A RESPONSABILIDADE DO BANCO POR OPERAÇÕES DE PAGAMENTO NÃO AUTORIZADAS NO *ONLINE BANKING,* DECORRENTE DO NOVO REGIME DE SERVIÇOS DE PAGAMENTO (RSP II)

Miguel Pestana de Vasconcelos

Resumo: o texto incide sobre a responsabilidade das operações não autorizadas no *online banking*. Aborda o âmbito de aplicação do RSP, os seus conceitos fundamentais, a autorização das operações de pagamento, com ênfase nas formas de autenticação, as obrigações do prestador de serviços de pagamento e do utilizador. Centra-se, depois, na responsabilidade pela execução de uma operação de pagamento não autorizada, definindo os traços centrais do regime de responsabilidade consagrado nesta sede. Termina-se com um conjunto de conclusões que permitem definir os princípios estruturantes da disciplina aqui consagrada, o que é da maior utilidade para afinar a aplicação do regime aos casos concretos.

Palavras-chave: serviços de pagamento; responsabilidade civil; responsabilidade bancária; responsabilidade por operações não autorizadas; *online banking*; contrato bancário geral.

1. INTRODUÇÃO

I. A moeda é hoje esmagadoramente escritural, estando inscrita em contas bancárias, que pertencem a um ou mais titulares. As contas podem ser à ordem ou a prazo. As primeiras são utilizadas para gerir os diversos pagamentos do dia a dia; as segundas para recolher poupança. A sua titularidade, o crédito ao saldo, consiste em qualquer das hipóteses num dos elementos mais importantes que compõem o património de uma pessoa, seja singular, seja coletiva. Mas em particular as primeiras, porque não é comum as pessoas coletivas constituírem poupanças, como sucede com as pessoas singulares, que a elas recorrem (muitas vezes para complementar as pensões de reforma ou para acudir a despesas inesperadas).

II. As regras de movimentação dessas contas, que consistem — dito de forma simples — na movimentação do dinheiro que aí está creditado (moeda escritural), têm, evidentemente, uma particular relevância. O que bem se compreende. A movimentação não autorizada, por terceiros, traduz um retirar do dinheiro da conta do seu titular — ou proprietário, em sentido amplo, ou constitucional do termo —, reduzindo-lhe o património na mesma medida. É, por isso, legítima a preocupação com a possibilidade de tal ocorrer.

III. Este texto visa justamente determinar qual a responsabilidade do banco sempre que se verifique uma operação de pagamento não autorizada no seio do denominado *homebanking*[1]. O que vale dizer qual o nível de proteção de que goza do cliente face à subtração ilícita por terceiro, através de uma operação bancária, do dinheiro escritural da sua conta. Havendo um regime, detalhado, quanto a essa matéria, o foco da análise recairá necessariamente sobre ele.

Torna-se, no entanto, necessário, de forma prévia, caracterizar a relação bancária, que se constitui com a celebração do contrato de abertura de conta: negócio esse que consiste num contrato-quadro no qual radicam, igualmente, os serviços de pagamento. E exige também que se passe em revista a jurisprudência dos nossos tribunais superiores — embora com outro quadro jurídico — nesta matéria.

2. O CONTRATO BANCÁRIO GERAL E OS SERVIÇOS DE PAGAMENTO

I. O contrato de abertura de conta tem um conteúdo muito mais extenso do que a constituição de uma conta no banco. É um negócio extremamente amplo e complexo, donde emerge a relação bancária geral[2]. Ele mantém-se independentemente de quantos negócios forem depois concluídos entre as partes, desde o início da relação, que funda, ao momento em que ela se extingue. Aí se integram também os contratos de conta corrente, de depósito e, pelo menos, de alguns serviços de pagamento[3].

II. Este contrato, o contrato bancário[4], embora não sendo legalmente típico, é, de forma clara, socialmente típico, tendo em conta, de entre outros aspetos, a uniformidade das cláusulas contratuais gerais a que os diversos bancos recorrem.

---

1 Que é definido no acórdão do STJ de 18/12/2013 (Ana Paula Boularot), *in*: www.dgsi.pt: como "Banco internético (do inglês *Internet banking*), *e-banking*, banco *online*, *online banking*, às vezes também banco virtual, banco eletrónico), concretizado pela possibilidade conferida pela entidade bancária aos seus clientes, mediante a aceitação de determinados condicionalismos, a utilizar toda uma panóplia de operações bancárias, online, relativamente às contas de que sejam titulares, utilizando para o efeito canais telemáticos que conjugam os meios informáticos com os meios de comunicação à distância (canais de telecomunicação), por meio de uma página segura do banco, o reveste de grande utilidade, especialmente para utilizar os serviços do banco fora do horário de atendimento ou de qualquer lugar onde haja acesso à Internet".

2 Entre nós neste sentido: A. Menezes Cordeiro, *Direito bancário*, 6.ª ed. (com a colaboração de A. Barreto Menezes Cordeiro), Almedina, Coimbra, 2016, p. 291; Almeno de Sá, *Direito bancário*, Coimbra Editora, Coimbra, 2008, p. 17; Maria Raquel Guimarães, *O contrato-quadro no âmbito de utilização de meios de pagamento electrónicos*, Coimbra Editora, Coimbra, 2011, pp. 343, ss., pp. 365, ss.. Ver, ainda: M. Pestana de Vasconcelos, *Direito bancário*, 2.ª ed., Almedina, Coimbra, 2019, pp. 73, ss..

3 Ver, sobre esta matéria, desenvolvidamente, M. Pestana de Vasconcelos, *Direito bancário*, cit., pp. 73, ss..

4 Designada de forma feliz como "contrato mãe" pelo acórdão do STJ de 13/12/2013 (Ana Paula Boularot), *in*: www.dgsi.pt.

