado como Dissertação de Mestrado com vista à obtenção do Grau de Mestre em Ciências Jurídico-Privatísticas na Faculdade de Direito da Universidade do Porto, sob a orientação da Professora Doutora Maria Raquel Guimarães.

[1] Cfr. Acórdão do Supremo Tribunal de Justiça (STJ) de 18.12.2013 (Ana Paula Boularot), disponível *in* <http://www.dgsi.pt> (consultado a 23.01.2015).

[2] Como refere CALVÃO DA SILVA, *Banca, Bolsa e Seguros – Direito Europeu e Português,* 4.ª ed. revista e aumentada, Coimbra, Almedina, setembro de 2013, p. 127, "*a internet, de espaço livre, lúdico e desinteressado de internautas, rapidamente evolui como ferramenta de transacções comerciais e mercado virtual de negócios. A tal ponto que o comércio eletrónico poderá constituir factor (maior) do desenvolvimento da internet*".

[3] O comércio eletrónico pode, de forma simples, ser definido como o processo de compra *on-line* de bens ou serviços através da internet ou outras redes eletrónicas. Para maiores desenvolvimentos, *vide* THEODOSIOS TSIAKIS/ GEORGE STHEPHANIDES, *"The concept of security and trust in electronic payments", in ScienceDirect - Computer Law & Security Report, Volume 24, 2005,* p. 11, <http://www.sciencedirect.com> (12.11.2014) e ainda JORGE MORAIS CARVALHO, "Comércio Electrónico e Protecção dos consumidores" *in THEMIS*, Ano VII, n.º 13, 2006, p. 41.

[4] Para uma análise mais detalhada sobre os meios de pagamentos, *vide* MARIA VICTÓRIA ROCHA, "Novos meios de pagamento no comércio electrónico (*e-commerce*)", *in Direito da Sociedade da Informação*, Vol. V, Coimbra Editora, julho de 2004, *passim*.

[5] JORGE MORAIS CARVALHO, "Prestação de Informação nos contratos celebrados à distância" *in Direito Privado e Direito Comunitário – Alguns ensaios*, Âncora Editora, Lisboa, 2007, p. 18: "*Acrescente-se até a circunstância de as sociedades comerciais, especialmente as de maior dimensão, terem vantagens na comercialização de bens e serviços à distância, pois observa-se, na generalidade dos casos, uma redução dos custos*".

[6] A evolução do comércio eletrónico sempre foi um dos objetivos da UE, tendo na falta de confiança nos meios de pagamento um entrave a esse crescimento. A estratégia da UE passou, como chamou à atenção MARIA VICTÓRIA ROCHA, *op. cit.*, p. 203, pelo enquadramento da matéria numa "'*moldura legal adequada', que permita aos intervenientes saber com o que contar, designadamente em termos de lei aplicável e de regime de responsabilidade*".

interna pelo Decreto-Lei n.º 317/2009 de 30 de outubro, publicando no anexo I o "Regime Jurídico que regula o acesso à actividade das instituições de pagamento e a prestação de serviços de pagamento". O anexo foi alterado pelo Decreto-Lei n.º 242/2012, de 7 de novembro[7], que o republica sob a designação de "Regime Jurídico dos Serviços de Pagamento e Moeda Eletrónica" – abreviadamente conhecido como Regime dos Serviços de Pagamento (RSP). A matéria dos meios de pagamento continuou a ser alvo da atenção das instâncias europeias, estando já aprovada a nova Diretiva sobre a matéria – Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015.

Numa altura em que mais de um milhão de portugueses já fará compras na internet com regularidade[8], estudos recentes demonstram o substancial crescimento do comércio eletrónico. Entre 2004 e 2013, o número de encomendas na internet registou uma taxa média de crescimento anual de 19,6%[9]. Em 2014, o montante gasto com cartões de crédito, que continua a ser o meio preferencial para pagamento de compras *on-line*[10], aumentou 11% em Portugal, acima da média europeia de 9,4%, apoiado no crescimento de 47% do volume de transações *on-line* – ultrapassando os 162 milhões de euros[11/12].

A continuação do crescimento destes números dependerá, naturalmente, da confiança colocada no sistema – note-se que a "*grande maioria dos consumidores* on-line *desiste no momento da compra*"[13]. A indispensável confiança e fiabilidade do sistema de pagamentos relaciona-se diretamente com o problema da fraude e da reparação dos prejuízos causados pela atuação de terceiros no seio da relação prestador do serviço de pagamento/cliente, exigindo um cuidado tratamento jurídico da questão.

É, precisamente, a enorme atualidade e importância da matéria dos pagamentos eletrónicos que justifica este estudo, principalmente, no que respeita aos litígios que possam ocorrer entre o cliente e o prestador do serviço de pagamento.

---

[7] Transpôs a Diretiva n.º 2009/110/CE, do Parlamento Europeu e do Conselho, de 16 de setembro, *relativa ao acesso à atividade das instituições de moeda electrónica, ao seu exercício e à sua supervisão prudencial*.

[8] ALEXANDRE NILO FONSECA, "*Comércio eletrónico é uma ferramenta essencial para superar a crise*" (artigo de opinião - 22.09.2009), *in* ACEPI – Associação da Economia Digital, disponível em <http://www.acepi.pt/> (19.02.2015).

[9] 25% dos participantes do Inquérito à utilização de Tecnologias de Informação e Comunicação pelas Famílias afirmaram ter efetuado encomendas pela internet – cfr. "A sociedade da informação em Portugal 2013", *in* <http://www.dgeec.mec.pt/> (20.04.2015). Registou-se um crescimento de 45% dos compradores *on-line* entre 2009 e 2012, prevendo-se um crescimento superior a 42% até 2017 – Estudo IDC/ACEPI "Economia digital em Portugal, 2009-2017", disponível *in* <http://www.acepi.pt/> (10.11.2014).

[10] Segundo um estudo recente realizado pela SIBS e Datamonitor, "*On-line Consumer Payments Analytics*", disponível *in* <http://www.sibs.pt> (22.07.2015), cerca de 53% das compras *on-line* são pagas com cartões de crédito. Contudo, como refere a SIBS, gestora da rede de Multibancos em Portugal, "*apesar de o cartão se revelar como uma ferramenta primordial e indispensável do sistema de pagamentos, as novas tecnologias têm vindo a assumir uma preponderância crescente, o que, já no curto prazo, tenderá a alterar o paradigma de utilização de meios de pagamento. O aumento dos volumes de transacções provenientes de dispositivo* mobile, *de lojas* online *resultam de uma progressiva integração dos ambientes físico e* online, *reflexo da disseminação de dispositivos que permitem um acesso omnipresente à internet"* – cfr. SIBS FPS: Relatório e Contas 2014, disponível *in* <http://www.sibs.pt> (30.06.2015).

[11] Segundo dados da ACEPI, publicados em 16.02.2015, disponível *in* <http://www.acepi.pt/> (19.02.2015). Este crescimento aparece diretamente relacionado com a evolução do comércio eletrónico.

[12] Em 2014, foram realizadas 12,9 milhões de compras *on-line,* representando um aumento de 14,2% em relação ao ano anterior – Estudo "*On-line Consumer Payments Analytics*", *cit.*, disponível *in* <http://www.sibs.pt> (22.0.2015).

[13] ACEPI – notícia de 19.01.2015, disponível *in* <http://www.acepi.pt/> (19.02.2015).

O RSP dedica-se a um tempo ao acesso à atividade e depois à própria prestação do serviço de pagamento[14]. Centrar-nos-emos na prestação do serviço, apontando apenas que as entidades prestadoras do serviço de pagamento podem ser, por exemplo, instituições de crédito, de pagamento, de moeda electrónica e entidades concessionárias do serviço postal universal[15].

A operação de pagamento é prevista no RSP como um serviço de pagamento – definido no art. 2.º, al. c) e no art. 4.º como o serviço que permite o depósito e o levantamento de numerário, a execução de operações de pagamento, incluindo a transferência de fundos, a execução de operações de pagamento no âmbito das quais os fundos são cobertos por uma linha de crédito, a emissão ou aquisição de instrumentos de pagamento e o envio de fundos[16]. Já o instrumento de pagamento (doravante IP) é definido na al. z) do art. 2.º, nos seguintes termos: "*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*", incluindo os cartões de crédito ou débito[17], os códigos de acesso e códigos pedidos no momento de finalizar as operações de pagamento no *homebanking*[18].

No uso de um deste IP poderemos fazer pagamentos *on-line* – dar ordens de pagamento. A rapidez inerente ao comércio eletrónico não permite, contudo, a negociação de cada uma dessas ordens de pagamento. Estes pagamentos têm de ser simples, céleres, quase automáticos, estando as regras que cada um – utilizador do IP e prestador do serviço – deve observar prévia e contratualmente estabelecidas. Neste sentido, começaremos este estudo pela identificação do negócio jurídico através do qual é possível utilizar um IP eletrónico. Na verdade, o uso do IP insere-se numa estrutura contratual complexa, "numa relação triangular em cujos os vértices se encontram o emissor do cartão, o titular deste e o comerciante ou fornecedor de bens ou serviços"[19]. Todavia, a análise deste ponto incidirá

---

[14] MENEZES CORDEIRO, *Manual de Direito Bancário*, 5.ª edição, Coimbra, Almedina, 2014, p. 576, distingue entre "*área institucional, que comporta as regras aplicáveis aos prestadores de serviços de pagamento e emitentes de moeda electrónica*" e "*área material, referente à prestação e à utilização de serviços de pagamento*".

[15] Cfr. art. 7.º do RSP. As instituições de pagamento terão de preencher os requisitos previstos nos art. 10.º a 20.º do RSP e ser autorizadas pelo Banco de Portugal (cfr. art. 10.º do RJSPME).

[16] O art. 4.º do RSP identifica os serviços de pagamento incluídos neste regime, enquanto o art. 5.º faz esta delimitação pela negativa.

[17] Segundo dados do Banco de Portugal, no final de 2015, existiam cerca de 18.343.000 cartões emitidos em Portugal (dados disponíveis em <http://www.bportugal.pt/EstatisticasWeb/>).

[18] Também apelidada de "banca ao domicílio" ou "banca eletrónica", é um instrumento cada vez mais utilizado. Nas certeiras palavras do STJ, no Acórdão de 17.05.2007 (Oliveira Rocha), disponível *in* <http://www.dgsi.pt> (25.10.2014): "*Com a dita revolução, os bancos, no seu interesse, não esquecendo que o cliente também viu facilitada a movimentação e controlo da sua conta, criaram sistemas informáticos capazes de prestar, com economia, rapidez e comodidade, os serviços de conta que, anteriormente, prestavam com um exército de funcionários*". O acesso ao sistema só é possível através da introdução de um conjunto de códigos de carácter secreto: número de conta ou de contrato e uma password, sendo exigido a indicação de outros códigos, presentes no cartão de coordenadas ou enviado por SMS, para a concretização de operações de pagamento.

[19] Cfr. Ac. do Tribunal da Relação de Évora (TRE) de 05.07.2007 (Fernando Bento), disponível *in* <http://www.dgsi.pt> (11.02.2015). Neste sentido, MARIA RAQUEL GUIMARÃES, *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos,* Coimbra, Wolters Kluwer/Coimbra Editora, 2011, pp. 174 e 175, refere que o uso do IP "*corresponde, no plano jurídico, a uma 'teia' de contratos, a uma série de relações jurídicas complexas".* A autora continua, ainda que referindo-se apenas a cartões, "*os procedimentos necessários para desencadear uma transferência electrónica de fundos que satisfaça o credor do titular de um cartão de pagamento, na sua aparente singeleza, são na realidade sustentados por três feixes de relações jurídicas interligadas entre si, que se estabelecem entre o titular do cartão e o beneficiário da ordem de*

apenas na relação entre o titular do IP e o prestador do serviço no âmbito do contrato-quadro[20], seguindo-se o estudo dos principais direitos e deveres impostos às partes na sua execução.

Muitos dos deveres impostos às partes no contrato visam aumentar a segurança do sistema. Ainda assim, a utilização de um IP eletrónico continua a apresentar fragilidades, essencialmente pela possibilidade de se verificarem operações de pagamento não autorizadas pelo titular do IP, não só em consequência de perda ou roubo do cartão, mas também pela indicação dos dados do IP que continue na posse do seu titular, ou ainda pela quebra da confidencialidade dos dispositivos que lhe estão associados. Assim, analisaremos as principais e mais comuns técnicas de utilização fraudulenta dos IP[21]: *phishing*[22] e *pharming.*

Vistas as origens das operações fraudulentas, a questão que imediatamente se coloca, e que mais nos ocupará, é a repartição dos prejuízos – quem, na relação prestador do serviço/cliente[23], assumirá as perdas decorrentes da utilização abusiva ou fraudulenta do IP? É esta a questão que mais se tem colocado aos tribunais, que mais litígios cria entre as partes e que mais preocupa os utilizadores dos IP.

Acreditamos que a utilização abusiva do IP encontra, atualmente, um adequado tratamento no RSP. Este regime representou um importante progresso no que respeita aos sistemas de pagamento, perante o escasso enquadramento normativo da matéria dos pagamentos. Além do estudo do regime legal, optamos pela análise da jurisprudência nacional para uma maior compreensão dos critérios fixados na legislação atual e das soluções dadas antes da entrada em vigor do RSP. Este, não se podendo aplicar a factos anteriores, não prejudica o enquadramento desses factos à luz das suas disposições. Na verdade, o regime resulta da transposição de uma Diretiva de 2007, que, em grande parte, consagra posições já assumidas – desde dos anos 80 – nas Recomendações Europeias[24], e que deveriam ser tidas

---

pagamento, entre o mesmo titular e o banco emissor do cartão e entre este último e o beneficiário do pagamento. Isto para não mencionar uma quarta relação, que se estabelece entre o banco emissor do cartão e o banco beneficiário do pagamento - uma vez que estes, as mais das vezes, não coincidirão -, na medida em que este último não assume um papel autónomo na operação de pagamento electrónico, actuando como um auxiliar o primeiro banco". Também JANUÁRIO GOMES, *Contratos Comerciais*, Coimbra, Almedina, 2012, pp. 212 e ss, identifica a relação de valuta, a relação de cobertura e a relação entre o banco e o comerciante.

[20] O RSP regula autonomamente as operações de pagamento no âmbito do contrato-quadro, distinguindo-as das operações de pagamento de carácter isolado.

[21] O termo fraude no seio dos pagamentos foi empregue na recomendação n.º 97/489/CE, enquanto os Avisos do Banco de Portugal evitavam ainda a expressão. "*A expressão pressupõe o uso intencional por parte de outrem dos elementos visíveis do cartão de crédito sem o consentimento ou sem o conhecimento do respectivo titular. Portanto, é dada uma ordem de pagamento através do cartão de crédito à revelia do autor*" – cfr. GRAVATO MORAIS, "A utilização fraudulenta de cartões de crédito na contratação à distância", *in Estudos em comemoração do décimo aniversário da Licenciatura em Direito da Universidade do Minho*, Almedina, Coimbra, 2004, p. 37.

[22] O *phishing* é uma técnica mais comum, baseada no uso de *spam*, para a qual, cada vez mais, os utilizadores estão atentos, tendo o número destes ataques vindo a decrescer. De acordo com o relatório de fevereiro da Symantec, disponível *in* <http://www.symantec.com/security_response/publications/> (05.04.2015), 1 em 1466 *e-mails* é um ataque de *phishing*, enquanto em janeiro deste mesmo ano a relação era de 1 em cada 1004 *e-mails*.

[23] Excluímos do presente estudo o tratamento jurídico-penal do comportamento fraudulento do terceiro.

[24] Referimo-nos à recomendação 87/598/CEE, de 8 de dezembro, à recomendação 88/590/CEE de 17 de novembro, e à recomendação 97/489/CE, de 30 de julho. Estas, ainda que não vinculativas, deveriam ser tidas

em conta na elaboração das condições gerais de utilização, nos termos do art. 3.º do D.L. n.º 166/95, de 25 de julho[25]. Acresce que, de acordo com o art. 101.º do RSP, a sua disciplina será aplicável aos contratos em vigor, na medida em que seja mais favorável aos utilizadores.

Pela dificuldade de acesso às sentenças de primeira instância, delimitamos o estudo às decisões dos tribunais superiores, sendo possível consultar grande parte da jurisprudência referida nas bases de dados jurídico-documentais do Instituto de Gestão Financeira e Equipamentos da Justiça do Ministério da Justiça, acessível em <www.dgsi.pt>. Pela importância do tema, que será desnecessário sublinhar, o estudo de decisões jurisprudenciais justifica-se, quanto a nós, pela grande variedade de casos com que os tribunais se têm deparado.

1. O contrato de utilização de instrumento de pagamento

O uso de um instrumento de pagamento eletrónico faz-se pela celebração de um contrato específico entre o cliente e o prestador de serviço, geralmente apelidado de contrato de utilização[26].

"Este contrato é uma das manifestações da revolução tecnológica no que toca às transferências electrónicas de fundos e que suscita 'complexos problemas de direito probatório - v.g., de repartição do ónus da prova -, bem como [...] em matéria de distribuição do risco'"[27].

em conta pelos nossos tribunais na resolução dos litígios que lhes eram colocados – *vide* CALVÃO DA SILVA, *Banca, Bolsa e Seguros – Direito Europeu e Português, op. cit.,* pp. 163-167.

[25] Sobre o alcance desta remissão, veja-se MARIA RAQUEL GUIMARÃES, "Comércio electrónico e transferências electrónicas de fundos" *in O comércio Eletrónico – Estudos jurídicos*, Coimbra, Livraria Almedina, 2002, pp. 74 e 75.

[26] Trata-se ainda de um contrato inominado, mas tem assim sido designado por MARIA RAQUEL GUIMARÃES nas suas obras sobre o tema, sendo, também, por nós adotada por colocar a tónica na determinação do modo de funcionamento do IP. A designação tem, igualmente, sido utilizada pela jurisprudência, sendo adotada pelo Supremo Tribunal de Justiça nos Acórdãos de 23.11.1999 (Garcia Marques), *in CJ-STJ*, III, 1999, p. 103; de 23.11.2000 (Sousa Inês), *in CJ-STJ*, III, 2000, p. 136; de 11.10.2001 (Silva Paixão), *in CJ-STJ*, III, 2001, p. 80; de 14.02.2002 (Ferreira de Almeida) *in CJ-STJ*, I, 2002, p. 101; de 19.11.2002 (Azevedo Ramos); de 17.05.2007 (Oliveira Rocha); de 15.05.2008 (Mota Miranda); de 21.10.2008 (Alves Velho), e de 20.03.2010 (Urbano Dias) acessíveis a partir do sítio <http://www.dgsi.pt> (consultados a 25.10.2014), embora referindo-se especificamente ao contrato de utilização de cartão; Também INÊS ISABEL DE CAMPOS MOURA, *O contrato de prestação de serviços bancários através da Internet*, JusJornal, n.º 1716, 25 de Junho de 2013, disponível *in* <http://jusjornal.wolterskluwer.pt/> (22.01.2015), tratando o contrato de utilização de *homebanking* que a autora denomina de 'contrato de prestação de serviços bancários através da internet', apesar de referir-se a este como contrato de utilização, salienta o facto de estarmos perante um negócio jurídico inominado, mas socialmente típico.

[27] Acórdão do Tribunal da Relação de Lisboa (Maria Amélia Ribeiro) de 26.10.2010 (25.10.2014), que cita o Ac. do STJ de 20.04.1999 (Garcia Marques), ambos acessíveis em <http://www.dgsi.pt>.

1.1. Contrato de adesão

Num primeiro passo na tentativa de resolução dos litígios que surgem no âmbito do uso de um IP eletrónico, a nossa jurisprudência tem analisado a relação contratual que se estabelece entre a entidade prestadora do serviço de pagamento e o utilizador[28], tendo o Supremo Tribunal de Justiça, por diversas vezes, se pronunciado no sentido da autonomia do contrato[29] que permite ao utilizador do IP movimentar fundos de forma simples e mecânica.

Os nossos tribunais começaram por identificá-lo apenas como contrato de adesão[30], sendo, maioritariamente, chamados a pronunciar-se sobre a validade das cláusulas contratuais gerais que o compõem (algo que já acontecia, embora mais raramente, no tratamento dos litígios decorrentes do uso do eurocheque[31]), assumindo uma clara intenção "de proteger o contraente aderente, necessariamente mais débil, das disfunções provocadas pela desigualdade contratual das partes"[32].

O comércio eletrónico, particularmente a atividade de pagamento, constitui uma área especialmente fértil para os contratos de adesão[33] ou, no uso da designação adotada pelo legislador português, contratos com recurso a cláusulas contratuais gerais. Estes contratos afastam-se daquilo que poderíamos chamar de *paradigma do processo de contratação*[34], pois assentam num conjunto de cláusulas prévia e unilateralmente definidas pela entidade bancária para serem utilizados nas relações com os seus clientes[35], sem possibilidade de

---

[28] A importância desta análise é referida pelo Tribunal da Relação do Porto, no Ac. de 12.04.2010 (Ana Paula Amorim) disponível em <http://www.dgsi.pt> (25.10.2014): "*Para apreciar da questão em discussão nestes autos – utilização abusiva do cartão por terceiros – e dos fundamentos do recurso, mostra-se de particular relevo analisar a natureza da relação contratual entre a instituição emitente do cartão e o seu titular".*

[29] É reconhecido como "*verdadeiro contrato autónomo*" no Acórdão do STJ de 15.10.2009 (Alberto Sobrinho) e no Ac. do Tribunal da Relação do Porto (TRP) de 28.09.2004 (Alberto Sobrinho), disponível em <http://www.dgsi.pt> (25.10.2014). Apesar de, por vezes, a jurisprudência ter tratado este contrato apenas como "*um contrato acessório instrumental, em relação ao contrato de depósito bancário ou ao de abertura de crédito em conta corrente, acessoriedade revelada não apenas pela função do próprio contrato, mas também pelo seu destino, dependente das vicissitudes daqueles tipos contratuais*" – cfr. Ac. STJ de 17.05.2007, já citado.

[30] A literatura especializada de outros países tem, também, chamado a atenção para a caracterização destes contratos como contratos de adesão. Em Espanha, MARIA DEL CARMEN GETE-ALONSO Y CALERA, *Las tarjetas de crédito*, Relaciones contractuales y conflictividade, Marcial Pons, Ediciones jurídicas y sociales, Madrid, 1997, p. 158: "*se trata de contratos, en particular com referencia al que se celebra entre la entidade emissora y el titular de la tarjeta (…), de adhesion, cuya regulacion contractual viene normalmente predeterminada o perfijada por las condiciones generales, previamente redactadas por la empresa que, ademas, las impone a la outra parte".*

[31] Neste caso, refira-se o Acórdão do Tribunal da Relação de Coimbra (TRC) de 16.03.2004 (Távora Victor), acessível em <http://www.dgsi.pt> (25.10.2014).

[32] Acórdão do TRC de 16.03.2004, *cit.*, disponível no sítio <http://www.dgsi.pt>.

[33] Neste sentido, QUIRINO SOARES, "Contratos Bancários", *in Scientia Iuridica*, separata janeiro - abril 2003, Tomo LII, n.º 295, Universidade do Minho, p. 110, refere que "*as instituições financeiras e de seguros, estão, precisamente, na primeira linha das empresas que recorrem por sistema a cláusulas contratais gerais*". Para maiores desenvolvimentos sobre a massificação e estandardização dos contratos na área da banca, *vide* CALVÃO DA SILVA, *Banca, Bolsa e Seguros – Direito Europeu e Português*, *op. cit.*, pp. 175 a 215.

[34] O paradigma do processo de contratação será, nas palavras do STJ, no Ac. de 17.05.2007 (Oliveira Rocha), o "*que está consagrado no nosso Código Civil; ou seja, as partes contratantes, em posição de igualdade e por aproximações sucessivas, vão definindo o que consideram ser seu interesse, até alcançarem o patamar final, livremente negociado, num processo do qual nunca está ausente o poder recíproco de aceitação ou de rejeição. Os contratos são concluídos, em regra, após negociações prévias, com propostas e contrapropostas, de tal sorte que uma das partes fique a saber dos seus direitos e obrigações quando os mesmos se formalizarem*" - disponível *in* <http://www.dgsi.pt> (25.10.2014).

[35] MENEZES CORDEIRO, *Manual de Direito Bancário*, 5.ª edição, *op. cit.*, p. 487, chama atenção para os elementos esclarecedores desta noção: generalidade e rigidez, apresentando as restantes características como "*não necessárias"*. Já para LUÍS CARVALHO FERNANDES, *Teoria Geral do Direito Civil*, Vol. II, 3.ª edição, Universidade

discussão do seu conteúdo, ou, como expressa o Acórdão de 28.09.2004 do Tribunal da Relação do Porto (Alberto Sobrinho), "impostas por um dos contraentes aos clientes que com ele contratam"[36], reduzindo a liberdade contratual destes à escolha de aceitar/aderir.

Neste campo, foi dado um importante passo pelo legislador comunitário e nacional, demonstrando nas normas do D.L. n.º 317/2009, de 30 de outubro, um perfeito conhecimento das cláusulas contratuais gerais normalmente utilizadas pelas instituições prestadoras de serviços de pagamentos, estabelecendo várias das regras que os tribunais faziam prevalecer por interpretação do D.L. n.º 446/85, de 25 de outubro.

Uma das questões que mais terá chegado aos nossos tribunais superiores prende-se com ações inibitórias intentadas com base no art. 21.º alínea f) e g) do D.L. n.º 446/85, relativas aos critérios de distribuição do risco[37/38] e repartição do ónus da prova[39]. A posição maioritária na jurisprudência, na esteira do entendimento espelhado no Acórdão do STJ de 23.11.1999, é de que são "nulas as cláusulas contratuais gerais insertas em contrato-tipo de adesão que violem normas imperativas de ordem pública, designadamente, as que invertam ou alterem a distribuição do risco e as regras de repartição do ónus da prova, ou que tenham como efeito a exclusão da responsabilidade de um dos contraentes se se verificarem determinados requisitos".

Estas questões encontram, hoje, regulação específica no art. 70.º e seguintes do referido D.L. n.º 317/2009 de 30 de outubro.

Desta forma, com a consagração deste regime, o Tribunal da Relação de Lisboa entendeu que "a questão [quer da distribuição do risco como quanto à repartição do ónus da prova] perdeu interesse face ao estatuído no art. 101º, do Dec. Lei n.º 317/2009. Nesse artigo estabelece-se o dever dos prestadores de serviços de pagamento adaptarem os contratos vigentes às disposições constantes do novo regime, e prescreve-se (n.º 1), 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'.* Sendo as disposições do citado diploma legal em matéria de culpa e

---

Católica Editora, Lisboa, 2001, p. 267 e 268, são "*características naturais a desigualdade entre as partes, a complexidade e a natureza formulária*".

[36] Disponível *in* <http://www.dgsi.pt> (25.10.2014);

[37] Veja-se, quanto a esta alínea, o Acórdão do STJ de 19.11.2002 (Azevedo Ramos), *cit.*, de 15.10.2009 (Alberto Sobrinho) e o Ac. do Tribunal da Relação de Lisboa (TRL) de 18.01.2011(António Santos), *in* <http://www.dgsi.pt> (25.10.2014). Estranha-se, quanto a este último, a não avaliação da cláusula contratual, não só pelo diploma das cláusulas contratuais gerais, mas pela legislação específica já em vigor, que se aplica aos contratos anteriores, desde que seja mais favorável ao titular do IP.

[38] ANA PRATA, *Contrato de adesão e Cláusulas contratuais Gerais,* Coimbra, Almedina, 2010, p. 496, refere, na análise destas cláusulas, que "*a atribuição pela empresa dos riscos à contraparte mais não é do que uma forma de alienar custos que lhe caberiam no regime geral*".

[39] No Supremo Tribunal de Justiça refira-se os Acórdãos de 23.11.1999 (Garcia Marques), *in CJ-STJ*, III, 1999; de 23.10.2000 (Sousa Inês) *in CJ-STJ*, III, 2000, de 11.10.2001 (Silva Paixão), *in CJ-STJ*, III, 2001, de 16.03.2004 (Moreira Alves) *in CJ-STJ,* I, 2004, pp. 127 – 132, de 02.03.2010 (Urbano Dias) (25.10.2014); de 15.10.2009 (Alberto Sobrinho) (25.10.2014); Acórdão do Tribunal da Relação do Porto de 28.09.2004 (Alberto Sobrinho) (25.10.2014); Ac. do TRL (Catarina Arêlo Manso) de 20.10.2011 e de 24.05.2012 (Ezagüy Martins) (ambos consultados a 10.01.2015), disponíveis *in* <http://www.dgsi.pt>.

distribuição do risco mais favoráveis aos autores, enquanto utilizadores de serviços de pagamento, são as mesmas aplicáveis ao caso"[40].

