HOME BANKING: Consequências jurídicas

Diana Beatriz Carrasco Campos

Maria do Mar Patrício Carmo

LLM (Catolica Global School of Law)

Working Paper No. 3/2017

Fevereiro 2017

Keywords: *Home banking*; Contrato quadro de *home banking* ; Instrumento de pagamento; Banco; Deveres jurídicos; Internet; Fraude informática; Repartição dos prejuízos; Autenticação.

HOME BANKING: Consequências jurídicas

Diana Beatriz Carrasco Campos

dianabeatrizcc@gmail.com

Maria do Mar Patrício Carmo

maria.do.mar.carmo@gmail.com

Abstract

Executive Summary

Home banking, also known as *Internet banking, e-banking* or *online banking* is an electronic payment system that enables bank customers to conduct a wide range of financial transactions in a distant location, such as checking balances on existing accounts, paying bills, transferring funds to another person's account or topping up a mobile phone. Through the *home banking* service, clients may conduct their banking transactions simply and secure, anywhere and at anytime, as long as they have access to the Internet.

The present paper is focused on the legal consequences of the *home banking* service currently offered by almost every banking institution in the world.

Beginning with an analysis of the contract that covers *home banking* services, we attempt to identify the leading obligations undertaken by the banking institution and the customer, parties when contracting this service. Secondly we present the problem of *online banking* fraud in particular *phishing* and *pharming*. Lastly, and taking into consideration some relevant Portuguese case law on the matter, we analyze how the allocation of losses due to computer fraud is processed under the current Portuguese legal framework. On this matter it is crucial a careful evaluation between the bundle of obligations undertaken by this service providers combined with their legal contractual liability for risk, and the role that the users conduct (enabler or hinder) had on the damages of unauthorized payments.

TABLE OF CONTENTS

LISTA DE ABREVIATURAS 5

INTRODUÇÃO 6

1. CARACTERIZAÇÃO DO CONTRATO DE HOME BANKING – UM CONTRATO-QUADRO 8

2. O CONTEUDO DA RELAÇÃO CONTRATUAL 10

   2.1. OBRIGAÇÕES QUE VINCULAM O PRESTADOR DO SERVIÇO DE *HOME BANKING* E O UTILIZADOR 10

      2.1.1. DEVERES DO BANCO ENQUANTO PRESTADOR DO SERVIÇO DE *HOME BANKING* 10

      2.1.2. DEVERES DO CLIENTE ENQUANTO UTILIZADOR DO SERVIÇO DE *HOME BANKING* 18

3. A REPARTIÇÃO DOS PREJUIZOS DECORRENTES DE FRAUDE INFORMATICA NO CONTRATO DE *HOME BANKING* A LUZ DO REGIME ATUAL E DA DIRETIVA 2015/2366 DO PARLAMENTO EUROPEU E DO CONSELHO, DE 25 DE NOVEMBRO DE 2015 (PSD2) 20

   3.1. A FRAUDE NAS OPERAÇÕES DE *HOME BANKING* E A ATRIBUIÇÃO DO ÓNUS DA PROVA À ENTIDADE BANCÁRIA 20

   3.2. REEMBOLSO IMEDIATO DOS MONTANTES DE OPERAÇÕES DE PAGAMENTO NÃO AUTORIZADAS 21

   3.3. A RESPONSABILIDADE PELOS PREJUÍZOS DECORRENTES DE OPERAÇÕES DE PAGAMENTO NÃO AUTORIZADAS ANTES DA NOTIFICAÇÃO DO BANCO 23

CONCLUSÃO 29

BIBLIOGRAFIA 31

LISTA DE JURISPRUDÊNCIA 34

Lista de Abreviaturas

Ac.	Acórdão
art.	artigo
CC	Código Civil
Cfr.	Confrontar
cit.	citado
DL	Decreto-Lei
n.º	número
p.	Página
pp.	Páginas
Proc.	Processo
PSD	Diretiva relativa aos Serviços de Pagamento 2007/64/CE
PSD2	Diretiva relativa aos Serviços de Pagamento 2015/2366 do Parlamento Europeu e do Conselho que revoga a Diretiva 2007/64/CE
RGICSF	Regime Geral das Instituições de Crédito e Sociedades Financeiras
RSP	Regime Jurídico dos Serviços de Pagamento e Moeda Eletrónica
STJ	Supremo Tribunal de Justiça
TRE	Tribunal da Relação de Évora
TRG	Tribunal da Relação de Guimarães
TRL	Tribunal da Relação de Lisboa
TRP	Tribunal da Relação do Porto
Vol.	Volume

INTRODUÇÃO

O contínuo desenvolvimento tecnológico tornou a prestação de produtos e serviços através da Internet uma realidade possível e com custos relativamente baixos quer para consumidores quer para prestadores. Destarte, também as relações bancárias foram objeto de uma verdadeira revolução: a utilização da Internet possibilitou a prestação de serviços *standard* ao mesmo tempo que alargou o leque de serviços bancários disponíveis ao cliente e, consequentemente, o tipo de clientes captados[1]. Os Bancos domésticos conseguem agora atrair novos clientes a nível global com baixos custos de marketing e os Bancos internacionais lançam novos produtos e serviços, em tempo real, a todos os seus clientes à escala mundial, permitindo-lhes desta forma testar eventuais novos mercados e a possível lucratividade de estabelecerem presenças físicas nesses locais.[2] Foi neste contexto que surgiram os serviços de *home banking.*

O *home banking,* também denominado banco internético (*Internet banking*), *e-banking,* banco *online* ou banca eletrónica, consiste num serviço à distância por meio de canais telemáticos, prestado por instituições bancárias através de páginas de Internet seguras ou por telefone, que permite aos clientes realizar uma multiplicidade de operações bancárias (consulta de saldos, pagamento de serviços/compras, carregamento de telemóveis, transferência de valores depositados para contas próprias ou de terceiros, para a mesma ou para diversa instituição de crédito) relativamente às contas que sejam titulares. [3]

Como bem aponta CAROLINA FRANÇA BARREIRA, com a prestação deste serviço "*o banco reforça o compromisso com os seus clientes no sentido do aperfeiçoamento e desenvolvimento da atividade bancária, designadamente pela capacidade de resposta rápida e eficiente, sem prejuízo dos deveres de informação, lealdade, diligência e transparência"*, cumprindo assim com as exigências consagradas nos artigos 74.º e 77.º do RGICSF [4] e prosseguindo o princípio da

---

[1] "*Technology has permitted the convergence of many financial management transactions that previously were considered disparate. This has opened the path for offering banking products and services to different customers with different banking needs, such as corporations, small businesses and individuals all within one Internet-based platform."* Law & Regulation of Electronic Finance & Internet Banking - Introduction and Overview (2014), p. 4.

[2] CENTENO, CLARA, Adoption of Internet Services in the Enlarged European Union - Lessons from the Internet banking case - Report EUR 20822 EN (Junho 2003). European Commission Joint Research Centre, p. 6.

[3] Cfr. Acórdão do STJ de 18.12.2013, Proc. 6479/09.8TBBRG.G1.S1, Relator Ana Paula Boularot, disponível em www.dgsi.pt.

[4] Aprovado pelo Decreto-Lei n.º 298/92, de 31 de dezembro com as alterações introduzidas pelo Decreto-Lei n.º 1/2008, de 3 de janeiro.

simplicidade, já que pela via informática o Banco simplifica a contratação e a prática de vários atos bancários diminuindo consideravelmente os custos de transação.[5]

É no âmbito da relação contratual prévia, complexa e com uma vocação de perpetuidade entre o cliente e a instituição bancária, iniciada pelo contrato de abertura de conta e da constituição de depósitos de montantes em conta por parte do cliente ou de abertura de crédito, que surge o contrato de *home banking.* Com efeito, e apesar de ser habitual os clausulados dos contratos de abertura de conta incluírem grande parte do leque de regras que regem o contrato de *home banking*[6], este continua a ser um contrato plenamente autónomo, porquanto caracteriza-se pela existência de um acordo vinculativo assente em duas declarações de vontade (proposta e aceitação) distintas, em objeto e vontade de vinculação, face ao contrato de abertura de conta, apesar de temporalmente coincidentes com aquele[7]. Concordando com a mesma autora[8], ao celebrarem um contrato de abertura de conta as partes visam " *estabelecer a relação bancária que se irá desenvolver, ao longo do tempo, entre o banco e o cliente*"; já no contrato de *home banking* " *os contraentes procuram estabelecer uma forma do cliente movimentar os fundos da conta bancária recorrendo a meios informáticos*."

Admitindo a movimentação dos fundos disponíveis ao cliente, a utilização do contrato de *home banking* pressupõe a existência de uma relação contratual entre o Banco e o cliente que fixe os termos em que aqueles fundos existem e se encontram disponíveis, ou seja, a celebração conexa com o contrato de abertura de conta de um contrato de depósito ou de abertura de crédito[9], sendo certo que o contrato de banca eletrónica surge com ele coligado mas assumindo um carácter acessório e instrumental. A interdependência entre estes tipos negociais juridicamente autónomos deriva do nexo funcional necessário estabelecido entre o contrato de *home banking* e um contrato que atribua ao utilizador do serviço um conjunto de fundos disponíveis e passíveis de ser movimentados através de canais telemáticos qualificando-se como uma coligação de contratos. Por isso mesmo se o contrato de depósito cessar, extinguir-se-á por consequência o contrato de *home banking*.

---

[5] CORDEIRO, ANTÓNIO MENEZES., Direito Bancário, Almedina, Coimbra (2014), pp. 147-150.

[6] Anexos 1 e 2 (clausulados contratuais relativos ao serviço de *home banking* do Novo Banco e da Caixa Geral de Depósitos).

[7] Esta autonomia tem sido amplamente reconhecida pela jurisprudência, nomeadamente o TRL, no Acórdão de 26/10/2010, Proc. 1943/09.1TJLSB.L1-7, Relator Maria Amélia Ribeiro, disponível em www.dgsi.pt, afirmou que "*Estamos no domínio de uma relação negocial complexa que necessariamente foi iniciada através de um contrato de abertura de conta, com pelo menos um depósito ou depósitos de quantias numa conta a prazo, por parte da Autora, e no âmbito da qual as partes inscreveram um novo contrato destinado a permitir a movimentação da conta "por via telefónica ou Internet e por outras formas de acesso remoto que venham a ser criadas* […]".

[8] BARREIRA, CAROLINA FRANÇA., Home Banking: A repartição dos prejuízos decorrentes da fraude informática, Revista Eletrónica de Direito (2015), p. 6.

[9]Concluindo que a *ratio* do contrato de utilização de cartão de pagamento é comum à do contrato de *home banking* e nas palavras de MARIA RAQUEL GUIMARÃES, "*a anterioridade [do contrato de depósito] é, relativamente ao contrato de utilização de um cartão de pagamento, senão cronológica, pelo menos lógica*." GUIMARÃES, MARIA RAQUEL, O Contrato-quadro… (2011), cit., p.179.