Ele consiste num contrato organizatório, complexo, com produção de efeitos imediatos, direitos e obrigações para as partes, correspondentes a tipos de prestação de serviços. Mas, mais para além, é composto por elementos normativos, ou seja, prevê logo o regime de contratos que as partes podem vir a celebrar entre elas.

A sua correta qualificação é a de contrato-quadro, visando-se destacar o carácter amplo e complexo do conjunto da relação bancária com o cliente[5]. Um dos seus principais efeitos, dada a tessitura de confiança que pressupõe, é o nascimento de deveres de proteção, aconselhamento e informação das partes, que podem revestir uma maior ou menor extensão, de acordo com os elementos que compõem o caso concreto. De entre esses elementos, destaca-se, por um lado, o conjunto e a natureza de negócios celebrados ou a celebrar (p. ex., sobre valores mobiliários, consumo, etc.) e, por outro, a pessoa do cliente (singular ou coletiva, profissional ou consumidor, com conhecimentos específicos na matéria ou não).

III. Dizíamos que o conteúdo fundamental do contrato de abertura de conta, e razão pela qual muitas vezes ele é celebrado, consiste nos serviços de pagamento. Com efeito, eles são fundamentais para um sujeito se inserir na vida moderna, constituindo, por essa razão, dos vetores mais relevantes dos serviços mínimos bancários. Os serviços de pagamento inserem-se no contrato inicial, sendo mesmo a sua parte mais relevante.

A conta bancária à ordem constitui para este efeito a conta de pagamento. Embora as operações de pagamento que os integram se possam fazer isoladamente, elas serão integradas no seio de um contrato-quadro específico "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" [art. 2.º, al. *i)*, do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RSP)]. Neste caso, ele integra-se no contrato inicial, mais amplo.

IV. Os créditos dos clientes sobre os bancos não se esgotam nos saldos de uma conta à ordem. Ela é, sem dúvida, o elemento central para a execução das diferentes ordens de pagamentos. Todavia, com, pelo menos, igual relevância, temos os créditos decorrentes de depósitos a prazo, sendo dessa forma que os particulares constituem as suas poupanças.

Esses depósitos têm regras específicas de movimentação, que são mais exigentes do que as decorrentes da conta à ordem. Além do mais, a sua movimentação, em particular, de valores elevados, é um ato a que o banco deverá estar especialmente atento, dadas as consequências patrimoniais que uma operação não autorizada nesse caso pode ter. Os deveres de proteção do património do cliente por parte do banco nesta hipótese são especialmente intensos.

---

[5] Na jurisprudência, o acórdão do STJ de 27/02/2014 (Tavares de Paiva), *in*: www.dgsi.pt: "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".

3. A JURISPRUDÊNCIA DOS TRIBUNAIS SUPERIORES NO ÂMBITO DO ANTERIOR RSP FACE A OPERAÇÕES NÃO AUTORIZADAS

I. Os casos analisados pela jurisprudência estão ligados a dois grupos amplos: o *phishing* e o *pharming*[6]. O primeiro consiste, essencialmente, no envio de mensagens para o correio eletrónico de um cliente bancário por uma entidade que se identifica como sendo o banco, solicitando os dados necessários para aceder à conta. Em regra, era solicitada tanto a palavra-passe, como o cartão matriz, elemento necessário para autorizar cada operação em si. O *pharming* traduz-se na falsificação de uma página na *internet* do banco para com os dados obtidos por essa via se aceder depois à conta do cliente defraudado[7].

Há, ainda, diversos casos de disponibilização a terceiros dos dados de acesso à conta, de guarda dos elementos por parte do cliente, bem como da extensão do dever de cuidado e a qualificação da culpa do utilizador.

O acórdão particularmente relevante neste quadro foi o do STJ de 13/12/2013 (Ana Paula Boularot), que distinguiu de forma clara ambas as situações e concluiu no sentido de que os "riscos da falha do sistema informático utilizado, bem como dos ataques cibernautas ao mesmo, têm de correr por conta do Réu".

II. O quadro em que as questões foram sendo resolvidas alterou-se com a entrada em vigor do novo regime, que, como iremos ver, criou outros mecanismos de segurança — de entre os quais tem especial relevo o recurso à autenticação forte — que tornam muito mais difícil o recurso, tanto ao *phishing*, como ao *pharming*. Por outro lado, há uma maior consciencialização para os riscos do *phishing*, tendo os bancos recorrido a diversos sistemas de aviso.

4. O NOVO REGIME DOS SERVIÇOS DE PAGAMENTO

4.1. Introdução

I. Os cartões, de débito e de crédito[8], o débito direto e as transferências são figuras bastante diversas utilizadas no tráfego comercial como instrumen-

---

6 Sobre ela, ver: Maria Raquel Guimarães, *As operações fraudulentas. Da homebanking na jurisprudência recente, Ac. do STJ de 18/12/2013, Proc. 6479/09*, Cadernos de Direito Privado, 2015, pp. 9, ss.; *idem*, *O phishing de dados bancários e o pharming de contas. Análise jurisprudencial*, *in*: III congresso de direito bancário (coord. Miguel Pestana de Vasconcelos), Almedina, Coimbra, 2018, pp. 405, ss.; Raquel Ribeiro Lima, *A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na jurisprudência portuguesa*, in: Revista Electrónica de Direito, 2016, n.º 3, pp. 1, ss..