Diferentemente do entendimento do Tribunal da Relação de Lisboa, expresso mais recentemente no Acórdão de 03.03.2015[41], acreditamos que a existência de lei específica não dispensa a análise das cláusulas contratuais gerais que compõe o contrato de utilização. A validade das cláusulas relativas à prova e ao risco, pelas maiores divergências que tendem a criar entre as partes, têm ainda de ser analisadas pelos tribunais, tendo em consideração quer o RSP como pelo diploma das cláusulas contratuais gerais[42]. Ainda assim, será mais caracterizador do seu regime a sua recondução a um outro esquema contratual: o contrato-quadro.

1.2. Contrato-quadro

A realização de uma operação de pagamento eletrónica, quer seja feita com o uso dos dados de um cartão ou através de *homebanking,* é antecedida de um complexo contratual que regula, prevê e simplifica as operações de pagamento a realizar no futuro com esse IP, podendo ser reconduzida ao esquema contratual do contrato-quadro[43/44].

O Regime jurídico que regula o acesso à atividade das instituições de pagamento e a prestação de serviços de pagamento, publicado no Anexo I ao D.L. n.º 317/2009, de 30 de outubro, com as alterações introduzidas pelo D.L. n.º 242/2012, de 7 de novembro, vem, pela primeira vez[45], clarificar a estrutura dos contratos para utilização de IP como um

[40] Acórdão de 05.11.2013 (Manuel Marques), disponível no sítio <http://www.dgsi.pt> (13.01.2015); Contrariamente, alguns tribunais continuaram a analisar as cláusulas inseridas neste contrato, mesmo depois de 2009, apenas pelo D.L. n.º 446/85, como o Ac. 20.10.2011, *cit*., com base na, suposta, *"ausência de legislação específica sobre a forma de utilização de cartões",* o que demonstra o desconhecimento desta lei por parte da jurisprudência, mesmo passados dois anos da sua entrada em vigor.

[41] Relator: Manuel Marques, disponível no sítio <http://www.dgsi.pt> (29.05.2015);

[42] Este era um regime importantíssimo na resolução dos litígios, pois, como afirma MENEZES CORDEIRO, *Manual de Direito Bancário*, 3.ª edição, Coimbra, Almedina, janeiro de 2006, p. 448, "*No sector bancário as cláusulas contratuais destinam-se a enfrentar a falta ou insuficiência das regras legais aplicáveis aos diversos contratos*". Contudo, mesmo na vigência do RSP, o regime mantém a sua utilidade pois, quando à prova, o RSP, como veremos, deixa espaço para a existência de presunções que deverão ser avaliadas pelo Tribunal. Desta forma, acompanhamos o TRE no Ac. de 22.05.2014 (Mata Ribeiro), onde é reconhecida, oficiosamente, a nulidade da cláusula que altera as regras da prova "*passando* [o utilizador] *a assumir o risco do negócio e a consequente responsabilidade por todos os prejuízos resultantes de uma utilização abusiva do serviço por terceiros*", disponível no sítio <http://www.dgsi.pt> (09.05.2015).

[43] A recondução deste complexo contratual ao esquema contratual do contrato-quadro é defendida por MARIA RAQUEL GUIMARÃES *in* "Texto que serviu de base à apresentação oral da tese de doutoramento com o título *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos*, em provas públicas realizadas na FDUP no dia 21 de junho de 2010", *in Revista da Faculdade de Direito da Universidade do Porto*, ano VIII, Coimbra, Coimbra Editora, 2011, *passim*.

[44] GALVÃO TELLES, *Manual dos Contratos em Geral*, 4.ª edição, Coimbra, Coimbra Editora, 2002, p. 242, privilegia a designação deste esquema contratual como *contrato-tipo.*

[45] O desdobramento da operação de pagamento eletrónico em diferentes momentos contratuais não foi tido em consideração pelo legislador nacional aquando da regulação do crédito ao consumo, no D.L. n.º 359/91, de 21 de setembro, nem mais tarde, no D.L. n.º 133/2009, de 2 de junho, que substitui o diploma anterior e estabelece um novo regime sobre a matéria. O mesmo aconteceu no D.L. n.º 143/2001, de 26 de abril, quanto à proteção dos consumidores. Também a doutrina, no geral, parecia não tomar consciência do complexo contratual que sustentava a operação, por exemplo, JOSÉ SIMÕES PATRÍCIO, *Direito Bancário Privado*, Quid Juris, Lisboa, 2004, p. 234, refere, citando MENEZES CORDEIRO, *"o contrato de emissão apresenta-se basicamente como*

contrato-quadro. No art. 2.º, alínea o), define o contrato-quadro de prestação de serviços de pagamento[46] como "*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*". Neste sentido, vem, no título relativo à "*prestação e utilização de serviços de pagamento*", distinguir "*operações de pagamento de carácter isolado*", "*contrato-quadro e (…) operações de pagamento por estes abrangidas*"[47].

A utilização do IP não surge como um ato pontual ou isolado, mas integrará um conjunto de operações sucessivas com contornos idênticos, embora com montantes e beneficiários distintos. Para que qualquer um de nós execute as operações de pagamento no dia-a-dia, de forma imediata, fácil e acessível através de qualquer ATM, telemóvel ou computador com acesso à internet, é necessário a celebração prévia de um contrato onde se estabelece as regras que irão reger as partes nas inúmeras operações de pagamento que se seguirão.

Em suma, o uso do IP eletrónico far-se-á pela celebração deste contrato-quadro específico, que será o contrato base destinado a preparar, facilitar e, podemos mesmo dizê-lo, potenciar a conclusão dos sucessivos contratos de execução. O programa contratual fica estabelecido neste contrato-quadro[48] e as posteriores ordens de pagamento são mecânicas, quase automáticas, ultrapassando a necessidade de negociação perante cada ordem de pagamento e correspondendo à celeridade e simplicidade de um mundo cada vez mais eletrónico e globalizado.

No momento da celebração deste primeiro contrato, os contraentes desconhecem quando utilizarão o IP, perante quem ou quais os montantes desses pagamentos (não permitindo reconduzir o contrato de utilização de IP à figura do contrato de execução continuada[49/50], não obstante ser ele próprio um contrato de execução continuada, pelo objetivo, que lhe é

---

mandado: 'mandado sem representação, de conteúdo especial´ (Menezes Cordeiro)". No mesmo sentido, JOANA DE VASCONCELOS, "Cartões de Crédito", *in RDES*, Ano XXXV, (VIII, 2ª série – Nº 1, 2, 3, 4), Editorial Verbo, p. 142.
Aqui a Diretiva 2007/64/CE é realmente inovadora, introduzindo (impondo, porque não dizê-lo) o contrato de utilização de IP como contrato-quadro. No entanto, como refere MARIA RAQUEL GUIMARÃES, *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos, op. cit.*, pp. 555 e 556, a designação de "contrato-quadro" não é suficiente para evidenciar a perceção sobre esta estrutura contratual complexa que sustenta as operações de pagamento, mas será um avanço para esse entendimento.

[46] Não será, contudo, o *nomen iuris* do contrato disciplinado, será apenas a designação utilizada para distinguir esta estrutura contratual das operações de carácter isolado. A importância económica do contrato-quadro e das operações de pagamento abrangidas é afirmada no preâmbulo daquele D.L., dizendo que "*são mais comuns e significativos de um ponto de vista económico do que as operações de pagamento de carácter isolado*".

[47] JANUÁRIO GOMES, *op. cit.,* pp. 231 e 232, recorda que em ambas as operações estamos na presença de contratos, num caso tratar-se-á do contrato de serviço de pagamento singular e no outro do contrato-quadro já referido.

[48] No contrato-quadro de utilização de um IP há um contrato-quadro interno e um externo. O primeiro respeita aos contratos sucessivos entre as partes – os contratos de execução (mandatos). Já o segundo é relativo aos contratos celebrados com terceiros, por norma comerciantes (contratos de compra e venda ou de prestação de serviços).

[49] Para maiores desenvolvimentos sobre a regulação das relações contratuais duradouras com recurso a contrato-quadro ou a contratos de execução continuada, *vide* MARIA RAQUEL GUIMARÃES, *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos, op. cit.,* pp. 153 a 163.

[50] Discordamos, assim, parcialmente da Relação de Guimarães que, no seu Acórdão de 25.11.2013 (Espinheira Baltar), caracteriza o contrato "*pelo qual os clientes do banco aderentes têm a possibilidade de aceder às suas contas bancárias e a outros serviços por ele disponibilizados*" como contrato de execução continuada, in <http://www.dgsi.pt>, consultado a 10.12.2014.

inerente, de se prolongar/perpetuar no tempo). É necessário, desta forma, existir uma renovação da vontade por parte do utilizador[51] e do prestador de serviços[52] em cada concreta operação de pagamento[53], *"é neste segundo momento que o banco toma conhecimento do 'quando, quanto e para quem'"*[54], celebrando-se um novo contrato – os sucessivos contratos de aplicação ou execução – com o conteúdo já definido naquele primeiro contrato-quadro. Cada utilização do IP é uma nova ordem de pagamento, um mandato de pagamento[55] ao banco.

O legislador entendeu existirem, de facto, diferentes momentos contratuais nas operações de pagamento, distinguindo as informações a serem fornecidas ao utilizador do IP mesmo antes da realização do contrato-quadro (arts. 52.º a 56.º) daquelas relativas às operações de execução do contrato base (arts. 57.º a 59.º). Podemos mesmo dizer que esta clarificação do complexo contratual *"permitiu ao legislador esclarecer de uma forma precisa quais as obrigações que impendem sobre as partes do contrato"*[56].

O contrato de utilização encontra no RSP um modelo normativo suficientemente completo, que permite considerá-lo legalmente típico[57], sendo, assim, um tipo de contrato de prestação de serviços de pagamento.

---

[51] A este propósito diz MARIA RAQUEL GUIMARÃES, "(Ainda) a responsabilidade pelo uso indevido de instrumento de pagamento electrónicos em operações presenciais e à distância- Análise do regime introduzido pelo Anexo I do Decreto-lei nº 317/2009, de 30 de outubro (RSP), e das alterações que se perspectivam face à proposta de directiva do Parlamento Europeu e do Conselho, de 24 de julho de 2013" *in I Congresso de Direito Bancário*, Almedina, 2015, p. 123, que *"a autorização genérica que possa ser prestada no contrato base de utilização do instrumento de pagamento (no contrato-quadro), não é suficiente para desencadear a operação. A lei exige uma renovação da vontade do utilizador do serviço, embora se baste, com a adopção dos comportamentos fixados no contrato para o efeito: marcação de um código secreto num terminal de um computador instalado no estabelecimento do beneficiário, assinatura manual, inserção de uma ou mais chaves de acesso no site do banco, através do teclado do computador do utilizador, no caso do homebanking, etc".*

[52] Quanto à renovação de vontade por parte do prestador de serviços de pagamento, a mesma autora, *ibidem,* refere: *"o prestador de serviço de pagamento é chamado a conferir a conformidade da ordem de pagamento recebida e a manifestar a sua concordância com a mesma";* Não existe por parte da entidade prestadora do serviço uma obrigação de concluir os futuros contratos de execução, podendo perante certas circunstâncias, recusar a ordem de pagamento. JEAN GATSI, *Le Contrat-Cadre*, L.G.D.J., Paris, 1998, p. 18, fala a este propósito de contrato-quadro sem obrigação de contratar.

[53] Para maiores desenvolvimentos, veja-se MARIA RAQUEL GUIMARÃES, *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos, cit*., pp. 422 a 447, 556 a 557, e da mesma autora "The debit and credit card framework contract and its influence on European legislative initiatives", *in InDret Comparado, Revista para el Análisis del Derecho*, n.º 2, 2012, pp. 12 e 13 (<http://www.indret.com/es>).

[54] MARIA RAQUEL GUIMARÃES, Texto que serviu de base à apresentação oral da tese de doutoramento com o título *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos*, em provas públicas realizadas na FDUP no dia 21 de junho de 2010, *cit.*, p. 465.

[55] O banco cumpre uma prestação pecuniária em nome próprio, mas por conta do seu cliente. Estes mandatos ligam apenas o banco e o seu cliente numa estrutura delegatória mais complexa, que se estabelece entre todos intervenientes negociais; Para uma panorâmica sobre o contrato de mandato, *vide* MENEZES LEITÃO, *Direito das Obrigações,* Vol. III, 9.ª edição, Coimbra, 2014, pp. 389 e ss. JANUÁRIO GOMES, *op. cit.,* p. 253, chama a atenção para *"a característica específica de ser um mandato profissional - mandato bancário – realizado por um profissional qualificado: a empresa bancária"*. Não teremos nestas páginas oportunidade para o estudo do mandato bancário, para maiores desenvolvimentos, *vide* PEDRO PAIS VASCONCELOS "Mandato Bancário" *in Estudos em homenagem ao professor doutor Inocêncio Galvão Telles*, vol. II, Direito Bancário, Coimbra, Almedina, dezembro de 2002, pp. 131 a 155.

[56] MARIA RAQUEL GUIMARÃES, "O pagamento com cartão de crédito no comércio electrónico: evoluções legislativas recentes", *in Revista da Faculdade de Direito da Universidade do Porto*, ano IX, Coimbra, Coimbra Editora, 2012, p. 163.

[57] Era já um contrato socialmente típico por constituir um modelo de negociação praticado há várias décadas, encontrando-se comummente difundido no tráfego bancário, mas, como exigido por PEDRO PAIS VASCONCELOS, *Teoria Geral do Direito Civil,* 7.ª edição, Coimbra, Almedina, 2012, p. 454, é também reconhecido no seio social onde se insere como prática estabilizada.

Não encontramos nenhuma decisão dos nossos tribunais superiores onde o contrato de utilização de IP seja identificado como contrato-quadro, mesmo quando aplicam o quadro legal instituído pelo diploma de 2009. Todavia, verifica-se uma maior abertura dos tribunais à afirmação de que o contrato de abertura de conta bancária "funciona como um contrato-quadro", nas palavras do Supremo Tribunal de Justiça, no seu acórdão de 03.04.2003 (Quirino Soares)[58]. Tem sido repetidamente afirmado pelos tribunais que o uso de um IP se insere na "relação negocial complexa iniciada através de um contrato de abertura de conta, e da constituição de depósitos de quantias em conta por parte do titular, numa verdadeira coligação de contratos"[59], entendimento que partilhamos.

1.3. Inserção na relação Bancária Geral

Nas palavras do Acórdão do STJ de 27.02.2014[60], "a relação banco/cliente desenvolve-se no contexto de um contrato bancário, enquanto contrato-quadro com natureza duradoura (…) O referido contrato de abertura de conta, aqui em causa, surge seguramente nesse contexto, de relacionamento entre o banco-cliente".

Neste sentido, o contrato-quadro de utilização de IP eletrónico será, também, um contrato de aplicação de um contrato-quadro necessariamente anterior: o contrato de abertura de conta[61], que dá início a uma especial relação que se estabelece entre o banco e o seu cliente, apelidada de relação bancária geral[62/63]. Será "*na orbita deste contrato de conta bancária (…)*

---

[58] Posição, igualmente, seguida pelo TRL nos seus Acórdãos de 03.06.2003 (Pimentel Marcos) e de 05.11.2013 (Manuel Marques), todos disponíveis no sítio <http://www.dgsi.pt> (consultados a 10.01.2015).

[59] Cfr. Acórdão do Tribunal da Relação de Guimarães (TRG) de 23.10.2012 (Filipe Caroço). Esta posição é também seguida pelo TRL nos seus Acórdãos de 26.10.2010 (Maria Amélia Ribeiro), de 24.05.2012 (Ezagüy Martins), de 05.11.2013 (Manuel Marques), e de 03.03.2015 (Manuel Marques). E pelo TRP, no Acórdão de 07.10.2014 (Ana Lucinda Cabral), todos disponíveis em <http://www.dgsi.pt> (10.01.2015). No sentido da coligação de contratos de emissão de cartão e depósito, também se manifestou o Supremo Tribunal de Justiça no Acórdão de 23.11.1999 (Garcia Marques) *in CJ-STJ*, III, 1999, no Acórdão de 12.10.2000 (Nascimento Costa) *in CJ-STJ*, III, 2000, e ainda no seu Ac. de 11.10.2001(Silva Paixão) *in CJ-STJ*, III, 2001.

[60] Relator: Tavares de Paiva - consulta disponível em < http://www.dgsi.pt> (27.01.2015).

[61] MENEZES CORDEIRO, *op. cit.*, 5.ª ed., p. 579, refere: "*Em rigor, o contrato-quadro de pagamento surge como uma cláusula (ou várias) inserida no contrato de abertura de conta*". A caracterização deste contrato como contrato-quadro tem sido defendida por grande parte da doutrina especializada, sendo também apelidado de *contrato bancário - vide* ALMENO DE SÁ, *Direito Bancário*, Coimbra, Coimbra Editora, 2009, pp. 17 e ss, ou *contrato de conta bancária* - ENGRÁCIA ANTUNES, *Direito dos Contratos Comerciais*, Coimbra, Almedina, 2009, p. 483; JOSÉ SIMÕES PATRÍCIO, *op. cit.,* p. 137, caracteriza, ainda, este contrato como contrato de execução continuada.

[62] Leia-se, a este propósito, o que é dito no Acórdão do STJ de 3.12.1998 (Armando Lourenço), *in CJ-STJ*, III, 1998, p. 142: "*Como se vê das próprias cláusulas gerais, os acordos de uso do cartão de crédito integram-se num contrato de abertura de conta. Em regra, esses contratos geram uma relação complexa entre o banco e o cliente. As operações mais vulgares incluídas nesse contrato são: depósitos, levantamento, transferências, informações, etc.";* Ideia, igualmente, presente no Ac. da Relação do Porto de 13.11.2000 (Santos Carvalho), onde se diz que "*as operações procedem de uma única causa (o contrato originariamente celebrado com o banco), em lugar de serem fragmentadas numa série de depósitos, empréstimos ou reembolsos sucessivos, que exigiriam de cada vez que se verificasse um novo concurso de vontades*"; Também o Ac. de 28.09.2004 (Alberto Sobrinho) e o Ac. do TRL de 27.09.2007 (Maria José Mouro), acessíveis através do sítio: <http://www.dgsi.pt> (consultados a 25.10.2014).

[63] A designação é utilizada por ANTÓNIO MENEZES CORDEIRO, *op. cit.,* 5.ª ed., pp. 253 e ss., para designar a teia de relações negociais encetadas entre o banco e o seu cliente. É também usada por PINTO MONTEIRO, "A resposta do ordenamento jurídico português à contratação bancária pelo consumidor" *in Revista de Legislação e de Jurisprudência*, n.º 3987, ano 143, julho/agosto 2014, Coimbra, Coimbra Editora, p. 379;

que gravitarão usualmente os contratos de depósito, cheque, emissão de cartões bancários, empréstimos, créditos ao consumo, e de todos e cada um dos demais contratos bancários individuais que venham porventura a existir subsequentemente"[64], no fundo é o *contrato nuclear*[65] ou o *contrato dos contratos*. Refere o Banco de Portugal, no Aviso n.º 11/2005 de 21 de julho: "*a abertura de conta de depósito bancário constitui uma operação bancária central pela qual se inicia, com frequência, uma relação de negócio duradoura entre o cliente e a instituição de crédito*"[66]. Os diferentes negócios celebrados entre eles, como este de utilização do IP, não são isolados. Antes terão, como bem caracteriza o Tribunal da Relação de Lisboa[67], citando Engrácia Antunes, este "tronco comum sobre o qual repousarão todas as relações jurídicas entre o banco e o cliente, inclusive contratuais" que se estabelece, como referimos, num contrato de abertura de conta que inicia uma relação bancária tendencialmente duradoura e estável, gerando de uma relação de confiança[68].

O contrato de utilização de um IP pode ser, e muitas vezes será, cronologicamente associado ao contrato de abertura de conta, contudo, são contratos juridicamente autónomos[69], apesar de, necessariamente, interdependentes[70]. Os nossos tribunais superiores vêm, também, há vários anos, sedimentando o entendimento de que existe, na articulação entre o contrato de abertura de conta e o contrato de utilização, uma coligação contratual, principalmente na esteira do Acórdão de 23.11.1999 do Supremo Tribunal de Justiça[71]. É, de facto, inegável a existência de um nexo entre o contrato de abertura de conta e o contrato de utilização, já que este depende geneticamente daquele. Celebrado o segundo, a influência entre eles é,

---

[64] ENGRÁCIA ANTUNES, *op. cit.,* p. 484.

[65] Socorrendo-nos das palavras de MIGUEL PESTANA VASCONCELOS, "Dos contratos de depósito bancário", *in Revista da Faculdade de Direito da Universidade do Porto*, ano VIII, Coimbra, Coimbra Editora, 2011, p. 166, "*é efectivamente o contrato nuclear donde emerge a relação bancária duradoura entre a instituição de crédito e a sua contraparte. É no seio do seu conteúdo complexo que se integra o contrato de depósito (assim como outros contratos), que dele depende. Neste aspecto podemos falar numa coligação de contratos com dependência unilateral.*"; No mesmo sentido, MENEZES CORDEIRO, *op. cit.* 5.ª ed., p. 532 e ss.; Identificando este contrato como o "*contrato bancário primogénito (…) que estabelece o quadro geral de regulação da maioria dos futuros negócios"* - ENGRÁCIA ANTUNES, *op. cit.,* pp. 483 e 484; E ainda, QUIRINO SOARES, *op. cit.*, p. 111, caracterizando-o simbolicamente de "*mãe de todos os contratos bancários*".

[66] Cfr. texto preambular do Aviso n.º 11/2005 do Banco de Portugal, revogado pelo Aviso n.º 5/2013.

[67] Acórdão de 24.05.2012 (Ezagüy Martins), *cit.* Em sentido semelhante, identificando este contrato como "*o ponto de partida para o vasto complexo negocial que constitui a relação bancária"* – Ac. do STJ de 18.12.2013 (Ana Paula Boularot), disponíveis *in* <http://www.dgsi.pt> (23.01.2015).

[68] Estabelece-se, entre o banco e o seu cliente, ao longo do tempo, uma complexa teia contratual que abrange autorizações de débito da conta, concessões de crédito pessoal ou à habitação, planos poupança, entre muitos outros contratos que se podem desenvolver no âmbito da relação bancária.

[69] Ainda que celebrado no mesmo momento, aquando da celebração do contrato de abertura de conta, e pelos mesmos sujeitos, é possível distinguir, quanto a este, uma verdadeira proposta contratual e uma aceitação, com objetos distintos. No contrato de abertura de conta as partes desejam estabelecer a relação bancária que se irá se desenvolvendo e ganhando intensidade com os futuros contratos. Já no contrato de utilização do IP, as partes visam estabelecer uma forma de movimentar a conta e emitir ordens de pagamento.

[70] Assim, MARIA RAQUEL GUIMARÃES, "Os cartões bancários e as cláusulas contratuais gerais na jurisprudência portuguesa e espanhola - Breve análise da jurisprudência mais recente dos tribunais superiores portugueses e espanhóis em matéria de cláusulas contratuais gerais inseridas nos contratos de utilização de cartões bancários", *in Revista de Direito e de Estudos Sociais*, ano XLIII, janeiro-março, 2002, n.º 1, Editorial Verbo, p. 62; E ainda da mesma autora, *As transferências electrónicas de fundos e os cartões de débito*, Almedina, Coimbra, 1999, p. 105.

[71] Cfr. Acórdão STJ (Garcia Marques), *cit.,* p. 103, ainda que referindo o contrato de depósito bancário, que é inserido no contrato de abertura de conta bancária, constituindo uma convenção acessória deste contrato. Este entendimento foi seguido pelo Supremo ainda no Ac. de 14.02.2002 (Ferreira de Almeida) *cit.,* p. 126, e, mais recentemente, no Ac. de 17.05.2007 (Oliveira Rocha), *cit.*, mas também pelo TRL nos seus Acórdãos de 19.10.2000 (Salazar Casanova) *in CJ,* tomo IV, 2000, p. 126 e de 19.05.2002 (Manuel Gonçalves), disponível *in* <http://www.dgsi.pt> (14.12.2014).

como refere o nosso Supremo Tribunal, recíproca e bilateral, concorrendo ambos para o fim económico que preside à relação bancária geral.

Na verdade, tendo já reconduzido os contratos em causa ao esquema contratual do contrato-quadro e funcionando um deles como "instrumento de segundo grau" na aplicação do primeiro contrato, o seu nexo traduzir-se-á num modo particular de coligação negocial[72].

No que se refere especificamente ao *homebanking,* tem havido jurisprudência mais rica, principalmente no que respeita à sua relação com o contrato de abertura de conta. Veja-se, a título de exemplo, o que é dito no Acórdão da Relação do Porto de 07.10.2014 (Ana Lucinda Cabral): "A factualidade em causa emerge da existência de um contrato de conta bancária (ou abertura de conta) celebrado entre o banco, ora Apelante, e o Apelado e um contrato de *homebanking* (…), o qual sendo autónomo do contrato de conta bancária com ele tem uma íntima ligação"[73].

A jurisprudência, apoiada na coligação de contratos, acabou, em muitos casos, por resolver os problemas decorrentes da utilização abusiva do IP com base nas regras da transferência do risco inerentes ao contrato de depósito e de mútuo[74], ao que adiantamos, desde já, a nossa discordância, pois não estamos perante um problema de definição da propriedade (e inerente risco do seu perecimento) do dinheiro depositado, mas perante uma questão de cumprimento/incumprimento do contrato de utilização do IP, logo perante um problema de natureza obrigacional, como defendido por Maria Raquel Guimarães[75].

---

[72] No sentido da existência de uma coligação peculiar, veja-se MARIA RAQUEL GUIMARÃES, *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos, cit*., pp. 377 a 381. A coligação tem, igualmente, sido reconhecida na literatura especializada de diversos países. Em Espanha, MARIA DEL CARMEN GETE-ALONSO Y CALERA, *El pago mediante tarjetas de crédito*, Editorial La Ley. Madrid, 1990, pp. 122 e 123 (nota 18).

[73] Disponível *in* <http://www.dgsi.pt> (14.12.2014).

[74] Os Tribunais recorriam às regras do depósito e do mútuo na ausência de legislação específica, ainda que os Avisos do Banco de Portugal ou as Recomendações da UE pudessem auxiliar na resolução dos litígios que lhe eram colocados. Um dos casos mais recentes será o Acórdão do TRP de 29.04.2014 (Francisco Matos), será também dos mais curiosos - as operações não autorizadas foram registadas em 2011, caindo no âmbito de aplicação do RSP. Aqui, o Tribunal deveria, salvo melhor opinião, recorrer àquele regime, sem necessidade de utilização das normas do Código Civil, não esquecendo a autonomia já afirmada do contrato de utilização, no âmbito do qual surge a questão controvertida colocada ao Tribunal.

[75] A Autora vem chamando a atenção e esclarecendo que não estamos perante a questão da titularidade dos valores depositados desde 1999, *in As transferências electrónicas de fundos e os cartões de débito*, *op. cit*., pp. 231 a 234, e mais recentemente, em **"**As operações fraudulentas de *home banking* na jurisprudência recente - Ac. do STJ de 18.12.2013" *in Cadernos de Direito Privado,* 2015, em fase de publicação, ponto 4, dizendo "*Não estamos, no nosso entender, nestas hipóteses de operações não autorizadas realizadas por terceiros, perante uma questão de direitos reais, de saber quem é o proprietário de uma coisa e quem suporta o correspondente risco do seu perecimento, mas em face de um problema de natureza obrigacional, de (in)cumprimento de um contrato, bancário, surgido da prática e que engloba prestações que não se cingem ao empréstimo de dinheiro ou à sua guarda…"* No entanto, parte da doutrina e da jurisprudência continua a tratar a matéria, analisando a questão da transferência da propriedade, veja-se CALVÃO DA SILVA, "Conta corrente bancária: operação não autorizada e responsabilidade civil", *in Revista de Legislação e de Jurisprudência*, Ano 144, n.º 3991, março/abril de 2015, Coimbra Editora, com um capítulo dedicado à temática intitulado "depósito bancário: transferência da titularidade e do risco", pp. 312 a 315.

2. Principais direitos e deveres associados ao uso do Instrumento de Pagamento

"*O titular do IP deve utilizá-lo de acordo com as condições que regem a sua emissão e utilização*" – esta será, tipicamente, uma das cláusulas presente nos contratos[76] que disciplinam a relação duradoura entre as partes e comportam, naturalmente, a criação de direitos e deveres[77]. Na verdade, o cerne do contrato-quadro de utilização é composto precisamente por esses direitos e deveres dos contraentes[78].