Propomo-nos agora a elaborar uma breve análise do contrato de *home banking* enquanto contrato-quadro e da teia obrigacional que dele deriva. Num último ponto centraremos a nossa atenção no fenómeno da fraude informática no serviço de banca eletrónica e consequente repartição dos prejuízos entre o Banco e o cliente de operações de pagamento não autorizadas por virtude de fraudes.

1. CARACTERIZAÇÃO DO CONTRATO DE HOME BANKING – UM CONTRATO-QUADRO

Tal como o contrato de abertura de conta, o contrato de banca eletrónica é um contrato socialmente típico mas legalmente atípico, formando-se em consonância com os princípios gerais da formação dos contratos e seguindo a tendência verificada quanto aos contratos bancários, isto é, através da utilização de cláusulas contratuais gerais para a definição do seu conteúdo. Consubstanciando uma prestação de serviços, a subscrição ao *home banking* faz-se mediante um contrato de adesão[10][11] e, com base nele, o cliente solicita à instituição bancária a utilização de um serviço informático de forma a movimentar os fundos depositados, surgindo o direito de utilizar este serviço apenas com a adesão ao contrato de banca eletrónica, mais precisamente a todas as condições de utilização previstas no contrato.

Segundo MARIA RAQUEL GUIMARÃES, entende-se por contrato-quadro o contrato de base que visa definir as principais regras às quais irão ser submetidos acordos a celebrar sucessivamente no futuro – contratos de execução do contrato-quadro – destinado a preparar, facilitar e até potenciar a conclusão destes, mas com eles não se confundindo[12]. Este contrato estipula, assim, uma parte substancial do conteúdo de uma pluralidade de contratos contemporâneos ou futuros[13] [14]. A principal virtualidade desta figura consiste na reunião de diferentes contratos singulares celebrados em virtude da sua execução num único "veículo jurídico" (*rechtliches Band)* conseguindo-se desta forma prosseguir objetivos de simplificação e racionalização[15].

---

[10] *"(…) o seu clausulado encontra-se pré-elaborado e é imposto à parte contratualmente mais fraca (cliente) que se limita a aceitar as condições pré-estabelecidas pelo outro contraente (Banco)." Idem, ibidem,* p. 14.

[11] São aplicáveis a este contrato de adesão os mecanismos legais de proteção do consumidor e controlo das cláusulas contratuais gerais, mais precisamente, a Lei n.º 24/96, de 31 de julho e o DL n.º 446/85, de 25 de outubro, respetivamente.

[12] GUIMARÃES, MARIA RAQUEL, O Contrato-quadro… (2011), cit., p.62.

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

[14] Podemos verificar que esta figura contratual potencia uma *"multiplicidade de outros contratos subsequentes, simplificados, na sua conclusão e execução, através do recurso a meios eletrónicos"* GUIMARÃES, MARIA RAQUEL., A repartição dos prejuízos decorrentes de operações fraudulentas de banca eletrónica (*home banking):* Acórdão do TRG de 23.10.2012, Proc. 305/09*, Cadernos de Direito Privado, n.º 41,* CEJUR, Braga (Janeiro-Março 2013), cit., p.59.

[15] GUIMARÃES, MARIA RAQUEL, O Contrato-quadro… (2011), pp.160-161.

O contrato de *home banking* é um contrato-quadro face às sucessivas operações de transferência eletrónica de fundos ordenadas através do serviço de banca eletrónica, pois regula, prevê e simplifica as operações de pagamento a realizar no futuro com este instrumento de pagamento. Deste modo, sempre que é realizada uma operação de pagamento eletrónica através do serviço de *home banking* é celebrado um novo contrato de execução do contrato-quadro de banca eletrónica. A celebração destes contratos de execução apenas se torna possível em virtude da adesão do cliente ao serviço de *home banking* por via do contrato-quadro. No mesmo sentido se pronunciou o legislador no regime jurídico que regula o acesso à atividade das instituições de pagamento e a prestação de serviços de pagamento, (RSP)[16], ao classificar o contrato para utilização de instrumento de pagamento (no qual se inclui o contrato de *home banking)* como contrato-quadro, na alínea *o*) do seu artigo 2.º definindo-o 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".*

Não obstante, tal como menciona RAQUEL LIMA, os contratos de aplicação e de execução são contratos distintos e autónomos face ao contrato-quadro e não meros atos de execução do mesmo, pois apresentam uma natureza negocial pressupondo uma nova troca de declarações negociais que acrescem às que definiram a vontade inicial de celebração do contrato quadro[17]. Veja-se o que sucede com o contrato de *home banking*: no momento da sua celebração, os contraentes desconhecem quando emitirão ordens de pagamento no âmbito daquele serviço, em benefício de quem e quais os seus montantes. É por isso necessário existir uma renovação da vontade por parte do utilizador e do prestador de serviços em cada concreta operação de pagamento, celebrando-se por conseguinte um novo contrato. Deste modo, podemos concluir que cada nova execução de uma ordem de pagamento resulta de um novo acordo de vontade entre a instituição bancária e o cliente.

[16] Contido no Anexo I do Decreto-Lei n.º 317/2009, de 30 de outubro, com as alterações do Decreto-Lei n.º 242/2012, de 7 de novembro que transpôs a Diretiva 2007/64/CE do Parlamento Europeu e do Conselho, de 13 de novembro da qual decorre a introdução deste conceito de contrato-quadro no âmbito dos serviços de pagamento.

[17] LIMA, RAQUEL SOFIA. A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na Jurisprudência Portuguesa, Dissertação de Mestrado em Direito - Ciências Jurídico-Privatistas, Faculdade de Direito da Universidade do Porto, Porto (Julho de 2015), p. 11.

2. O CONTEÚDO DA RELAÇÃO CONTRATUAL

2.1 Obrigações que vinculam o prestador do serviço de *home banking* e o utilizador

A celebração do contrato de *home banking* gera uma relação obrigacional complexa donde avultam direitos subjetivos, deveres primários de prestação, deveres secundários e deveres acessórios. Previamente já aludimos à qualificação operada pelo RSP deste contrato enquanto contrato-quadro, originador de sucessivas operações de pagamentos eletrónicos, pelo que será também deste enquadramento legal regulador da utilização de instrumentos de pagamento que retiraremos um conjunto de direitos e deveres a cargo do utilizador de serviços de pagamento (cliente) e do prestador dos mesmos (instituição bancária). Este regime legal é imperativo quanto aos consumidores e quanto às microempresas, nos termos do artigo 62.º n.º1[18].

2.1.1 Deveres do Banco enquanto prestador do serviço de *home banking*[19]

I. Dever de emissão e entrega ao utilizador dos dispositivos de segurança associados ao *home banking* (códigos de acesso e cartão matriz)

Tendo sido celebrado o contrato de utilização do serviço de banca eletrónica, o Banco enquanto prestador do serviço obriga-se a emitir e a entregar à contraparte (cliente) os dispositivos de segurança associados (credenciais), nomeadamente o cartão matriz e os códigos de acesso. Trata-se de um dever secundário acessório[20] face à prestação principal, que apresenta como base legal a alínea *a)* do n.º1 do artigo 68.º do RSP.

Tanto os códigos de acesso como o cartão matriz assumem uma função de autenticação, enquanto dispositivos de segurança personalizados, em virtude do artigo 2.º alínea *v)* do RSP. Isto significa que só através dos mesmos é que o cliente pode aceder aos serviços abrangidos pelo *home banking*, em especial a realização de operações de pagamento (crédito ou débito), já que é com a inserção dos dados presentes nos mesmos que a operação de pagamento se

---

[18] Para efeitos de aplicação do RSP e do contrato aqui em análise considera-se consumidor toda e qualquer pessoa singular que no contrato de *home banking* atua com objetivos alheios às suas atividades comerciais e profissionais (alínea n) do artigo 2.º) e microempresa "*uma empresa que, no momento da celebração do contrato de prestação de serviços de pagamento, seja uma empresa de acordo com a definição constante do artigo 1.º e dos n.ºs 1 e 3 do artigo 2.º do anexo à Recomendação n.º 2003/361/CE, da Comissão, de 6 de Maio*" (alínea *c)* do artigo 2.º).

[19] De ressalvar ainda que aos deveres analisados neste ponto acrescem os deveres acessórios de conduta por parte do prestador de serviços de *home banking* constantes das alíneas *b)*, *c)*, *d)* e *e)* do nº 1 do artigo 68.º do RSP.

[20] ALMEIDA COSTA, MÁRIO JÚLIO DE., Direito das Obrigações, 17ª edição, Almedina, Coimbra, 2009, p.77.

considera autorizada pelo cliente e, por conseguinte, passível de ser executada pelo prestador do serviço/instituição bancária.

Importa referir que o sistema de autenticação que é exigido atualmente pelo RSP se encontra aquém das exigências comunitárias definidas para os pagamentos realizados na Internet[21]. Efetivamente, o artigo 97.º n.º1 da nova Diretiva PSD2 impõe a necessidade de os Estados Membros assegurarem que os prestadores de serviços de pagamento aplicam uma autenticação forte do cliente em caso de operações de pagamento eletrónico, devendo incluir elementos que associem de forma dinâmica a operação a um montante específico e a um beneficiário específico (n.º2).

Entende-se por autenticação forte do cliente, segundo o artigo 4.º nº 30," *uma 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* ".

A PSD2 faz desta autenticação forte uma prioridade, razão pela qual "sanciona" o prestador do serviço de pagamento quando o mesmo não a impõe, nomeadamente agravando a sua responsabilidade, uma vez que estabelece no seu artigo 74.º n.º2 que o cliente apenas suportará as perdas relativas a operações de pagamento não autorizadas quando atua fraudulentamente. Fora desses casos, será o prestador de serviços de pagamento, que não exigiu a autenticação forte do cliente, a suportar as perdas financeiras deste, mesmo que este tenha atuado em violação dos deveres de guarda e sigilo relativamente aos dispositivos de segurança que lhe estão associados.

No âmbito do envio dos códigos de acesso e cartão matriz ao cliente surgem por vezes problemas resultantes da sua interceção por terceiros. Relativamente a esta questão remetemos para o ponto IV onde aprofundamos com maior precisão e detalhe a obrigação do Banco de assegurar que os códigos de acesso e o cartão matriz só são acessíveis ao cliente e não a terceiros.

II. Dever de correta execução das ordens de pagamento autorizadas, reunidas todas as condições previstas no contrato de *home banking*

Aquando a celebração do contrato-quadro de *home banking*, nem o utilizador do serviço (cliente), nem o prestador do mesmo (Banco) conhecem de antemão o momento em que serão emitidas ordens de pagamento através daquele, em benefício de quem, e quais os seus

[21] Com efeito a Diretiva de Sistemas de Pagamento 2007/64/CE (PSD I) que o RSP transpôs para o ordenamento jurídico português, será revogada com a entrada em vigor no dia 13 de Janeiro de 2018 da Diretiva 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno (PSD2).

montantes. Significa isto que a celebração do contrato de banca eletrónica não constitui uma autorização genérica para todas as ordens de pagamento que o utilizador deste serviço pretenda realizar[22].