7 Ver o acórdão do STJ de 13/12/2013 (Ana Paula Boularot), cit..

8 Sobre eles, ver Maria Raquel Guimarães, *As transferências electrónicas de fundos e os cartões de débito*, Almedina, Coimbra, 1999, *passim.*

tos de pagamento[9]. A lei, contudo, não estabelece um regime diferenciado para cada uma delas, mas prevê um único regime global para todas[10].

Trata-se do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, aprovado pelo Decreto-Lei n.º 91/2018, de 12 de novembro, que transpõe a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015[11], que consiste já na segunda Diretiva de Serviços de Pagamento (DSP 2[12]). Como se trata de uma diretiva de harmonização máxima, obtém-se um regime de elevada integração nesta matéria no âmbito da UE, sendo o objetivo a criação de um mercado de pagamentos uniforme.

A disciplina daqui decorrente é muito complexa e extensa[13] (falando-se mesmo numa pequena codificação)[14], assente numa "armadura" extensíssima de definições, cujo domínio é fundamental. Serão vistas mais à frente.

II. O novo regime procura acompanhar a notável evolução tecnológica neste campo, a entrada de novos atores de fora do sistema bancário, de novos tipos de serviços de pagamento (serviços de informação sobre contas e serviços de iniciação de pagamentos) e, em particular, vem reforçar substancialmente, como veremos, os deveres de segurança dos prestadores de serviços de pagamento[15].

Como se refere no considerando 7 da diretiva: "Nos últimos anos, assistiu-se a um aumento dos riscos de segurança relacionados com os pagamentos eletrónicos, ao volume cada vez maior deste tipo de pagamentos à escala mundial e ao aparecimento de novos tipos de serviços de pagamento. A existência de serviços de pagamento seguros constitui uma condição indispensável para o bom funcionamento do mercado de serviços de pagamento".

---

9 Sobre as transferências e os débitos diretos, ver, desenvolvidamente, F. Mendes Correia, *Moeda bancária e cumprimento*, Almedina, Coimbra, 2017, pp. 695, ss..

10 Stefan Grundmann, *European Law and Principles on commercial and investment banking contracts: an advanced area of codification*, *in*: Towards and European Civil Code (org.: Arthur Hartkamped, Martijn W. Hesselink; Ewoud H. Hondius, Chantal Mak & C. Edgar du Perron), fourth revised and expanded edition, Kluwer Law, The Netherlands, 2011, p. 792.

11 Revogou a Diretiva 2007/64/CE do Parlamento Europeu e do Conselho de 13 de novembro (primeira diretiva dos serviços de pagamento ou DSP 1), que havia sido transposta para o ordenamento nacional pelo Decreto-Lei n.º 317/2009, de 30 de outubro.

12 Sobre o novo regime, ver Werner, *Bargeldloser Zahlungsverkehr (Girogschäft), in*: Bank- und Kapitalmarktrecht, de Peter O. Mülbert, Andreas Früh, Thorsten Seyfried, Otto Schmidt, Colónia, 2019, pp. 628, ss. Para o regime anterior, ver M. Januário da Costa Gomes, *Contratos comerciais*, Almedina, Coimbra, 2012, pp. 220, ss..

13 Mesmo "próxima do labiríntico", M. Januário da Costa Gomes, *Contratos comerciais*, cit., p. 223.

14 S. Grundmann, *European Law and Principles on commercial and investment banking contracts: an advanced area of codification*, cit., p. 792.

15 Ver Francisco Mendes Correia, *Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento*, in: III congresso de direito bancário (coord. Miguel Pestana de Vasconcelos), Almedina, Coimbra, 2018, p. 388. Ainda sobre o regime da DSP 2, ver Mafalda Miranda Barbosa, *Serviços de pagamentos, repartição do risco e responsabilidade civil — algumas reflexões a propósito da nova diretiva dos serviços de pagamentos (DSP2)*, Revista de Direito Comercial, 2017, pp. 551, ss.; Alan Berner, *Payment Service Directive II and Its Implications,* in: *Disrupting finance, Fintech and strategy in the 21st century* (edited by Theo Lynn, John G. Mooney, Pierangelo Rosati, Mark Cummings), Palgrave, Macmillian, Cham, Switzerland, 2018, pp. 103, ss..

III. Diga-se, em abono da precisão, que esta atividade não é exclusivamente bancária, não sendo, como se começou por afirmar, unicamente as instituições de crédito que a podem desenvolver (cfr. art. 7.º RSP). Contudo, ela, como também se assinalou anteriormente, é fundamentalmente desempenhada por elas, sendo mesmo marcante na sua caracterização. Por isso, se inclui no âmbito do direito bancário.

4.2. O âmbito de aplicação do RSP

4.2.1. *Os serviços de pagamento abrangidos*

I. O diploma aplica-se aos serviços de pagamento, tal como definidos pela articulação dos arts. 4.º e 5.º do RSP. O primeiro elenca um conjunto de atividades em que eles se desdobram, vindo depois a norma seguinte a fazer um recorte negativo, afastando do âmbito de aplicação do regime algumas operações.

II. Consistem, assim, em serviços de pagamento os serviços que permitam depositar ou levantar numerário numa conta de pagamento, bem como todas as operações necessárias para a gestão dessa conta (art. 4.º, als. *a)* e *b)*, RSP). Incluem-se, também, neste âmbito, a execução de operações de pagamento, incluindo a transferência de fundos depositados numa conta de pagamento aberta junto do prestador de serviços de pagamento do utilizador ou de outro prestador de serviços de pagamento, de que a lei faz de seguida uma enumeração exemplificativa: a execução de débitos diretos, incluindo os de carácter pontual, a execução de operações de pagamento através de um cartão de pagamento ou de um dispositivo semelhante, e a execução de transferências a crédito, incluindo ordens de domiciliação (art. 4.º, als. *c)-i)*, *ii)*, *iii)*, RSP).