Os direitos e obrigações com maior destaque nesta relação serão a emissão e entrega dos instrumentos de pagamento; o dever de informação e de esclarecimento do conteúdo do contrato e das principais causas de fraude[79]; o dever de guarda do IP e de sigilo relativamente aos dispositivos de segurança que lhe estão associados; a correta execução das ordens de pagamento e a manutenção de um sistema de pagamentos funcional, sem deficiência técnicas; o dever de comunicar o extravio/perda do IP ou qualquer operação não autorizada e de imediato cancelamento do IP extraviado; o dever de reembolso imediato dos montantes de operações de pagamento não autorizadas; o dever de aviso prévio em caso de modificação do contrato de utilização e em caso de denúncia de contrato de duração indeterminada; discutindo-se na doutrina se haverá ainda um outro dever – o dever de vigilância da entidade bancária relativamente aos fundos depositados pelo seu cliente.

Vários destes deveres resultavam já da recomendação da Comissão 97/489/CE, de 30.07.1997, relativa às transações realizadas com recurso a IP eletrónico e às relações entre emitente e detentor. No art. 5.º deste diploma prevê-se a obrigação do detentor do IP "*tomar todas as precauções razoáveis para garantir a segurança do instrumento de pagamento*" e de comunicar, logo que tenha conhecimento, "*o extravio ou furto do instrumento de pagamento*" (cfr. alínea a) e b)), tendo o emissor de disponibilizar os meios que permitam, 24 horas por dia, fazer tal comunicação (art. 9.º da recomendação). Resultavam ainda dos Avisos do Banco de Portugal relativos a esta matéria, pelo que não

[76] É uma regra, igualmente, consagrada pelo art. 56.º da Diretiva n.º 2007/64/CE e pelo art. 67.º do D.L. n.º 317/2009.

[77] Estamos perante um contrato sinalagmático e bilateral, dele emergindo direitos e obrigações na esfera jurídica de ambos os contratantes.

[78] MARIA RAQUEL GUIMARÃES, *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos, op. cit.,* p. 281, refere que este direitos e deveres decorrentes do contrato de utilização constituem, precisamente, o conteúdo da relação contratual em causa.

[79] Os requisitos de informação surgem no RSP no capítulo I do título III relativo à transparência das condições. O legislador nacional assumiu uma posição protecionista da parte que adere ao contrato, consagrando um especial dever de informação, que constitui um dever acessório de conduta decorrente da especial relação de confiança entre as partes. É previsto um elevado nível de informação, que deve ser prestado tendo em consideração os conhecimentos técnicos de cada utilizador. Estão previstas informações pré-contratuais, informações no âmbito contratual e pós-contratual, podendo o utilizador solicitar novas informações em qualquer momento. Contudo, este regime foi acusado de ser excessivo e demasiado protetor do utilizador – veja-se INÊS ISABEL DOS CAMPOS MOURA, *op. cit.*, nota de rodapé 121. Será ainda ao prestador do serviço de pagamento que cabe provar que cumpriu os requisitos de informação, nos termos do art. 44.º do RSP. Finalmente, quanto a este dever, importa considerar a necessidade de conjugar este regime com o regime do crédito aos consumidores, D.L. n.º 133/2009, de 2 de junho, e com o D.L. n.º 95/2006, de 29 de maio, que estabelece o regime aplicável à informação pré-contratual e aos contratos relativos a serviços financeiros prestados a consumidores através de meios de comunicação à distância – cfr., sobre este ponto, JANUÁRIO GOMES, *op. cit.,* pp. 228 e 229 e, para maior desenvolvimento sobre o dever de informação, pp. 230 a 239.

poderá atribuir-se à Diretiva n.º 2007/64/CE do Parlamento Europeu e do Conselho, de 13 de novembro de 2007, transposta para o ordenamento interno pelo diploma de 30 de outubro de 2009, um carácter particularmente inovador quanto a este ponto. Antes apresenta um objetivo de uniformização[80].

O regime dos direitos e obrigações é aplicável independentemente da qualidade do utilizador. Mas às partes é permitido, exceto quando se tratem de consumidores ou microempresas - a quem é aplicável o regime dos consumidores -, afastarem, no todo ou em parte, a disciplina estabelecida neste capítulo, de acordo com o art. 40.º n.º 3 do RSP.

2.1. Emissão e entrega dos instrumentos de pagamento

Será, naturalmente, ao prestador dos serviços de pagamento que cabe, cumprindo um dever secundário com carácter meramente acessório[81], colocar o seu cliente na posse do IP que lhe irá permitir proceder às operações de pagamento que executam o contrato de utilização, sendo a forma (segura) dessa entrega o núcleo fundamental deste dever[82].

Acompanhamos o Tribunal da Relação de Coimbra no Acórdão datado de 15.06.2010 (Arlindo Oliveira)[83], embora referindo-se especificamente ao chamado cartão de plástico, no sentido de que "(a) entrega, através de meio seguro do cartão e do respectivo PIN, é fundamental à boa execução do contrato que se consubstancia num dever acessório da prestação principal, destinado a permitir que só o detentor do cartão o receba e só ele o possa utilizar nos termos contratados (…) cabe ao banco emissor do cartão multibanco estabelecer as regras de segurança e especiais deveres de cuidado a adoptar no envio do cartão ao utente". Quanto ao *homebanking,* a jurisprudência caminha no mesmo sentido, destacando "a obrigação de assegurar que os dispositivos de segurança personalizados só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento, sendo seu [da entidade prestadora do serviço] o risco de envio ao utilizador de um instrumento de pagamento ou dos respectivos dispositivos de segurança personalizados"[84].

O Banco de Portugal vinha já chamando a atenção para o problema da apropriação por parte de terceiros do IP enviado, principalmente no caso de cartões e o respetivo código secreto,

[80] O RSP regula os direitos e obrigações relativos à prestação e utilização do serviço de pagamento no capítulo II do título III.
[81] Sobre a distinção entre deveres secundários com carácter meramente acessório da prestação principal e deveres secundários com prestação autónoma, ALMEIDA COSTA, *Direito das Obrigações*, 12.ª ed. revista e atualizada, Coimbra, Almedina, novembro de 2009, p. 77.
[82] Em Portugal, é comum essa entrega ser feita pela via postal, considerando-se os serviços prestados pelos CTT -Correios de Portugal seguros. Todavia, em Espanha, a jurisprudência e a doutrina consideram que o uso dos meios postais não corresponde a uma prática segura, como referido por MARIA DEL CARMEN GETE-ALONSO Y CALERA, *Las tarjetas de crédito…*, *op. cit.,* pp. 166 e 167.
[83] Disponível no sítio <http://www.dgsi.pt> (11.02.2015).
[84] Cfr. Ac. do TRG de 17.12.2014 (Fernando Fernandes Freitas), disponível <http://www.dgsi.pt> (consultado em 23.02.2015).

utilizando as expressões "*especial cuidado*" e "*adequadas regras de segurança*" [85], incutindo a ideia de que a possibilidade de apropriação do IP por terceiro deve ser reduzida ao máximo[86]. Daqui se retira que as operações abusivas praticadas por terceiros que se tenham apoderado do IP no percurso de entrega "*terão de ser suportadas pelo primeiro, que não cumpriu devidamente a sua obrigação de entrega*"[87].

No caso do Acórdão citado, o Tribunal bem entendeu, a nosso ver, que a entidade emissora não deve enviar o cartão pronto a utilizar, isto é, já ativado, "fazendo[-o] viola as regras de segurança do sistema de acesso aos serviços proporcionados por tal cartão e em flagrante desrespeito pelo comando ínsito no art. 11.º do Aviso n.º 11/2001 do Banco de Portugal, pelo que deve ser responsabilizado pelos prejuízos sofridos pelo titular da conta, resultantes de tal omissão". Neste sentido, o tribunal condenou a entidade emissora a indemnizar os prejuízos, desconsiderando o facto do titular do IP ter mudado de residência sem que disso tivesse dado conhecimento à entidade emissora.

É importante ter em conta que mesmo o envio do cartão não ativado, pode não ser capaz de evitar o extravio e consequentemente o seu uso, pois também a ativação poderá ser fraudulentamente conseguida por meios informáticos. Perante a possibilidade de apropriação abusiva, o RSP vem consagrar a responsabilidade, já afirmada pelo Banco de Portugal e pelo Tribunal da Relação de Coimbra, do prestador do serviço no art. 68.º n.º 2, prevendo que "*o risco do envio ao ordenante de um instrumento de pagamento ou dos respectivos dispositivos de segurança personalizados corre por conta do prestador do serviço de pagamento*". O emissor responde, assim, pelas operações abusivas resultantes do extravio do IP ou dos dispositivos de segurança associados enviados ao utilizador (nomeadamente por via postal).

2.2. Dever de guarda do IP e de sigilo relativamente aos dispositivos de segurança que lhe estão associados

Os contratos de utilização elaborados pelo prestador dos serviços de pagamento aos seus clientes contêm, usualmente, uma ou mais cláusulas onde se prevê os deveres de guarda do instrumento, de preservação e confidencialidade dos dispositivos de segurança que lhe estão

[85] Cfr. art. 11.º do Aviso do Banco de Portugal n.º 11/2001, de 20 de novembro.
[86] Contudo, não eram apresentadas pelo Banco de Portugal (BdP) quaisquer soluções concretas para o problema. Aquela entidade, no sentido de evitar extravios do cartão, considerava que o contrato se mostrava celebrado quando o cartão e cópia do contrato fossem entregues ao utilizador (cfr. art. 9.º do aviso n.º 11/2001), sendo que, para esse entendimento, a entrega do cartão consubstancia um requisito da celebração do contrato. Contudo, os Avisos do BdP tem natureza regulamentar, pelo que prevalece a posição presente no Código Civil (arts. 224.º e 232.º), bastando o encontro de vontades para que o contrato se considere realizado. No mesmo sentido, veja-se MARIA RAQUEL GUIMARÃES, "Algumas considerações sobre o Aviso n.º 11/2001 relativo aos cartões de crédito e de débito", *Revista da Faculdade de Direito da Universidade do Porto*, I, p. 251.
[87] MARIA RAQUEL GUIMARÃES / MARIA REGINA REDINHA, "A força normativa dos Avisos do Banco de Portugal – reflexão a partir do Aviso n.º 11/2001, de 20 de novembro", *Nos 20 anos do Código das Sociedades comerciais – Homenagem aos profs. Doutores A. Ferrer Correia, Orlando Carvalho e Vasco Lobo Xavier*, Coimbra Editora, 2007, p. 720.

associados[88]. Estes, apelidados de "*dispositivos de segurança personalizados*" no RSP, serão o comum PIN ou outros "*procedimento(s) que permite(m) ao prestador do serviço de pagamento verificar a utilização de um instrumento de pagamento específico*", permitindo a autenticação do seu titular[89].

Ao prestador de serviços de pagamento impõe-se a obrigação de "*assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento*" (art. 68.º/1, a)), devendo proporcionar ao utilizador um sistema de segurança eficaz, impeditivo (em princípio) de uma utilização abusiva por terceiros[90]. Enquanto ao utilizador cabe a guarda do seu IP[91] e o dever de "*tomar todas as medidas razoáveis, em especial ao receber um instrumento de pagamento, para preservar a eficácia dos seus dispositivos de segurança personalizados*" (art. 67.º/2 do RSP), tendo o dever primordial de não facultar a terceiros os elementos de segurança que lhe são atribuídos, atendendo à sua função de autenticação das operações de pagamento.

O cumprimento deste dever tem também sido analisado pelos nossos tribunais, numa enorme variedade de situações, como é típico da vida. Partilhamos do entendimento do STJ perante uma destas situações mais correntes: "quem traz o PIN numa agenda acessível a qualquer pessoa que a leia infringe de forma grave um dever contratual, pelo que a imputação de culpa do titular nos parece incontroversa"[92/93].

---

[88] Estes serão deveres laterais ou deveres de conduta, que encontrarão a sua génese numa norma legal, no contrato ou no princípio da boa fé - cfr. ALMEIDA COSTA, *op. cit.*, p. 77. A obrigação do utilizador tomar todas as medidas razoáveis era já prevista na recomendação da Comissão 97/489/CE de 30 de julho de 1997, no seu art. 5.º al. a) e c).

[89] Cfr. al. v) do art. 2.º do RSP.

[90] No âmbito da banca eletrónica, a segurança do sítio da internet é garantida frequentemente por sistemas de codificação da informação (chaves de encriptação de 128bits) e pela certificação digital do *site.*

[91] Dever-se-á ter presente que o dever de guarda não significará trazer sempre consigo o cartão, em certas situações, representará, pelo contrário, guardá-lo num local seguro. MANUEL CASTILLA CUBILLAS, *La tarjeta de crédito - Tratado de Derecho Mercantil*, Tomo 28, Marcial pons, Madrid, 2007, pp. 192 e 193, apresenta uma decisão do SAP de Castellón de 12.02.2000, onde o Tribunal entendeu que guardar o cartão dentro do carro estacionado num parque público – onde se pudesse esperar que houvesse algum tipo de sistema de vigilância – não podia configurar negligência grave. Entre nós, o STJ no Ac. de 19.11.2002, *cit.,* entendeu existir violação grave do dever de guarda do titular que, enquanto foi à praia, "*deixa um cartão de débito no interior de um veículo de matrícula estrangeira (ainda que dentro de uma carteira debaixo de um banco da frente), aparcada em lugar público, e só regressa a essa viatura cerca de sete horas e trinta minutos mais tarde*". Perguntamos nós, se este comportamento seria também considerado negligente se o roubo do cartão fosse consequência de um "arrastão" que ocorreu na praia, ou ocorresse enquanto o titular se encontrava na água, deixando o IP com os seus pertences junto à toalha?

[92] Cfr. Ac. de 02.03.2010 (Urbano Dias) disponível *in* <http://www.dgsi.pt> (25.10.2014). Numa situação semelhante, em que o titular do IP transportava o PIN no verso de uma fotografia junto ao cartão, o TRL no Ac. de 19.09.2006 (Maria Amélia Ribeiro), *in* <http://www.dgsi.pt> (25.10.2014), entendeu que o titular suporta os prejuízos emergentes do furto, pois "*foi o risco por ela própria criado que levou a que num curtíssimo período de tempo entre as 20.19h e as 20.42h fosse retirado a totalidade da quantia que a A. tinha depositada na sua conta bancária".* De facto, porque o seu comportamento foi grosseiramente negligente, o titular deve suportar os prejuízos até ao limite do saldo ou linha de crédito associada ao IP.

[93] Internacionalmente, a questão do cumprimento do dever de guarda tem sido igualmente abordada, REINHARD STEENNOT, "Allocation of liability in case of fraudulent use of an electronic payment instrument: the new directive on payment services in the internal market", *in ScienceDirect - Computer Law & Security Report*, Volume 24, issue 6, 2008, p. 557, <http://www.sciencedirect.com> (12.11.2014), apresenta dois casos curiosos: um caso em que o utilizador do cartão anotou num papel o PIN como se de um contacto telefónico se tratasse - o tribunal alemão, Court of Kassel (AG Kassel 16 November 1993, W.M., 1994, 2110), decidiu existir negligência grosseira; Já na Holanda (GCB 24 September 1994, T.V.C. 1995, 183), o tribunal entendeu que o facto do utilizador guardar o PIN como contacto telefónico na sua agenda não configurava negligência grave.

Já no uso do *homebanking,* tem sido colocado aos tribunais vários casos em que o utilizador, convicto de que está na página *on-line* do prestador do serviço, fornece os seus dados e as posições do cartão-matriz. A maioria das decisões tem sido favoráveis ao titular, considerando não existir uma violação deste dever[94]. Contudo, têm surgido Acórdãos, ainda que em números mais discretos, que enveredam pela tese contrária, defendendo que esta atuação do titular consubstancia negligência grave ou grosseira: é o caso do Acórdão do Tribunal da Relação de Guimarães de 25.11.2013 (Espinheira Baltar)[95].

2.3. Correta execução das ordens de pagamento e manutenção de um sistema de pagamentos funcional e sem deficiências técnicas

Uma vez introduzidos no sistema os códigos ou elementos de acesso que identifiquem o titular do IP, os prestadores de serviços de pagamentos obrigam-se a aceitar os mandatos porquanto assumem que a ordem provém do legítimo titular[96], devendo ainda colocar à disposição dos seus clientes os meios técnicos necessários à utilização do IP em pleno funcionamento e sem deficiências técnicas[97], respondendo pela ocorrência de quaisquer deficiências.

---

[94] Veja-se, a título de exemplo, o Acórdão do Tribunal da Relação de Lisboa de 26.10.2010, o Ac. do TRG de 17.12.2014, o Ac. do TRP de 29.04.2014, *cit.*, Ac. do TRL de 28.06.2013 (Anabela Calafate) e, em especial, o Ac. do TRG de 30.05.2013 (Rita Romeira) onde se defende não existir "*uma conduta imprudente, descuidada ou negligente*", considerando que as páginas falsas são, nas palavras do tribunal, "*muitas vezes iguais às páginas do banco e identificadas como ligações seguras",* não tendo o utilizador "*qualquer controlo sobre os sofisticados meios informáticos da entidade bancária, nem dispõe da assessoria técnica com que os departamentos respectivos daquela se apetrecham",* disponíveis *in* <http://www.dgsi.pt> (26.02.2015).

[95] O Tribunal decidiu que há negligência grave do "*utente que fornece todo o conteúdo do cartão matriz perante uma solicitação numa página idêntica à do banco, uma vez que contraria toda a lógica do sistema de segurança que não pode ser desconhecida por parte do utilizador*". Julgamos que tal entendimento se prende, sobretudo, com a informação prestada e pela presença de avisos no acesso à pagina *on-line* do prestador do serviço. O Juiz Relator deste Ac., Dr. Espinheira Baltar, apresenta no Ac. do mesmo Tribunal datado de 17.12.2014, voto de vencido com o mesmo fundamento; No mesmo sentido, manifestou-se o Tribunal da Relação de Lisboa no Ac. de 12.12.2013, *cit.*, considerando que a utilizadora "*fez uma utilização imprudente, negligente e descuidada desse serviço"*; Num caso semelhante, o utilizador forneceu os seus dados na página *web* falsa, quando eram já divulgados avisos/alertas da existência de fraude através de uma falsa *demo* de transferência direta, o Julgado de Paz na sentença de 21.09.2012 (Maria Judite Matias), disponível em <http://www.dgsi.pt> (10.03.2015), defendeu que quanto ao banco "*não houve falha na prestação do serviço, nem mesmo negligência no que respeita à segurança do site disponibilizado*", enquanto o utilizador foi negligente "*no sentido de não ter tido as necessárias cautelas, de não ter prestado mais atenção ao que lhe estava sendo solicitado, precavendo-se das fraudes que eram anunciadas no próprio site do banco, com alertas e informações (…) não cometendo a imprudência de informar terceiros dos seus dados pessoais e sigilosos*".

[96] Estando preenchidos os requisitos estabelecidos no contrato-quadro, o prestador do serviço não pode, nos termos do art. 76.º do RSP, recusar a execução da ordem de pagamento, independentemente desta ser emitida pelo titular, pelo beneficiário ou através dele, salvo disposição legal em contrário. A execução destas ordens de pagamento serão a finalidade deste contrato de utilização, não executando a mesma ou verificando-se uma execução incorreta (a execução incorreta significa o cumprimento defeituoso da obrigação - inclui as transferências com atraso ou com montantes incorretos), o prestador do serviço viola um dever contratual, tendo, de acordo com o art. 86.º do RSP, de reembolsar o utilizador, sem atrasos injustificados, do montante da operação não executada ou incorretamente executada e, se for caso disso, repor a conta debitada na situação em que estaria se não tivesse ocorrido a execução incorreta da operação de pagamento, prevendo-se ainda a indemnização de certos danos indiretos como dos encargos suportados e dos juros a que esteja sujeito.

[97] Caixas automáticas (ATM's) e terminais de pagamento automático (POS). Quanto às operações de banca ao domicílio, devem as entidades bancárias manter operacionais os sistemas informáticos, proporcionando um sistema eficaz e seguro, exigido, também, pelo art. 73.º do Regime Geral das Instituições de Crédito e

O dever de contratar imposto à entidade prestadora do serviço[98], e as suas consequências, vem consagrado no RSP. No art. 86.º n.º 1 estabelece-se que "*caso uma ordem de pagamento seja emitida pelo ordenante, a responsabilidade pela execução correta da operação de pagamento perante o ordenante cabe ao respetivo prestador de serviços de pagamento…*" e no art. 70.º n.º 1: "*(…) incumbe ao respetivo prestador do 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*"[99].

Anteriormente à previsão do RSP, a questão tinha já chegado aos tribunais sob a forma de controlo de validade das cláusulas contratuais gerais contidas nos contratos de utilização. Desta forma, os nossos mais altos tribunais tinham já declarado nula a cláusula que fazia correr o risco de mau funcionamento ou avaria da máquina de rede por conta do cliente, maioritariamente seguindo a posição do Supremo Tribunal de Justiça no seu Acórdão de 03.12.1998 (Armando Lourenço), entendendo que fazer a prova de que a operação de pagamento não foi afetada por avaria técnica era extremamente difícil para alguém que não domina os sistemas em causa. Aqui estaria em consideração ainda uma questão de responsabilidade contratual "pela não prestação de um serviço acordado na tal relação complexa" [100].

2.4. Comunicação do extravio, perda ou roubo do instrumento de pagamento ou de qualquer operação não autorizada e imediato cancelamento do IP extraviado

Se anteriormente afirmamos que cabia ao titular do IP a sua guarda, será, naturalmente, a este que cabe comunicar, logo que lhe seja possível, a sua perda, roubo ou extravio, ou qualquer utilização não autorizada, enquanto ao prestador do serviço cabe o dever de disponibilizar, a todo o tempo, os meios adequados à realização desta notificação[101] e o

Sociedades Financeiras (RGICSF), aprovado pelo Decreto-Lei n.º 298/92, de 31 de dezembro: "*as instituições bancárias devem assegurar, em todas as atividades que exerçam, elevados níveis de competência técnica…*"

[98] Quanto a este dever, no uso de cartão de crédito surge, obviamente, o correlativo dever de reembolsar a quantia e respetivos juros, sempre que o pagamento seja diferido, à entidade emissora do IP que se obrigou em termos semelhantes aos das entidades creditícias. A este propósito veja-se, MARIA RAQUEL GUIMARÃES, *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos, cit.,* pp. 286 a 289.

[99] Nos considerandos iniciais, o diploma sublinha a importância das regras estabelecidas quanto à prova, afirmando que são nulas as condições contratuais que "*tenham por efeito agravar o ónus da prova que recai sobre o consumidor ou atenuar o ónus da prova que recai sobre o emitente*" – considerando 33.

[100] Cfr. Ac. do STJ de 03.12.2008, *cit.* – a nulidade da cláusula foi declarada com base no arts. 18.º al. c) e 21.º al. e) do D.L. n.º 446/85 de 25 de outubro. Em sentido idêntico, *vide* os Acórdãos do STJ de15.05.2008 (Mota Miranda) e de 21.10.2008 (Alves Velho), disponível *in* <http://www.dgsi.pt>; Estas decisões acompanham a recomendação da Comissão n.º 97/489/CE de 30 de junho de 1997, que responsabiliza a entidade prestadora do serviços pelas operações não executadas ou incorretamente executadas, ainda que iniciada em dispositivos/terminais/equipamentos que aquela não controla diretamente – cfr. art. 8.º n.º 1, al. a).

[101] Não tendo o prestador disponibilizado os meios que permitam, a todo tempo, fazer esta comunicação, o titular do cartão não suporta quaisquer consequências da utilização abusiva do seu IP, nos termos do art.

dever de proceder ao seu cancelamento logo que rececione a comunicação do titular. O cumprimento destes deveres terá uma consequência direta na repartição dos prejuízos emergentes das operações fraudulentas.

A comunicação por parte do titular do IP estabelece o momento temporal a partir do qual o titular do cartão não suporta quaisquer consequências financeiras resultantes das operações não autorizadas[102]. De acordo com o que é afirmado pelo STJ já em 2002, "o titular do cartão será responsável na medida do cumprimento das suas obrigações relativas à segurança desse cartão e do código de acesso que lhe foi atribuído, sendo que tal responsabilidade se estende até ao momento em que comunicar ao banco o extravio ou furto do cartão"[103]. Será, então, ao prestador do serviço de pagamento que cabe a responsabilidade pelas operações registadas em momento posterior à comunicação, na medida em que será este quem tem os mecanismos capazes de impedir novas utilizações[104].

Também o RSP consagrou estes deveres, atribuindo ao momento do seu cumprimento este papel "delimitador" da responsabilidade das partes. Assim, estabelece que, após ter procedido à comunicação, o utilizador do IP "*não suporta quaisquer consequências financeiras resultantes da utilização de um instrumento de pagamento perdido, roubado ou abusivamente apropriado, salvo em caso de atuação fraudulenta*", nos termos do art. 72.º n.º 4[105]. Trata-se da solução já prevista na recomendação da Comissão 97/489/CE, de 30.07.1997, mas contrária ao Aviso do Banco de Portugal de 2001, que permitia que o titular do cartão suportasse os prejuízos causados depois da comunicação, ainda que não se verificasse qualquer comportamento censurável, sempre que não estivesse em causa uma "*utilização electrónica do cartão*"[106].

72.º/5 do RSP; JANUÁRIO GOMES, *op. cit.,* p. 247, entende ser "*patente que o prestador de serviços que, numa situação deste tipo, pretendesse imputar o risco ao utilizador, atua de má fé, em* venire contra factum proprium". O prestador do serviço de pagamento deve, ainda, disponibilizar os meios necessários para o utilizador fazer a prova de que efetuou a comunicação (cfr. art. 68.º/1, al. d)).

[102] A importância desta comunicação é, de forma muito clara, afirmada pelo TRC no Ac. de 15.06.2010. Baseando-se em MARIA RAQUEL GUIMARÃES, o Tribunal refere: "*com tal comunicação quebra-se o nexo de causalidade que une os danos sofridos à actuação eventualmente negligente do titular do cartão, em termos em que a responsabilidade pelo uso indevido do cartão se transfere para a instituição bancária, que não sofrerá prejuízos se, diligentemente, tomar todas as medidas de segurança adequadas*". Na mesma linha, *vide* o Ac. do STJ de 19.02.2002, *cit*.

[103] Cfr. Acórdão de 19.11.2002, *cit.*

[104] O Supremo expressou-se neste sentido no Ac. de 02.03.2010, *cit*., decidindo que o prestador do serviço, após a comunicação do titular, "*podia e devia ter accionado todos os mecanismos necessários, de modo a evitar novas utilizações*"; Assim, ANA PRATA, *op. cit.*, p. 506 e CALVÃO DA SILVA, "Conta corrente bancária: operação não autorizada e responsabilidade civil", *cit.,* que caracteriza este dever como uma "*obrigação de resultado*", p. 323. Já REINHARD STEENNOT, *op. cit.,* p. 556, defende a responsabilidade do prestador do serviço pelas operações registadas após a receção da comunicação, não obstante este ter ou não os meios necessários e capazes para evitar as futuras operações - "*Whether the payment service provider is actually able to prevent further use of the instrument is irrelevant. As soon as notification has taken place the payment service provider is liable for all transactions taking place*".

[105] Este dever de comunicação é exigido ao titular do IP perante uma situação de perda, roubo, extravio do mesmo ou quando detete alguma operação não autorizada. Ainda que o contrato de utilização preveja outros deveres, como a comunicação do incidente à polícia, o incumprimento destes não libera o prestador do serviço da responsabilidade que lhe é atribuída após a notificação feita pelo titular – neste sentido, *vide* REINHARD STEENNOT, *cit*., p. 556.

[106] A distinção consoante a utilização não autorizada fosse praticada após ou anteriormente à comunicação era feita pelo art. 8.º do Aviso do BdP n.º 11/2001, embora, distinguindo no n.º 2 do preceito se a utilização do cartão era eletrónica ou não. Enquanto no primeiro caso o titular não responde por qualquer utilização posterior à notificação, na hipótese de utilização não eletrónica o titular suporta também os prejuízos das utilizações

Hoje, com a comunicação da perda, roubo ou extravio do IP, o prestador do serviço deve, de imediato, cancelar o IP em causa, impedindo *"qualquer utilização do instrumento de pagamento logo que a notificação prevista na alínea b) do n.º 1 do artigo anterior tenha sido efectuada"*, nos termos do art. 68.º/1, e) do RSP.