Ao invés, cada operação de pagamento realizada em execução deste contrato representa a celebração de um contrato de execução do mesmo, com o conteúdo já definido por aquele (ver *supra*), carecendo da verificação de manifestações negociais por parte do utilizador (autorização) e do prestador de serviços (concordância) para que sejam executadas.

Nos termos do artigo 65.º n.º1 da RSP só se considera autorizada uma operação de pagamento quando o ordenante/cliente que subscreveu o contrato de *home banking* consentir na sua execução. Segundo o n.º3 deste preceito legal, o consentimento do cliente deve ser manifestado segundo a forma acordada entre este e o prestador de serviço de pagamento, implicando o incumprimento daquela uma falta de autorização da operação pedida. Adaptando esta regra ao serviço de banca eletrónica, o consentimento apenas se verifica quando o cliente efetua uma operação de autenticação digitando as suas credenciais (os códigos de acesso e os números do cartão matriz) disponibilizados pelo Banco na plataforma de banca eletrónica desta instituição bancária.

A autenticação visa, por um lado, permitir ao utilizador que solicita o acesso ao serviço de *home banking* identificar-se perante a instituição bancária enquanto cliente que o subscreveu junto do Banco e portanto enquanto legítimo credor do serviço bancário que o Banco se obrigou a prestar; e por outro assegurar ao prestador de serviço (Banco) que a ordem de pagamento emitida pelo utilizador foi efetivamente consentida e deve por isso ser executada. Contudo, e para que uma ordem de pagamento emitida pelo ordenante/cliente seja executada pela instituição bancária/prestador de serviço, é ainda exigida a manifestação de vontade negocial de execução da ordem de pagamento por parte da instituição bancária.

Com efeito, como refere MARIA RAQUEL GUIMARÃES "*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* "[23]. Daqui se retira que não existe por parte do prestador do serviço *home banking* uma obrigação de concluir os contratos de execução (ordens de pagamento) podendo até recusar o cumprimento de ordens de pagamento. Tal resulta expressamente do disposto no artigo 76.º n.º2 do RSP, segundo o qual a instituição bancária pode recusar a ordem de pagamento do utilizador quando não se encontram cumpridas todas as condições estabelecidas no contrato-quadro de banca eletrónica para a sua execução.

---

[22] GUIMARÃES, MARIA RAQUEL, (Ainda) a responsabilidade pelo uso indevido de instrumentos de pagamento eletrónicos em operações presenciais e à distância: análise do regime introduzido pelo Anexo I do Decreto-Lei n.º 317/2009, de 30 de Outubro (RSP), e das alterações que se perspetivam face à Proposta de Diretiva do Parlamento Europeu e do Conselho, de 24 de Julho de 2013, I Congresso de Direito Bancário, Almedina, Coimbra (2015), p. 123.

[23] GUIMARÃES, MARIA RAQUEL, (Ainda) a responsabilidade... (2015), p. 123.

Veja-se o caso de o cliente emitir uma ordem de pagamento que ultrapassa os limites do saldo disponível da conta à ordem não estando prevista contratualmente a possibilidade de o mesmo realizar operações a descoberto, nem existindo qualquer crédito concedido ao mesmo por via de um contrato de abertura de crédito. Nesta situação, e segundo o artigo 76.º n.º2 do RSP deve o prestador de serviço notificar o utilizador dessa recusa, das razões que a justificam e do procedimento que o utilizador deve adotar para corrigir os erros que viciam a sua ordem de pagamento.

Cumpridos os requisitos de autenticação e as demais condições previstas no contrato de *home banking* não há qualquer fundamento legal que permita uma recusa lícita da execução da ordem de pagamento nos termos do artigo 76.º nº1 do RSP. Por conseguinte, deve a instituição bancária cumprir o único dever principal que sobre ela incorre na sequência da celebração do contrato de *home banking* - o dever de executar corretamente a ordem de pagamento.

III. Dever de manutenção de um serviço de *home banking* sem deficiências técnicas, eficaz e seguro

Segundo MARIA RAQUEL GUIMARÃES[24], o Banco ao disponibilizar o serviço de *home banking* tem o dever de manter operacionais os sistemas informáticos que o sustentam, bem como de assegurar que não se verificam falhas técnicas durante as operações de pagamento. Estamos perante um dever acessório de conduta da entidade bancária de prestar um serviço de *home banking* seguro e eficaz, decorrente do artigo 73º do RGICSF segundo o qual "*as instituições bancárias devem assegurar, em todas as atividades que exerçam, elevados níveis de competência técnica, garantindo que a sua organização empresarial funcione com os meios humanos e materiais adequados a assegurar condições apropriadas de qualidade e segurança*".

Assim, compete ao Banco, enquanto prestador do serviço de banca eletrónica, criar um sistema informático de acesso à conta bancária que seja seguro e no qual o utilizador confie para realizar as suas operações de pagamento. Este dever assume implicações práticas, nomeadamente, quando operações de pagamento solicitadas pelo utilizador não são executadas ou são incorretamente executadas, *i.e.*, quando o sistema informático que suporta o *site* do Banco e que gere os pedidos de ordens de pagamento sofre uma falha técnica que determine: i) não execução; ii) execução com um atraso considerável; iii) execução em benefício de destinatários incorretos; iv) execução em montantes errados, das operações de pagamento[25].

---

[24] GUIMARÃES, MARIA RAQUEL, A repartição dos prejuízos decorrentes… (2013), p.60.

[25] O caso *PACTO vs.People's United Bank/Ocean Bank* representou um marco na jurisprudência americana por ter sido o primeiro grande caso a chegar ao Federal Court of Appeals que responsabilizou o Banco pela falta de procedimentos de segurança razoáveis. Estava em causa um conjunto de operações de pagamento não autorizadas pela empresa PACTO que viu os seus serviços informáticos pirateados. Não obstante, considerou o douto tribunal que apesar de no caso se ter verificado a existência de procedimentos de autenticação a vários níveis, o Banco é

IV. Dever do Banco de assegurar que os códigos de acesso e o cartão matriz só são acessíveis ao cliente

O RSP prevê expressamente no artigo 68.º n.º1 alínea *a)* um dever do Banco assegurar que os mecanismos de segurança personalizados associados ao instrumento de pagamento apenas sejam acessíveis ao utilizador a quem foi conferido o direito à sua utilização. Isto é, o Banco deve adotar todas as medidas que estejam ao seu alcance para impedir que os códigos de acesso e o cartão matriz que entregou ao utilizador do serviço de *home banking*, essenciais na sua autenticação, não sejam intercetados por terceiros.

Este dever manifesta-se, numa primeira dimensão, no especial dever de cuidado que recai sobre o Banco no momento em que envia os códigos de acesso e cartão matriz ao cliente, na sequência do cumprimento do dever acima referido no ponto I. Como já mencionado, o envio daqueles dispositivos de segurança pode ser intercetado por terceiros estranhos à relação contratual entre o Banco e o cliente.[26]

Atualmente o artigo 68.º n.º2 do RSP responde a esta questão estabelecendo 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.*" Consequentemente, o prestador do serviço de *home banking* suportará as perdas resultantes do extravio ou interceção dos dispositivos de segurança personalizados, nomeadamente dos códigos de acesso e do cartão matriz que permitem o acesso àquele serviço e que em muitos casos são enviados por correio postal aos utilizadores. Compreende-se a *ratio* deste artigo na medida em que o risco só poderia incorrer sobre o Banco, já que o utilizador em nenhum momento controla o envio destes dispositivos de segurança.

V. Dever de informação qualificado acerca das medidas que o utilizador deve adotar para preservar a segurança dos códigos de segurança e cartão matriz

O dever referido no ponto anterior manifesta-se, numa segunda dimensão, na especial obrigação de informação qualificada acerca das medidas que o utilizador deve adotar para preservar a segurança dos códigos de segurança e cartão matriz. O cumprimento deste dever

---

responsável por não ter prestado atenção aos avisos de possível fraude criados pelo próprio sistema. O acórdão está disponível em http://ef67fc04ce9b132c2b32-8aedd782b7d22cfe0d1146da69a52436.r14.cf1.rackcdn.com/patco-ach-fraud-ruling-reversed-eresource-1-a-4919.PDF.

[26] Esta questão começou por ser levemente abordada pelo Banco de Portugal no artigo 11º do Aviso 11/2001 de 20 de Novembro (regulamenta contratos de utilização ou de emissão de um cartão de crédito ou de débito) onde se referiu que " *a entrega aos titulares quer do cartão quer do respectivo código (…) deve ser rodeada de especial cuidado, devendo ser adoptadas adequadas regras de segurança que impeçam a utilização do cartão por terceiros*". [sublinhado nosso]. Neste aviso o Banco de Portugal assumiu como principal preocupação a proteção dos interesses dos titulares dos instrumentos de pagamento que foram intercetados por terceiro, contudo não se comprometeu com a indicação de quem é que suportaria as perdas resultantes do extravio ou interceção dos mesmos. GUIMARÃES, MARIA RAQUEL (Ainda) a responsabilidade pelo uso indevido de instrumentos de pagamento… (2015), cit. pp. 125 e 126.

possibilita também ao Banco assegurar que os dispositivos de segurança só são acessíveis ao cliente (ver *supra*).

Citando MARIA RAQUEL GUIMARÃES, trata-se de "*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*"[27]. Comparando-o a uma "máquina industrial perigosa", a autora defende que se impõe ao Banco um dever de elucidação do cliente por via de alertas constantes acerca das formas sofisticadas de fraude de terceiros de que o mesmo pode ser alvo e dos meios ao seu dispor para se prevenir das mesmas[28].

Este dever de informação qualificado encontra-se estabelecido no RSP no artigo 53.º, alínea *e)*, subalínea *i)* segundo o qual deve a instituição bancária descrever ao utilizador do serviço de *home banking* um conjunto de medidas que o mesmo deve adotar para preservar a segurança dos seus cartões de acesso e cartão-matriz. Apesar do artigo 52.º n.º1 do RSP caracterizar este dever como um dever de informação pré-contratual, por força da sua remissão para o artigo 53.º, este dever é de realização progressiva ao longo da execução do contrato de *home banking.*

Em virtude da sofisticação e aperfeiçoamento das técnicas de fraude eletrónica, o cumprimento efetivo deste dever atualmente não se basta com a prestação de informação por parte da entidade bancária ao cliente, no momento inicial de execução do contrato, das condições de acesso ao seu portal de banca eletrónica e de uma recomendação de consulta de uma pasta com regras de segurança. Os Bancos "*viram a necessidade de refinar os alertas de fraude - de uma atitude passiva do utilizador, a quem se exigia que consultasse uma pasta com as regras de segurança (o que não é compatível com situações de pressão como aquelas com que diariamente nos deparamos) para uma posição activa, "obrigando" o utilizador a atentar nos alertas."*[29].