O mesmo regime aplica-se quando os fundos a transferir são obtidos por via de uma linha de crédito concedida por um utilizador de serviços de pagamento (art. 4.º, al. *d)*, RSP), como sucede, p. ex., com o descoberto em conta.

São ainda serviços de pagamento: a emissão de instrumentos de pagamento ou aquisição de operações de pagamento, o envio de fundos, os serviços de iniciação do pagamento e de serviços de informação sobre conta (art. 4.º, als. *e)*, *f)*, *g)* e *h)*, RSP).

III. As exclusões são bastante limitadas em termos económicos, embora o elenco seja vasto. Destacamos as seguintes. Afastam-se, desde logo, os pagamentos com numerário, de forma direta, entre ordenante o ordenado, sem intermediação como sucede nos pagamentos de dia a dia, em geral (mas não necessariamente) com um valor reduzido. São também retirados do âmbito de aplicação do regime os pagamentos com cheques, letras e livranças. Com efeito, a realização de operações de pagamento com recurso a qualquer destes instrumentos sacados sobre um prestador de serviços de pagamento com vista a colocar fundos à disposição do beneficiário é abrangida por regras próprias, onde se destacam as respetivas leis uniformes (art. 5.º, al. *h)*, RSP).

Por sua vez, as operações de pagamento no âmbito de valores mobiliários regem-se por disposições diferentes das previstas neste regulamento (art. 5.º, als. *h)* e *i)*, RSP).

4.2.2. *Os conceitos centrais do RSP*

I. Como referimos, seguindo de perto a técnica legislativa da diretiva, o RSP 2 começa com uma extensa lista de definições de caráter altamente técnico, cujo conhecimento é fundamental para a compreensão do regime. Não é mesmo possível, sequer, definir na integralidade o que sejam serviços de pagamento, sem se recorrer a outras definições (como, em particular, a de operação de pagamento, à qual aquela recorre, como se viu no número anterior).

No seio do conjunto destes elementos, têm especial relevância os de caráter subjetivo, onde se insere o ordenante e o utilizador dos serviços de pagamento, e os objetivos, onde se incluem as noções de ordem de pagamento, operações de pagamento e instrumento de pagamentos. Vejamos de seguida.

II. O ordenante vem definido como a uma "pessoa singular ou coletiva que é titular de uma conta de pagamento e que autoriza uma ordem de pagamento a partir dessa conta, ou, na ausência de conta de pagamento, uma pessoa singular ou coletiva que emite uma ordem de pagamento" (art. 2.º, al. *mm)*, RSP).

O utilizador de serviços de pagamento é a "pessoa singular ou coletiva que utiliza um serviço de pagamento a título de ordenante, de beneficiário ou em ambas as qualidades" (art. 2.º, al. *eee)*, RSP).

III. A ordem de pagamento consiste numa "instrução dada por um ordenante ou por um beneficiário ao seu prestador de serviços de pagamento requerendo a execução de uma operação de pagamento" (art. 2.º, al. *ll)*, RSP).

IV. As operações de pagamento, em si, consistem no "ato, iniciado pelo ordenante ou em seu nome, ou pelo beneficiário, de depositar, transferir ou levantar fundos, independentemente de quaisquer obrigações subjacentes entre o ordenante e o beneficiário" (art. 2.º, als. *z)* e *aa)*, RSP), devendo distinguir-se entre as operações de pagamento baseadas em cartões e as operações de pagamento remotas.

As primeiras consistem num "serviço baseado na infraestrutura e nas regras comerciais de um sistema de pagamento com cartões para efetuar operações de pagamento por meio de cartões, dispositivos ou programas de telecomunicações, digitais ou informáticos, que dá origem a uma operação com cartões de débito ou de crédito. As operações de pagamento baseadas em cartões excluem as operações baseadas noutros tipos de serviços de pagamento".

As segundas, que são aquelas que neste momento nos interessam, são as iniciadas "através da Internet ou através de um dispositivo que possa ser utilizado para comunicação à distância" (art. 2.º, al. *bb)*, RSP).

V. Instrumento de pagamento consiste num "dispositivo personalizado ou conjunto de procedimentos acordados entre o utilizador e o prestador de serviços de pagamento e a que o utilizador de serviços de pagamento recorra para emitir uma ordem de pagamento" (art. 2.º, al. *aa)*, RSP).

Por seu lado, "«Instrumento de pagamento baseado em cartões» é um instrumento de pagamento, incluindo cartões, telemóveis, computadores ou outros dispositivos tecnológicos que contenham a aplicação de pagamento adequada, que permite ao ordenante iniciar uma operação de pagamento baseada num cartão, com exceção de transferências a crédito e de débitos diretos na aceção do art. 2.º do Regulamento (UE) n.º 260/2012, de 14 de março de 2012" (art. 2.º, al. *bb)*, RSP).

VI. Por último, um sistema de pagamentos configura um sistema de transferência de fundos que se rege por disposições formais e normalizadas e por regras comuns relativas ao processamento, compensação ou liquidação de operações de pagamento" (art. 2.º, al. *ww)*, RSP)[16].

4.3. Operações de caráter isolado e contratos-quadro

I. Um dos traços fundamentais do diploma é o da distinção entre as operações de pagamento de caráter isolado (arts. 82.º e segs. RSP) e aquelas que têm por base um contrato-quadro (arts. 89.º e segs. RSP). Estas são as mais vulgares. De facto, como vimos aquando da análise do contrato bancário geral, é igualmente concluído, nesse seio, um contrato-quadro que as disciplina. Pelo seu relevo, é sobre operações de pagamento abrangidas por um contrato-quadro que recairá a nossa atenção.