O art. 69.º do mesmo diploma acrescenta que a comunicação de (outras) operações não autorizadas ou incorretamente executadas deve, igualmente, ser feita após ter tomado conhecimento, sem atraso injustificado, num prazo máximo de treze meses a contar da data do débito.

Esta repartição de responsabilidades com base num critério temporal – tendo em consideração o momento da comunicação do titular do IP – assenta na ideia, já afirmada pela nossa jurisprudência, em relação aos cartões, de que "(s)e se afigura justo e equitativo que o banco emissor do cartão seja responsável pelos movimentos efectuados após a comunicação do seu extravio, na medida em que dispõe de meios para evitar o seu uso, também se justifica a responsabilização do titular pelos danos ou parte dos danos decorrentes desse uso indevido no período anterior a essa comunicação, por ser uma exigência do dever de diligência que sobre ele impende"[107].

A questão que mais dificuldades levanta na análise deste dever prende-se, precisamente, com o prazo para efetuar essa comunicação. No RSP diz-se que essa comunicação deve ser feita *sem atrasos injustificados* (art. 67.º/1, b)), sem que, contudo, seja previsto um prazo ou se esclareça o que poderá configurar um atraso justificado[108].

A nossa jurisprudência, mesmo anterior a este regime, manifestou diferentes entendimentos quanto ao momento em que deve ser feita a comunicação. Vejamos alguns exemplos: o STJ, no Acórdão de 19.11.2002[109], em que um cartão foi furtado dentro de um veículo, a que o seu utilizador voltou 7 horas mais tarde, comunicando nessa altura o furto, entendeu existir negligência grave[110], condenando o utilizador a suportar todos os prejuízos emergentes das

---

realizadas nas 24h após a comunicação, podendo suportar para além desse prazo se tiver agido com dolo ou negligência grosseira – cfr. JOANA VASCONCELOS, "Sobre a repartição do risco de utilização abusiva do cartão", *cit.,* pp. 498 e ss; e MARIA RAQUEL GUIMARÃES, "Algumas considerações sobre o Aviso n.º 11/2001…" *cit.,* pp. 254 e ss.

[107] Cfr. Acórdão do TRP de 28.09.2004 (Alberto Sobrinho) e do STJ de 15.10.2009 (Alberto Sobrinho), *cit*. A responsabilidade do titular do IP, antes da comunicação, será limitada a parte dos prejuízos, mais precisamente a €150, sempre que não se prove um comportamento doloso ou grosseiramente negligente da sua parte.

[108] A utilização do conceito indeterminado terá de ser preenchida pela doutrina, atendendo também aos importantíssimos contributos da jurisprudência. Em Espanha, MANUEL CASTILLA CUBILLAS, *op. cit.,* p. 195, dá conta de duas decisões jurisprudenciais, do SSAP de Salamanca 07.06.2004 e de Baleares de 25.06.1999, onde foi afirmado que seria exagerado exigir ao titular que comprovasse a cada hora do dia se ainda mantinha a posse do cartão. Mas é afirmado o dever de comunicar com celeridade o roubo ou extravio, ainda que não tenha certeza, quando tenha suspeitas fundamentadas. Nas palavras do autor, *"éstos so terminus amplios que dejam cierto espácio a la labor del intérprete para que decida en cada caso si há existido diligencia o negligencia en el cumplimiento del deber de notificación".*

[109] Relator: Azevedo Ramos, *cit.*

[110] Para este entendimento do tribunal pesou a ponderação da violação do dever de comunicação atempada (o tribunal defendeu existir *"omissão do dever de efectuar a comunicação daquelas ocorrências, com a devida prontidão")*, mas também do dever de guarda do IP, a que já fizemos referência. Note-se, todavia, que o titular comunicou o roubo logo que dele teve conhecimento. A sentença dos Julgados de Paz de 16.10.2006, acessível no sítio <http://www.dgsi.pt> (09.03.2015) defende uma posição diametralmente oposta, entendendo que não poderá exigir-se ao titular "*o aviso de imediato (…) A obrigação de comunicação só pode, assim, ser entendida a partir do momento em que se tornou possível ou conhecido o delito*".

operações não autorizadas integralmente registadas antes da comunicação. Em dois casos muito similares – roubo de cartão no estrangeiro – o Tribunal da Relação de Lisboa manifestou orientações contrárias: no Acórdão de 19.05.2002, o furto do cartão aconteceu em Barcelona a 10 de dezembro e a comunicação foi feita no dia seguinte (11 de dezembro), considerou que a demora na notificação representava uma violação manifesta do dever de comunicação imediata; no segundo, o Acórdão de 16.04.2004, o mesmo tribunal entendeu atempada a comunicação efetuada também no dia seguinte ao roubo do cartão em Bruxelas, não sendo o utilizador responsável pelas operações abusivas realizadas 15 dias depois. Já numa decisão recente, o Tribunal da Relação de Guimarães desconsiderou o facto do utilizador do sistema de "banca eletrónica" ter utilizado o instrumento após terem sido praticadas sete operações não autorizadas, sem que se apercebe-se delas, só as tendo comunicado seis dias depois[111].

Não será possível, cremos, definir um prazo específico para essa comunicação, não podendo exigir-se, como ao prestador do serviço de pagamento, que este dever seja *imediatamente* cumprido, mas também não poderá admitir-se um prazo demasiado alargado para efetuar a comunicação. Terá de ser feita uma avaliação casuística[112], verificando-se no momento da comunicação o grau de diligência (ou negligência) colocado por parte titular do IP no cumprimento deste dever[113]. Quanto à jurisprudência referida, não parece que perante o furto do IP no estrangeiro, sendo a comunicação feita no dia seguinte, exista necessariamente descuido por parte do titular no cumprimento desse dever. Antes haverá de considerar a facilidade de realizar tal comunicação no estrangeiro, que, em alguns casos, poderá ser diferente da existente em território europeu. Mais dúvidas levanta a consideração do STJ, no Acórdão de 19.11.2002, de que existe "*omissão do dever de efectuar a comunicação*" do titular que notifica o banco do roubo logo que do mesmo teve conhecimento, sendo que tal ocorre ao regressar à viatura, ainda que, cerca de sete horas mais tarde. Discordamos também da Relação de Guimarães no Acórdão de 17.12.2014, que não se pronuncia quanto ao cumprimento do dever de comunicação pelo titular, pois o cumprimento desta obrigação deveria ser ponderado na análise da responsabilidade das partes. Desde logo, porque a comunicação atempada das operações não autorizadas ou perda/extravio do IP, só poderá ser feita pelo utilizador que o use com atenção e diligência, demonstrando o titular do IP fraudulentamente utilizado, naquele caso, uma clara negligência ao utilizar o IP sem detetar as *sete* operações não autorizadas já praticadas.

---

[111] Ac. de 17.12.2014 (Fernando Fernandes Freitas) disponível *in* <http://www.dgsi.pt> (23.02.2015).

[112] No Considerando 33 da Diretiva 2007/64/CE prevê-se que sejam tidas em consideração "*todas as circunstâncias*" para avaliar a negligência do utilizador do IP.

[113] Não poderemos perder de vista que o tempo desta comunicação demostrará não só a diligência colocada pelo titular no cumprimento deste dever, mas também no dever de guarda, no que se refere aos cartões de plástico, pois só poderá comunicar a partir do momento em tenha percebido o delito. Assim, somos conduzidos à questão levantada por REINHARD STEENNOT, *op. cit.*, p. 557, "terá o titular de verificar constantemente se o IP desapareceu?" (tradução nossa) – o Tribunal da Bélgica, Court of Appeal in Brussels, decidiu que o titular do cartão não age com negligência grosseira se descobrir um mês depois que o cartão desapareceu; noutro caso, o mesmo tribunal, defendeu que, perante a entrega da carteira por um terceiro depois desta ter caído, não é necessário verificar imediatamente se o cartão ainda se encontra guardado na carteira.

O cumprimento atempado deste dever será cada vez mais importante pela constante evolução e rapidez das transações, não sendo de esquecer o novo sistema de *Contactless* dos cartões para pagamentos presenciais de pequenos montantes (até €20), tornando possível fazer pagamentos apenas com a aproximação do cartão ao terminal[114].

2.5. Dever de reembolso imediato dos montantes de operações de pagamento não autorizadas

O RSP estabelece a regra geral quanto ao reembolso no seu art. 71.º n.º 1: "*o prestador de serviços de pagamento do* ***ordenante*** *deve reembolsá-lo imediatamente do montante da operação de pagamento não autorizada e, se for caso disso, repor a conta de pagamento debitada na situação em que estaria se a operação de pagamento não autorizada não tivesse sido executada*". Deve, no entanto, fazer-se uma interpretação corretiva da letra da lei nesta matéria, lendo-se *titular do IP fraudulentamente utilizado* ou "*titular de serviços de pagamento que negue ter autorizado uma operação de pagamento executada*"[115] no lugar de *ordenante,* pois aqui está em causa, precisamente, o facto do titular do IP nada ter ordenado. O ordenante será o terceiro que atua fraudulentamente (o mesmo deve fazer-se quanto ao art. 72.º do diploma).

Esta obrigação imposta ao prestador dos serviços de pagamentos não encontra, contudo, fundamento na tese que se vinha sedimentando na nossa jurisprudência de que o Banco deveria reembolsar o seu cliente com base na transferência de risco que ocorre a quando do depósito dos seus valores, tendo o dever de guarda desses bens[116].

Até 1 de novembro de 2009, dispunha o art. 10.º do D.L. n.º 143/2001, de 26.04, que, perante a utilização fraudulenta do cartão em operações à distância, o "*consumidor*" poderia solicitar a "*anulação*" do pagamento efetuado e a restituição dos montantes já debitados pela entidade emissora do cartão no prazo de 60 dias. Este era um regime imperativo, cominando com a nulidade qualquer estipulação em contrário. Assim, salvaguardava-se a posição do

---

[114] A Visa criou este novo sistema com base na fórmula "*shop, pay, go*", destinada aos pagamentos de pequeno valor, bastando a aproximação do cartão com esta tecnologia *Contactless* ao terminal do comerciante, sem digitar o PIN, até um montante diário frequentemente no valor de €60 – para maiores desenvolvimentos, veja-se o sítio: <http://clientebancario.bportugal.pt/pt-PT/instrumentosdepagamento/Cartoes/Paginas/CartoesContactless.aspx>.

[115] Assim, MARIA RAQUEL GUIMARÃES, "The debit and credit card framework contract and its influence on European legislative initiatives" *cit.,* p. 13. É também a expressão utilizada nos arts. 69.º e 70.º do diploma de 2009.

[116] Pode ler-se no Acórdão do TRL de 24.05.2012, *cit.*: "*dificilmente alguém poderá sustentar o razoável de o depositante individual suportar – ainda que em parte – o risco de a instituição de crédito a quem confiou os seus valores, se revelar afinal incapaz de assegurar a intangibilidade daqueles por terceiros*"; E no Ac. do STJ de 12.02.2009 (Helder Roque), "*considerando que ao contrato de depósito bancário se aplica o regime do contrato de mútuo, as coisas mutuadas tornam-se propriedade do mutuário pelo facto da entrega, correndo o risco do seu perecimento por conta do adquirente, ou seja, do banco devedor, que não fica exonerado pelo facto de desaparecerem das contas dos seus clientes os fundos com que se dispunha a cumprir, enquanto a prestação for possível com coisas do género estipulado, isto é, com dinheiro*", disponível para consulta no sítio <http://www.dgsi.pt> (19.02.2015).

titular – consumidor[117] – que via os dados do seu cartão utilizados por terceiros, só detetando tal operação ao receber o extrato mensal[118].

Este regime foi revogado pelo art. 9.º do diploma de 2009 e no novo regime dos direitos dos consumidores, introduzido pelo D.L. n.º 24/2014 de 14 de fevereiro[119], ressurgiu de forma efémera no art. 18.º – foi revogado pela Lei n.º 47/2014, de 28 de julho. Será, contudo, errado pensar-se que o regime atual é menos protetor[120]. Hoje, prevê-se a devolução *imediata*, estabelecendo as consequências da mora[121]: *"Sempre que o ordenante não seja imediatamente reembolsado pelo respetivo prestador de serviços de pagamento nos termos do número anterior, são devidos 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, calculados 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"* (cfr. art. 71.º n.º 2)[122]. Além disto, este regime estende a proteção, antes prevista apenas para os contratos celebrados à distância, também aos contratos presenciais, sendo independente do IP utilizado: cartões, sistemas de *homebanking* ou outros.

Foi intenção do legislador comunitário assegurar em primeiro lugar o reembolso do titular do serviço de pagamento, previamente à discussão da repartição da responsabilidade das partes. Desta forma, quem responderá pelos prejuízos, na relação entre titular do IP e entidade prestadora do serviço de pagamento, será esta e não o terceiro que atue fraudulentamente (a relação entre estes e o prestador do serviço colocar-se-á num outro plano)[123]. A transferência de fundos do prestador do serviço para o utilizador do IP

---

[117] O mesmo decreto-lei define consumidor como "*qualquer pessoa singular que atue com fins que não pertençam ao âmbito da sua actividade profissional*" (art. 1º, n.º 3, al. a)), não tendo em conta que nestas situações não é o titular que atua, mas o terceiro que age fraudulentamente. Este direito de exigir a "anulação" do pagamento fraudulento surge na relação entre o banco prestador do serviço de pagamento e o seu cliente, não no âmbito do contrato celebrado à distância, verificando essa qualidade no momento de adesão ao serviço.

[118] MARIA RAQUEL GUIMARÃES, "O pagamento com cartão de crédito no comércio eletrónico", *cit.,* p. 159.

[119] Procedeu à revogação do diploma relativo aos contratos à distância, resultando da transposição para a ordem interna da Diretiva n.º 2011/83/UE do Parlamento Europeu e do Conselho, de 25 de outubro de 2011, relativa aos direitos dos consumidores.

[120] A ideia de que a revogação desta norma provocou um retrocesso na proteção dos pagamentos feitos na internet foi largamente difundida pela comunicação social. Veja-se, por exemplo, a notícia publicada no jornal Público a 05.06.2014, disponível *in* <http://www.publico.pt/economia/noticia/maioria-revoga-art.-que-dava-maior-proteccao-nos-pagamentos-pela-internet-1638719> (24.02.2015). Não obstante o que se foi defendendo publicamente, a verdade é que esta norma não poderia coexistir com o RSP, porque o art. 86.º da Diretiva 2007/64/CE, que está na base deste regime, estabelece que esta é uma diretiva de harmonização plena. Os Estados-Membros não podem manter ou introduzir disposições diferentes, apenas é permitido aos prestadores de serviços de pagamento conceder condições mais favoráveis ao utilizador do serviço de pagamento. Porém, o art. 18.º vigorou entre 13 de junho e 29 de julho, momento em que entrou em vigor a Lei n.º 47/2014. O seu regime será, todavia, inaplicável às operações abusivas que possam ter acontecido nesse lapso temporal, por contrário à diretiva de harmonização plena.

[121] Enquanto aquele regime previa o reembolso no prazo de 60 dias, sem estabelecer qualquer consequência para a eventual mora do prestador do serviço

[122] Todavia, não conhecemos nenhuma decisão dos nossos tribunais que apliquem esta norma. Por exemplo, no Ac. do TRL de 21.05.2015 (Ezagüy Martins), onde se colocou a questão do cálculo de juros, o Tribunal, apesar de aplicar o RSP e, inclusive, tendo transcrito esta norma no texto do aresto, decidiu que os juros contam desde da citação e não desde que o titular negue ter consentido a operação.

[123] A entidade prestadora do serviço poderá agir contra estes terceiros, que responderão perante aquela. O titular, desconhecendo, na grande maioria das vezes, os terceiros que atuam abusivamente, procura a reparação dos prejuízos junto da entidade que melhor conhece: o seu banco. Até porque o titular do IP fraudulentamente utilizado não poderá intentar ações de regresso contra o comerciante que aceitou o seu

fraudulentamente utilizado justifica-se pelo cumprimento deste dever de devolução dos montantes debitados com base em operações abusivas, imposto pelo contrato de utilização e pelo RSP.

2.6. Dever de vigilância da entidade bancária relativamente aos fundos depositados pelo seu cliente

A atuação de vigilância da entidade prestadora do serviço sobre os fundos do cliente pode revelar-se fundamental contra operações fraudulentas, porque, por vezes, o titular do IP pode não detetar imediatamente essas operações**,** permitindo que nesse hiato temporal ocorram várias operações não autorizadas. Ainda assim, a existência de um dever de vigilância sobre os fundos do cliente é polémica. A lei não o consagra, mas deixa indícios da sua existência nos arts. 66.º n.º 2, a) e b)[124], e 73.º n.º 1 do RSP[125].

Admitindo a sua existência, terá o banco, no seu cumprimento, de ter em conta as operações habituais/o perfil/o padrão dos seus clientes? Pode fazê-lo, mas tratar-se-á de uma obrigação? Será a relação que se estabelece entre o banco e o seu cliente capaz de gerar este dever lateral de cuidado?

A lei, apesar dos indícios, não impõe um dever de vigilância, mas permite que o contrato preveja esta possibilidade. No nosso entendimento, será de afirmar a existência de um dever lateral de cuidado[126/127] com o património da contraparte. Trata-se de um dever assente na

---

cartão crédito sem conferir a identidade do utilizador. Como refere o Tribunal da Relação de Lisboa de 04.12.2006 (Luís Espírito Santo), "*não existe qualquer relação jurídica conexa susceptível de fundamentar o pretendido direito de regresso entre o dono do estabelecimento comercial e o titular do cartão de crédito*" - disponível *in* < http://www.dgsi.pt> (20.03.2015).

[124] Art. 66.º n.º 2: "*Mediante estipulação expressa no contrato quadro, o prestador de serviços de pagamento pode reservar-se o direito de bloquear um instrumento de pagamento por motivos objetivamente fundamentados, que se relacionem com:*
a) A segurança do instrumento de pagamento;
b) A suspeita de utilização não autorizada ou fraudulenta desse instrumento";
JANUÁRIO GOMES, *op. cit.*, p. 243, considera que este comportamento - bloquear o cartão - que "*considere adequadamente a situação efectiva ou presumível do ordenante: é um dever que resulta do princípio da boa fé*", tendo, necessariamente, de fazer-se uma interpretação hábil deste preceito quanto à referência ao *ordenante,* conforme a interpretação corretiva *supra* referida. Recorde-se, por fim, que o bloqueio que possa acontecer nestas circunstâncias não corresponde à resolução do contrato, mas à mera suspensão do segmento dos serviços associados ao IP.

[125] Art. 73.º n.º 1: "*O ordenante tem direito ao reembolso por parte do respetivo prestador do serviço de pagamento, de uma operação de pagamento autorizada, iniciada pelo beneficiário ou através deste, que já tenha executada, caso estejam reunidas as seguintes condições:*
a) A autorização não especificar o montante exato da operação de pagamento no momento em que a autorização foi concedida; e
b) O montante da operação de pagamento exceder o montante que o ordenante poderia razoavelmente esperar com base no seu perfil de despesas anterior, nos termos do seu contrato quadro e nas circunstâncias específicas do caso".

[126] Para ANTUNES VARELA, *Das Obrigações em Geral,* Vol. I, 10.ª ed., Coimbra, Almedina, 2010, p. 123, são deveres acessórios de conduta "*que, não interessando directamente à prestação principal, nem dando origem a qualquer acção autónoma de cumprimento (cf. Arts. 817.º e segs.*[CC]*), são todavia essenciais ao correcto processamento da relação obrigacional em que a prestação se integra*".

[127] JOEL TIMÓTEO RAMOS PEREIRA, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris, Lisboa, 2005, p. 873, ainda que com base no art. 9.º da Lei de Defesa do Consumidor n.º 24/96, defende tratar-se "*de um*

relação de confiança que se estabelece entre as partes no seio desta relação duradoura[128], da qual surgem, de acordo com pinto monteiro, "*deveres de colaboração e lealdade mútua, protecção dos interesses do cliente, prevenção, diligência e cuidado*"[129]. Iremos mais longe, defendendo existir um dever de informação perante as despesas ou movimentos estranhos em comparação com o perfil habitual do utilizador, o que, no fundo, corresponderá a um verdadeiro dever de vigilância[130].

Acompanhamos, assim, o Tribunal da Relação de Guimarães no seu Acórdão datado de 17.12.2014[131], onde se refere – numa analogia à atuação do Google, que constrói o perfil do utilizador com base na sua conta de correio eletrónico – a facilidade com que o prestador do serviço, principalmente as instituições de crédito, poderão traçar o perfil do utilizador, "barrando as operações a quem, v.g. pela hora tardia e inusitada, tenta fazer 'transferências' para terceiros, ou, pela repetição de transferências inusitada num curto espaço de tempo, enfim, tudo o que saia da normalidade que o cliente vem revelando". A Relação de Évora, no Ac. de 22.05.2014, foi mais peremptória, considerando que "atendendo ao perfil de utilizador do autor ao longo dos anos (…) denota não ter tido a diligência que se impunha relativamente à transacção em causa".

A afirmação deste dever, que para alguns bancos constituiu já uma boa prática, será mais um contributo para a segurança do sistema e para o aumento da confiança que os utilizadores depositarão no sistema proporcionado.

3. Utilização abusiva do Instrumento de Pagamento

O princípio basilar para a realização de operações de pagamento é claramente o da necessidade de autorização da operação de pagamento, que hoje encontra consagração expressa no art. 65.º do RSP, sob a epígrafe "consentimento e retirada de consentimento"[132].

---

dever colateral típico no âmbito de uma relação obrigacional complexa: o dever de protecção e cuidado para com a pessoa e o património dos intervenientes".

[128] HUGO LUZ DOS SANTOS, "Plaidoyer por uma 'distribuição dinâmica do ónus da prova' e pela 'teoria das esferas de risco' à luz do recente acórdão do Supremo Tribunal de Justiça, de 18/12/2013: o (admirável) 'novo mundo' no *Homebanking*?" *in RED - Revista Electrónica de Direito*, fevereiro de 2015, n.º 1, WWW.CIJE.UP.PT/REVISTARED (20.04.2015), p. 15, refere que "*emerge daquele (o contrato-quadro) um feixe de deveres de protecção, a cargo do prestador do serviço de* homebanking, *que se desdobram e autonomizam dos deveres acessórios de conduta, e que têm por finalidade conservar a actual situação jurídica dos bens de ambos os sujeitos da relação obrigacional complexa, tutelando-os contra ingerências lesivas na sua pessoa, na propriedade ou no seu património*".

[129] *Op. cit*., p. 379. Em sentido próximo, CALVÃO DA SILVA, "Conta corrente bancária: operação não autorizada e responsabilidade civil", *cit*., fala em "*deveres de protecção dos legítimos interesses do cliente*", p. 310.

[130] MARIA RAQUEL GUIMARÃES, *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos, op. cit., p. 317,* fala a este propósito na substituição do dever de ingerência por um dever de atuação, *"sempre que o banco de aperceba de operações inabituais pelos seus montantes, pela periodicidade ou volume, ou de operações originadas em países suspeitos e, portanto, passíveis de esconderem situações de fraude".*

[131] *Cit.,* disponível no sítio <http://www.dgsi.pt> (23.02.2015).

[132] Importa ter em conta que a retirada de consentimento só pode, logicamente, ocorrer até ao momento em que a ordem de pagamento se torna irrevogável, nos termos do art. 77.º. Qualquer operação de pagamento

Todavia, a fraude[133], que pode ocorrer no uso de IP eletrónicos, é o fator gerador de maior desconfiança e receio na sua utilização, constituindo, ainda, um entrave aos objetivos de expansão da sociedade de informação e ao comércio eletrónico[134/135].

a) No campo particular do uso dos cartões no comércio eletrónico, a principal dificuldade prende-se, maioritariamente, com a facilidade de autenticação por parte do utilizador do IP[136]. A realização destas operações não exige a posse do IP, só o conhecimento dos elementos gravados no próprio cartão: o número do cartão, a data de validade ou o código secreto presente nos cartões de crédito. Desta forma, poderá existir a indicação abusiva desses elementos por alguém que tenha contacto direto com o cartão ou, por alguma forma, os conheça. Também o terceiro que tenha a posse de um cartão válido extraviado, roubado, perdido ou copiado pode indicar o seu número de série, o nome do seu titular, a data de validade e o código de verificação impresso no seu verso, muitas vezes, suficiente para concretizar pagamentos *on-line*[137/138].

---

registada depois da sua revogação deve ser considerada não autorizada. Contudo, e apesar de o princípio geral nesta matéria ser a livre revogação do mandato, nos termos do art. 1170.º do CC, não pode aqui existir o pressuposto de que a partir da revogação não é possível a execução, pela celeridade das operações previstas do RSP. Como recorda JANUÁRIO GOMES, *op. cit.*, p. 250, "*estamos, na verdade, perante situações nas quais é de presumir que a execução se segue de imediato à ordem, por via electrónica, não podendo aplicar-se um regime pensado, digamos, para outra velocidade*".

133 Sobre a fraude virtual, veja-se LUIZ GUSTAVO CARATTI DE OLIVEIRA, *Responsabilidade civil dos bancos nos casos de fraudes pela internet que lesam as contas de seus clientes, in* <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=9110> (02.03.2015); Este autor explica que a fraude virtual *"(é) utilizada em muitos casos de crimes económicos, como (…) transferências de dinheiro, etc, (…) A fraude virtual é o crime de computador mais comum, mais fácil de ser executado, porém, um dos mais difíceis de ser esclarecido. Não requer conhecimento sofisticado em computação e pode ser cometido por qualquer pessoa que obtenha acesso a um computador e a uma linha telefónica. Tradicionalmente, a fraude envolve o uso de dados bancários roubados ou furtados"* (sublinhado do Autor). E continua: *"atualmente a fraude virtual mais aplicada na internet que prejudica o sistema bancário é a chamada 'salami slicing' ou seja, fatias de salame. Os ladrões utilizando vários recursos, realizam transferências eletrónicas, de pequenas quantias, de milhares de contas"*. Em sentido próximo, veja-se NICOLE VAN DER MEULEN, "You've been warned: Consumer liability in Internet banking fraud", *Computer Law & Security Review*, vol. 29 (2013), p. 713, *in* <http://www.sciencedirect.com> (01.02.2016).

134 São objetivos da União Europeia, presentes na nova Diretiva do Parlamento Europeu e do Conselho relativa aos serviços de pagamento no mercado interno, que altera as diretivas 2002/65/CE, 2013/36/CE e 2009/110/CE e revoga a diretiva 2007/64/CE. Os serviços de pagamento são, na nova Diretiva, destacados como "*essenciais para o funcionamento de atividades económicas e sociais da máxima importância*", sendo a "*evolução continuada de um mercado interno integrado de pagamentos eletrónicos seguros fundamental para apoiar o crescimento da economia da União*" – cfr. considerando 7 e 5.

135 CALVÃO DA SILVA, *Banca, Bolsa e Seguros, op. cit.*, p. 163, recorda: "O *desenvolvimento do comércio electrónico, também como seio de contratação de serviços financeiros (…) passa muito pela melhoria da segurança dos pagamentos na ou via internet, em ordem a aumentar e reforçar a confiança dos agentes económicos e dos consumidores /investidores e a sua protecção*".

136 Numa operação de pagamento presencial exige-se, normalmente, a autenticação do titular do cartão pela assinatura manuscrita semelhante à aposta no cartão, a apresentação de um documento de identificação ou, mais comum, pela marcação do código pessoal secreto - o PIN do cartão. Mas nos contratos à distância "*abdica-se destes procedimentos de segurança em ordem a facilitar a contratação*", como refere MARIA RAQUEL GUIMARÃES, *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos, op. cit.*, p. 298.