Tornou-se assim prática bancária para o cumprimento deste dever a colocação de alertas nas páginas oficiais dos Bancos para que os utilizadores destas plataformas: (i) não abram mensagens de correio eletrónico com remetente desconhecido; (ii) mantenham o computador protegido por meio de um antivírus atualizado; (iii) não acedam à página do Banco através de *links* que constem de mensagens de correio eletrónico ou da lista de favoritos do browser, devendo digitar o site oficial do Banco na barra de pesquisa; (iv) utilizem computadores pessoais e de confiança para o acesso à página do Banco, conectados a uma rede de Internet doméstica.

---

[27] GUIMARÃES, MARIA RAQUEL - A repartição dos prejuízos... (2013), p. 62.
[28] GUIMARÃES, MARIA RAQUEL– A repartição dos prejuízos… (2013), p. 62.
[29] Cfr. Acórdão do TRG de 17 de Dezembro de 2014, Proc. n.º1910/12.8TBVCT.G1, Relator Fernando Fernandes Freitas, disponível em: www.dgsi.pt.

Os clientes também são informados de que o Banco nunca lhes irá exigir mais do que três dos dígitos que constam do cartão matriz para a concretização de operações de pagamento na banca eletrónica. Confrontado com esse pedido o cliente nunca deve fornecer tais dados pois trata-se de uma tentativa de intrusão na sua conta *on-line*[30].

Todas estas recomendações visam evitar que os clientes do serviço de *home banking* cedam os seus dados pessoais (códigos de acesso e cartão matriz) a terceiros (piratas informáticos) que, através de esquemas fraudulentos criam a ilusão de se tratarem do próprio Banco. São exemplos as técnicas de *phishing* e *pharming*, às quais iremos fazer referência no último ponto deste trabalho.

Em suma, os Bancos procuram alertar os seus clientes para o cumprimento de regras de segurança durante a execução do contrato de *home banking* que se mostram fundamentais para que os clientes possam aceder às suas contas on-line sem que terceiros o possam fazer igualmente e, com isso, realizar operações de pagamento sem o seu consentimento.

Não nos esqueçamos, porém, que as técnicas de pirataria informática estão em constante desenvolvimento e aperfeiçoamento, pelo que se mostra difícil para os Bancos conseguir prever as novas técnicas de fraude eletrónica desenvolvidas pelos piratas informáticos e alertar os seus clientes acerca das mesmas. Daí que o cumprimento rigoroso daquelas regras de segurança não impeça que o cliente seja alvo de uma intrusão por parte de um pirata informático. Não obstante, tal como veremos no último ponto deste trabalho, isso não afasta a responsabilidade do Banco pela operação de pagamento não autorizada, que se materializa na obrigação de reembolso por parte do Banco relativamente ao cliente, no valor dessa operação de pagamento.

VI. Dever de criação de um perfil de utilizador para efeitos de vigilância das operações de pagamento

Está aqui em causa um dever de vigilância da entidade bancária relativamente às operações de pagamento realizadas pelo utilizador que se mostra fundamental na prevenção de operações fraudulentas já que as mesmas podem não ser detetadas imediatamente pelo utilizador e isso pode potenciar o a realização de operações de pagamento não autorizadas durante esse lapso temporal[31]. Hodiernamente, é possível afirmar que o cumprimento deste dever constitui uma prática comum em alguns Bancos, que veem nele uma forma de reforçar a segurança do sistema e de aumentar a confiança dos utilizadores no mesmo. Admitindo, deste modo, que os Bancos exercem esta atividade de vigilância das operações de pagamento

[30] Os anexos 3 a 5 demonstram exemplos de alguns daqueles alertas disponíveis nas páginas eletrónicas do Novo Banco e do Millennium BCP.
[31] LIMA, RAQUEL, A responsabilidade pela utilização abusiva…. p. 28.

realizadas pelo utilizador em conformidade com o seu perfil, discute-se se tal constitui uma obrigação imposta por lei ou contratualmente acordada[32].

No ponto 1 abordámos a complexidade da relação bancária e o seu carácter tendencialmente duradouro, razão pela qual é exigida às partes uma conduta conforme à boa-fé (artigo 762.º do Código Civil). Como bem denota o STJ no seu acórdão de 18 de Novembro de 2008[33], "*essa especial relação complexa, de confiança mútua e dominada pelo intuitus personae, impõe à instituição financeira padrões profissionais e éticos elevados, traduzidos em deveres de protecção dos legítimos interesses do cliente, em consonância com os ditames da boa fé.".* Os deveres de proteção dos interesses do cliente ali referidos configuram-se dogmaticamente como deveres acessórios de conduta, nos quais se inclui o dever de proteção e cuidado relativo ao património da contraparte[34] que tem como propósito conservar a situação jurídica dos bens do utilizador do serviço de *home banking* protegendo-o de ingerências lesivas de terceiros. Concordando com RICARDO DIAS, o interesse tutelado por este dever de proteção é o da "*manutenção do status quo dos bens jurídicos da contraparte na pendência da relação*."[35]

Ora, é possível defender que do dever acessório da entidade bancária de proteção da integridade dos fundos depositados pelo cliente resulta um dever de informação do cliente acerca de movimentos suspeitos realizados na sua conta bancária e, por conseguinte, um dever de vigilância. Somos assim da opinião de que o dever aqui em análise apresenta uma natureza legal.

Ao abrigo deste dever pode a instituição bancária impor ao cliente o cumprimento de determinados procedimentos de autenticação mais exigentes (v.g. confirmando a operação por via de assinatura com certificado digital ou por via de um código de validação da operação enviado por SMS ao cliente), para executar ordens de pagamento por si tidas como suspeitas por não serem conformes com o padrão de operações de pagamento realizadas pelo utilizador ou porque realizadas em local suspeito (por via da identificação do I.P. do computador que acedeu ao site do Banco).[36] Assim, ao forçar estes procedimentos de autenticação mais exigentes, a entidade bancária pretende assegurar-se que o ordenante da ordem de pagamento tida como suspeita é de facto o cliente que subscreveu o serviço de *home banking*.

---

[32] De facto, este dever de vigilância não se encontra expressamente estabelecido no regime legal do RSP, surgindo apenas alguns indícios do mesmo nos artigos 66.º n.º2 alíneas a) e b) e 73.º n.º1 alínea b), mas isso não impede uma certa franja da doutrina e jurisprudência portuguesas de defender a natureza legal deste dever em análise.

[33] Proc. n.º 08B2429, Relator Santos Bernardino, disponível em www.dgsi.pt.

[34] ALMEIDA COSTA, MÁRIO JÚLIO DE Direito das Obrigações, 17ª edição, Almedina, Coimbra (2009), p.78.

[35] DIAS, RICARDO GASPAR, Deveres de proteção e a fronteira entre responsabilidade civil contatual e extracontratual: um problema (também) de direito internacional privado? Dissertação de Mestrado em Direito, Universidade Católica do Porto, p. 8.

[36] No mesmo sentido Maria Raquel Guimarães, defende um dever de atuação " *sempre que o Banco se 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."* GUIMARÃES, MARIA RAQUEL, O contrato-quadro… (2011), p. 317.

Ao defender-se a existência de um dever de vigilância dos Bancos relativamente às operações de pagamento realizadas pelos seus clientes, procura-se deste modo determinar que aqueles reajam de forma preventiva e não meramente reativa (por via de alertas de fraudes) às fraudes realizadas por piratas informáticos. Nesse mesmo sentido pronunciou-se o TRG no seu Acórdão de 17 de Dezembro de 2014, que por via de uma analogia entre o Banco e a empresa Google – que traça um perfil dos titulares de contas correio eletrónico – entendeu que também as instituições de crédito teriam facilidade em traçar o perfil do seu cliente utilizador do serviço de *home banking*. Com base nesse perfil, os Bancos deveriam conseguir prevenir a prática de fraudes "*barrando as operações a quem, v.g. pela hora tardia e inusitada, tenta fazer "transferências" para terceiros, ou, pela repetição de transferências inusitada num curto lapso de tempo, enfim, tudo o que saia da normalidade que o cliente vem revelando, contribuindo assim para uma maior segurança do sistema, que se quer, até onde for possível, blindado*"[37][38]

2.1.2. Deveres do cliente enquanto utilizador do serviço de *home banking*

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

Nos termos do artigo 67.º n.º1 alínea *a)* do RSP o cliente deve utilizar o serviço de *home banking* de acordo com as condições que regem a sua emissão e utilização, podendo estas ser resumidas em dois tópicos principais. Por um lado, é exigido ao cliente que, para aceder ao serviço de banca eletrónica e autorizar ordens de pagamento o faça utilizando os dispositivos de segurança, mais precisamente códigos de acesso e cartão matriz. Por outro, é exigido ao cliente que quando utilize o serviço de *home banking* o faça no limite da provisão existente na sua conta bancária, no caso de ser uma conta à ordem, abstendo-se de efetuar operações a descoberto, salvo se tal tiver sido previamente acordado.[39]

---

[37] Proc. n.º 1910/12.8TBVCT.G1, Relator Fernando Fernandes Freitas, disponível em www.dgsi.pt.

[38] De igual modo se pronunciou o TRE de 22 de Maio de 2014, Proc. n.º 11/13.6T2ASL.E1, Relator Mata Ribeiro, disponível em www.dgsi.pt , ao sindicar o comportamento da instituição bancária como não diligente por não ter atendido ao perfil do utilizador do serviço de *home banking* para prevenir a prática de uma operação fraudulenta, senão veja-se "*atendendo ao perfil de utilizador do autor ao longo dos anos, no que se refere ao serviço de homebanking, (…) denota não ter tido a diligência que se impunha relativamente à transação em causa*".

[39] Note-se que se o cliente tiver celebrado um contrato de abertura de crédito com o Banco pode movimentar fundos superiores à provisão da sua conta bancária, no entanto deve fazê-lo respeitando as condições gerais acordadas com o Banco.

II. Dever de sigilo relativamente aos dispositivos de segurança associados ao *home banking* e dever de guarda do cartão matriz

Ao abrigo do artigo 67.º n.º2 do RSP, o cliente do serviço de *home banking* deve tomar todas as medidas razoáveis para preservar a eficácia dos códigos de acesso e cartão matriz associados.

Trata-se aqui de um dever de confidencialidade por parte do cliente relativamente aos dados que constam naqueles dispositivos e que permitem o seu acesso ao sistema de *home banking*. Com efeito, e como já anteriormente referido, uma vez digitados os códigos de acesso e os três dígitos do cartão matriz, o sistema reconhece o utilizador do serviço de banca eletrónica como o legítimo portador daqueles dispositivos e, por conseguinte, enquanto cliente com o qual o Banco celebrou o contrato de *home banking*.

Sendo este serviço não presencial mas eletrónico, apenas com base na introdução daqueles dados personalizados e únicos entregues ao cliente, consegue o Banco assegurar que as operações de pagamento foram efetivamente autorizadas nada obstando à sua execução. Resulta então como natural a exigência do Banco ao cliente de um dever de sigilo e de não transmissão a terceiros, ainda que seus mandatários, dos dispositivos de segurança em causa, sob pena de toda a base de confiança em que assenta este contrato se desvirtuar. Este dever de confidencialidade consta geralmente de forma expressa no contrato de *home banking*, sendo usual pedir-se ao cliente que memorize os códigos de acesso abstendo-se de os anotar, muito menos no próprio cartão-matriz que também deve ser guardado pelo cliente num local seguro e inacessível a terceiros.