4.4. A autorização das operações de pagamento

I. O prestador de serviços de pagamento só pode executar uma operação (ou um conjunto de operações) que tenha sido devidamente autorizada.

Para o efeito, é central o consentimento, nos termos acordados, pelo ordenante (arts. 103.º, n.os 1 e 3, RSP) ou, eventualmente, através do beneficiário ou do prestador de serviços de iniciação de pagamentos (art. 103.º, n.º 4, RSP).

Ele terá de ser prévio à operação, salvo se for convencionado entre as partes que seja dado em momento subsequente (art. 103.º, n.º 2, RSP). Não tendo sido prestado nos termos referidos, a operação considera-se não autorizada (art. 106.º, n.º 5, RSP).

---

16 Estes serviços, de grande relevo no comércio *online*, criam "uma ponte telemática entre o sítio *web* do comerciante e a plataforma bancária em linha do prestador de serviços de pagamento que gere as contas do ordenante, a fim de iniciar pagamentos através da Internet com base numa transferência a crédito" (considerando 22 da DSP 2).

Dado o consentimento, tanto a uma operação isolada como a um conjunto de operações autorizadas, ele pode ser retirado em qualquer momento, desde que a ordem não se tenha tornando irrevogável, nos termos definidos no art. 121.º RSP (art. 106.º, n.º 6), como sucede, em regra, depois de ela ter sido recebida pelo prestador de serviços de pagamento do ordenante (art. 121.º, n.º 1, RSP).

A execução de uma ordem depois deste momento, tendo a revogação sido realizada nos termos acordados pelas partes, leva a que operação seja não autorizada, com todos os efeitos daí decorrentes para o prestador de serviços (art. 106.º, n.os 7 e 8, RSP).

4.4.1. *A autenticação*

I. A execução da ordem exige que o cliente tenha sido autenticado pelo prestador do serviço através de um procedimento que lhe permite "verificar a identidade de um utilizador de serviços de pagamento ou a validade da utilização de um instrumento de pagamento específico, incluindo a utilização das credenciais de segurança personalizadas do utilizador" (art. 2.º, al. *c)*, RSP).

A lei impõe em certos casos — os mais relevantes — que o prestador de recorra a uma "autenticação forte do cliente" (art. 2.º, al. *d)*, RSP). Ela exige a 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).

Assim, p. ex., uma palavra-passe — aquilo que o consumidor conhece —, um dipositivo, como um telemóvel (ou melhor: a receção de uma mensagem no telemóvel), ou um cartão introduzido num leitor — aquilo que só o utilizador tem — ou o reconhecimento digital ou facial — aquilo que o utilizador é. Mas não é suficiente. Estes elementos têm de ser independentes, na medida em que a violação de um deles não pode comprometer a fiabilidade dos outros.

Em regra, estes requisitos estão preenchidos com a indicação de uma palavra-passe associada depois a uma mensagem específica para o telemóvel com um código criado para autorizar aquela operação.

II. Como dizíamos, os prestadores de serviços de pagamento devem aplicar a autenticação forte do cliente[17] se o ordenante aceder em linha à sua conta de pagamento (p. ex., através do *homebanking* ou da aplicação móvel fornecida pelo banco, nomeadamente, para consultar saldos ou movimentos da conta) ou realizar uma ação, através de um canal remoto, que possa envolver um risco de fraude no pagamento ou de outros abusos (p. ex, ao

[17] Os prestadores de serviços de pagamento passaram a estar obrigados a aplicar a autenticação forte do cliente a partir de 14 de setembro de 2019, uma vez que foi nessa data que entrou em vigor o Regulamento Delegado (UE) 2018/389 da Comissão, de 27 de novembro de 2017.

criar uma transferência recorrente a ser efetuada no início de cada mês ou alterar dados da conta) (art. 104.º. n.º 1, als. *a)*, e *c)*, RSP) ou iniciar uma operação de pagamento eletrónico (p. ex., uma transferência a crédito ordenada no *homebanking* ou uma compra *online*) (art. 104.º. n.º 1, al. *b)*, RSP).

Neste último caso (operação de pagamento eletrónico), se se tratar de uma operação de pagamento remota (art. 104.º, n.º 2 RSP), a lei vai mais longe: a autenticação forte do cliente deve incluir elementos que associem de forma dinâmica a operação a um montante específico e a um beneficiário específico (p. ex., através do envio de um código de confirmação da operação para o telemóvel do cliente, a chamada senha de utilização única[18])[19].

III. A lei impõe aos prestadores de serviços de pagamento a adoção de medidas de segurança suficientes para proteger a confidencialidade e a integridade das credenciais de segurança personalizadas dos utilizadores de serviços de pagamento[20]. A norma tem necessariamente de ser interpretada de forma conjugada com o art. 73.º do Regime Geral das Instituições de Crédito e Sociedades Financeiras, que impõe às instituições de crédito elevados níveis de competência técnica. Norma que marca a relação bancária, onde os serviços de pagamento se inserem.

Ou seja, é obrigação do prestador de serviços adotar as medidas em termos de meios humanos e, em especial, materiais, em particular, de caráter informático (como o recurso a sofisticados sistemas de encriptação), para proteger as credenciais dos clientes. O que implica a cada momento proceder às atualizações necessárias face ao risco de obtenção ilícita desses dados por parte de terceiros, para as proteger. Se o seu sistema informático for violado, incumpriu essa obrigação.