137 Esta circunstância levou a que alguma jurisprudência considerasse que "*o cartão de crédito como instrumento de pagamento e de crédito, não é ainda um meio seguro, designadamente no que respeita à protecção contra a sua utilização abusiva, mais propriamente a utilização não autorizada pelo respectivo titular, por terceiros, na sequência da sua perda ou furto*"- cfr. Ac. do TRP de 12.04.2010, *cit.*

138 Quanto às operações presenciais em que o cartão seja utilizado, existiu na jurisprudência a tese de que sendo o cartão utilizado com indicação do PIN, se presumia a utilização pelo seu titular, cabendo ao mesmo demonstrar que não realizou a operação – veja-se, a título de exemplo, o Ac. do TRL de 16.06.1994 (Noronha de Nascimento), disponível *in* <http://www.dgsi.pt> (10.03.2015), e o Ac. do mesmo Tribunal de 19.01.2006 (Manuel Gonçalves), *CJ*, n.º 188, ano XXXI tomo I/2006, pp. 80-82; Na sentença de 27.09.2012 do Julgado de Paz (Luís Filipe Guerra), onde o cartão de crédito é utilizado presencialmente, defendeu-se não bastar ao

Aqui acresce a técnica de *phishing*[139], frequentemente utilizada, que consiste no uso intensivo do *spam* – são enviados milhares de mensagens na tentativa de obter aquelas informações dos titulares dos cartões, tendo as mensagens uma aparência fidedigna, de mensagens provenientes da própria instituição de que o destinatário é cliente. O destinatário é convidado a clicar numa hiperligação que conduz o utilizador a um *site* falso, onde insere os seus dados pessoais, ou a descarregar um anexo que instala um programa malicioso no computador, guardando as informações sensíveis do seu utilizador. Estas mensagens com aparência legítima, podem, ainda, simplesmente convidar o destinatário a indicar os seus dados (número de conta, senhas, etc.) com base numa suposta necessidade de atualização de dados do banco, proporcionando as informações pessoais que permitirão o acesso à sua conta bancária. No fundo, no uso das certeiras palavras do Tribunal da Relação do Porto no Acórdão de 07.10.2014, "o *phishing*, numa primeira fase consiste na apropriação de informações de outra pessoa (…) para serem utilizadas fraudulentamente nas fases seguintes da trama".

Ainda no que respeita a cartões de plástico, poder-se-á verificar a duplicação ou contrafação de cartões através de cartões roubados, perdidos ou intercetados, ou pela técnica de *skimming*. Este método consiste na cópia dos dados encriptados gravados na fita magnética do cartão por meio de um aparelho colocado numa caixa automática (ATM) ou no próprio estabelecimento comercial onde o cartão é utilizado em operações presenciais, transferindo-os para um cartão falso. O cartão contrafeito ou *clonado* é depois utilizado em operações presenciais (refletindo na fatura emitida na compra a leitura magnética do cartão verdadeiro), como em operações de comércio eletrónico.

A utilização fraudulenta dos dados do cartão na internet, em operações de *card-not-present*, obtidos por qualquer dos meios apresentados ou em operações presenciais, onde o cartão é manuseado por terceiro, será o problema mais comum e que ocorrerá mais vezes no comércio eletrónico[140].

"*titular invocar que não foi ele quem efectuou as mesmas transacções, para o eximir do seu pagamento (…) carecia de provar que não foi ele quem utilizou o seu cartão de crédito em cada uma das três operações controvertidas e que essa utilização não decorreu de incumprimento do seu dever de guarda e manutenção do cartão",* disponível *in* <http://www.dgsi.pt>.
Contudo, é hoje sólida a tese de que cabe ao prestador do serviço a prova de que o uso do cartão com os dispositivos de segurança que lhe estão associados se deve a culpa do titular. STEPHEN MASON, "Electronic banking and how courts approach the evidence" *in ScienceDirect - Computer Law & Security Report,* volume 29, 2013, pp. 147 e 148, <http://www.sciencedirect.com> (12.11.2014), apresenta uma decisão do Supremo Tribunal da Lituânia (ZS vs Lietuvos taupomasis bankas) onde se defende que será o banco quem está na melhor posição para fazer essa prova, por controlar e ser o responsável pela segurança do sistema. Nesta medida, é a este que cabe o ónus da prova de que as medidas de segurança foram quebradas e que o cartão foi utilizado com todos os seus dados por culpa do cliente.

[139] A expressão deriva do verbo inglês "*fishing"* que significa pescar. Esta técnica permite ao *hacker* conhecer os dados do cartão para utilizações fraudulentas em operações não presenciais, conhecidas como "*card-not-present*". No fundo, como caracteriza DEMÓCRITO REINALDO FILHO, "A Responsabilidade dos bancos pelos prejuízos resultantes do 'phishing'", *Jus Navigandi*, Teresina, ano 13, n.º 1838, julho 2008, disponível *in* <http://jus.com.br/artigos/11481> (09.03.2015), a mensagem funcionará como "isca", sendo o *phishing,* "*uma modalidade de spam em que a mensagem além de indesejada é também fraudulenta (scam)".*

[140] Acreditamos, todavia, que não será o uso do cartão em compras *on-line* que torna este instrumento inseguro ou fragiliza especialmente a segurança que lhe está associada. Na verdade, a sua utilização em operações presenciais possibilitará, com maior facilidade, o conhecimento dos seus dados por terceiros. Na mesma linha, MARIA RAQUEL GUIMARÃES, "A fraude no comércio electrónico: o problema da repartição do risco por

b) No uso do *homebanking*, o risco de utilização abusiva e fraudulenta é potenciado pela realização de operações através de qualquer computador ou telemóvel com acesso à internet, como espaço aberto, e não na rede controlada do banco (intranet)[141], impondo-se a este um especial dever de informação sobre os riscos e métodos mais comuns de fraude[142]. A divulgação de avisos/alertas na página inicial do serviço de banca eletrónica, que terão de ser fechados para introduzir os dados pessoais de acesso, será uma forma de cumprir esta obrigação de informação[143].

O utilizador, para realizar uma operação de banca electrónica, terá de conhecer um conjunto de códigos secretos que deverá inserir para que o banco verifique a coincidência entre aquele que solicita o acesso ao serviço eletrónico e o cliente que celebrou o contrato de utilização, servindo, consequentemente, para imputar a operação àquele titular do serviço.

O acesso não autorizado à conta do titular pode aqui ser conseguido pela quebra de segurança do sistema controlado pelo banco, havendo a interceção das senhas enquanto estão a ser digitadas (conhecido por *keylogging*), mas será mais comum ser conseguido através do uso dos códigos de acesso do utilizador. Os dados pessoais (número de conta ou de contrato, senha e os códigos de validação das operações) serão conhecidos pelo terceiro que atua fraudulentamente através de ataques de *phishing*[144] ou pela técnica de *pharming.*

O pharming é uma modalidade de fraude mais sofisticada na medida em que o utilizador é redirecionado pelo programa de navegação (*browser*) instalado no seu computador para uma página falsa, em tudo semelhante à verdadeira, quando digitaliza o endereço correto do serviço de banca *on-line*[145/146]. Esta modalidade pode ser dirigida, não só a um computador

---

pagamento fraudulentos" *in Infracções Económicas e Financeiras: Estudos de Criminologia e de Direito,* Coimbra, Coimbra Editora, 2013, p. 588, chama a atenção que o uso do cartão no comércio eletrónico "*apenas acresce às demais situações de utilização do cartão e, portanto, constitui uma hipótese adicional de conhecer os seus dados relevantes".*

[141] Os riscos serão potenciados pela realização de operações num espaço aberto e não nos computadores disponibilizados no interior dos balcões ou nos ATM.

[142] Para MARIA RAQUEL GUIMARÃES, "A repartição dos prejuízos decorrentes de operações fraudulentas de banca electrónica (homebanking)", *cit.,* p. 62, trata-se do cumprimento de um dever lateral de conduta, "*um dever imposto à entidade bancária de explicar as situações mais comuns de fraude e os perigos específicos dos diferentes serviços que fornece, em função do tipo de utilizador envolvido e dos seus conhecimentos técnicos*".

[143] O TRG considerou, no Ac. datado de 25.11.2013, que a entidade prestadora do serviço cumpria este dever, mesmo antes de existir estas mensagens de alerta, ao colocar num menu do *site* "*toda a informação disponível sobre segurança, que os utentes têm o dever de consultar, para prevenirem fraudes*".

[144] PEDRO VERDELHO, "*Phishing* e outras formas de defraudação nas redes de comunicação" *in Direito da sociedade de informação,* Vol. III, Coimbra, Coimbra Editora, 2009, p. 413, refere que o *phishing* está "*actualmente mais dirigido para a defraudação na área do* homebanking", sendo que no *e-mail* surge o *link* de acesso à página falsa do banco.

[145] Haverá no computador do titular do IP um software malicioso que automaticamente direciona o utilizador para a página "clonada". Nestes casos, o utilizador não recebe um *e-mail*, nem necessita de clicar num link, é redirecionado para o *site* falso mesmo escrevendo o endereço correto da página do banco. DEMÓCRITO REINALDO FILHO, *op. cit*., recorda que "*ao contrário do* phishing*, o qual uma pessoa mais atenta pode evitar simplesmente não respondendo ao e-mail fraudulento, o* pharming *é praticamente impossível de ser detetado por um usuário comum da internet, que não tenha maiores conhecimentos técnicos*". Também o BdP apresenta este método como mais sofisticado e mais difícil de detetar, apresentando uma página destinada à descrição de alguns dos cuidados a ter, em <www.bportugal.pt> (11.11.2014).

[146] Tal aconteceu num caso colocado ao TRP no Ac. de 29.04.2014 (Francisco Matos), onde "*uma fraude informática levada a efeito por terceiros clonando a página do R. fizeram crer ao A. que estava no site do Réu/homebanking levando aquele a fazer as suas certificações e operações usuais".*

pessoal mas a um servidor DNS (*Domain Name System*), sendo apelidado de "*DNS poisoning".* Neste caso, serão atingidos um enorme número de utilizadores que digitem o endereço (URL) correto da página de *homebanking,* que automaticamente, por alteração do endereço armazenado no DNS, são redirecionados para a página falsa[147].

Nestas páginas falsas, o utilizador indica os códigos pessoais (número de contrato e senha) que permitem ao terceiro aceder à conta na página verdadeira. É, com frequência, pedida a atualização do cartão de coordenadas, vulgarmente conhecido como cartão matriz[148]. Este pedido, leva o titular menos atento a indicar todos as combinações da sua matriz, permitindo ao terceiro a conclusão das operações de pagamento[149].

São, precisamente, estes os casos de fraude informática no seio deste serviço de pagamento que mais têm chegado aos nossos tribunais. No Acórdão de 23.10.2012 do Tribunal da Relação de Guimarães, foi dado como provado que o utilizador "forneceu todas as combinações de números do seu cartão matriz de acesso à sua conta bancária relativo àquele serviço e do cartão matriz dos autores seus pais, por tal lhe ter sido pedido pela internet (…) ao fornecer a terceiros desconhecidos os dados pessoais, secretos e intransmissíveis dos autores no acesso às suas contas, foi vítima de *phishing*, por *hacker* da *internet*". Contudo, pela descrição dos factos, não parecerá tratar-se de uma situação de fraude através da técnica de *phishing,* mas de *pharming*. Em nenhum momento resulta do Acórdão que os códigos pessoais fossem cedidos em resposta a uma mensagem de correio eletrónico[150].

A confusão entre estas duas técnicas de fraude é também manifestada pelo mesmo Tribunal na decisão de 30.05.2013. Neste caso, a factualidade descrita no Acórdão torna ainda mais clara a afirmação de que existiu fraude através da técnica de *pharming*: é relatado que o banco reconheceu a "existência de uma página web falsa, imitando a sua página de abertura"[151]. A confundibilidade entre os conceitos foi, quanto a este caso, resolvida pelo Supremo Tribunal de Justiça. O nosso mais alto Tribunal vem, assim, esclarecer "estar-se em presença de uma fraude de *pharming,* não de *phishing*, posto que esta técnica pressupõe a

[147] A página verdadeira é "sequestrada", conduzindo para o *site* falso todas as pessoas que tentam aceder àquela. Para maiores desenvolvimentos, veja-se o estudo de DEMÓCRITO REINALDO FILHO, *op. cit.*, onde estes conceitos são apresentados com enorme clareza. Este estudo, com todas as suas virtudes e defeitos, foi seguido de perto pelo TRP no Ac. de 07.10.2014, *cit.*, para resolução da questão de fraude informática colocada a este tribunal. E, ainda, 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;

[148] Nos sistemas de *homebanking* em que não é usado cartão de coordenadas, mas o envio do código por SMS, pelo hacker é normalmente pedido informações acerca do telemóvel do utilizador (marca, modelo e sistema operativo), recebendo o utilizador um código por mensagem, é pedido para também o indicar na página falsa. Uma destas situações foi colocada ao TRP no Acórdão de 29.04.2014, *cit*.

[149] Como caracteriza o TRG, no Ac. de 25.11.2013, *cit.*, "*uma vez na posse de todos os dados de validação, o pirata informático passa no sistema como se* [do titular] *se tratasse, cumprindo todas as ordens que lhe forem solicitadas*. *O sistema não tem a virtualidade de distinguir o verdadeiro do falso dono. Apenas conhece as credenciais de validação, e uma vez introduzidas, quem as digitalizou é reconhecido como se fosse o verdadeiro dono".*

[150] No mesmo sentido, manifestou-se MARIA RAQUEL GUIMARÃES, na análise deste acórdão, *in* "A repartição dos prejuízos decorrentes de operações fraudulentas de banca electrónica (homebanking)" *op*. *cit.,* p. 63.

[151] O Tribunal bem define *phishing* como uma técnica de fraude que ocorre por "*email, mensagem instantânea, SMS, dentre outros",* mas entendeu que a situação ocorrida é *"idêntica, àquelas que usualmente são designadas de* 'phishing*'* ".

abertura e resposta a *spamming* de mensagens de correio eletrónico (…) este acesso directo a uma página, que pensamos ser a verdadeira, é o elemento caracterizador do *pharming*"[152].

O maior desafio na utilização *on-line* dos IP será, precisamente, o de superar os riscos de fraude, aumentando a segurança e confiança dos utilizadores da internet[153]. Os prestadores de serviços de pagamentos disponibilizam informações sobre as boas práticas a adotar nos pagamentos pela internet, porque a execução destas operações implica, naturalmente, a divulgação dos dados de identificação da conta ou do cartão. Quanto aos cartões, é aconselhável a utilização de IP com características de segurança acrescida (saldo/plafond limitado ou prazos de validade mais curtos) ou o uso de sistemas como o MBnet – permite a criação de um cartão de pagamento virtual e temporário (de uma utilização ou mensal), a que pode ser atribuído o *plafond* necessário para o pagamento pretendido, realizando compras *on-line* sem fornecer dados do cartão de pagamento verdadeiro. O utilizador deverá, igualmente, evitar aceder à página do serviço de banca ao domicílio ou fazer pagamentos em computadores públicos, manter o antivírus atualizado, não clicar em hiperligações apresentadas em *e-mails*, digitar o endereço da página de *homebanking,* entre outros cuidados necessários a preservar a segurança do sistema de pagamentos eletrónicos e que poderão ser analisados pelos tribunais na ponderação da atuação do utilizador. Quanto a nós, cabe-nos definir a responsabilidade pela utilização abusiva *on-line* do IP eletrónico, tentando, também, contribuir para a indispensável fiabilidade e credibilidade dos sistemas de pagamento[154].

4. Repartição dos prejuízos causados por operações não autorizadas

Atribuímos a este capítulo a epígrafe de repartição dos prejuízos, pela consideração de que não estamos perante, pelo menos não o será em todos os casos, uma verdadeira questão de

[152] Da decisão do TRG coube recurso para o STJ, que se pronunciou no Acórdão datado de 18.12.2013, *cit.* O Tribunal defendeu: *"a designação (…) no que tange à técnica electrónica utilizada (…) pode e deve ser corrigida por este Supremo Tribunal".* Este esclarecimento será de enorme utilidade para que a jurisprudência demonstre um maior rigor e à-vontade no tratamento destas situações de fraude. Todavia, a tese de que "*quer fosse uma das técnicas ou a outra, qualquer delas consubstancia fraudes informáticas, conduzindo aos mesmos resultados em termos de responsabilidade*" terá de ser entendida com alguma cautela. Na verdade, a atuação do utilizador perante cada um destes ataques será diferente, assim como a censura de que possa ser alvo (permitimo-nos remeter para o que foi dito na nota n.º 145).

[153] Os esforços das entidades prestadoras dos serviços de pagamentos poderão ser, e cada vez mais são, direcionados também à vertente de detetação de operações fraudulentas, num campo de prevenção concreta, feita com base no perfil do utilizador. Este trabalho, passará pela classificação ou distinção entre operações legítimas e operações fraudulentas. Para maiores desenvolvimentos sobre a matéria, *vide* ADNAN M. AL.KHATIB "Electronic Payment Fraud Detection Techniques" *in World of computer Science and Information Tecnology Journal (WCSIT),* Vol. 2, N.º 4, 2012, pp. 137 a 141.

[154] Com a definição da responsabilidade pelas operações abusivas operadas como consequência da ocorrência de práticas fraudulentas, esperamos contribuir para aumentar a clareza jurídica da questão, diminuindo a incerteza acerca de quem e em que medida suporta estes prejuízos e ajudando a desdramatizar (quase desmitificar, em alguns casos) o processo de repartição dos prejuízos, que será para muitos um obstáculo à finalização de contratos *on-line*.

responsabilidade, mas de repartição do risco[155]. Como é afirmado pelo Supremo Tribunal de Justiça, "podem ocorrer prejuízos causados pela actuação de terceiros (…) apesar de nem o utilizador nem o Banco emissor terem tido qualquer conduta negligente adequada a provocar tais prejuízos. Caímos, então, no domínio da repartição da responsabilidade pelo risco ou, segundo alguns autores, perante uma questão de responsabilidade pelo risco"[156/157].

A questão da repartição dos prejuízos pelas partes no contrato é, verdadeiramente, a questão mais sensível no âmbito da utilização fraudulenta de IP. Os nossos tribunais resolveram muitos dos casos que lhes foram colocados com base nas regras relativas ao depósito irregular e ao contrato de mútuo[158], a que tivemos já oportunidade de referir a nossa discordância, pois tal significa retirar autonomia ao contrato de utilização do IP, excluindo-o muitas vezes do contexto decisório. A solução assente na transferência do risco que ocorre com a entrega da coisa nos contratos de mútuo, tornava desnecessária a ponderação de quem deve suportar os prejuízos. Como refere o Tribunal da Relação de Lisboa, a questão da repartição do risco é "excluída quando se pressupõe, como é o caso, a transferência da propriedade do dinheiro depositado para o banco depositário"[159]. Os Tribunais não poderão, também, deixar de fazer esta ponderação, limitando-se a condenar os prestadores dos serviços de pagamento a suportar todos os prejuízos das operações fraudulentas com base na caracterização desses valores como "uma gota de água no oceano do volume de negócios do banco"[160].

---

[155] A repartição de prejuízos de que estamos a tratar é feita no seio da relação prestador do serviço/cliente. O verdadeiro "responsável", civil e criminalmente, será o terceiro que concretiza as operações abusivas. Ressalvamos, contudo, que também há situações em que as partes contribuíram para a utilização ilícita do IP. Situações em que as operações fraudulentas foram consequência, ainda que não direta, de comportamentos descuidados ou negligentes, em violação das obrigações assumidas no contrato de utilização e que identificamos no presente trabalho. AMÁVEL RAPOSO, *cit.*, pp. 18 e ss., tratava a questão distinguindo a *responsabilidade baseada na culpa* e a *responsabilidade pelo risco*.

[156] Cfr. Acórdão do STJ de 16.03.2004 (Moreira Alves) *CJ - STJ*, n.º 173, Ano XII, Tomo I/2004, janeiro/fevereiro/março, p. 131.

[157] JANUÁRIO GOMES, *op. cit.*, p. 218, expressa a mesma ressalva: "*conquanto os textos normativos e contratuais refiram, com frequência, a responsabilidade, estamos, no essencial perante matéria de risco, salvo no caso - que é de responsabilidade – em que o emitente do cartão, regularmente notificado pelo titular, permite, ainda assim, a continuação da utilização irregular do cartão por parte de terceiros".* Apesar do Autor identificar apenas este caso, será de recordar que também o titular do IP poderá, conforme a sua atuação, ser alvo de censura, tendo de suportar parte destes prejuízos nos termos do RSP.

[158] O Acórdão do TRL de 24.05.2012 discute a natureza do depósito bancário, numa tentativa de perceber se este estará mais próximo do contrato de depósito, ainda que irregular, ou do contrato de mútuo. O Tribunal entendeu que qualquer das "*abordagens referenciadas remeter-nos-ão para resultados finais idênticos, quando não por via da consideração da transferência do domínio da coisa e, consequentemente, da transferência do risco, por via da obrigação de restituição no mesmo género e qualidade que (…) impende sobre o banco, por aplicação das regras do mútuo"*. O Tribunal identifica o contrato de utilização da banca eletrónica, no seio do qual surge a relação controvertida que lhe é colocada, mas não lhe confere a autonomia suficiente no sentido de responder cabalmente ao caso no âmbito do mesmo, com base no cumprimento das suas obrigações contratuais. Defende que apesar da "*diferenciação da sede formal dos contratos, o de serviços de "B" Online interfere diretamente na área normativa própria do contrato de abertura de conta e de depósito*". É verdade que o reembolso será feito, logicamente, porque existe o depósito anterior, mas terá de fazer-se uma repartição dos prejuízos entre as partes (ponderação prejudicada neste entendimento).

[159] Cfr. Ac. de 24.05.2012, *cit.*

[160] Tal caracterização foi feita pelo TRL no Ac. de 26.10.2010. O tribunal defendeu ainda que a quantia peticionada pelo titular do IP fraudulentamente utilizado estaria, para o banco, "*no plano das insignificâncias mas, para a A., não será exagero afirmar, estará no domínio da própria subsistência"*. Não esquecendo a importância social das decisões judiciais, não entendemos que este argumento se trate, na verdade, de um argumento jurídico. Por outro lado, não podemos perder de vista que tal não será afirmado apenas perante um cliente, mas perante uma miríade de potenciais casos.

Acreditamos que é no âmbito do contrato, que permite ao cliente o uso de um IP eletrónico, que deve ser distribuído o risco e analisadas as posições do banco e do cliente[161].

No uso eletrónico do IP, encontramo-nos no âmbito de sistemas informáticos que permitem concretizar as operações de pagamento, mas comportam naturalmente riscos[162]. A segurança do sistema estará dependente da atuação diligente de todos os seus utilizadores e intervenientes. Assim, há-de fazer-se uma repartição dos prejuízos entre as partes, tendo em consideração a atuação de cada uma delas no cumprimento dos deveres que lhe são impostos pelo contrato[163]. Nas palavras do Tribunal da Relação de Lisboa, ainda que se referindo especificamente aos cartões, "(a) responsabilidade pela utilização fraudulenta de um cartão de crédito, por um terceiro, deverá ser repartida entre o titular do cartão e o emitente do mesmo, com base numa ideia de distribuição equitativa dos prejuízos causados, na medida do incumprimento dos deveres contratuais que sobre cada um impende, decorrentes do princípio geral da boa fé"[164]. Atualmente, o RSP estabelece um regime de repartição dos prejuízos baseada na culpa que possa ser imputada ao titular do IP abusivamente utilizado[165/166]. A prova de que este agiu com negligência grave ou violou

---

[161] Consciente desta realidade mostrou-se o Tribunal da Relação de Lisboa no seu Acórdão datado de 15.06.2010, *cit.*, recordando que "*ao lado do contrato de depósito bancário e com ele articulado ou conexo existe o contrato de utilização do cartão, por força do qual o seu detentor adquire a disponibilidade directa e imediata sobre os fundos depositados, podendo-os movimentar e/ou levantar, sem que o depositário nisso tenha qualquer intervenção. Daqui resulta, pois, que em primeira linha, importaria analisar o clausulado do contrato de utilização do cartão*".

[162] Nas primeiras decisões jurisprudenciais sobre a matéria, foi salientado que o titular é completamente alheio à escolha do sistema informático e de segurança do banco, sendo um risco da instituição. Pode ler-se no Ac. de 16.03.2004 do STJ: "*é o Banco (ou empresas associadas) que gere o sistema informático colocado à disposição dos seus clientes, sobre os quais estes não têm o menor controlo. É o Banco que, no âmbito da sua liberdade organizativa, investe mais ou menos no nível de segurança do sistema… Consequentemente, tais falhas do sistema traduzem simplesmente o risco que a sua utilização envolve, risco esse que deve correr por conta do banqueiro, face aos princípios gerais da boa fé contratual e à confiança que justifica que o cliente entregue à guarda do banqueiro o seu dinheiro. Enfim, estamos perante aquilo a que a doutrina chama 'risco de empresa'* ". Este entendimento foi partilhado por alguma doutrina, a título de exemplo, veja-se ALICE MEDEIROS, "Responsabilidade pelo uso fraudulento de cartões de crédito", *in Conflitos de Consumo*, Almedina, março de 2006, p. 178: "*embora a questão da responsabilidade sobre o uso fraudulento de cartões seja uma questão sem resposta clara na lei, a solução apresentada parece ser a mais condizente com a maior facilidade que a entidade bancária ou financeira tem de controlar esse uso fraudulento*".

[163] MARIA RAQUEL GUIMARÃES, *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos, op. cit.,* p. 303, recorda: "*Existe todo um conjunto de hipótese de condutas mais ou menos diligentes que os tribunais podem ponderar na avaliação da contribuição do titular para a potenciação do risco de fraude*".

[164] Cfr. Acórdão do TRL (Ondina Carmo Alves) datado de 04.07.2013, acessível em <http://www.dgsi.pt> (consultado a 22.02.2015).

[165] A responsabilidade do titular do IP é amplamente prevista no art. 72.º do RSP. O TRL, no Ac. de 05.11.2013 e de 03.03.2015, *cit.*, entendeu que a responsabilidade estabelecida n.º 1 deste artigo – até €150 – é feita a "*título de culpa leve ou risco*". O segundo nível de responsabilidade previsto respeita às situações onde o titular demonstre negligência grave. O Ac. de 17.12.2014 do TRG identificou, citando ANA PRATA, esta negligência como "*negligência grosseira, erro imperdoável, desatenção inexplicável, incúria indesculpável, vistos em confronto com o comportamento do comum das pessoas, mesmo daquelas que são pouco diligentes*". Está ainda prevista a hipótese de fraude ou incumprimento deliberado das suas obrigações (dolo). O mesmo Tribunal recorda que a "*Directiva equipara, quanto aos efeitos, a actuação com negligência grave à actuação fraudulenta, mas o nosso legislador interno optou por uma graduação até ao limite 'do saldo disponível' ou 'da linha de crédito associada à conta ou ao instrumento de pagamento' em função 'da natureza dos dispositivos de segurança personalizados do instrumento de pagamento e das circunstâncias da sua perda, roubo ou apropriação abusiva' "*, quanto à negligência grave, assumindo todos os prejuízos o titular que atue fraudulentamente ou com dolo.

[166] Não sendo provada a culpa do titular, será à entidade prestadora do serviço que cabe suportar todos os prejuízos. Como refere MARIA RAQUEL GUIMARÃES, "A repartição dos prejuízos decorrentes de operações fraudulentas de banca electrónica (*home banking*); Anotação ao Acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09", *in Cadernos de Direito Privado*, n.º 41, Janeiro/Março 2013, p. 65, "*é o prestador de serviço de pagamento electrónicos – independentemente da modalidade de instrumento de*

deliberadamente alguma das suas obrigações cabe, nos termos do art. 70.º n.º 1[167], à entidade prestadora do serviço[168].

Importa recordar que esta problemática respeita apenas aos prejuízos das operações fraudulentas registadas antes da notificação feita pelo titular à entidade prestadora do serviço, posteriormente à comunicação será o prestador do serviço de pagamento quem suporta todos os prejuízos, exceto se o titular agiu fraudulentamente[169]. Desde 2009, sobre este recai a obrigação de "*impedir qualquer utilização do instrumento de pagamento logo que a notificação (…) tenha sido efectuada*"[170/171], sendo para este efeito indiferente o momento em que a comunicação é feita.

Muitos dos Acórdãos analisados respeitam a factos anteriores à entrada em vigor do RSP, não sendo regulados por este regime, que, naturalmente, não poderá aplicar-se a factos anteriores, ainda que, nos termos do art. 101.º, se aplica aos contratos em vigor, desde que as suas disposições "*se mostrem mais favoráveis aos utilizadores de serviços de pagamento*"[172]. Não obstante, tentaremos fazer um enquadramento dos mesmos na disciplina introduzida, tendo em conta que muitas das suas soluções encontravam-se já consagradas em várias recomendações comunitárias elaboradas nas décadas de 80 e 90.

O Tribunal da Relação de Lisboa no Acórdão de 20.10.2011, recorda que, mesmo sem carácter vinculativo, "o DL 166/95 de 15/7 prescreve no seu art.3º que as entidades emitentes de cartões bancários, ao elaborarem as respectivas condições gerais de utilização, deverão ter em conta as recomendações emanadas da União Europeia (…) Acresce que, esse

pagamento utilizado – que deve arcar com os danos potenciados pelas fragilidades dos sistemas de pagamento que comercializa".

[167] A norma prescreve: "*Caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, ou alegue que a operação não foi corretamente efetuada, incumbe ao respetivo prestador do serviço de pagamento 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*".