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

Nos termos do artigo 67.º n.º1 alínea *b)* do RSP incumbe ao cliente notificar "sem atrasos injustificados" o Banco logo que tenha conhecimento da execução de uma operação de pagamento não autorizada pelo mesmo, ou do extravio dos códigos de acesso e cartão matriz.

Com efeito, se incumbe ao cliente o dever de guarda e de sigilo destes dispositivos de segurança, é natural que seja também sobre ele que impende o dever de comunicar ao Banco o seu extravio. Já ao Banco incumbirá o dever de disponibilizar, a todo o tempo, os meios adequados à realização desta notificação por força do artigo 68.º n.º1 alínea *c)* do RSP. Esta notificação assume uma importância decisiva pois estabelece o momento a partir do qual o cliente não suporta as consequências financeiras resultantes das operações de pagamento não autorizadas, matéria sobre a qual incidirá em parte o último ponto deste trabalho.

3. A REPARTIÇÃO DOS PREJUÍZOS DECORRENTES DE FRAUDE INFORMÁTICA NO CONTRATO DE *HOME BANKING* À LUZ DO REGIME ATUAL E DA DIRETIVA 2015/2366 DO PARLAMENTO EUROPEU E DO CONSELHO, DE 25 DE NOVEMBRO DE 2015 (PSD2)

3.1. A fraude nas operações de *home banking* e a atribuição do ónus da prova à entidade bancária

Não obstante as reconhecidas vantagens de comodidade e celeridade proporcionadas pelo serviço de *home banking aos* clientes bancários, este serviço encontra-se sujeito a um conjunto atual e dinâmico de ameaças à sua segurança que colocam em perigo as contas bancárias dos clientes[40]. No âmbito do contrato de banca eletrónica o paradigma de atuações fraudulentas traduz-se na intromissão de pessoa não autorizada em determinada rede informática através de um computador, acompanhada da movimentação do saldo bancário para contas de terceiros[41] de forma deliberada, com o fim imediato de obtenção de uma vantagem patrimonial em prejuízo do titular da conta bancária afetada.

A doutrina e a jurisprudência têm reconhecido os fenómenos do *phishing* e do *pharming* como as principais modalidades de fraude informática[42]. O *phishing* caracteriza-se pela confluência de dois comportamentos: pressupõe por um lado tentativas de aquisição de dados pessoais através do envio de *e-mails* com uma pretensa proveniência da entidade bancária do cliente, que reclamam o fornecimento de informações pessoais (códigos de acesso, combinações do cartão matriz, por exemplo) ou que contêm arquivos ou links para outras páginas capazes de adquirir esses dados; por outro lado um comportamento do cliente que possibilita esta aquisição ilícita dos dados essenciais à autenticação, ainda que não desconfiando deste invulgar pedido. O *pharming* visa o desvio do tráfego da página do Banco para uma outra, falsa, que a copia de forma quase integral, simulando o próprio nome de domínio (*domain name*) do prestador de serviço de *home banking*. É neste processo que surge o chamado *man in the middle:* o cliente crê estar a aceder à página fidedigna do Banco cumprindo todos os passos de autenticação quando na verdade o está a fazer numa página *Web* falsa sendo toda a informação por ele digitada visível para os *men in the middle* que, fazendo uso da mesma, a introduzem em tempo real na verdadeira página da instituição

[40] É do reconhecimento da realidade sagaz própria das técnicas de pirataria informática, seja na forma de ataques informáticos por *hackers* ou da interceção dos códigos de acesso introduzidos pelo cliente enquanto este os digita no âmbito do processo de autenticação (vulgo *keylogging*), que surgem dois dos já aludidos deveres: o dever da instituição bancária de manutenção de um serviço eficaz e seguro e o dever do cliente de sigilo relativamente aos dispositivos de segurança.

[41] GUIMARÃES, MARIA RAQUEL., As transferências eletrónicas de fundos… (1999), cit., p.209

[42] Estas intrusões não autorizadas num sistema informático configuram um crime de falsidade informática previsto no artigo 3.º da Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro), punível com pena de prisão de um a cinco anos.

bancária, alterando alguns dos dados da operação, podendo assim realizar outras operações sem que o cliente se aperceba das mesmas.

Será sobre a repartição das perdas resultantes destes tipos de fraude informática que versarão os próximos pontos.[43][44]O artigo 70.º do RSP atribui ao prestador do serviço de banca eletrónica o ónus de provar que as ordens de pagamento dadas pelo cliente foram devidamente autorizadas através da utilização efetiva dos mecanismos de autenticação disponibilizados, foram corretamente registadas e contabilizadas, e que a sua execução foi isenta de qualquer avaria técnica ou deficiência do sistema informático. A propósito do conteúdo exigido a tal prova, o n.º2 do referido artigo esclarece que o mero registo da operação de pagamento em causa não pode ser interpretado como um sinal inequívoco da autorização do titular[45]. Uma vez feita esta prova, caso o Banco se queira exonerar do dever de suportar os prejuízos decorrentes da operação de pagamento não autorizada, *i.e.,* débito indevido (ver *infra* 3.3), compete-lhe ainda provar, no caso concreto, o grau de participação do cliente na operação de pagamento não autorizada e o grau de culpa com que este atuou, ou seja, a prova de um comportamento negligente, fraudulento ou que traduza o incumprimento deliberado de deveres do utilizador.

3.2. Reembolso imediato dos montantes de operações de pagamento não autorizadas

Segundo o artigo 71.º n.º1 do RSP[46], depois de o cliente tomar conhecimento de uma operação de pagamento por si não autorizada e de notificar o Banco desse facto, deve a instituição bancária reembolsá-lo imediatamente no valor do montante indevidamente debitado em virtude dessa operação de pagamento. Este dever de reembolso imediato por parte do Banco dos valores subtraídos de forma fraudulenta previsto no RSP apresenta similitudes com a cláusula *solve et repete*[47] da qual resulta que primeiro lugar o Banco paga e

---

[43] GUIMARÃES, MARIA RAQUEL, A repartição dos prejuízos… (2013), p. 69.

[44] Como bem aponta CAROLINA FRANÇA BARREIRA, "*Devemos ainda ter presente durante a análise desta problemática que podem ser aplicadas disposições legais diferentes aos utilizadores de serviços de pagamento que sejam consumidores e aos que não o sejam pois, geralmente, estes últimos encontram-se em melhor posição para avaliar o risco de fraude e tomar medidas de salvaguarda."* BARREIRA, CAROLINA FRANÇA., Home Banking: A repartição dos prejuízos … (2015), *op. cit,* p. 36. Está aqui em causa a aplicação do nº 2 do artigo 62.º do RSP mas tal como a autora, centraremos a nossa análise nos casos em que os utilizadores vítimas destes tipos de fraude são consumidores e sendo-lhes por isso aplicável o regime dos artigos 70º a 72º do RSP.

[45] Ainda que o RSP não consagrasse tal regra chegaríamos a conclusão semelhante já que está aqui em causa a alegação de facto negativo (a não autorização da operação de pagamento) que justifica a atribuição à contraparte (o Banco) da prova do facto positivo contrário.

[46] A letra deste preceito legal carece de uma interpretação corretiva pois resulta do mesmo que o ordenante deve ser reembolsado pelo Banco, sendo o ordenante no âmbito de uma operação de pagamento não autorizada o terceiro que a realizou de forma fraudulenta. Por isso, em vez de "ordenante" dever-se-ia ler "titular do instrumento de pagamento utilizado fraudulentamente". Esta interpretação corretiva também deve ser realizada no artigo 72.º do RSP por idênticos motivos.

[47] BARREIRA, CAROLINA FRANÇA., Home Banking: A repartição dos prejuízos … (2015), *op. cit,* p. 60. LIMA, RAQUEL SOFIA. A responsabilidade pela utilização abusiva … (2015), *op.cit*, p.28

só depois se discute a repartição da responsabilidade entre as partes[48]. Consequentemente, o reembolso corresponde ao montante indemnizatório que seria apurado caso fosse o Banco considerado o único responsável pelos danos decorrentes da operação fraudulenta – débito indevido.

Como consequências civis da demora do Banco no reembolso imediato do montante da operação de pagamento não autorizada, o artigo 71.º n.º2 do RSP prevê a contagem de juros moratórios diários desde a data em que o cliente negou ter autorizado a operação de pagamento executada, até à data do reembolso efetivo, calculados segundo a taxa legal definida no Código Civil acrescida de dez pontos percentuais, não se afastando a possibilidade de haver lugar a indemnização suplementar.[49] Para além disso, há lugar a responsabilidade contraordenacional do Banco por se recusar a reembolsar o cliente do montante aqui em causa, ao abrigo do artigo 95.º alínea *p)* do RSP, podendo ser -lhe aplicada uma coima de 10 000€ a 5 000 000€ [50].

Importa ainda fazer alusão à PSD2 que, nos termos do artigo 73.º n.º1, continua a prever este dever de reembolso imediato clarificando que o mesmo deve ser cumprido o mais tardar até ao final do primeiro dia útil seguinte à tomada de conhecimento pelo Banco, sob pena de incorrer em mora. Esta Diretiva exclui o dever de reembolso imediato se o Banco tiver motivos razoáveis para suspeitar de fraude e comunicar por escrito esses motivos à autoridade nacional relevante (Banco de Portugal). Assim, com base nesta Diretiva permite-se ao Banco discutir a responsabilidade do cliente antes de o reembolsar pela quantia indevidamente debitada da sua conta.

Numa lógica de proteção do consumidor de serviços de pagamento a PSD2 veio estabelecer no artigo 73.º n.º1 o dever do Banco assegurar que a data-valor do crédito na conta de pagamento do cliente não seja posterior à data em que o montante foi debitado indevidamente[51].

---

[48] Apesar de o RSP não ser claro nesse sentido, constitui prática bancária a averiguação por parte do Banco de que cliente não foi o autor das operações de pagamento não autorizadas antes de proceder a qualquer devolução, não vá dar-se o caso de o próprio cliente estar a tentar defraudar o seu Banco.

[49] Note-se que os juros moratórios segundo este preceito normativo contam-se a partir da data em que o cliente negou ter autorizado a operação de pagamento e não a partir do momento em que a mesma foi realizada por terceiro de forma fraudulenta.

[50] Como as instituições bancárias são pessoas coletivas não lhes é aplicável o intervalo de 4 000€ a 2 000 000€ específico das pessoas singulares previsto igualmente no artigo 95.º do RSP.

[51] Por outras palavras, o legislador quis assegurar que os juros pagos ao cliente pelo montante que lhe foi creditado se calculam a partir da data em que essa mesma quantia lhe foi debitada indevidamente, já que, se não tivesse havido lugar a essa operação de pagamento não autorizada o cliente estaria a beneficiar desses juros sobre aquela quantia que já seriam devidos por força do seu contrato de depósito bancário.