Importa deixar claro que esta obrigação não é uma obrigação de meios, mas uma verdadeira obrigação de resultado (assegurar a integralidade da rede e a inviolabilidade das contas), a aproximar-se muito de uma obrigação de garantia. Com efeito, a responsabilidade do prestador de serviços só é afastada em casos de força maior, casos esses que a lei delimita de forma muito restrita (art. 135.º RSP).

4.5. O direito (e o dever) de bloqueio do instrumento de pagamento

I. Se acordado de forma expressa no contrato-quadro, o prestador de serviços de pagamento pode reservar-se o direito de bloquear um instrumento

---

18 Considerando 96 da DSP 2.

19 Estes aspetos são depois detalhados no Regulamento delegado (EU) 2018/389 da Comissão de 27 de novembro de 2017 que complementa a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras.

20 Elas consistem nos elementos personalizados fornecidos pelo prestador de serviços de pagamento a um utilizador de serviços de pagamento para efeitos de autenticação (art. 2.º, al. *j)*, RSP).

de pagamento por "motivos objetivamente fundamentados", que estejam relacionados com a segurança do instrumento de pagamento, a suspeita de utilização não autorizada ou fraudulenta desse instrumento ou aumento significativo do risco de o ordenante não poder cumprir as suas responsabilidades de pagamento, caso se trate de um instrumento de pagamento com uma linha de crédito associada (art. 108.º, n.º 2, als. *a)*, *b)* e *c)*, RSP).

Quando o fizer, o prestador do serviço de pagamento está obrigado a informar o ordenante do bloqueio do instrumento de pagamento e da respetiva justificação pela forma acordada. Este dever terá de ser cumprido sempre que seja possível ainda antes do bloqueio do instrumento ou, caso não o seja, o mais tardar, imediatamente após o bloqueio, a não ser que essa informação não possa ser prestada por "razões de segurança objetivamente fundamentadas" ou se for "proibida por outras disposições legais aplicáveis" (art. 108.º, n.º 3, RSP).

Cessando os motivos que levaram ao bloqueio, deve este, igualmente, cessar, com o desbloqueio do instrumento ou a sua substituição por um novo (art. 108.º, n.º 4, RSP).

II. Este direito estará em regra previsto de forma expressa nos contratos-quadro.

Trata-se, em rigor, de um direito-dever. Estando em jogo a segurança do instrumento de pagamento, bem como a suspeita de utilização não autorizada ou fraudulenta desse instrumento, recai sobre o prestador de serviços um dever de proteção do património do decorrente da boa fé[21].

Já vimos que ela é mais intensa — caracterizante, mesmo — na relação bancária, traduzindo-se, de entre outros, em deveres de proteção do património do cliente que lhe está confiado.

Cremos mesmo que ainda que esse direito não esteja previsto nos contrato-quadro de serviços de pagamento, ainda assim, mesmo sem essa permissão específica, o prestador de serviços estava vinculado (não só podia, mas devia) a atuar com vista a tutelar os interesses patrimoniais do cliente.

Este dever tem mesmo uma particular intensidade, porque ele é um dos baluartes da defesa do património do cliente. O banco tem de se dotar dos meios tecnológicos mais avançados para poder estar em posição de detetar se a segurança do instrumento não estará comprometida, se não está a ser utilizado de forma não autorizada ou fraudulenta.

O recurso a instrumentos informáticos e a aplicações de inteligência artificial permite estabelecer padrões de comportamento de um dado cliente, quanto à frequência de utilização da conta, os horários, os montantes de que

---

21 Face ao regime anterior, M. Januário da Costa Gomes (*Contratos comerciais*, cit., p. 243) sublinhava a necessidade de o prestador de serviços de pagamento "adotar um comportamento que considere adequadamente a situação efetiva ou presumível do ordenante: é um dever que resulta da boa fé". O que sustentamos em texto é que esse princípio conforma a posição jurídica do banco em termos de lhe impor um dever de atuar.

dispõe, os IP utilizados. Há ainda formas técnicas de detetar sintomas de utilização potencialmente abusiva. Há padrões de abuso e de fraude[22].

O banco tem de se dotar de todos os meios que permitam fazer essa deteção e, havendo suspeita objetiva, exercer o direito de bloqueio nos termos definidos na norma — o que passa em primeiro lugar, e sempre que possível, pelo contacto com o utilizador.

4.6. As obrigações do utilizador associadas aos instrumentos de pagamento (art. 110.º RSP)

I. O utilizador do instrumento de pagamento deve utilizá-lo de acordo com as condições que regem a sua emissão e utilização, as quais têm de ser "objetivas, não discriminatórias e proporcionais". Para esse efeito, deverá, logo que o receba, tomar todas "as medidas razoáveis" para preservar a segurança das suas credenciais de segurança personalizadas (art. 110.º, n.os 1, al. *a)*, e 2, RSP).

Deve, ainda, comunicar, "logo que tenha conhecimento dos factos e sem atraso injustificado", ao prestador de serviços de pagamento ou à entidade designada por este último a perda, o furto, o roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento (art. 110.º, n.º 1, al. *b)*, RSP).

II. Se não cumprir deliberadamente, ou seja, com dolo, uma ou mais destas obrigações, ou atuar de forma fraudulenta, cabe-lhe suportar todas as perdas decorrentes das de operações de pagamento não autorizadas (art. 115.º, n.º 3, RSP). A lei estende a imputação de perdas ao ordenante nos casos de negligência grosseira, fazendo sobre ele recair as perdas, mas, nesse caso, até ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento (art. 115.º, n.º 4, RSP).

Importa sublinhar que a negligência grosseira deve ser devidamente separada da diligência ordinária ou culpa leve. Não basta a falta de cuidado que um bom pai de família, que aqui significa simplesmente um utilizador cuidadoso, desses instrumentos tivesse adotado, dentro das circunstâncias do caso concreto.