[168] Neste sentido, manifestou-se o STJ no Ac. de 18.12.2013, defendendo que ao prestador do serviço cabia o "*ónus de alegar e provar que a operação de pagamento fora autorizada pela autora, ou que esta agira de forma fraudulenta ou que não cumprira, deliberadamente ou por forma gravemente negligente as suas obrigações contratuais, cfr artigos 70º, nº3 e 72º, nº1 (continuamos no âmbito de presunções, as quais decorriam já do disposto no artigo 796º, nº1 do CCivil, que o aqui recorrente não logrou afastar)*". Posição assumida por outras instâncias, e recentemente pelo TRL, no Ac. de 03.03.2015, dizendo-se que "*o utilizador não podia ser colocado na necessidade de fazer prova sobre o funcionamento de um sistema informático complexo da entidade bancária e que não domina*".

[169] Além das referências jurisprudenciais já citadas a este propósito, veja-se o que é dito no Ac. do TRP datado de 12.04.2010, *cit.: "A comunicação à instituição emissora do cartão desonera o titular de qualquer responsabilidade pelo uso abusivo do cartão a partir desse momento, fazendo recair sobre essa instituição toda a responsabilidade*". Esta solução não é, contudo, inteiramente correspondente ao que se previa no Aviso do BdP n.º 11/2001 de 20 de novembro. No seu art. 8.º n.º 6 previa-se que o titular que agisse fraudulentamente ou com negligência grave, responderia pela totalidade das perdas, mesmo que posteriores à comunicação.

[170] Cfr. art. 68.º n.º 2 do RSP.

[171] Tivemos já a oportunidade de demonstrar, a propósito da identificação do dever imposto a esta entidade de imediato cancelamento do IP, que a jurisprudência anterior ao diploma de 2009 fazia, igualmente, recair sobre a entidade prestadora do serviço o risco das operações registadas posteriormente à notificação do titular. A regra está hoje consagrada no art. 72.º n.º 4 do RSP.

[172] Este regime jurídico só se aplicará, assim, a factos ocorridos a partir de 1 de novembro de 2009. Estranhamente, o STJ aplica o RSP retroativamente aos factos analisados no Ac. de 18.12.2013, com base no seu art. 101.º.

entendimento também é defendido pelo aviso do Banco de Portugal n.11/2001, de 6.11 (D.R.I, Série B, de 20.11.2001)"[173/174].

Apesar do dever que se impõe ao prestador do serviço de pagamento de reembolsar de imediato o titular do IP que negue ter autorizado as operações realizadas, a questão de quem e em que medida suportará os prejuízos continua a revelar-se de extrema importância. Todavia, este dever permite que esta discussão seja feita pelo titular do IP colocado numa posição de maior conforto, garantindo-lhe, o imediato reembolso dos valores debitados com base nas operações não autorizadas.

A repartição equitativa dos prejuízos, que nos propomos apresentar, será, também, um meio de tornar o sistema de pagamentos mais seguro, pelo incentivo à diligência de ambas as partes no cumprimento dos deveres que lhe são impostos pelo contrato de utilização do IP[175].

Algumas das soluções foram já adiantadas ao longo do texto, mas analisemos a repartição dos prejuízos emergentes das operações abusivas decorrentes de cada tipo de fraude estabelecida no RSP, comparando-a com o que vem sendo decidido pela nossa jurisprudência.

4.1. Cartões

a) Nas operações realizadas com cartões intercetados antes da chegada à posse do titular, já o dissemos, será o prestador do serviço quem suportará as perdas decorrentes das operações realizadas com o cartão apropriado[176]. Este era já o entendimento da jurisprudência, afirmado no Acórdão do Tribunal da Relação de Coimbra datado de 15.06.2010, que, com base nos Avisos do Banco de Portugal[177], configura a obrigação de

[173] Cfr. Ac. do TRL de 20.10.2011 (Catarina Arêlo Manso), *cit.;* No mesmo sentido, veja-se os Ac. do STJ de 15.05.2008 e de 02.03.2010, *cit*.

[174] Este entendimento justificaria também que os tribunais não recorressem às regras comuns para resolverem os litígios que lhes eram colocados, podendo responder, pelo contrário, com muitas das soluções que hoje encontram consagração no RSP. O percurso argumentativo das instâncias seria significativamente diferente, ainda que a solução material dada pudesse ser semelhante.

[175] Na mesma linha, o Ac. do TRC datado de 15.06.2010, *cit.:* "*será a solução mais justa e equitativa e reforça a segurança do sistema, na medida em que incentiva a diligência dos contraentes*".

[176] No mesmo sentido, MARIA RAQUEL GUIMARÃES, "(Ainda) a responsabilidade pelo uso indevido de instrumento de pagamento electrónicos em operações presenciais e à distância", *cit.,* p.126;

[177] O Tribunal entendeu ser intenção do Aviso do BdP n.º 11/2001, com o uso das expressões "*especial cuidado*" e "*adequadas regras de segurança*", exigir aos "*bancos emissores de tal tipo de cartões que, ao proceder ao respectivo envio ou entrega ao seu titular, se rodeiem de todas as cautelas de forma a evitar que o mesmo seja recebido ou entregue a um terceiro*". Hoje, a solução é ainda mais clara, porque a lei, além de prever este dever de envio, expressamente faz recair sobre o emitente o risco das operações fraudulentas realizadas antes do cartão chegar ao seu legítimo titular, incentivando a uma maior diligência e cuidado no envio do IP.

envio como um dever fundamental que permite ao legítimo titular do cartão usufruir de todos os serviços que o mesmo proporciona[178].

Era já pacífico na doutrina que a entrega do IP corresponde a uma obrigação da entidade emissora e nestes casos haverá a violação deste dever contratual. No RSP, a questão foi prevista no art. 68.º n.º 2: "*o risco do envio ao ordenante de um instrumento de pagamento ou dos respetivos dispositivos de segurança personalizados corre por conta do prestador do serviço de pagamento*". Desta forma, ao caso do referido Acórdão, ainda que analisado à luz desta disciplina, seria dada a mesma solução, mesmo perante a atuação do titular (mudar de residência sem ter avisado o emitente do cartão, sendo o IP enviado para a morada antiga).

b) Perante operações realizadas com cartões duplicados ou com a indicação dos elementos gravados no cartão sem que haja a apropriação do IP[179], típicas dos contratos à distância, a resposta será igualmente simples. Estas operações constituem uma verdadeira surpresa para o titular do IP, que o mantém na sua posse e guardado, assim como aos dispositivos de segurança que lhe estão associados, com toda a diligência que lhe é exigida[180]. Consequentemente, estas situações não cabem na previsão do art. 72.º n.º 1 do RSP, onde o titular responde até €150[181]. Pelo que valerá, aqui, inteiramente a regra do reembolso imediato dos prejuízos por parte do prestador do serviço de pagamento, consagrada no art. 71.º daquele regime[182]. Ainda assim, sempre se aplicará o n.º 2 do art. 72.º[183], respondendo por todos os prejuízos resultantes do incumprimento deliberado dos deveres previstos no art. 67.º ou da sua atuação fraudulenta.

---

[178] O Tribunal de primeira instância tinha já entendido que incidia sobre o banco o especial dever de cuidado no envio destes elementos, para que só o titular o receba e o possa utilizar, baseando-se no disposto do art. 486.º do CC, omitindo estes deveres especiais de cuidado, imponha-se a sua condenação a suportar os prejuízos que decorreram para o titular do cartão.

[179] Não há apropriação porque não há quebra da confidencialidade. O IP é utilizado sem que haja a indicação dos dispositivos de segurança personalizados.

[180] Estas situações foram reconhecidas pelos nossos tribunais superiores, veja-se a título de exemplo o Ac. de 20.10.2011 do TRL, *cit.*: "*Pode acontecer, não obstante o titular do cartão cumprir todas as obrigações contratuais, que seja confrontado com uma utilização abusiva do cartão – clonagem de cartões de crédito sem que o titular se aperceba de tal e através da qual sejam levantadas, ilicitamente, da sua conta, determinadas quantias. Por outro lado, o banco pode contribuir para possíveis utilizações ilícitas do cartão, na verdade, não cabe ao titular do cartão a escolha dos sistemas de segurança aplicados ao cartão, nem controla os meios tecnológicos empregues no sistema, sendo facto do conhecimento público que os cartões de débito com banda magnética são facilmente duplicáveis*". Contudo, o Tribunal conclui genericamente "*que a solução mais equitativa é a repartição de responsabilidades entre o banco emissor e o titular do cartão (…) quando não há culpa de nenhuma das partes*", enquanto pensamos ter demonstrado que o titular do cartão falsificado não deveria assumir qualquer prejuízo.

[181] Antes deste regime, a questão da falsificação do IP era, nos contratos de utilização elaborados pela entidade prestadora e no Aviso do BdP n.º 11/2001, prevista juntamente com o roubo ou furto do cartão, por norma, responsabilizando o titular do cartão falsificado por parte dos prejuízos decorrentes de operações abusivas antes da comunicação. A questão é hoje clara, estando a hipótese de falsificação ou duplicação excluída do artigo que estabelece a responsabilidade do titular do IP – o art. 72.º do RSP.

[182] Esta era também a solução apontada pela doutrina anterior a este regime. Veja-se o que é defendido por AMÁVEL RAPOSO, *op. cit.*, p. 21: "*A verdade é que nada assegura que não possam existir levantamentos apesar dos meios de acesso fornecidos pelo banco ao cliente não terem sido utilizados por este ou por terceiro, ou terem sido utilizados sem colaboração culposa do cliente (v.g., quebras de confidencialidade ou de segurança no seio da banca, pirataria). Tais levantamentos, bem como todos os que não possam ser imputáveis a acto ou omissão do consumidor, correm por conta do banqueiro*".

[183] Este número é o único que no seu texto não prevê expressamente as hipóteses de *perda, de roubo ou da apropriação abusiva de instrumento de pagamento*, sendo aplicável a todas as situações.

Uma destas situações, em que o titular do IP só no extrato mensal se apercebeu de operações não autorizadas, continuando na posse do cartão, inclusive, utilizando-o posteriormente às operações abusivas, foi decidido pela sentença de Julgado de Paz de 16.10.2006. Apesar de não ter sido dado como provado que existiu de facto falsificação do cartão, parece ser o que realmente aconteceu, pois, o IP esteve sempre na posse do seu titular e a assinatura aposta no talão de compra era "efectivamente, dissemelhante da assinatura aposta no cartão"[184]. O Julgado de Paz, mesmo sem afirmar que as operações foram realizadas com um cartão clonado, defendeu: "correm por conta da empresa exploradora do cartão de crédito os riscos do seu empreendimento"[185].

c) Já as situações de perda, roubo ou apropriação do IP são anteriores às operações fraudulentas, pelo que se exigirá ao titular o cumprimento do dever de notificar o extravio à entidade prestadora[186], tendo o seu comportamento, também no que respeita ao dever de guarda do cartão e dos dispositivos de segurança, de ser pesado para a repartição dos prejuízos entre as partes.

A repartição da responsabilidade nestes casos será uma das questões mais controvertidas e que mais diferendos suscita entre o emissor do cartão e o respetivo titular. O nosso Supremo Tribunal teve já a oportunidade de defender que o titular pode ser responsabilizado por perdas registadas antes da comunicação, porque "(a)o portador do cartão incumbe a sua guarda e, se por qualquer motivo ele se extravia, tem a obrigação de comunicar ao banco emitente para que este tome as adequadas providências, designadamente impedir o seu uso abusivo por parte de terceiros"[187].

Contudo, a ponderação da diligência colocada pelo titular na guarda do IP e na comunicação do seu extravio nem sempre foi feita pela jurisprudência. O Tribunal da Relação do Porto, no Acórdão de 12.04.2010, respondeu à questão considerando apenas o momento da comunicação. Desta forma, afirmou que "o Autor, na qualidade de titular do cartão é responsável pelo pagamento das quantias debitadas na conta-cartão até ao momento da comunicação do extravio"[188/189]. Não podemos acompanhar a posição tomada por este

[184] Na sentença é dito que "*não é possível aferir, com segurança, se o cartão foi clonado e se o foi, de que forma*", sempre se adiantando que "*a clonagem é uma fraude que se vem tornando comum*". O Banco insurgia-se dizendo que o titular permitiu tais operações, tendo omitido o dever de efetuar a comunicação daquela ocorrência "*com a necessária prontidão*". Tal argumento foi – bem, consideramos – rejeitado pelo Julgado de Paz, defendendo que "*a obrigação de comunicação só pode, assim, ser entendida a partir do momento em que se tornou possível ou conhecido o delito*".

[185] Como, de resto, era já entendimento dos nossos tribunais superiores – veja-se, por exemplo, o Ac. do STJ de 16.04.2004, *cit.*

[186] Nas palavras de MARIA RAQUEL GUIMARÃES, "(Ainda) a responsabilidade pelo uso indevido de instrumento de pagamento electrónicos em operações presenciais e à distância" *cit.*, p. 137, "*só o atraso na realização desta comunicação potencia os prejuízos inerentes ao extravio do instrumento de pagamento*".

[187] Cfr. Ac. do STJ de 15.10.2009, *cit*. A diligência do titular é aqui ponderada e, no mesmo aresto, o nosso mais alto Tribunal admite que o titular "*até pode não ter tomado prévio conhecimento da sua utilização abusiva e nem ter qualquer responsabilidade nessa indevida utilização*". Assim, Ac. TRP de 28.09.2004, *cit*.

[188] No caso colocado ao Tribunal, o cartão foi utilizado de forma abusiva em duas operações registadas no dia 18 de setembro, quando o seu titular se encontrava em Milão. O titular só se apercebeu do extravio do cartão ao ser contactado pelo banco, no dia 20, momento em que já se encontrava em Portugal. O Tribunal entendeu que o titular teria de suportar todas as perdas decorrentes dessas operações. No Acórdão discute-se ainda a

Tribunal. Importa recordar, socorrendo-nos das palavras do Tribunal da Relação de Lisboa no Acórdão de 20.10.2011, que "o titular do cartão pode não ter culpa na perda, extravio, furto ou roubo do cartão, pelo que não é razoável que seja ele sempre a suportar o risco, quaisquer que sejam as circunstâncias que ocorram antes da comunicação"[190].

Na mesma linha, vem o RSP, no art. 72.º, definir a responsabilidade do titular perante a perda ou extravio do cartão. A aplicação deste artigo justifica, devido à falta de clareza da norma[191], a sua interpretação conforme ao art. 61.º n.º 1 da Diretiva 2007/64/CE, entendendo-se que a indicação de "*quebra de confidencialidade dos dispositivos de segurança imputável ao ordenante*" apenas respeita à apropriação do IP, não sendo exigível nas hipóteses de roubo ou perda.

Assim, quando haja apropriação do IP *com quebra da confidencialidade dos dispositivos de segurança personalizados imputável ao ordenante*, perda ou roubo do cartão, nos termos do art. 72.º n.º 1, o titular suporta prejuízos dentro do limite do saldo disponível ou da linha de crédito associada até ao limite máximo de €150, quando não atue com negligência grave ou fraudulentamente.

A afirmação deste limite pelo qual será o titular do cartão a responder, constituirá o regime geral para estas situações. Pelo que, o reembolso imediato das perdas decorrentes das operações não autorizadas, previsto no art. 71.º do RSP, deve ser realizado subtraindo os €150 da responsabilidade do titular do IP[192].

Na verdade, a solução de repartição dos prejuízos presente no art. 72.º do RSP resultava já da recomendação 88/590/CE de 17 de novembro[193] e da recomendação 97/489/CE de 30 de

---

responsabilidade da seguradora, pela apólice de seguro realizado para cobrir os prejuízos decorrentes de fraude suportados pelo titular do cartão.

[189] O TRL no Ac. de 18.01.2011, *cit.*, a propósito da análise das cláusulas contratuais gerais, manifestou-se no mesmo sentido: "*de acordo com a boa fé, bem se compreende e aceita, porque justo e equitativo, que em caso de extravio e/ou furto, seja o aderente o responsável por qualquer utilização indevida até ao momento em que, junto do banco predisponente, cumpra a sua obrigação de denúncia/aviso de situação na perigosa".* A afirmação cega de que o titular responde por qualquer utilização abusiva anterior à comunicação, será merecedora de crítica por desconforme às recomendações comunitárias e à própria Diretiva de 2007. A ação inibitória foi analisada com base no D.L. n.º 446/85, de 25 de outubro, olvidando que o D.L. n.º 166/95 de 15 de abril, prescrevia nos contratos de utilização fossem tidas em conta as Recomendações da UE. Na verdade, a jurisprudência, em desrespeito pelas Recomendações, fazia corresponder este limite ao plafond/limite de crédito ou saldo da conta para os casos "*de perda, extravio, furto ou roubo (sem culpa)*" – cfr. Ac. do TRL de 14.02.2000 (Torres Veiga), *in CJ*, ano XXV, 2000, tomo I, p. 113. Situação que o Aviso n.º 11/2001 não veio resolver.

[190] No mesmo sentido, pronunciou-se o STJ no Ac. de 15.05.2008, *cit.*, "*o titular do cartão pode não ter conhecimento prévio da utilização abusiva e pode nem ter tido qualquer responsabilidade nessa utilização, certo ainda que o conhecimento dessa utilização só lhe pode advir após os actos ilícitos de terceiro sem qualquer violação dos deveres de diligência*".

[191] O artigo prevê: "*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".*

[192] Este entendimento resulta da Diretiva de 2007, onde o art. 61.º, esclarecia que o regime aí consagrado surge "*em derrogação do artigo 60.º*", artigos correspondentes ao 70.º e 71.º do regime sob análise.

[193] Previa o n.º 8.3 da recomendação: "*O titular suportará os prejuízos que ocorram até ao momento da notificação, em consequência da perda, furto ou reprodução do mecanismo de pagamento, mas apenas até ao montante de 150 ECU para cada uma das ocorrências; todavia, este limite não será aplicável se o titular agiu com a extrema negligência ou fraudulentamente*";

julho[194/195]. Neste sentido, o Tribunal da Relação do Porto na decisão *supra* identificada, ainda que não utilizando o RSP, poderia ter aplicado regras semelhantes às atualmente consagradas. E limitar a responsabilidade do titular do cartão a perdas até €150, pois não se verificou da parte deste qualquer comportamento grosseiramente negligente ou fraudulento, conforme previsto nas Recomendações.

Um caso semelhante é analisado pelo Julgado de Paz na sentença de 27.09.2012, sendo que aqui o pedido do titular do cartão improcedeu, "uma vez que não provou não ter sido ele a efetuar as mesmas [operações] nem que a utilização do seu cartão de crédito não tenha decorrido de omissão dos seus deveres de guarda." Tendo em conta que o RSP é aplicável aos contratos já em vigor, desde que seja mais favorável, será ao prestador do serviço de pagamento que cabe fazer a prova de que a operação foi autorizada ou consentida pelo titular, que este agiu com negligência grave ou violou deliberadamente os seus deveres, nos termos do art. 70.º daquele regime. Neste sentido, o ónus da prova teria de ser julgado do prisma inverso – não tendo o prestador provado a culpa do titular do IP, seria aquele a responder pelos prejuízos ocorridos.

Caracterizamos o regime previsto no n.º 1 do art. 72.º, como o regime geral a aplicar no caso de operações não autorizadas resultantes de perda, roubo ou apropriação do cartão com quebra da confidencialidade dos dispositivos que lhe estejam associados, pelo que teremos, agora, de considerar as situações de exceção previstas no RSP.

Uma dessas situações ocorrerá quando exista negligência grave do titular do IP, devendo este, de acordo com o art. 72.º n.º 3, suportar perdas "*até ao limite do saldo disponível ou linha de crédito associada à conta ou ao instrumento de pagamento, ainda que superiores a (euro) 150, dependendo da natureza dos dispositivos de segurança personalizados do instrumento de pagamento e das circunstâncias da sua perda, roubo ou apropriação abusiva*"[196].

Identificamos anteriormente as situações em que o titular aponta o PIN junto do cartão, trazendo-o consigo, como violadoras do dever de guarda dos dispositivos de segurança

[194] A recomendação estabelece no seu art. 6.º n.º 1: "*Até à comunicação, o detentor suportará as perdas incorridas em consequência do extravio ou do furto do instrumento de pagamento electrónico até um limite que não pode exceder 150 ecus, salvo se tiver agido com extrema negligência (…) ou de forma fraudulenta, caso em que o referido limite não é aplicável*".

[195] JANUÁRIO GOMES, *op. cit.,* p. 246, nota n.º 828, considera que o RSP prevê "*o regime que, ao fim e ao cabo, já resultava de várias recomendações comunitárias, as quais não tinham logrado consagração no Aviso do BdP nº 11/2001, não obstante o teor do decreto-lei 166/95 de 15 de julho*".

[196] A medida concreta da responsabilidade do titular não está prevista na lei, dependerá da segurança do IP e das circunstâncias em que ocorre a sua perda, roubo ou apropriação abusiva e da possibilidade de evitar tais circunstâncias. Para JANUÁRIO GOMES, *op. cit.,* p. 246, nota n.º 829, interpretando este artigo do RSP de acordo com a Diretiva, teríamos de conceber esta solução como "*uma situação* intermédia *entre a, digamos, situação fraudulenta ou de incumprimento deliberado de uma ou mais das obrigações previstas no artigo 67 do RSP (artigo 56 da Diretiva). Na verdade, o artigo 61/3 da Diretiva permite aos Estados Membros que reduzam a responsabilidade prevista nos números 1 e 2 do artigo 'tendo especialmente em conta a natureza dos dispositivos de segurança personalizados do instrumento de pagamento e as circunstâncias da sua perda, roubo ou apropriação abusiva'. Em função do regime plasmado no artigo 72/3 do RSP, numa situação de negligência grave do ordenante que tenha um saldo disponível razoavelmente superior a €150, a falta de acordo gerará, com grande probabilidade, um litígio entre ordenante e prestador de serviços de pagamento".* CALVÃO DA SILVA, "Conta corrente bancária: operação não autorizada e responsabilidade civil", *cit.,* critica o tratamento diferenciado feito pelo legislador nacional, p. 326.

personalizados associados ao IP. Desta forma, a circunstância de o cartão ter sido roubado juntamente com o PIN, representará negligência grosseira do seu titular, tendo de suportar prejuízos anteriores à comunicação, ainda que superiores a €150[197].

A recomendação 97/489/CE, de 30 de julho, referia explicitamente que manter o PIN junto ao cartão constituía negligência grave[198]. No mesmo sentido, manifestava-se a nossa jurisprudência, referindo: "é da sua [do titular] inteira responsabilidade o facto de terceiros terem tido acesso ao *pin*, designadamente por incúria, desleixo ou negligência daquele, ao expô-lo, por exemplo, num local acessível e junto ao cartão"[199].

O nosso mais alto Tribunal expressou-se no sentido de "se só o próprio possuidor (…) deverá ser o depositário de tal número (secreto), não vemos como possa deixar de considerar, na hipótese em análise, como sendo sua – e apenas sua – a responsabilidade pelo uso do cartão, precisamente através do conhecimento do PIN"[200]. O Supremo Tribunal de Justiça ia mais longe, considerando válida a presunção de que existia negligência do titular se a utilização abusiva do cartão fosse feita com o uso do PIN. Este entendimento, foi de forma representativa, expresso no Acórdão de 15.05.2008 do mesmo Tribunal: "Em tais cláusulas estabelece-se uma presunção – presunção de uso do cartão; presunção de que foi utilizado pelo titular quando for correcta a digitalização do PIN e presunção de que o uso foi consentido ou facilitado culposamente pelo titular quando usado por terceiro. Com esta dupla presunção faz-se recair sobre o aderente a prova de que o cartão não foi por si usado e de que não consentiu ou facilitou culposamente o seu uso a terceiro. Simplesmente, esta presunção encontra-se em consonância com as regras que estabelecem os princípios que norteiam as normas de distribuição do ónus de prova (artigo 342º e seguintes)"[201].

---

[197] Assim, MENEZES CORDEIRO, *op. cit.*, 3.ª ed. 2006, p. 523: "*é considerado negligência grave o facto de alguém perder um cartão e uma agenda da qual constava o PIN, disfarçado de número de telefone";* Veja-se ainda, JOANA VASCONCELOS, "Sobre a repartição entre titular e emitente do risco de utilização abusiva do cartão de crédito no direito português", *cit.*, pp. 490 a 496. Internacionalmente, já na análise da diretiva, era referida a necessidade de definição do conceito de negligência grave para os casos de autenticação da operação de pagamento – veja-se SYLVIA MERCADO-KIERKEGAARD, "Harmonising the regulatory regime for cross-border payment services", *Computer Law and Security Review*, vol. 23 (2007), *in* <http://www.sciencedirect.com> (01.02.2016), p.183.

[198] A obrigação de não registar o número de identificação pessoal no cartão ou sobre qualquer outro elemento que conserve junto do IP estava prevista no art. 5.º al. c). A violação desta regra consubstancia extrema negligência, nos termos art. 6.º n.º 1.

[199] Cfr. Ac. do TRL de 19.09.2006, *cit.*; O Tribunal analisava uma situação de roubo de uma carteira onde se encontrava o cartão e uma fotografia que no verso tinha apontado o PIN.

[200] Cfr. Ac. do STJ de 20.10.2011, *cit.*

[201] A posição do Tribunal, também manifestada no Ac. de 02.03.2010, funda-se na ideia de que "*a atribuição do cartão é pessoal, cabendo ao seu titular a obrigação de manter secreto o PIN que lhe foi atribuído. Daí que o uso por terceiro ou o conhecimento por terceiro desse PIN, pela ordem natural das coisas, resulte de incumprimento dessas obrigações do titular do cartão. E assim sendo, ao titular do cartão caberá fazer a prova de que o cartão não foi usado, nem que não consentiu no seu uso, fazendo a prova da factualidade 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. Por isso, não há qualquer inversão do ónus de prova, retirando-a do banco e fazendo-a recair sobre o titular do cartão*"- cfr. Ac. STJ de 15.05.2008, *cit*. A decisão contou, contudo, com dois votos vencidos. O conselheiro Dr. Paulo Sá discordou da validade da cláusula referindo: "*se o titular refere que o cartão lhe foi furtado e foi coagido a revelar o PIN, carece de justificação que se presuma a sua culpa, se invoca o referido circunstancialismo e não há razões para duvidar dessas afirmações (repare-se que o sistema tem formas de controlar o invocado furto do cartão e apropriação ilícita do PIN, desde logo as câmaras de vigilâncias instaladas nos diversos ATM). Neste caso, o que é lógico é que se recorra à responsabilização pelo risco, distribuindo-o de forma equitativa e não continuar a situar a responsabilidade no âmbito contratual e a obrigar o titular a afastar a presunção de culpa, mesmo quando o*

Não poderemos acompanhar a posição do STJ, quanto à consideração desta presunção como válida, pois tal criaria um ónus da prova demasiado oneroso para o titular do cartão que vê o seu cartão fraudulentamente utilizado, cabendo-lhe ilidir a presunção "natural", segundo a tese do Tribunal. Os documentos que contém os registos informáticos das operações não podem, igualmente, valer para criar esta presunção[202].

Todavia, a existência de uma presunção neste sentido existiu também noutros países da UE, mantendo-se inclusive no regime resultante da transposição da Diretiva de 2007. Reinhard Steennot[203], chama atenção para falta de uniformização da transposição da responsabilidade assumida na PSD para os ordenamentos internos dos Estados-Membros, dando conta de países onde foi consagrada uma presunção de negligência grave ou grosseira por parte do titular, quando o seu IP é utilizado por terceiro juntamente com o número pessoal de identificação. A existência de uma presunção deste género, significa atribuir o ónus da prova ao utilizador e retira toda a utilidade ao regime geral que limita as perdas suportadas pelo titular do IP até ao valor de €150, obrigando o prestador do serviço a reembolsar de imediato o remanescente[204].

Mais perto da solução atualmente consagrada no RSP, foi a solução dada pelo Tribunal da Relação de Lisboa no Acórdão de 04.07.2013: "tendo a ré (…) actuado com negligência grave, mantendo o cartão e o código PIN no interior do veículo de onde os mesmos foram retirados, responderá pelas perdas resultantes dos abastecimentos (…) até aos limites contratualizados, suportando a autora, enquanto proprietária dos cartões, pelos valores que excedam tais limites".

O titular não beneficiará, ainda, do limite de €150, suportando todos os prejuízos, quando atue fraudulentamente ou incumprimento deliberado de uma ou mais obrigações previstas no art. 67.º do RSP[205].

---

banco tem elementos de confirmação sobre o roubo do cartão e sob a coacção. Tal segmento impõe ao titular um ónus de prova agravado, inaceitável, nos termos do artigo 21.º, al. g), do Dec. Lei n.º 446/85, sendo certo que a cláusula até se apresenta como eivada de má-fé, porquanto parece excluir qualquer responsabilidade do titular, salvo provando-se má-fé ou negligência, quando afinal a responsabilidade será toda sua, se não conseguir provar que não teve culpa na utilização abusiva do PIN".