3.3. A responsabilidade pelos prejuízos decorrentes de operações de pagamento não autorizadas antes da notificação do Banco

Num segundo momento, representando o reembolso um encargo oneroso para a instituição bancária a mesma irá querer discutir se o mesmo é devido e em que termos, por força da aplicação do instituto da responsabilidade civil contratual (ver supra 3.1).

A responsabilidade do Banco enquanto prestador de um serviço de *home banking*, à luz da RSP e da PSD2 é uma responsabilidade contratual pelo risco. Com efeito, o sistema informático que suporta o serviço de banca eletrónica é complexo e tem inerentes riscos próprios, nomeadamente, o risco de ocorrerem utilizações fraudulentas potenciadas pelo facto de as operações bancárias serem realizadas em "ambiente aberto", através da Internet e não numa rede privada do banco[52]. Ensina ANTUNES VARELA que a teoria do risco se baseia no facto de que " *quem cria ou mantém um risco em proveito próprio, deve suportar as consequências prejudiciais do seu emprego, já que deles colhe o principal benefício*" (ubi commodum ibi incommodum)[53].

Daqui resulta que é a entidade bancária que responde pelo risco do sistema informático, que sustenta o serviço de *home banking,* não ser seguro e permitir a intromissão de terceiros, já que é aquela que maiores benefícios colhe ao disponibilizar este serviço aos seus clientes.[54][55]

I. Apreciação do comportamento do utilizador

O artigo 72.º do RSP estabelece uma repartição da responsabilidade do Banco e do utilizador do serviço de *home banking* a partir da ponderação da contribuição das condutas de ambos, em especial do risco criado pelo Banco e da culpa do cliente, para o dano, *i.e*, para o débito indevido por força de uma operação fraudulenta executada por terceiro. Assim, havendo contribuição culposa do lesado/cliente para a concretização da operação fraudulenta, opera-se uma diminuição do *quantum* indemnizatório devido pelo Banco. Trata-se de repartir a responsabilidade pelo dano entre o lesado/cliente e o Banco em vista a uma "repartição justa e equilibrada".[56][57] É sobre a diferença entre o montante reembolsado e o *quantum*

---

52 GUIMARÃES, MARIA RAQUEL, As transferências eletrónicas de fundos…, *op cit*., pp. 44-45.

53 VARELA, ANTUNES, Obrigações em Geral, vol 1. 10.ª edição, Almedina, Lisboa (2000), p. 663.

54" *É o prestador de serviço de pagamento eletrónicos – independentemente da modalidade de instrumento de pagamento utilizado – que deve arcar com os danos potenciados pelas fragilidades dos sistemas de pagamento que comercializa".* BARREIRA, CAROLINA FRANÇA., Home Banking: A repartição dos prejuízos … (2015), op. cit, p. 65.

55 Não obstante ter direito de regresso sobre os beneficiários das operações de pagamento não autorizadas pelo cliente (terceiros, piratas ou hackers informáticos), tendo assim a entidade bancária legitimidade para agir contra estes procurando reaver dos mesmos os montantes que reembolsou ao cliente na sequência da fraude bancária.

56 PROENÇA, JOSÉ BRANDÃO, A conduta do lesado como pressuposto e critério de imputação do dano extracontratual", Porto (1996) p. 143.

57 É assim inerente a este artigo 72.º um principio valorativo de auto responsabilidade com base na qual se entende que " *Não seria razoável mas pouco natural, que a pessoa que concorreu adequadamente para o seu dano, que lesou os seus*

indemnizatório efetivamente devido pelo Banco a título de responsabilidade civil, que incide o direito de crédito do Banco face ao cliente. Em especial sobre o regime da culpa do lesado no ordenamento jurídico português BRANDÃO PROENÇA afirma que o facto de se estar em sede de responsabilidade contratual não impede a configuração de situações de culpa do lesado[58], para além de que se mostra perfeitamente possível o concurso entre risco e culpa do lesado apesar de a hipótese típica ser a do concurso entre culpa do lesado e culpa do lesante assim configurada no artigo 570.º do CC[59]. De notar que não sendo possível dar como provado algum tipo de comportamento do utilizador censurável por ser capaz de contribuir de alguma forma para a produção do resultado danoso (i.e. o débito indevido), responde o Banco por todos os prejuízos (responsabilidade pelo risco).

II. Dolo do utilizador

Caso o Banco logre provar que o cliente atuou com dolo, isto é, que incumpriu de forma deliberada os seus deveres enquanto utilizador do serviço de *home banking* previstos no artigo 67.º do RSP ou facilitou a execução desta operação de pagamento movido por intuitos fraudulentos, deve a responsabilidade do Banco ser totalmente excluída. Deve por isso o cliente devolver ao Banco a totalidade do montante reembolsado por aquele.

Considerou o legislador que nesta hipótese a conduta do cliente foi causa exclusiva na produção do dano (débito indevido da sua conta à ordem) não tendo o risco associado aos meios informáticos, contribuído de qualquer forma para a produção daquele dano.

III. Negligência grave do utilizador

Dispõe o n.º3 do artigo 72.º do RSP que se a operação de pagamento não autorizada resultar de negligência grave do cliente, este terá de suportar *"as perdas resultantes de operações de pagamento não autorizadas até ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, ainda que superiores a (euro) 150, dependendo da natureza dos dispositivos de segurança personalizados do instrumento de pagamento e das circunstâncias da sua perda, roubo ou apropriação abusiva." (sublinhado nosso)*

A aplicação prática deste preceito legal depende do alcance que se conferir ao conceito de "negligência grave", não tendo o RSP se comprometido com qualquer definição[60][61].

---

bens pessoais ou materiais por não ter tido certo cuidado (…) pudesse deslocar todo o dano para a esfera do lesante (…)" PROENÇA, BRANDÃO, A conduta do lesado como… (1996), cit., p. 415.

58 " *Pode afirmar-se, genericamente que o responsável pode alegar e provar a contribuição «culposa» do lesado para o dano, em qualquer pedido de indemnização fundamentado em responsabilidade pré-contratual, contratual ou extracontratual*" PROENÇA, BRANDÃO, A conduta do lesado como… (1996), cit., p. 30.

59 PROENÇA, JOSÉ BRANDÃO, A conduta do lesado como… (1996), cit., p. 32.

60 O mesmo já não acontece com a PSD2 que, no seu considerando 72 define como negligência grosseira como algo que deverá significar "*mais do que mera negligência, envolvendo uma conduta que revela um grau significativo de imprudência (…)".*

Primeiramente cumpre distinguir os vários graus em que se decompõe a negligência em função da ilicitude e da culpa. De acordo com o STJ, no seu acórdão de 9 de junho de 2010, Proc. n.º 579/09.1YFLSB, Relator Sousa Grandão, "*será levíssima quando o agente tiver omitido os deveres de cuidado que uma pessoa excepcionalmente diligente teria observado; será leve quando o parâmetro atendível for o comportamento de uma pessoa normalmente diligente e será grave quando a omissão corresponder àquela em que só uma pessoa especialmente descuidada e incauta teria também incorrido"*[62].

Um primeiro caso a apontar de negligência grave será o da notificação tardia da apropriação abusiva por parte de terceiros dos códigos de acesso e cartão-matriz por parte do cliente ao Banco[63]. Dada a difícil tarefa de demonstração em sede de prova do momento exato em que o cliente tomou conhecimento da fraude, considera-se suficiente a prova do momento em que o cliente não podia ignorar a ocorrência, nomeadamente quando consultou o seu extrato bancário que continha as operações fraudulentas[64]. Assim, tendo o Banco logrado provar que o cliente só o notificou da fraude dias após o conhecimento da mesma não poder ter sido por ele ignorado, considera-se provada a atuação com negligência grave por parte do cliente por este ter contribuído para a agravação dos danos devido à sua incúria e desatenção inexplicáveis que não teriam reflexo no padrão de comportamento "*mesmo daquelas [pessoas] que são pouco diligentes*"[65].

Todavia não é este o caso que tem assumido maior protagonismo nos tribunais portugueses. Efetivamente, a jurisprudência portuguesa é copiosa na discussão acerca da imputação ao cliente dos prejuízos resultantes de operações de pagamento não autorizadas a título de negligência grave, por o cliente ter fornecido o seu código de acesso ao *home banking* e todos os algarismos do seu cartão matriz a terceiros (piratas informáticos).

No nosso entender a resolução desta problemática cinge-se a duas questões essenciais: a prova da divulgação por parte do Banco de alertas na sua página *on-line* acerca dos procedimentos fraudulentos de que a serem seguidos pelo cliente teriam evitado a concretização da operação fraudulenta (cumprimento do dever de informação qualificado); e a

---

[61] Por isso, a jurisprudência portuguesa tem-se socorrido dos contributos doutrinários de ilustres autores portugueses para preencher este conceito indeterminado. Como bem aponta ANTUNES VARELA "O grau de reprovação ou de censura será tanto maior quanto mais ampla for a possibilidade de a pessoa ter agido de outro modo, e mais forte ou intenso o dever de o ter feito." in VARELA, ANTUNES Obrigações em Geral, vol. 1. 10.ª edição, Almedina, Lisboa, 2000, p. 574. Segundo ANA PRATA negligência grave define-se como sendo "*negligência grosseira, erro imperdoável, desatenção inexplicável, incúria indesculpável, vistos em confronto com o comportamento do comum das pessoas, mesmo daquelas que são pouco diligentes*" PRATA, ANA, Cláusulas de Exclusão e Limitação da Responsabilidade Contratual, 2005, Almedina, Lisboa, p. 308.

[62] Disponível em www.dgsi.pt.

[63] Como já referido, por força do artigo 67.º alínea *b)* do RSP recai sobre o cliente um dever de comunicação imediata, sem atrasos injustificados logo que tenha conhecimento da execução de uma operação de pagamento não autorizada pelo mesmo ou de extravio dos códigos de acesso e cartão-matriz.

[64] Consumer liability in case of fraud with electronic payment instruments: an analysis of European and Russian rules , Faculty of Law, University of Oslo, , p. 17 consultado no dia 18 de novembro de 2016.

[65] PRATA, ANA, Cláusulas de Exclusão …, 2005, op. cit, p. 308.

prova por parte do Banco de que o cliente forneceu os seus códigos de acesso e todos ou a maioria dos algarismos do seu cartão matriz aos piratas informáticos[66].

Aprofundando o conteúdo do dever de informação qualificado do Banco *supra* identificado, no que diz respeito às fraudes informáticas este consubstancia-se na disponibilização de alertas de segurança na página de acesso ao serviço de *home banking* que permitam ao cliente detetar indícios de fraude com base em comportamentos estranhos face ao contratualmente definido no contrato de banca eletrónica. São exemplos o facto de o Banco nunca pedir a confirmação de todas as combinações do cartão matriz, nem a atualização de dados pelo telemóvel, na página ou por *e-mail*, nem o *download* de aplicações para a realização de operações. Esta informação para além de constar em separadores próprios da página do Banco também é comum ser transmitida por via de *banners popups* ("avisos que surgem ao abrir a ligação de acesso ao *home banking* e que têm de ser fechados pelo cliente para conseguir aceder a este serviço")[67]. Os *banners* asseguram que a informação neles contida foi dada efetivamente a conhecer ao cliente, permitindo assim ao Banco cumprir com aquele dever, cuja prova se mostra mais facilitada uma vez que o Banco possui o registo do fecho destas janelas de informação pelo cliente.