Vai para lá dessa medida. Implica um nível de falta de cuidado quase escandaloso, de um desleixo inadmissível seja para quem for (p. ex., deixar o seu nome de utilizador ou palavra passe à vista ou num local de acesso a terceiros fora do seu círculo familiar ou de confiança próxima).

A porta para a imputação de perdas ao utilizador por esta via é, assim, bastante apertada.

---

22 Sublinha-se que o prestador de serviços de pagamento está obrigado a uma avaliação "exaustiva e atualizada" dos riscos operacionais e de segurança que enfrenta, bem como da adequação das medidas de mitigação e dos mecanismos de controlo implementados (art. 95.º, n.º 2, RSP).

4.7. As obrigações do prestador de serviços de pagamento associadas aos instrumentos de pagamento (art. 111.º RSP)

I. O prestador de serviços de pagamento que emite um instrumento de pagamento deve assegurar que as credenciais de segurança personalizadas do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento, sem embargo, porém, de a sua contraparte ter de cumprir os deveres que sobre ela impendem, nos termos do art. 110.º RSP (art. 111.º, al. *a)*, RSP)

Deverá, ainda, abster-se de enviar instrumentos de pagamento não solicitados, salvo quando um instrumento deste tipo já entregue ao utilizador de serviços de pagamento deva ser substituído (art. 111.º, al. *b)*, RSP).

Cabe-lhe igualmente garantir a disponibilidade, *a todo o momento*, de meios adequados para permitir ao utilizador de serviços de pagamento proceder à comunicação da perda, do furto, do roubo, da apropriação abusiva ou de qualquer utilização não autorizada do instrumento de pagamento (art. 110.º, n.º 1, al. *b)*, RSP).

O que significa, de entre outros aspetos, que os canais de comunicação com o banco para este efeito devem ser de muito fácil acesso e estar disponíveis 24 horas (e ser acessíveis também de forma simples fora do país). Esses sistemas devem valer, igualmente, para solicitar o desbloqueio logo que deixem de se verificar os motivos que levaram ao bloqueio do instrumento de pagamento (art. 108.º, n.º 4, RSP, art. 111.º, al. *c)*, RSP)[23].

Da mesma forma, terá de impedir a utilização do instrumento de pagamento, mal a referida comunicação lhe seja realizada (art. 110.º, n.º 1, al. *e)*, RSP). Mais, tem mesmo de facultar ao utilizador do serviço de pagamento, a pedido deste, os meios necessários para ele poder fazer prova, durante 18 meses após a comunicação, que ela foi efetuada ou que ele solicitou o desbloqueio nos termos acabados de referir (art. 110.º, n.º 1, al. *d)*, RSP).

II. Note-se que o risco do envio ao utilizador de serviços de pagamento de um instrumento de pagamento ou das respetivas credenciais de segurança personalizadas corre por conta do prestador do serviço de pagamento (art. 110.º, n.º 1, al. *d)*, RSP). Razão pela qual os cartões e as *passwords* são enviadas em separado.

4.8. A responsabilidade pela execução de uma operação de pagamento não autorizada

I. Não tendo a operação de pagamento sido autorizada nos termos legais, cabe ao prestador do serviço a restituição do valor, após ter tido conhecimento

---

[23] Efetuada a título gratuito, só podendo o prestador de serviços de pagamento cobrar apenas, e se for caso disso, os custos diretamente imputáveis à substituição do instrumento de pagamento (art. 110.º, n.º 2, RSP).

da operação ou após esta lhe ter sido comunicada o mais tardar até ao final do primeiro dia útil seguinte àquele conhecimento ou comunicação (art. 114.º, n.º 1, RSP).

Só pode deixar de o fazer, se tiver motivos razoáveis para suspeitar de atuação fraudulenta do ordenante e comunicar por escrito esses motivos, no prazo indicado no número anterior, às autoridades judiciárias nos termos da lei penal e de processo penal (art. 114.º, n.º 2, RSP).

O prestador de serviço do ordenante, sendo esse o caso, repõe a conta de pagamento debitada na situação em que estaria se a operação de pagamento não autorizada não tivesse sido executada, devendo assegurar que a data-valor do crédito na conta de pagamento do ordenante não é posterior à data em que o montante foi debitado na conta (art. 114.º, n.os 3 e 4, RSP).

Na eventualidade de não terem sido detetados motivos razoáveis que constituam fundamento válido de suspeita de fraude, ou essa suspeita não tenha sido comunicada, por escrito, à autoridade judiciária nos termos da lei penal e de processo penal, se o prestador de serviços não reembolsar de imediato o ordenante, este terá direito a juros de mora, contados dia a dia desde a data em que o utilizador de serviços de pagamento tenha negado que autorizou a operação de pagamento executada, até à data do reembolso, "calculados à taxa legal, fixada nos termos do Código Civil, acrescida de 10 pontos percentuais" (art. 114.º, n.º 10, RSP).

A lei, nesta eventualidade, admite ainda que o ordenante possa demonstrar danos de valor superior, tendo, nessa circunstância, direito a uma indemnização suplementar (art. 114.º, n.º 10, RSP).

II. Sendo este um dos nódulos das dificuldades que se podem gerar neste quadro, a lei consagrou um regime detalhado que, na essência, é altamente protetor do utilizador dos serviços.

Vejamos de forma sintética.

4.8.1. *O ónus da prova*

I. O primeiro elemento a ter em conta do ónus da prova (art. 113.º, n.º 1, RSP).

Se o utilizador de serviços negar ter autorizado a operação, ou alegar que ela foi incorretamente efetuada, cabe ao prestador do serviço de pagamento provar que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência do serviço prestado pelo prestador de serviços de pagamento[24].