[202] O STJ vem há vários anos afirmando que estes documentos "*são apreciados livremente pelo julgador*", pelo que não se pode permitir que a entidade emitente do IP "*construa documentalmente a prova que a favoreça, em caso de conflito de interesses, em detrimento do particulares, violando o disposto no artigo 21, alínea e) do Decreto-Lei de 25 de Outubro, que proíbe as cláusulas contratuais gerais que alterem as regras respeitantes ao ónus da prova*" - cfr. o Ac. de 20.06.1995 (Pais de Sousa), disponível *in* <http://www.dgsi.pt> (consultados a 27.03.2015).

[203] *Op. cit.*, p. 558.

[204] A Diretiva não é muito clara quanto à possibilidade de existência de uma presunção de negligência grave do titular do IP. No art. 57.º n.º 2 prevê-se: "*caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, a utilização do instrumento de pagamento registada pelo prestador de serviço de pagamento, por si só, não é necessariamente suficiente para provar que a operação de pagamento foi autorizada pelo ordenante ou que este último agiu de forma fraudulenta ou não cumpriu, deliberadamente ou por negligência grave, uma ou mais das suas obrigações decorrentes do art. 56.º*". A expressão, "*necessariamente suficiente*", como refere-se MARIA RAQUEL GUIMARÃES, "A repartição dos prejuízos decorrentes de operações fraudulentas de banca electrónica (home banking)", *cit.*, p. 60, "*não condena definitivamente uma presunção nesse sentido, deixando espaço ao julgador para a sua apreciação*". Caberá ao juiz apreciar a existência de um comportamento do utilizador que represente negligência grave e decidir o valor e a credibilidade atribuída aos registos informáticos.

[205] Cfr. art. 72.º n.º 2 do RSP. No fundo, significará que o titular responde ilimitadamente quando atue fraudulentamente ou viole os deveres de cuidado com o IP e os dispositivos de segurança que lhe são exigidos.

4.2. *Homebanking*

O sistema de banca eletrónica merecerá um tratamento autónomo pelas especificidades apresentadas por este IP. Aqui não podemos falar de todas as situações que identificamos quanto aos cartões, mas apenas da apropriação abusiva do IP com quebra dos dispositivos de segurança que lhe estejam associados, imputável ou não ao titular[206]. Assim, quanto à responsabilidade do titular que vê a sua conta ser abusivamente movimentada, será de aplicar o regime previsto no art. 72.º do RSP[207]. No caso de apropriação abusiva do IP com quebra da confidencialidade imputável ao titular, este responderá por prejuízos até €150[208], respondendo acima deste valor quando atue com negligência grave ou, por todos os prejuízos, se agir de forma fraudulenta ou em incumprimento deliberado dos seus deveres, nos termos n.º 2 e 3 do referido artigo. Nas situações em que o comportamento do titular não mereça censura, será o banco a suportar os prejuízos decorrentes das operações abusivas, porque a este cabe, como o Tribunal da Relação de Lisboa defendeu, diligenciar para que o serviço prestado "seja seguro e nele possa o cliente confiar", tendo de "suportar o risco do seu sistema de home banking não ser seguro e permitir a intromissão de terceiro"[209].

Quando podemos considerar que a quebra da confidencialidade dos dispositivos de segurança é imputável ao titular? Quais as situações que demonstram negligência?

A nossa jurisprudência tem começado por afirmar a obrigação do titular "utilizar esse serviço seguindo as regras de segurança que lhe tenham sido comunicadas pelo Banco e aquelas que, segundo um padrão de normalidade, o comum utilizador da internet sabe que devem ser observadas, nomeadamente, a não divulgação dos códigos e passwords de acesso"[210].

O alargamento da responsabilidade do titular dependerá, naturalmente, da prova feita, sendo aqui exigível uma prova complementar aos registos informáticos da operação, que "*por si só, não é necessariamente suficiente*", nos termos do art. 70.º n.º 2 do RSP.

[206] O Ac. do TRG, datado de 25.11.2013, *cit*., refere, quanto ao *homebanking*, a exigência de "*muitas cautelas devido aos perigos a que estava sujeita. É como alguém que pisa terreno minado e não se informa e toma os cuidados devidos para as circunstâncias. Corre um grande risco de ser atingido por uma mina e sofrer graves danos*". Merece-nos, salvo o devido respeito pelo Tribunal, crítica a precipitação da instância nesta comparação, pois a entidade prestadora do serviço, ainda que de minas se tratasse, teria de informar e esclarecer o utilizador dos perigos associados e das boas práticas de forma a minimizar esses riscos, não apenas com artigos num menu relativo à segurança (na data dos factos analisados pelo Tribunal, ainda não existiam as mensagens de alerta, hoje comuns, que surgem automaticamente antes do utilizador introduzir os seus dados de acesso) mas também no momento da adesão ao serviço, não cabendo só ao utilizador a procura dessa informação.

[207] LUIZ GUSTAVO CARATTI DE OLIVEIRA, *op. cit.*, trata a questão defendendo que *"os bancos são responsáveis pelos prejuízos advindos das fraudes virtuais que lesam as contas de seus correntistas efetuadas através dos sites das respectivas instituições financeiras, ou seja, 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".* Este Autor nem equaciona as situações em que, como refere o TRP no Ac. de 07.10.2014, "*são os próprios utilizadores do sistema que fornecem (ainda que involuntariamente) as senhas aos infractores*", devendo o comportamento do titular do serviço que facilite essa fraude ser aqui avaliado.

[208] O TRL no Ac. de 05.11.2013, *cit.,* entendeu que a imputação de quebra de confidencialidade referida no n.º 1 do art. 72.º será "*a título de culpa leve ou risco*".

[209] Cfr. Ac. de 05.11.2013. No caso concreto, o Tribunal decidiu que "*ignorando-se como é que os terceiros acederam às chaves ou códigos de acesso, recai sobre o banco o dever de reembolsar os autores dos montantes das operações de pagamento (art. 71º), não tendo sequer estes de suportar os prejuízos até ao montante de €150,00*". Na verdade, não será imputável ao titular a quebra dos dispositivos de segurança, quando estes sejam conseguidos através da quebra da segurança do próprio *site* do banco.

[210] Cfr. Ac. do TRL de 28.06.2013, *cit*.

Neste sentido, haverá quebra da confidencialidade associada ao *homebanking*, quando este divulgue, ainda que sem culpa grave, os códigos e os dados de acesso. Maria Raquel Guimarães, recorda que poderá existir incumprimento deliberado dos seus deveres "*dependendo do 'esquema' concreto através do qual os dados do utilizador são obtidos e do seu grau de 'ingenuidade' ao facultar esses dados"*[211].

a) Nas situações de fraude por *phishing* haverá apropriação do IP com *quebra da confidencialidade imputável ao titular*, para efeitos do n.º 1 do art. 72.º, mas acreditamos que, atualmente, poderão ser imputáveis ao titular prejuízos superiores a €150 a título de negligência grosseira.

O Tribunal da Relação de Lisboa, numa decisão de 2010, condenou o banco a suportar todas as perdas decorrentes do ataque de *phishing*[212]. A atuação do titular – e o inerente juízo de censura – terá de ser avaliado à data dos factos. Cada vez mais, os utilizadores da internet estão conscientes dos perigos de abrir e descarregar ficheiros de *e-mails* desconhecidos e com aparência duvidosa[213]. Pelo que, hoje, neste tipo de situações, haverá responsabilidade do titular que abre o *e-mail* suspeito e descarregue algum nos seus anexos, agindo, cremos, com negligência grave se ceder os seus dados de acesso ao sistema em resposta ao *e-mail*. Contudo, não tendo o banco provado um comportamento grosseiramente negligente do seu cliente, este teria de responder, pelo menos, por prejuízos até €150.

b) Já a técnica de *pharming* é mais difícil de ser detetada por um utilizador comum[214]. As páginas fraudulentas são "muitas vezes iguais às páginas do banco e identificadas como ligações seguras"[215], pelo que, a censura que se possa atribuir ao utilizar poderá ser, aqui, diferente.

O Acórdão de 29.04.2014 do Tribunal da Relação do Porto numa destas situações, entendeu que não se demonstrou "qualquer violação por parte de A. dos deveres de sigilo e confidencialidade dos códigos e senhas de acesso de utilização do sistema *homebanking*, mas sim uma quebra da segurança nos meios de acesso ao sistema informático do Réu cuja

---

[211] MARIA RAQUEL GUIMARÃES, "A fraude no comércio electrónico: o problema da repartição do risco por pagamento fraudulentos", *cit.*, p. 594.

[212] Referimo-nos ao Ac. de 26.10.2010, em que o utilizador do serviço de *homebanking* "*foi vítima de extorsão por um cracker agindo em ambiente informático, a partir da Rússia, utilizando a técnica de phishing".* O Tribunal considerou "*numa óptica de defesa do consumidor, não tendo o banco demonstrado a culpa da A. na movimentação fraudulenta da conta, o mesmo terá de suportar as consequências de fraude no circuito cuja a fiabilidade, de resto, ele próprio se comprometeu contratualmente a garantir*".

[213] Segundo o relatório sobre ameaças à segurança na internet - tendências 2013, volume 19, publicado em abril 2014, em 2013, um em cada 392 *emails* continha ataque de *phishing*, consultado em <http://www.symantec.com/pt/pt/security_response/publications/thretreport.jsp> (30.03.2015). Trata-se de uma realidade comum, para a qual os utilizadores da internet estarão atualmente mais atentos.

[214] Na mesma linha, o Ac. de 07.10.2014 do TRP: "*ao contrário do phishing, o qual uma pessoa mais atenta pode evitar simplesmente não respondendo ao e-mail fraudulento, o pharming é praticamente impossível de ser detectado por um utilizador comum da internet*".

[215] Cfr. Ac. do TRG de 30.05.2013 (Rita Romeira), onde se defende não existir "*uma conduta imprudente, descuidada ou negligente*" do utilizador vítima deste tipo de fraude. Na mesma linha, Ac. do TRE de 22.05.2014, *cit*.

responsabilidade (…) lhe é imputável seja porque a este incumbe (…) 'assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao utilizador e serviços de pagamento que tenha direito a utilizar o referido instrumento (…)' (artigo 68º, nº1, alínea a) do DL n.º 317/2009, de 30/10, seja porque não logrou ilidir a presunção de culpa que, enquanto depositário, lhe advém do perecimento de coisas cujo o domínio lhe foram transferidas por via contratual"[216]. Aqui diz-se que o titular na página falsa realizou "as certificações e operações habituais", pelo que não tendo respondido a nenhum pedido incomum da página falsa, não recairia sobre a sua atuação qualquer censura a título de culpa. No entanto, este Tribunal decidiu na mesma linha na decisão de 07.10.2014, considerando não lhe ser imputável a quebra de confidencialidade do sistema, num caso em que o titular do serviço, em resposta à solicitação que surgiu depois de aceder ao *homebanking,* indicou o modelo e marca de telemóvel e descarregou para o mesmo uma aplicação, tendo posteriormente indicado o código que recebeu por SMS[217]. O Tribunal da Relação de Évora, num caso semelhante analisado no Acórdão de 22.05.2014, quando já existiam alertas na página de acesso ao serviço, entre outros, de que o sistema nunca solicitava o número de telemóvel, considerou que o utilizador que cede informações sobre o seu telemóvel numa página falsa[218], não tem um comportamento "menos cuidadoso do que qualquer utilizador com baixos conhecimentos informáticos". Em ambos os casos, ainda que não fosse atribuído ao comportamento do titular um juízo de especial censura, este teria de suportar prejuízos até ao limite de €150, porque lhe é imputável a quebra da confidencialidade do sistema[219].

Os tribunais superiores nacionais têm, também, vindo a afastar a consideração de negligência grave do titular vítima deste tipo de fraude. O Tribunal da Relação de Guimarães, no Acórdão de 17.12.2014 refere: "o depositante nem sequer representa como possível não ter entrado no site (verdadeiro) do banco e, por isso, fornece os seus dados movido apenas pelo sentimento de confiança que nele deposita. E como várias pessoas 'caíram' na mesma

---

[216] No mesmo sentido, o STJ no Ac. 18.12.2013, *cit.*: "*da factualidade apurada pelas instâncias não resulta que tenha havido por banda da Autora qualquer comportamento indiciador de quebra de segurança no acesso ao site BX.Net, que tivesse proporcionado a um terceiro (?) as coordenadas para a realização das operações bancárias via* homebanking *(…) não tendo o Réu provado que a Autora tivesse tido um qualquer comportamento que pudesse por em causa a segurança do sistema, nomeadamente que tivesse quebrado o seu dever de segredo sobre as chaves de acesso e que por algum modo, voluntário, grosseiro, negligente ou outro as tivesse cedido a terceiro, de forma a poder ser responsabilizada pela ocorrência fraudulenta".*

[217] Cfr. Ac. do TRP de 07.10.2014, *cit*. O Tribunal entendeu "*afastar, sem qualquer hesitação, o dolo ou intencionalidade no comportamento do apelado e mesmo uma negligência consciente ou culpa grave. Resta apurar se actuou com negligência ou culpa leve (…) era necessário que o Apelado fosse uma pessoa muito experiente e muito conhecedora do meio de navegação em ambiente eletrónico para que pudesse desconfiar do isco que lhe foi lançado nas circunstâncias mencionadas*", considerando, assim, não existir sequer negligência leve por parte do titular.

[218] Deu-se como provado que o utilizador, num acesso anterior tinha-se deparado com "*uma página fraudulenta e forneceu inadvertidamente, a informação referente às chaves de acesso e telemóvel associado à autorização por SMS*" (facto provado 20), numa altura em que o banco já publicava alertas na página de acesso ao serviço, como o "o … Net nunca solicita a introdução do seu nº de telemóvel" (facto provado 23 e 24), disponível <http://www.dgsi.pt> (09.05.2015).

[219] Assim, MARIA RAQUEL GUIMARÃES, *in* "A repartição dos prejuízos decorrentes de operações fraudulentas de banca electrónica (*home banking*); Anotação ao Acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09", *cit.*, p. 64. Nestas situações, foram os titulares que indicaram na página falsa os seus dados de acesso. A quebra da confidencialidade já não será imputável ao titular nas situações em que hackers conseguem esses elementos de acesso por intromissão no *site* verdadeiro/legítimo da banca eletrónica.

situação não podemos, por comparação com o homem comum, dizer que ele agiu de uma forma particularmente negligente".

Contudo, tem surgido decisões em sentido contrário, embora em números mais discretos. Os Julgados de Paz na sentença de 21.09.2012, tendo em consideração os alertas colocados na página de *homebanking* da "existência de fraude através de falsa demo de transferência direta", defendeu que o titular ao disponibilizar "a hackers os dados do seu equipamento telefónico, incluindo o número associado ao SMS TOKEN, introduzindo no respectivo computador um código que lhe foi disponibilizado por SMS, depois de ter visionado a 'demonstração' de uma operação de transferência" deve responder por todas as perdas[220]. Nesta situação, ainda que não se possa considerar que o titular violou *deliberadamente* o dever de guarda dos dispositivos de segurança pessoais associados ao serviço, a verdade é que agiu de forma descuidada, demonstrando negligência grave.

É a existência destes avisos, logo na página inicial do *site,* que tornará a conduta do titular do IP especialmente censurável. O utilizador é constantemente alertado para os indícios de fraude[221], de maneira a estar, naturalmente, consciente de que os pedidos feitos nestas páginas falsas não são legítimos. Responder a um pedido incomum na página clonada, por exemplo com a indicação de todas as combinações do cartão matriz, demonstrará um enorme descuido e desatenção do titular do IP[222]. Neste sentido, manifestou-se o Tribunal da Relação de Lisboa, num caso em que o titular, quando já existiam estes alertas de segurança, "transcreveu para ecrã que lhe surgiu no computador que estava a usar a totalidade das 64 possíveis combinações do seu cartão matriz, divulgando na internet todas as combinações possíveis". Aí se defendeu que o titular "deu azo a que terceiros acedessem ao 'sistema' e procedessem ao desvio dessas quantias (…) o que permite concluir ter feito uma utilização imprudente do serviço"[223].

É ao banco que cabe provar o comportamento negligente do titular e a medida em que esse contribuiu para as operações não autorizadas, realizando prova complementar dos registos

---

[220] O Julgado de Paz considerou, quanto a nós bem, que "*foi a negligência no sentido de não ter tido as necessárias cautelas, de não ter prestado mais atenção ao que lhe estava sendo solicitado, precavendo-se das fraudes que eram já anunciadas no próprio site do banco, com alertas e informações para que os consumidores se tivessem habilitados a se prevenir e as pudessem evitar, não cometendo a imprudência de informar terceiros dos seus dados pessoais e sigilosos*" – cfr. sentença de 21.09.2012, *cit*.

[221] Antes de inserir os dados de acesso à sua conta, o utilizador terá de fechar o alerta de segurança. As mensagens preventivas são curtas, facilmente apreendidas e variáveis, alertando que o banco nunca pedirá todas as combinações do cartão matriz, nem a atualização de dados pelo telemóvel, na página ou por *e-mail*, etc.

[222] Assim, MARIA RAQUEL GUIMARÃES, "As operações fraudulentas de *home banking* na jurisprudência recente - Ac. do STJ de 18.12.2013", *op. cit.*, ponto 3, referindo que o titular só será passível de censura quando "*o procedimento que tenha de levar a cabo seja muito distinto do habitual e o seu banco o tenha alertado para este tipo de fraude*". Continua prevendo um caso semelhante ao apresentando, "*Já será censurável o seu comportamento se fornece mais informações do que aquelas que habitualmente lhe é pedida – se, nomeadamente, facultar todas as coordenadas do seu cartão matriz, quando o banco enuncia que estas nunca são pedidas para a mesma operação…*".

[223] Cfr. Ac. de 12.12.2013 do TRL, *cit.*; Uma situação próxima foi decidida pelo TRG, no Ac. de 25.11.2013. No momento em que a fraude analisada pelo Tribunal ocorreu, ainda não existiam estes alertas, apenas informações sobre métodos de fraude e detalhes sobre segurança num menu apresentado no site. Mesmo assim, o Tribunal não deixou de sublinhar que "*apesar da aparência genuína do site, a solicitação dos dígitos do cartão matriz, em si, é muito estranha, dentro do contexto e lógica do sistema de segurança implementado pela ré (…) Assim, é de concluir que o comportamento da autora foi negligente, violador das regras de segurança impostas pelo contrato, que foram causa directa da movimentação das suas contas por terceiros*".

informáticos. Pois, não é possível "retirar da circunstância de as movimentações da conta do Autor terem sido 'executadas porque introduzidos os códigos que permitiam o acesso àquela conta bancária' essa falta de cuidado exigível, nas circunstâncias concretas do caso"[224].

4.3. Conclusão

Das decisões judiciais a que tivemos acesso, pese embora parte não utilize o regime jurídico apresentado, é clara a intenção de repartir os prejuízos de forma justa, fazendo dos benefícios retirados do sistema e do controlo/domínio sobre o sistema informático os principais critérios para essa repartição, na ausência de culpa das partes.

A maioria dos tribunais tem condenado a entidade prestadora do serviço a assumir a totalidade dos prejuízos decorrentes para o titular. No entanto, para imputar perdas a título de culpa, os tribunais terão de analisar o cumprimento dos deveres previstos na lei e no contrato e o grau de censura das condutas das partes. Assim, "*o cliente do banco vê a sua posição agravada conforme vai aumentando o grau de censura sobre a sua conduta. Na medida em que seja, ele próprio, o autor da fraude, então já o banco não assumirá qualquer prejuízo pelas operações realizadas*"[225]. É, precisamente, esta a repartição dos prejuízos consagrada no RSP.

Contudo, sente-se por parte dos tribunais alguma resistência em imputar prejuízos aos titulares do *homebanking*, mesmo pela quebra de confidencialidade do sistema – situações em que o titular tem de assumir prejuízos até 150€. Note-se que nas decisões do Tribunal da Relação do Porto e do Tribunal da Relação de Évora, *infra* apresentadas, não foi sequer entendido que as operações fraudulentas resultem da *apropriação abusiva do IP com quebra da confidencialidade dos dispositivos de segurança personalizados imputável ao 'ordenante'*, quando se provou – pelo menos, nos casos em que o titular cedeu as informações sobre o telemóvel, perante a existência de alertas – um comportamento merecedor de censura na forma de preservar a eficácia dos dispositivos de segurança personalizados a que o titular está obrigado[226].

[224] Cfr. Ac. do TRL de 24.05.2012, *cit*. Na mesma linha, veja-se o Ac. de 28.06.2013 do mesmo Tribunal e o Ac. do TRP de 07.10.2014. No Ac. de 29.10.2013 do TRP (Francisco Matos), disponível *in* <http://www.dgsi.pt> (23.03.2015), discutiu-se a inversão do ónus da prova que onerava o banco. O Tribunal entendeu que ao banco cabe demonstrar "*que o computador dos AA foi infectado com um programa de código malicioso, que abriu uma brecha na segurança do referido aparelho, permitindo aos terceiros ter acesso aos dados confiados aos AA e executar operações no seu computador, como se deles próprios se tratasse",* considerando não se verificar a inversão do ónus da prova pelo facto dos utilizadores terem instalado um novo sistema informático que dificultou a perícia ao computador.

[225] MARIA RAQUEL GUIMARÃES, "A repartição dos prejuízos decorrentes de operações…" *cit.,* p. 66.

[226] Referimo-nos ao Ac. de 07.10.2014 e 22.05.2014, respetivamente.

5. As Alterações introduzidas pela Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015

O RSP tem recebido críticas pela acentuada complexidade e introdução de novos conceitos, muitas vezes caracterizados pela abstração com que são apresentados[227] e pela falta de uniformização na transposição para os diferentes Estados-Membros.

Consciente da enorme importância da matéria, a Comissão Europeia lançou, em 2012, o Livro Verde *para um mercado europeu integrado dos pagamentos por cartão, por Internet e por telemóvel*[228]. No caminho aberto pelo Livro, o legislador comunitário aprovou, em 2013, a proposta de nova Diretiva sobre a matéria dos sistemas de pagamento, conhecida como PSD II, que altera as Diretivas 2002/65/CE, 2013/36/CE e 2009/110/CE e revoga a Diretiva 2007/64/CE, que entrou em vigor no passado dia 12 de janeiro como Diretiva (UE) 2015/2366 do Parlamento Europeu e Conselho, de 25 de novembro de 2015. Esta obriga os Estados-Membros a adotarem e publicarem as disposições necessárias para dar cumprimento à presente diretiva até 13 de janeiro de 2018[229], data em que a Diretiva 2007/64/CE deixa de vigorar[230].

Esta Diretiva mantém a estrutura do regime anterior, apresentando, no anexo II, uma tabela de correspondência com a Diretiva anterior, mas introduz algumas alterações merecedoras de destaque. Tendo em atenção a sofisticação dos meios de fraude, a PSD II vem estabelecer o conceito de "*autenticação forte do cliente*"[231] para os serviços de pagamento à distância. Porém, não impõe esta autenticação "forte", atendendo ao disposto no seu art. 74.º n.º 2, apenas incentiva a sua aplicação ao agravar a responsabilidade do prestador do serviço que não a exige no acesso ao seu serviço.

A repartição dos prejuízos estabelecida na lei atualmente em vigor não inclui os serviços intermediários, isto é, não abrange os intervenientes que não dispõem, a qualquer momento, dos fundos do ordenante ou do beneficiário, deixando uma enorme lacuna na regulação dos pagamentos no comércio eletrónico. Será, desta forma, importante alargar o alcance do regime, *prestador do serviço de iniciação do pagamento*[232], uniformizando a regulação dos pagamentos eletrónicos. Na PSD II, a responsabilidade do terceiro prestador de serviços de

---

[227] Por todos, JANUÁRIO GOMES, *op. cit.*, p. 223. O autor refere que a complexidade do diploma estará "*próxima do labiríntica*". A crítica é, igualmente, feita à diretiva que esteve na base do RSP, acrescentando que "*o legislador nacional não fez um real esforço, ficando-se, praticamente, pela solução, mais simples, de reproduzir a versão em língua portuguesa do texto comunitário".*

[228] Publicado a 11.01.2012, disponível *in* <http://ec.europa.eu/green-papers/index_pt.htm>.

[229] Cfr. art. 115.º da Diretiva (UE) 2015/2366 do Parlamento Europeu e Conselho, de 25 de novembro de 2015.

[230] Cfr. art. 114.º da Diretiva (UE) 2015/2366 do Parlamento Europeu e Conselho, de 25 de novembro de 2015.

[231] Definida no art. 4.º n.º 30, como "*autenticação baseada na utilização de dois ou mais elementos pertencentes às categorias conhecimento (algo que só o utilizador conhece), posse (algo que só o utilizador possui) e inerência (algo que o utilizador é), os quais são independentes, na medida em que a violação de um deles não compromete a fiabilidade dos outros, e que é concebida de modo a proteger a confidencialidade dos dados de autenticação*". Na prática corresponderá à exigência de indicação de outros elementos além do habitual PIN, por exemplo, o já utilizado sistema de SMS Token, enviando um segundo código por sms, ou exigindo uma ou mais coordenadas.

[232] Os intermediários dos serviços de pagamento vêm assim designados na nova Diretiva, definindo serviço de iniciação do pagamento como o "*serviço que inicia uma ordem de pagamento a pedido do utilizador do serviço de pagamento relativamente a uma conta de pagamento detida noutro prestador de serviços de pagamento*" (cfr. art. 4.º n.º 15).

pagamento é prevista e regulada nos mesmos termos aplicáveis ao prestador do serviço. Consequentemente, terá se ser este a demonstrar que *operação de pagamento foi autenticada e devidamente registada, e não foi afetada por qualquer avaria técnica ou por outra deficiência relacionada com o serviço de pagamento pelo qual é responsável*[233] , sendo o dever de reembolso cumprido pelo prestador do serviço de pagamento que detenha os fundos os utilizador, quando o prestador do serviço de iniciação do pagamento seja responsável pela operação não autorizada, deve indemnizar aquele dos danos sofridos ou pelos montantes pagos em resultado do reembolso ao ordenante[234].

A repartição das perdas decorrentes das operações não autorizadas continua a ser a pedra de toque do regime. O titular do cartão perdido ou roubado e nos casos de apropriação abusiva do IP *com quebra da confidencialidade imputável ao ordenante* responde, hoje, até ao limite de €150, exceto quando atue com negligência grave, em incumprimento deliberado dos seus deveres ou fraudulentamente. Este limite, é na PSD II, reduzido para €50 para "*operações de pagamento não autorizadas resultantes da utilização de um instrumento de pagamento perdido ou furtado ou da apropriação abusiva de um instrumento de pagamento*", retirando-se da previsão a fórmula "*com quebra da confidencialidade imputável ao ordenante*". Desta forma, independentemente das circunstâncias da apropriação do IP, o titular responderá por perdas até €50[235], podendo assumir perdas superiores a este limite, quando seja demonstrado pelo prestador do serviço ou pelo intermediário, que agiu com dolo ou negligência grosseira em incumprimento dos seus deveres ou fraudulentamente[236]. Na proposta da diretiva retirou-se a possibilidade do legislador nacional dar um tratamento diferenciado à negligencia grave e às situações de fraude ou incumprimento deliberando, que o nosso legislador adotou no RSP, apresentando um regime de repartição dos prejuízos mais simplificado. Mas na Diretiva (UE) 2015/2366, esta possibilidade volta a surgir, permitindo-se reduzir a responsabilidade do utilizador que atue negligência grave "*tendo especialmente em conta a natureza das credenciais de segurança personalizadas e as circunstâncias específicas da perda, furto ou apropriação abusiva do instrumento de pagamento"*[237].