Face ao exposto, somos da opinião que um cliente diligente é aquele que apreende efetivamente o conteúdo dos avisos que constam da página do Banco e/ou de *banners* e os assimila, de tal modo que quando confrontado com um dos indícios de fraude os reconheça como tal e não divulgue os seus dados pessoais de acesso ao serviço de *home banking*. A não adoção deste comportamento revela um enorme descuido e desatenção por parte do cliente em que só uma pessoa especialmente descuidada e incauta teria também incorrido, sendo por isso censurável a título de negligência grave[68].

Entendemos que foi também neste sentido que se pronunciou o TRG quando no seu acórdão de 25 de Novembro de 2013[69], analisando um caso de *pharming*, considerou o comportamento do cliente censurável a título de negligência, por ter digitado numa página clonada do Banco todos os números do seu cartão matriz, perante solicitação da página nesse sentido, justificando a sua posição da seguinte forma: *"Pois, para um utilizador informático minimamente diligente, cuidadoso, e minimamente informado no uso desta tecnologia, sabendo ou tendo o dever de saber dos perigos que assolavam o sistema (através da informação prestada*

---

[66] Não podemos olvidar o carácter "diabólico" que esta prova simboliza uma vez que representa um encargo demasiado pesado para o Banco por dizer respeito "*a factos que estão fora da sua esfera de controlo*"- nomeadamente a *e-mails* pessoais dos utilizadores (*phishing*) ou aos registos informáticos de páginas clonadas (*pharming*), BARREIRA, CAROLINA FRANÇA., Home Banking: A repartição dos prejuízos …(2015),cit. p. 50.

[67] Acórdão do TRP de 29 de Abril de 2014, Proc.n.º 225/12.6TJVNF.P1, Relator, Francisco Matos, disponível em www.dgsi.pt.

[68] No mesmo sentido, BARREIRA, CAROLINA FRANÇA, op.cit. 2015, p. 79; GUIMARÃES, MARIA RAQUEL, As operações fraudulentas… p. 32; LIMA, RAQUEL SOFIA RIBEIRO de, A responsabilidade pela utilização abusiva… op.cit. p. 50 e 51.

[69] Proc.n.º 2869/11.4TBGMR.G1, Relator Espinheira Baltar, disponível em www.dgsi.pt.

pela ré sobre o assunto e colocada no site onde as pessoas eram logo alertadas e podiam informar-se melhor acedendo ao menu segurança) e a Web em geral, tinha que se questionar perante tal solicitação. E, perante esta dúvida, tinha um de dois caminhos a seguir, ou contactava rapidamente com a ré, via telefone, ou ignorava a solicitação e comunicava o acontecimento à ré. E só em face da solução que lhe fosse dada, é que continuaria a usar o programa. Tinha de ter a consciência que estava numa situação que não era normal e tinha de sanar a dúvida."

Mais, o Tribunal censura o comportamento dos utilizadores do serviço de *home banking* que apenas se focam no acesso imediato ao serviço para realizarem operações na sua conta, desinteressando-se dos anúncios e avisos que constam da página do Banco ou dos *banners*, isto porque sobre os mesmos incide um dever de confidencialidade relativamente aos códigos de acesso e cartão matriz cujo cumprimento é exigido ao longo da execução do contrato de banca eletrónica, nomeadamente por via da tomada de conhecimento dos alertas de segurança que permitem evitar acessos de terceiro a esses dados.

Fora destes casos [em que o Banco consegue provar a publicação de avisos de segurança que a serem seguidos pelo cliente, não teriam permitido a execução da operação fraudulenta, bem como a prova da revelação pelo cliente a terceiros de todos os seus dados pessoais de acesso ao serviço de *home banking*], há que distinguir duas situações. Por um lado, não provando o Banco que ao tempo da operação fraudulenta tivesse disponibilizado aos clientes informações acerca daquela fraude em concreto, mas sendo ainda o comportamento do cliente passível de censura, o mesmo só responderá pelos prejuízos resultantes de operações de pagamento não autorizadas se atuar a título de negligência leve[70]. Em contrapartida, provada a divulgação por parte do Banco de alertas na sua página *Web* acerca dos procedimentos fraudulentos de que o cliente pode ser vítima mas não conseguindo a instituição bancária provar que o cliente disponibilizou a terceiros não autorizados os seus códigos de acesso e todos ou a maioria dos dados do seu cartão-matriz, os prejuízos não são imputáveis ao utilizador, nem a título de negligência leve[71].

---

[70] Enquadramos aqui o caso alvo de apreciação pelo TRP de 7 de Outubro de 2014, Proc n. 747/12.9TJPRT.P1, Relator Ana Lucinda Cabral, pois apesar dos avisos de segurança não visarem em concreto a situação de fraude de que o cliente foi vítima no processo, o certo é que o cliente não era inexperiente nem insensível aos riscos inerentes a este serviço. Por conseguinte perante um pedido de *download* estranho ao até então praticado pelo Banco, o cliente deveria duvidar da sua proveniência, pois seria esse o padrão de comportamento exigido a um utilizador normalmente diligente, e não realizar o download solicitado sem antes contactar o Banco acerca desta alteração aos procedimentos habituais para aquela operação. Tal quadro leva a que por isso deva ser ainda que a título de negligência leve censurada a sua conduta, apesar de não ter sido essa a posição ao adotada pelo douto Tribunal, que entendeu não ser censurável a conduta do cliente que fez o *download* da aplicação.

[71] Veja-se o acórdão do TRL de 5 de Novembro de 2013, Proc. n.9821/11.8T2SNT.L1-1, Relator Manuel Marques, onde da factualidade apurada não se deu como provado a cedência por parte da utilizadora das suas credenciais a terceiros pelo que não se pôde concluir ser imputável àquela uma quebra da confidencialidade dos dispositivos de segurança.

IV. Negligência leve do utilizador

Nos termos do n.º1 do artigo 72.º, se o Banco lograr provar que a quebra de confidencialidade dos códigos de acesso e cartão matriz é imputável ao cliente a título de negligência leve, o cliente responde pelos prejuízos resultantes da operação fraudulenta dentro do limite do saldo disponível ou da linha de crédito associada à sua conta à ordem, até ao limite máximo de 150€. O Banco responderá pelos prejuízos remanescentes decorrentes da operação de pagamento não autorizada, a título de risco, pois compete a este suportar o risco do sistema informático que suporta o serviço de *home banking* não ser seguro por permitir a intromissão de terceiros. Esta solução legal vigora com algumas modificações na PSD2. Efetivamente, o legislador comunitário pretendeu, neste diploma legal, evitar a ocorrência de operações de pagamento não autorizadas, incentivando os utilizadores dos instrumentos de pagamento a detetarem a perda, o furto ou a apropriação abusiva do instrumento de pagamento antes da ocorrência da operação de pagamento fraudulenta. Para tal, estabeleceu que nos casos em que seja possível ao utilizador do instrumento de pagamento detetar tais eventos com a antecedência suficiente que lhe permita notificar o Banco acerca dos mesmos, e mesmo assim não o faça, realizando-se a operação de pagamento não autorizada, o cliente responde no montante máximo de 50€[72].

[72] Parece-nos assim que o legislador comunitário considerou que o cliente ao não adotar uma postura preventiva quanto às apropriações por terceiros dos seus instrumentos de pagamento atua a título de negligência leve. Tal conclusão resulta também do considerando 71 da PSD2.

CONCLUSÃO

Atualmente é inegável a adaptação da banca tradicional à era digital. Progressivamente assistimos a uma substituição do Banco enquanto local físico ao qual os clientes bancários se dirigem por um Banco cujos serviços estão disponíveis *on-line* em qualquer lugar, a qualquer momento, através da utilização de um computador ou dispositivo móvel. Segundo Francisco González, presidente do Banco BBVA "*A sobrevivência da banca de retalho passa não só pelo negócio bancário mas sobretudo pela capacidade de se transformar em empresa de software*"[73].

Esta aposta na tecnologia enquanto modelo de negócio deve-se por um lado, à alteração dos hábitos dos clientes bancários que num mundo "*always-on*" estão cada vez mais habituados a gerir a sua vida *on-line* exigindo por isso das instituições bancárias uma experiência digital de prestação de serviços bancários, e por outro a uma necessidade de recuperação da rentabilidade do setor bancário. Assim, numa ótica de simplificação e de redução dos custos de transação, compatível com as exigências de uma sociedade digital globalizada, tornou-se premente a diversificação de canais utilizados para a contratação de serviços bancários, sendo o *home banking* um desses exemplos. O *home banking* permite aos clientes bancários realizar uma multiplicidade de operações bancárias através de páginas seguras de Internet mas, sendo este um serviço disponibilizado pelo Banco, incumbe-lhe a ele assegurar que o mesmo é eficaz e seguro[74].

Todavia, e não negando a utilidade e comodidade que proporciona aos seus utilizadores, a banca eletrónica ao fazer depender o seu acesso da utilização da Internet encontra-se sujeita a ataques cibernéticos que podem visar quer a própria infraestrutura técnica que suporta o *home banking* quer o cliente através da obtenção fraudulenta de fundos pela interceção das suas credenciais. Estas quebras da segurança e eficácia do serviço, quando conjugadas com o feixe de deveres que competem ao prestador deste serviço, permitem retirar a conclusão que será a instituição bancária a arcar com os prejuízos das operações fraudulentas (débito indevido).

A responsabilidade que sobre os Bancos corre deve por isso ser atenuada pela combinação de uma política de autenticação forte com o exercício cada vez mais eficiente de um dever de informação qualificado[75], introduzindo nas suas páginas oficiais avisos, alertando

---

[73] Cfr. Notícia de 6-10-2015 do jornal Expresso "*Economia digital obriga banca a reinventar-se*", disponível em http://expresso.sapo.pt/iniciativaseprodutos/click-portugal/2015-10-06-Economia-digital-obriga-banca-a-reinventar-se consultada a 22 de Novembro de 2016.

[74] Nesta senda cumpre destacar o papel impulsionador das EBA *Guidelines on the security of Internet payments* publicadas em 2014 e que entraram em vigor no espaço europeu a 1 de Agosto de 2015, que visam reforçar a base legal para a implementação de políticas de fiscalização e supervisão a serem seguidas pelos prestadores de serviços de pagamento, bem como os contributos que o Anti-Phishing Working Group e o Anti-Phishing Mobile Working Group têm trazido para a discussão e adoção de melhores práticas e soluções técnicas que permitam uma resposta verdadeiramente eficaz no combate ao cibercrime financeiro.