A norma do RSP que estabelece a responsabilidade do titular do serviço perante operações não autorizadas, vimos, não inclui, exceto no n.º 2, as operações de pagamento em que haja dispensa de cartão, conhecidas como *card-not-present,* onde não se exige a indicação dos

[233] Cfr. art. 72.º n.º 1.
[234] Cfr. art. 73.º n.º 2
[235] Cfr. art. 74.º n.º 1. Operou-se a redução do valor pelo qual responde o titular, na ausência de culpa, mas esse aparece agora estabelecido para todos os casos de roubo, perda ou apropriação abusiva de um IP, "*a fim de incentivar o utilizador do serviço de pagamento a notificar o prestador, sem demora indevida, o prestador do serviço de pagamento de qualquer furto ou perda de um instrumento de pagamento, reduzindo assim o risco de operações de pagamento não autorizadas, o utilizador só deverá ser responsável por um montante muito limitado, salvo em caso de atuação fraudulenta ou de negligência grosseira da sua parte. Neste contexto, afigura-se adequado um montante de 50 euros para garantir um nível elevado e harmonizado de proteção dos utilizadores na União*, referindo-se expressamente que *"(a) presente diretiva não deverá prejudicar a responsabilidade dos prestadores de serviços de pagamento pela segurança técnica dos seus próprios produtos"* – cfr. considerando 71 da PSD II. O titular deve, também aqui, ser imediatamente reembolsado do remanescente, prevendo-se agora que esse reembolso deve ser feito *"o mais tardar até ao final do primeiro dia útil seguinte",* (art. 73.º n.º 1).
[236] Cfr. art. 74.º n.º 1 (2º parágrafo).
[237] Cfr. art. 74.º n.º 1 (3º parágrafo).

dispositivos de segurança personalizados, que só o titular deve conhecer, mas apenas os dados gravados no próprio IP[238]. Na proposta de PSD II, estas hipóteses são tratadas de forma mais clara, prevendo o art. 74.º n.º 2: "*Caso o prestador de serviços de pagamento do ordenante não exija a autenticação forte do cliente, o ordenante só suporta as eventuais perdas financeiras se tiver atuado fraudulentamente*"[239]. A única situação em que o titular terá de suportar perdas será, então, quando atue fraudulentamente[240], tendo o prestador do serviço demonstrado essa atuação. Existindo *autenticação forte*, hipótese que não vem prevista na Diretiva, a repartição dos prejuízos será reconduzida ao regime geral de perda, roubo ou apropriação abusiva do IP[241]. As operações abusivas feitas através do *homebanking* ou o conhecimento das coordenadas do cartão matriz, pela técnica de *phishing* ou *pharming,* serão, exatamente, uma destas situações onde existirá a *apropriação abusiva do instrumento de pagamento.*

6. Considerações finais

O acompanhamento da realidade dos pagamentos eletrónicos pelo Direito, é algo fundamental, louvando-se o empenho da UE na evolução e uniformização da regulação da matéria que transcende, na grande generalidade dos casos, as fronteiras dos Estados-Membros. Propusemo-nos, com esta dissertação, colocar em relevo a vertente jurídica dos pagamentos eletrónicos que têm registado um crescimento, por si só, capaz de evidenciar a importância do tema. Pretendeu-se, assim, oferecer um pequeno contributo ao diálogo científico, sendo ainda poucas e muito recentes as decisões jurisprudenciais que utilizam o regime legal em vigor, que será em breve substituído.

A regulação desta matéria é maioritariamente protetora do cliente que se limita a aderir ao contrato de utilização, libertando-o do ónus da prova, consagrando um princípio de limitação dos prejuízos a assumir pelo titular, caso não atue com culpa, recaindo o remanescente – qualquer que seja o montante – sobre a entidade prestadora do serviço e conferindo-lhe o direito de reembolso imediato dos prejuízos decorrentes de operações abusivas/não autorizadas.

O objetivo de uniformização do regime aplicável aos pagamentos não foi, contudo, totalmente conseguido com a Diretiva de 2007. A nova Diretiva sobre a matéria mantém esse objetivo e consegue superar algumas das críticas feitas à anterior. O alargamento do

[238] O n.º 1, 3 e 4 do art. 72.º do RSP referem no seu texto expressamente as situações de "*perda, roubo ou apropriação abusiva do instrumento de pagamento*".
[239] A norma continua: "*Caso o beneficiário ou o seu prestador de serviços de pagamento não aceite a autenticação forte do cliente, reembolsa os prejuízos financeiros causados ao prestador de serviços de pagamento do ordenante".*
[240] Hoje, o art. 72.º n.º 2, além desta hipótese de fraude, prevê que o titular seja responsável por todos os prejuízos quando se prove o incumprimento deliberado de uma das obrigações previstas no art. 67.º do RSP.
[241] Neste sentido, MARIA RAQUEL GUIMARÃES, "(Ainda) a responsabilidade pelo uso indevido de instrumento de pagamento electrónicos em operações presenciais e à distância", *cit.,* pp. 135 e 136;

regime aos terceiros prestadores dos serviços feito pela PSD II é aplaudível, aumentando o alcance da regulação dos pagamentos que passa a abranger todos os participantes na operação. O limite de perdas a assumir pelo titular do IP foi reduzido para €50 para os casos de perda, roubo ou apropriação abusiva do IP, excluindo, de forma mais clara, as situações de falsificação do IP ou de *card-not-present* deste regime geral[242].

Não obstante, a PSD II mantém alguns dos erros que vinham já da anterior Diretiva. O legislador comunitário não corrigiu a terminologia utilizada nos artigos relativos às operações fraudulentas, referindo ainda o titular do IP fraudulentamente utilizado como *ordenante*. Esperamos que, pelo menos, o legislador nacional na transposição da Diretiva corrija esta referência, em nome da correção terminológica e da precisão jurídica. Espera-se, igualmente, que o legislador, adoptando a possibilidade de conceder um tratamento diferenciado aos casos em que se prove a negligência grave do utilizador (já adoptada a quando da transposição da Diretiva de 2007), o faça em termos mais claros, por exemplo, definindo uma moldura concreta dos prejuízos a assumir pelo utilizador capaz de superar as críticas feitas neste ponto ao RSP.

Na evolução dos números do comércio eletrónico, assim como da utilização do *homebanking* – apontado já como o canal preferencial de comunicação com o banco, também o Direito tem um papel essencial, respondendo de forma cabal e clara à questão da reparação dos prejuízos que, para muitos, será o fator decisivo no momento de utilização de um IP na internet, contribuindo para aumento da confiança e da segurança no uso de IP eletrónicos.

O contrato que permite o uso do IP, reconhecido na prática bancária, é hoje um contrato legalmente típico, sendo reconduzido ao esquema do contrato-quadro, pela sua patente aptidão para regular as futuras e sucessivas operações de pagamento. Os direitos e deveres das partes nesta relação encontram contornos e consequências concretas no RSP, que apresenta um equilibrado e adequado regime de repartição do risco e de responsabilidade entre as partes, sendo, desta forma, capaz de responder aos litígios que possam surgir entre as partes no contrato de utilização de IP eletrónico.

A repartição dos prejuízos apresentada no RSP incentiva a diligência de ambas as partes, contribuindo para o aumento da segurança associada ao sistema. É também esta a solução que deve ser dada pelos tribunais, pois, ainda que muitos salientem a enorme vantagem para as entidades prestadoras dos serviços, conseguindo "enormes poupanças de escala"[243], a verdade é que o sistema de pagamento apresenta benefícios recíprocos, devendo exigir-se uma atuação cuidadosa do titular do IP, que, não tendo culpa, estará amplamente protegido pela lei.

Na verdade, a nossa jurisprudência caminhou em diferentes sentidos ao longo dos anos. Quanto às situações de roubo de cartões, não foi incomum os tribunais adotarem entendimentos mais rígidos quanto ao dever de comunicar o roubo do IP e do dever de

[242] Cfr. art. 74.º n.º 1 a) e n.º 2 da Diretiva (UE) 2015/236.
[243] Cfr. Ac. do TRL de 24.05.2012 (Ezagüy Martins), *cit*.

guarda do mesmo impostos ao titular, condenando-o, em vários casos, a assumir totalidade dos prejuízos decorrentes das operações abusivas[244]. Já nos casos de operações não autorizadas realizadas no *homebanking*, através de técnicas de fraude recentes, os tribunais assumiram uma postura mais protetora do titular, que não tem especiais conhecimentos informáticos, desconsiderando comportamentos indiciadores de menor cuidado por parte do utilizador do serviço[245]. Só mais recentemente, primeiro no Acórdão da Relação de Guimarães de 25.11.2013, se começou a contrariar esta tendência protecionista.

Nota-se, igualmente, um certo desconhecimento do regime em vigor nalgumas decisões que julgam factos ocorridos já na sua vigência – e, portanto, caindo no seu âmbito de aplicação – ou analisam cláusulas de contratos anteriores, aos quais se aplica o RSP desde que as suas disposições sejam mais favoráveis, como ficou demonstrado. Esta é, felizmente, uma crítica que vem perdendo relevância, para tal tendo contribuído o Acórdão do STJ de 18.12.2013, sendo certo que os tribunais têm mais recentemente decidido os litígios que lhe são colocados à luz do RSP. No entanto, a jurisprudência continuou a aplicar as regras relativas ao contrato de mútuo, numa espécie, parece-nos, de complemento ao estatuído no RSP.

Por fim, refira-se que, sem prejuízo do acesso aos tribunais, os prestadores de serviços de pagamento devem permitir o acesso a meios extrajudiciais eficazes e adequados para a resolução de litígios de valor igual ou inferior à alçada da primeira instância (art. 92.º do RSP). O titular poderá, ainda, apresentar reclamações junto do Banco de Portugal, nos termos do art. 93.º do RSP, podendo esta entidade aplicar coimas[246].

A resolução dos litígios é, assim, uma questão nuclear na matéria dos serviços de pagamento e a União Europeia continua a manifestar essa preocupação, prevendo nos considerandos iniciais que os prestadores de serviços de pagamento disponham de procedimentos eficazes de reclamações, anteriores ao processo judicial[247].

Bibliografia

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

ANTUNES, JOSÉ A. ENGRÁCIA, *Direito dos Contratos Comerciais*, Coimbra, Almedina, setembro de 2009;

[244] Referimo-nos aos casos já apresentados do Ac. do STJ de 19.11.2002, do TRL datado de 19.05.2005, do TRP de 12.04.2010 e do TRL de 18.01.2011, *cit*.
[245] Veja-se, por ex., o Ac. do TRP de 07.10.2014 e o Ac. TRE de 22.05.2014, *cit*.
[246] Segundo informações disponíveis no Relatório de Supervisão comportamental do BdP, disponível em <http://clientebancario.bportugal.pt/pt-PT/Publicacoes/>, foram instaurados 34 processos de contraordenações com base no RSP, por incumprimento dos seus imperativos legais.
[247] Cfr. considerando 98 da PSD II.

CARVALHO, JORGE MORAIS, "Comércio Electrónico e Protecção dos consumidores" *in THEMIS*, Revista da faculdade de Direito da Universidade Nova, Ano VII, n.º 13, 2006, pp. 41-62;

CARVALHO, JORGE MORAIS, Prestação de Informação nos contratos celebrados à distância" *in Direito Privado e Direito Comunitário – alguns ensaios,* Âncora Editora, Lisboa, 2007, pp. 13-144;

CASTILLA CUBILLAS, MANUEL, *La tarjeta de crédito – Tratado de Derecho Mercantil,* Tomo 28*,* Marcial Pons, Ediciones Jurídicas y sociales, Madrid, 2007;

CORDEIRO, ANTÓNIO MENEZES, *Manual de Direito Bancário*, 5.ª edição, revista e atualizada, Coimbra, Livraria Almedina, maio de 2014;

CORDEIRO, ANTÓNIO MENEZES, *Manual de Direito Bancário*, 3.ª edição, revista e atualizada, Coimbra, Livraria Almedina, janeiro de 2006;

COSTA, MÁRIO JÚLIO DE ALMEIDA, *Direito das Obrigações,* 12.ª edição, revista e atualizada, Coimbra, Almedina, novembro de 2009;

FERNANDES, LUÍS A. CARVALHO, *Teoria Geral do Direito Civil*, Vol. II, 3.ª edição, revista e actualizada, Lisboa, Universidade Católica Editora, 2001;

FILHO, DEMÓCRITO REINALDO, "A Responsabilidade dos bancos pelos prejuízos resultantes do 'phishing'", Jus Navigandi, teresina, ano 13, n.º 1838, julho 2008, disponível *in* <http://jus.com.br/artigos/11481> (09.03.2015);

FONSECA, ALEXANDRE NILO, "Comércio eletrónico é uma ferramenta essencial para superar a crise" *in* ACEPI – Associação da Economia Digital, artigo de opinião 22.09.2009, disponível *in* <http://www.acepi.pt/> (19.02.2015);

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;

GATSI, JEAN, *Le Contrat-Cadre*, L.G.D.J., Paris, 1998;

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

GETE-ALONSO Y CALERA, MARIA DEL CARMEN, *El pago mediante tarjetas de crédito*, Editorial La Ley. Madrid, 1990;

GETE-ALONSO Y CALERA, MARIA DEL CARMEN, *Las tarjetas de crédito*, Relaciones contractuales y conflictividade, Marcial pons, ediciones jurídicas y sociales, SA, Madrid, 1997*;*

GUIMARÃES, MARIA RAQUEL**,** "A fraude no comércio electrónico: o problema da repartição do risco por pagamento fraudulentos" *in Infracções Económicas e Financeiras: Estudos de Criminologia e de Direito,* Coimbra, Coimbra Editora, 2013, pp. 581-597;

GUIMARÃES, MARIA RAQUEL, "A repartição dos prejuízos decorrentes de operações fraudulentas de banca electrónica (*home banking*); Anotação ao Acórdão do Tribunal da Relação de

Guimarães de 23.10.2012, Proc. 305/09", *in Cadernos de Direito Privado*, n.º 41, janeiro/março de 2013, pp. 45-69;

GUIMARÃES, MARIA RAQUEL, "Algumas considerações sobre o Aviso n.º 11/2001 do Banco de Portugal, de 20 de Novembro, relativo aos cartões de crédito e de débito", *in Revista da Faculdade de Direito da Universidade do Porto*, I, pp. 247-276.

GUIMARÃES, MARIA RAQUEL, "'(Ainda) a responsabilidade pelo uso indevido de instrumento de pagamento electrónicos em operações presenciais e á distancia' - Análise do regime introduzido pelo Anexo I do Decreto-lei nº 317/2009, de 30 de outubro(RSP), e das alterações que se perspectivam face à proposta de directiva do Parlamento Europeu e do Conselho, de 24 de julho de 2013" *in I Congresso de Direito Bancário*, Coimbra, Almedina, 2015, pp. 115 a 144;

GUIMARÃES, MARIA RAQUEL,"As operações fraudulentas de *home banking* na jurisprudência recente - Ac. do STJ de 18.12.2013" *in Cadernos de Direito Privado,* 2015, em fase de publicação;

GUIMARÃES, MARIA RAQUEL, *As Transferências electrónicas de fundos e os cartões de débito*, Almedina, Coimbra, 1999;

GUIMARÃES, MARIA RAQUEL, "O pagamento com cartão de crédito no comércio electrónico. Alguns problemas relativos à natureza jurídica, enquadramento contratual e regime aplicável, numa perspectiva comparada de Direito Português, Espanhol e Comunitário", *in Revista da Faculdade de Direito da Universidade do Porto*, ano IV, Coimbra, Coimbra Editora, 2007, pp. 311-366;

GUIMARÃES, MARIA RAQUEL, *O contrato-Quadro no âmbito da utilização de meios de pagamento electrónicos,* Coimbra, Wolters Kluwer/Coimbra Editora, 2011;

GUIMARÃES, MARIA RAQUEL, "O pagamento com cartão de crédito no comércio electrónico: evoluções legislativas recentes", *in Revista da Faculdade de Direito da Universidade do Porto*, ano IX, Coimbra, Coimbra Editora, 2012, pp. 153-167;

GUIMARÃES, MARIA RAQUEL, "Os cartões bancários e as cláusulas contratuais gerais na jurisprudência portuguesa e espanhola - Breve análise da jurisprudência mais recente dos tribunais superiores portugueses e espanhóis em matéria de cláusulas contratuais gerais inseridas nos contratos de utilização de cartões bancários", *in Revista de Direito e de Estudos Sociais*, ano XLIII, janeiro/março, 2002, n.º 1, Editorial Verbo, pp. 55-91;

GUIMARÃES, MARIA RAQUEL,"Texto que serviu de base à apresentação oral da tese de doutoramento com o título *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos*, em provas públicas realizadas na FDUP no dia 21 de Junho de 2010", *in Revista da Faculdade de Direito da Universidade do Porto*, ano VIII, Coimbra, Coimbra Editora, 2011, pp. 461- 472;

GUIMARÃES, MARIA RAQUEL, "The debit and credit card framework contract and its influence on European legislative initiatives", *in InDret Comparado, Revista para el Análisis del Derecho*, n.º 2, 2012, (<http://www.indret.com/es>);

GUIMARÃES, MARIA RAQUEL/REDINHA, MARIA REGINA, "A força normativa dos Avisos do Banco de Portugal – reflexão a partir do aviso n.º 11/2001, de 20 de novembro", *Nos 20 anos do Código das Sociedades comerciais – Homenagem aos profs. Doutores A. Ferrer Correia, Orlando Carvalho e Vasco Lobo Xavier*, Coimbra Editora, 2007, pp. 707-723;

LEITÃO, LUÍS MENEZES, *Direito das Obrigações,* Vol. III, 9.ª edição, Almedina, Coimbra, 2014;

MASON, STEPHEN, "Electronic banking and how courts approach the evidence" *in ScienceDirect - Computer Law & Security Report,* Volume 29, 2013, pp. 144-151, <http://www.sciencedirect.com> (12.11.2014);

MEDEIROS, ALICE, "Responsabilidade pelo uso fraudulento de cartões de crédito", *in Conflitos de Consumo*, Almedina, março de 2006, pp. 175-178;

MERCADO-KIERKEGAARD, SYLVIA, "Harmonising the regulatory regime for cross-border payment services", *in ScienceDirect - Computer Law and Security Review*, volume 23, 2007, pp. 177-187, <http://www.sciencedirect.com> (01.02.2016).

MONTEIRO, ANTÓNIO PINTO, "A Resposta do Ordenamento Jurídico Português à Contratação Bancária pelo Consumidor" *in Revista de Legislação e Jurisprudência,* n.º 3987, ano 143, julho/agosto de 2014, Coimbra Editora, pp. 376-390;

MORAIS, GRAVATO, "A utilização fraudulenta de cartões de crédito na contratação à distância", *in Estudos em comemoração do décimo aniversário da Licenciatura em Direito da Universidade do Minho*, Almedina, Coimbra, janeiro de 2004, pp. 27-48;

MOURA, INÊS ISABEL DE CAMPOS, "O contrato de prestação de serviços bancários através da Internet", *JusJornal,* n.º 1716, 25 de junho de 2013, disponível *in* <http://jusjornal.wolterskluwer.pt/> (22.01.2015);

OLIVEIRA, LUIZ GUSTAVO CARATTI DE, *Responsabilidade civil dos bancos nos casos de fraudes pela internet que lesam as contas de seus clientes* - Monografia de conclusão de curso apresentada ao curso de Pós-Graduação em Direito Civil e Processo Civil da Universidade Castelo Branco, disponível *in* <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=9110> (02.03.2015);

PATRÍCIO, JOSÉ SIMÕES, *Direito Bancário Privado*, Quid Juris, Lisboa, 2004;

PEREIRA, JOEL TIMÓTEO RAMOS, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris, 1.ª edição, Lisboa, 2005;

PRATA, ANA, *Contrato de adesão e Cláusulas contratuais Gerais – anotação ao Decreto-Lei n.º 446/85, de 25 de outubro*, Coimbra, Amedina, julho de 2010;

RAPOSO, AMÁVEL, "Alguns Aspectos Jurídicos dos Pagamentos através das Caixas Automáticas: Responsabilidade e Prova", *in Boletim do Ministério da Justiça*, n.º 377, junho, 1988, pp. 5-30;

ROCHA, MARIA VICTÓRIA, "Novos meios de pagamento no comércio electrónico (*e-commerce*)", *in Direito da Sociedade da Informação,* Vol. V, Coimbra Editora, julho de 2004, pp. 203-214;

SÁ, ALMENO DE, *Direito Bancário*, Coimbra, Coimbra Editora, 2009;

SANTOS, HUGO LUZ DOS, "Plaidoyer por uma 'distribuição dinâmica do ónus da prova' e pela 'teoria das esferas de risco' à luz do recente acórdão do Supremo Tribunal de Justiça, de 18/12/2013: o (admirável) 'novo mundo' no Homebanking?" *in RED -Revista Electrónica de Direito*, n.º 1, Fev. 2015, CIJE/FDUP <www.cije.up.pt/revistared> (20.04.2015);

SILVA, JOÃO CALVÃO DA, *Banca, Bolsa e Seguros – Direito Europeu e Português,* 4.ª edição, revista e aumentada, Coimbra, Almedina, Setembro de 2013;

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

SOARES, QUIRINO, "Contratos Bancários", *in Scientia Iuridica,* separata janeiro-abril 2003, tomo LII, n.º 295, Universidade do Minho, pp. 109-128;

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", *in ScienceDirect - Computer Law & Security Report,* Vol. 24, issue 6, 2008, pp. 555-561, <http://www.sciencedirect.com> (12.11.2014);

TELLES, INOCÊNCIO GALVÃO, *Manual dos Contratos em Geral*, 4.ª edição, Coimbra, Coimbra Editora, 2002;

TSIAKIS, THEODOSIOS / STHEPHANIDES, GEORGE, "The concept of security and trust in electronic payments", *in ScienceDirect - Computer Law & Security Report,* Volume 24, 2005, pp. 10-15, <http://www.sciencedirect.com> (12.11.2014);

VAN DER MEULEN, NICOLE, "You've been warned: Consumer liability in Internet banking fraud", *in ScienceDirect - Computer Law & Security Review*, volume 29, 2013, pp. 713-718 <http://www.sciencedirect.com>, (01.02.2016).

VASCONCELOS, JOANA DE, "Cartões de Crédito", *in Revista de Direito e de Estudos Sociais*, 1993, Ano XXXV, (VIII, 2ª série – N.º 1-2-3-4), pp. 71-181, pp. 305-347;

VASCONCELOS, JOANA DE, "Sobre a repartição entre titular e emitente do risco de utilização abusiva do cartão de crédito no direito português*" in Estudos em Homenagem ao Prof. Doutor Inocêncio Galvão Telles,* Vol. II, Coimbra, Almedina, 2002, pp. 487-517;

VASCONCELOS, MIGUEL PESTANA, "Dos contratos de depósito bancário", *in Revista da Faculdade de Direito da Universidade do Porto*, ano VIII, Coimbra, Coimbra Editora, 2011, pp. 141-178;

VASCONCELOS, PEDRO PAIS, "Mandato Bancário" *in Estudos em homenagem ao professor doutor Inocêncio Galvão Telles*, Vol. II - Direito Bancário, Coimbra, Almedina, dezembro de 2002, pp. 131-155;

VASCONCELOS, PEDRO PAIS, *Teoria Geral do Direito Civil,* 7.ª edição, Coimbra, Almedina, novembro de 2012;

VARELA, JOÃO ANTUNES, *Das obrigações em geral,* Vol. I, 10.ª edição, Coimbra, Almedina, março de 2010;

VERDELHO, PEDRO, "*Phishing* e outras formas de defraudação nas redes de comunicação" *in Direito da Sociedade da Informação,* Vol. VIII, Coimbra Editora, 2009, pp. 407-419.

Outros materiais consultados:

"A sociedade de informação em Portugal 2013" - Inquérito à utilização de Tecnologias de Informação e Comunicação pelas Famílias, disponível *in* <http://www.dgeec.mec.pt> (consultado a 20.04.2015);

"Economia digital em Portugal, 2009 – 2017" – Estudo IDC/ACEPI, disponível *in* <http://www.acepi.pt/> (10.11.2014);

"Online Consumer Payments Anaytics" - Estudo SIBS e Datamonitor publicado na edição SIBS Market Report, disponível *in* <http://www.sibs.pt/> (consultado a 22.07.2015).

Relatório sobre ameaças à segurança na internet - tendências 2013, volume 19, publicado em abril 2014, disponível em

<http://www.symantec.com/pt/pt/security_response/publications/thretreport.jsp> (30.03.2015)

Sinopse de Atividade de Supervisão Comportamental, disponível em <http://www. http://clientebancario.bportugal.pt/pt-PT/Publicacoes/RSC/Paginas/RSC.aspx> (02.11.2015).

SIBS FPS: Relatório e Contas 2014, disponível *in* <http://www.sibs.pt/> (consultado a 30.06.2015).

Jurisprudência

Salvo indicação em contrário, a jurisprudência citada pode ser consultada nas bases de dados jurídico-documentais do Ministério da Justiça, acessível em <www.dgsi.pt>.

Supremo Tribunal de Justiça

Acórdão de 20.06.1995 (Pais de Sousa), in CJ - STJ, ano III, 1995, II, pp.136-138;

Acórdão de 03.12.1998 (Armando Lourenço), in CJ - STJ, ano VI, 1998, III, pp. 140-145;

Acórdão de 20.04.1999 (Garcia Marques);

Acórdão de 23.11.1999 (Garcia Marques), in CJ - STJ, ano VII, 1999, III, pp. 100-108;

Acórdão de 12.10.2000 (Nascimento Costa), in CJ - STJ, ano VIII, 2000, III, pp. 67-70;

Acórdão de 23.11.2000 (Sousa Inês), in CJ - STJ, ano VIII, 2000, III, pp. 133-138;

Acórdão de 11.10.2001 (Silva Paixão), in CJ - STJ, ano IX, 2001, III, pp. 78-81;

Acórdão de 14.02.2002 (Ferreira de Almeida), in CJ - STJ, ano X, 2002, I, pp. 92-103;

Acórdão de 19.11.2002 (Azevedo Ramos), in CJ - STJ, ano X, 2002, III, pp. 135-139;

Acórdão de 16.03.2004 (Moreira Alves) in CJ - STJ, ano XII, 2004, I, pp. 127-132.

Acórdão de 17.05.2007 (Oliveira Rocha);

Acórdão de 15.05.2008 (Mota Miranda);

Acórdão de 21.10.2008 (Alves Velho);

Acórdão de 12.02.2009 (Hélder Roque);

Acórdão de 15.10.2009 (Alberto Sobrinho);

Acórdão de 02.03.2010 (Urbano Dias);

Acórdão de 18.12.2013 (Ana Paula Boularot).

Tribunal da Relação de Coimbra

Acórdão de 16.03.2004 (Távora Victor);

Acórdão de 15.06.2010 (Arlindo Oliveira).

Tribunal da Relação de Évora

Acórdão do de 05.07.2007 (Fernando Bento);

Acórdão do de 22.05.2014 (Mata Ribeiro).

Tribunal da Relação de Guimarães

Acórdão de 23.10.2012 (Filipe Caroço);

Acórdão de 30.05.2013 (Rita Romeiro);

Acórdão de 25.11.2013 (Espinheira Baltar);

Acórdão de 17.12.2014 (Fernando F. Freitas).

Tribunal da Relação de Lisboa

Acórdão de 16.06.1994 (Noronha de Nascimento), in CJ, ano XIX, 1994, III, pp.121-127;

Acórdão de 14.02.2000 (Torres Veiga), in CJ, ano XXV, 2000, I, pp. 110 a 113;

Acórdão de 19.10.2000 (Salazar Casanova), in CJ, ano XXV, 2000, IV, pp. 124 a 127;

Acórdão de 19.05.2002 (Manuel Gonçalves);

Acórdão de 03.06.2003 (Pimentel Marcos);

Acórdão de 19.01.2006 (Manuel Gonçalves), in CJ, ano XXXI, 2006, I, pp. 80 a 82;

Acórdão de 19.09.2006 (Maria Amélia Ribeiro);

Acórdão de 04.12.2006 (Luís Espirito Santo);

Acórdão de 27.09.2007 (Maria José Mouro);

Acórdão de 26.10.2010 (Maria Amélia Ribeiro);

Acórdão de 18.01.2011 (António Santos);

Acórdão de 20.10.2011 (Catarina Arêlo Manso);

Acórdão de 24.05.2012 (Ezagüy Martins);

Acórdão de 28.06.2013 (Anabela Calafate);

Acórdão de 04.07.2013 (Ondina Carmo Alves);

Acórdão de 05.11.2013 (Manuel Marques);

Acórdão de 12.12.2013 (Tomé Ramião);

Acórdão de 03.03.2015 (Manuel Marques);

Acórdão de 21.05.2015 (Ezagüy Martins).

Tribunal da Relação do Porto

Acórdão de 13.11.2000 (Santos Carvalho);

Acórdão de 28.09.2004 (Alberto Sobrinho);

Acórdão de 12.04.2010 (Ana Paula Amorim);

Acórdão de 29.10.2013 (Francisco Matos);

Acórdão de 07.10.2014 (Ana Lucinda Cabral);

Acórdão de 29.04.2014 (Francisco Matos).

Julgados de Paz

Sentença de 16.10.2006 (Cristina Moraes);

Sentença de 21.09.2012 (Maria Judite Matias);

Sentença de 27.09.2012 (Luís Filipe Guerra).