[75] "*Education is a key priority for the mitigation of risks caused by customers' lack of awareness (…) [and] should not only cover financial topics, but also techonological features associated with mobile or online payments*" FINCONET INTERNATIONAL

os clientes de indícios de fraude de que podem ser vítimas e de quais as precauções que os mesmos devem tomar. Trata-se aqui de chamar o cliente bancário a exercer de forma ativa o seu dever de confidencialidade relativamente aos códigos de acesso e cartão matriz cujo cumprimento é exigido ao longo da execução do contrato de *home banking* e que inclui a tomada de conhecimento dos alertas de segurança acima referidos. Por isso mesmo somos da opinião que as consequências das operações fraudulentas realizadas por via do sistema de *home banking* são tanto mais desvantajosas para o utilizador do serviço quanto mais censurável se revelar a sua conduta. Não pode o cliente bancário adotar uma postura de total indiferença perante os riscos inerentes aos sistemas informáticos, e ignorar os avisos que surgem na página do Banco, porquanto faz perigar a confidencialidade dos instrumentos de autenticação que possui violando o seu dever sigilo quanto aos mesmos.

Procuramos defender no presente trabalho a importância da análise do comportamento do cliente antes da notificação ao Banco da operação de pagamento não autorizada. À medida que a atuação do utilizador se revela mais censurável, e por isso potenciadora do débito indevido, este responde, de forma mais alargada, pelos prejuízos até ao limite máximo da desresponsabilização total do Banco, nos casos de dolo ou comportamento fraudulento do mesmo. É este o critério adoptado pelo RSP e também pela PSD2 e que, no nosso entender, opera uma repartição justa e adequada dos danos. Com efeito, não obstante o sistema informático que suporta o serviço de *home banking* estar sujeito a um risco de intromissão de terceiros porque opera numa rede aberta de Internet e não numa rede privada do Banco, nem sempre esse fator é causa exclusiva da obtenção fraudulenta de fundos por piratas informáticos. Em muitos dos casos é o utilizador, com a sua conduta negligente ou dolosa, que concorreu adequadamente para a concretização da operação de pagamento fraudulenta, nomeadamente conferindo aos piratas informáticos os seus códigos de acesso e cartão matriz sabendo de antemão, por via de avisos de segurança do Banco que não o deve fazer.

FINANCIAL CONSUMER PROTECTION ORGANIZATION, Online and mobile payments - Supervisory challenges to mitigate security risks. FinCoNet International Financial Consumer Protection Organization, cit., p. 49 (Setembro 2016).

BIBLIOGRAFIA

ALMEIDA, Carlos Ferreira de, *Contratos II,* Almedina, Coimbra (2012);

ALMEIDA, Carlos Ferreira de, *Contrato bancário geral e depósito bancário*, Coleção de Formação Contínua – Direito Bancário, Lisboa: Centro de Estudos Judiciários (2015). Acedido em 30 de Outubro de 2016, a partir de http://www.cej.mj.pt/cej/recursos/ebooks/civil/Direito_Bancario.pdf;

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

ANTUNES, José A. Engrácia, *Direito dos contratos comerciais,* Almedina, Coimbra (2011);

BARREIRA, Carolina França, *Home Banking: A repartição dos prejuízos decorrentes da fraude informática,* Revista Eletrónica de Direito (2015). Acedido em 12 de Outubro de 2016, a partir de http://www.cije.up.pt/content/home-banking-reparti%C3%A7%C3%A3o-dos-preju%C3%ADzos-decorrentes-de-fraude-inform%C3%A1tica

CENTENO, Clara, *Adoption of Internet Services in the Enlarged European Union - Lessons from the Internet banking case - Report EUR 20822 EN,* European Commission Joint Research Centre (Junho 2003);

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

CORREIA, Pedro Miguel Alves Ribeiro; JESUS, Inês Oliveira Andrade de, *Combate às transferências bancárias ilegítimas pela Internet no direito português: entre as experiências domésticas e as políticas globais concertadas,* Revista Direito GV, São Paulo (Maio-Agosto 2016). Acedido em 12 de Outubro, a partir de http://dx.doi.org/10.1590/2317-6172201622;

CRONIN, Mary J., *Banking and Finance on the Internet,* John Wiley & Sons, Inc, New York, USA (1997). Acedido em 23 de Outubro, a partir de https://books.google.ie/books?id=l94FEs-lMu4C&printsec=frontcover&hl=pt-PT&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false;

DIAS, Ricardo Gaspar, *Deveres de proteção e a fronteira entre responsabilidade civil contratual e extracontratual: um problema (também) de direito internacional privado?*, Dissertação de Mestrado em Direito - Área de Direito Privado. Porto: Faculdade de Direito - Escola do Porto da Universidade Católica Portuguesa (2012);

FINCONET INTERNATIONAL FINANCIAL CONSUMER PROTECTION ORGANIZATION, *Online and mobile payments - Supervisory challenges to mitigate security risks.* FinCoNet International Financial Consumer Protection Organization (Setembro 2016);

GKOUTZINIS, Apostolos Ath, *Internet Banking and the Law in Europe - Regulation, Financial Integration and Electronic Commerce,* Cambrisge University Press, New York, United States (2006);

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

GUIMARÃES, Maria Raquel, *(Ainda) a responsabilidade pelo uso indevido de instrumentos de pagamento eletrónicos em operações presenciais e à distância: análise do regime introduzido pelo Anexo I do Decreto-Lei n.º 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,* I Congresso de Direito Bancário, Almedina, Coimbra (2015), pp. 115-144;

GUIMARÃES, Maria Raquel, *As operações fraudulentas de homebanking na jurisprudência recente: Acórdão do Supremo Tribunal de Justiça de 18.12.2013, Proc.6479/09*, Cadernos de Direito Privado, n.º 49, CEJUR, Braga (Janeiro-Março 2015), pp. 9-33;

GUIMARÃES, Maria Raquel, *A fraude no comércio electrónico: o problema da repartição do risco por pagamentos fraudulento*s, Infrações económicas e financeiras: estudos de criminologia e direito, Coimbra Editora, Coimbra (2013), pp. 581- 597;

GUIMARÃES, Maria Raquel, *A repartição dos prejuízos decorrentes de operações fraudulentas de banca electrónica (home banking): Acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09*, Cadernos de Direito Privado, n.º 41, CEJUR, Braga, Janeiro-Março (2013), pp. 45-69;

GUIMARÃES, Maria Raquel, *O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos*, Coimbra Editora, Coimbra (2011);

GUIMARÃES, Maria Raquel, *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 - Volume III - Homenagem aos Profs. Doutores A. Ferrer Correia, Orlando de Carvalho e Vasco Lobo Xavier, Coimbra Editora, Coimbra (2007), pp. 707-723;

GUIMARÃES, Maria Raquel, Algumas considerações sobre o aviso nº 11/2001 do Banco de Portugal de 20 de Novembro relativo aos cartões de crédito e de débito, *Revista da Faculdade de Direito da Universidade do Porto, A.1* (2004), pp. 247-276;

GUIMARÃES, Maria Raquel, *As transferências eletrónicas de fundos e os cartões de débito: alguns problemas jurídicos relacionados com as operações de levantamento de numerário e de pagamento por meios eletrónicos*, Coimbra: Almedina (1999);

INFOLAWGROUP LPP, *The duty to authenticate identity: the online banking breach lawsuits,* 17 de Abril de 2012. Acedido em 23 de Outubro de 2016, a partir de http://www.infolawgroup.com/2012/04/articles/reasonable-security/the-duty-to-authenticate-identity-the-online-banking-breach-lawsuits/

PROENÇA, José Brandão, *A conduta do lesado como pressuposto e critério de imputação do dano extracontratual*, Porto (1996);

KILONZO, Kethi D., *An Analysis of the Legal Challenges posed by Electronic Banking*, Kenya Law Review, Vol. 1 (2007), pp. 323-341;

*LAW & REGULATION OF ELECTRONIC FINANCE & INTERNET BANKING - INTRODUCTION AND OVERVIEW, C*entre for Financial and Management Studies, SOAS, University of London, University of London (2014). Acedido em 14 de Outubro de 2016, a partir de http://www.cefims.ac.uk/documents/sample-120.pdf

LIMA, Raquel Sofia, *A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na Jurisprudência Portuguesa*, Dissertação de Mestrado em Direito - Ciências Jurídico-Privatistas, Faculdade de Direito da Universidade do Porto, Porto (Julho de 2015);

OLIVEIRA, Fernando Baptista de, *Contratos Privados - Das Noções à Prática Judicial*, Vol. II, Coimbra Editora, Coimbra (2014);

NEGAS, Mário Fernando Carrilho; LOPES, José Manuel Martinho; BERNARDO, Maria do Rosário Matos, *Access to Homebanking Services: A portuguese perspective*. *7th Iberian Conference on Information Systems and Technologies*. Madrid: Associação Ibérica de Sistemas e Tecnologias de Informação (AISTI) Universidade Politécnica de Madrid (Junho 2012), pp.76-81;

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 Tribunal de Justiça, de 18/12/2013: o (admirável) "mundo novo" no homebanking?,* Revista Eletrónica de Direito (Abril de 2014). Acedido em 12 de Outubro de 2016, a partir de http://www.cije.up.pt/content/plaidoyer-por-uma-%E2%80%9Cdistribui%C3%A7%C3%A3o-din%C3%A2mica-do-%C3%B3nus-da-prova%E2%80%9D-e-pela-%E2%80%9Cteoria-das-esferas-de-ris;

SOARES, Quirino, *Contratos Bancários*, Scientia Iuridica Tomo III-n.º 295 (Janeiro-Abril, 2003), pp. 109-128;

Lista de Jurisprudência

A jurisprudência portuguesa citada pode ser consultada em <www.dgsi.pt>

Acórdão do STJ de 18.12.2013, Proc. n.º 6479/09.8TBBRG.G1.S, Relator Ana Paula Boularot

Acórdão do STJ, de 9.06..2010, Proc. n.º 579/09.1YFLSB, Relator Sousa Grandão

Acórdão do TRE de 22.05.2014, Proc. n.º 11/13.6T2ASL.E1, Relator Mata Ribeiro

Acórdão do TRG de 25.11.2013 Proc.n.º 2869/11.4TBGMR.G1, Relator Espinheira Baltar

Acórdão do TRG de 17.12.2014, Proc. n.º1910/12.8TBVCT.G1, Relator Fernando Fernandes Freitas

Acórdão do TRL de 26.10.2010, Proc. n.º 1943/09.1TJLSB.L1-7, Relator Maria Amélia Ribeiro

Acórdão do TRL de 5.11.2013, Proc. n.º 9821/11.8T2SNT.L1-1, Relator Manuel Marques

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

Acórdão do TRP de 29.04.2014, Proc.n.º225/12.6TJVNF.P1, Relator, Francisco Matos

*

PATCO v. People's United Bank, Ocean Bank – United States Court of Appeals for the First Circuit, 3 de julho de 2012 (disponível em http://ef67fc04ce9b132c2b32-8aedd782b7d22cfe0d1146da69a52436.r14.cf1.rackcdn.com/patco-ach-fraud-ruling-reversed-eresource-1-a-4919.PDF)