---

[24] Se a operação de pagamento tiver sido iniciada através de um prestador do serviço de iniciação do pagamento, recai sobre este último o ónus de provar que, no âmbito da sua esfera de competências, a 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 por si prestado (art. 113.º, n.º 2, RSP).

Contudo, note-se que a simples utilização do instrumento de pagamento registada pelo prestador de serviços (incluindo o prestador do serviço de iniciação do pagamento, quando for o caso) não é necessariamente suficiente, por si só, para provar que a operação de pagamento foi autorizada pelo ordenante, que este último agiu de forma fraudulenta ou que não cumpriu, com dolo ou negligência grosseira, uma ou mais obrigações previstas no art. 110.º (art. 113.º, n.º 2, RSP). Para afastar a sua responsabilidade, o prestador de serviços terá de apresentar elementos que demonstrem a existência de fraude, de dolo ou de negligência grosseira da parte do utilizador de serviços de pagamento (art. 113.º, n.º 4, RSP). A imposição ao prestador de serviços de apresentar provas da alegada negligência resulta do facto de, como se refere na DSP 2 (considerando 72), o ordenante apenas dispor de meios muito limitados para o efeito.

II. Trata-se de uma carga probatória muito pesada. Ou o prestador de serviços consegue demonstrar a existência de uma fraude, recorrendo aos meios técnicos à sua disposição para o efeito, onde se incluem evidentemente aqueles destinados a esse fim, ou então terá de demonstrar o dolo ou negligência grosseira. Note-se, conforme já se sublinhou, que não basta negligência simples (ou culpa leve), é preciso negligência grosseira, o que significa uma falta de cuidado extremamente grave[25], que só uma pessoa muito pouco cuidadosa teria. Mas não será fácil ao prestador fazer a prova.

4.8.2. *A imposição de perdas ao ordenante*

I. O dever de restituição integral que a lei impõe ao utilizador é mitigado — mas ainda assim de forma muito limitada — nos casos de utilização de um instrumento de pagamento perdido, furtado, roubado ou da apropriação abusiva de um instrumento de pagamento. Nesta eventualidade, a lei impõe ao utilizador perdas dentro do limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, mas no máximo de €50 (art. 115.º, n.º 1, RSP[26]).

II. Afasta-se dessa forma, parcialmente, o regime da restituição integral decorrente do art. 114.º RSP. Sublinhe-se que não se trata de um caso de responsabilidade do ordenante, que levaria a uma obrigação de indemnizar, como se refere na epígrafe da norma ("Responsabilidade do ordenante em caso de operação de pagamento não autorizada"), mas antes da limitação do dever de restituição do banco até aos montantes referidos.

---

25 Para a distinção, ver I. Galvão Telles, *Direito das obrigações*, Coimbra Editora, Coimbra, 1997, pp. 354-355; L. Menezes Leitão, *Direito das obrigações*, vol. I, 13.ª ed., Almedina, Coimbra, 2016, pp. 286, ss..

26 O limite da lei anterior (art. 72.º, n.º 1 do RSP I — aprovado pelo Decreto-Lei n.º 317/2009, de 30 de outubro) era de €150. A Diretiva, na linha do reforço da tutela do utilizador, baixou-o para €50, o que consistiu num reforço considerável de proteção do utilizador.

No fundo, o utilizador assume o risco de perdas até este valor, uma vez que não se exige qualquer culpa sua (art. 115.º, n.º 1, RSP)[27].

A situação em termos de limitação das perdas verifica-se, igualmente, naqueles casos em que o ordenante tenha agido com culpa leve. Neste caso, não se trata de risco, mas de limitar as consequências do ato culposo do qual resultou um dano para o ordenante a esse valor. E fazer o restante recair sobre o prestador.

III. Todavia, mesmo nestas circunstâncias, este prejuízo limitado é afastado se a perda, o furto, o roubo ou a apropriação abusiva de um instrumento de pagamento não pudesse ser detetada pelo ordenante antes da realização de um pagamento ou a perda tiver sido causada por atos ou omissões de um trabalhador, de um agente ou de uma sucursal do prestador de serviços de pagamento ou de uma entidade à qual as suas atividades tenham sido subcontratadas (art. 115.º, n.º 2, als. *a)* e *b)*, RSP). Estes riscos correm todos por parte do prestador de serviços, traduzindo-se na restituição integral.

IV. O quadro exposto altera-se em duas circunstâncias: nos casos de fraude, dolo ou negligência grosseira.

Assim, se o ordenante tiver agido, se atuar de forma fraudulenta ou incumprir de forma deliberada — leia-se, dolosa — as obrigações que sobre ele impendem quanto aos serviços de pagamento, como se começou por referir *supra* (art. 115.º, n.º 3, RSP) suporta *todas as perdas* resultantes de operações de pagamento não autorizadas. Fica excluída a responsabilidade do banco.

Por outro lado, se o ordenante atuar com negligência grosseira, suporta as perdas até *ao limite* do saldo disponível ou da linha de crédito associada à conta (p. ex., um descoberto) ou ao instrumento de pagamento, sem o limite dos €50. Percebe-se: trata-se de um ilícito acompanhado pela forma mais grave de negligência, não havendo assim fundamento para impor a responsabilidade ao prestador para além daquele limite, sendo, pelo contrário, essa perda imputada ao utilizador (art. 115.º, n.º 4, RSP).

V. Estamos sempre dentro do âmbito da *autorização forte*. Na verdade, se o prestador de serviços de pagamento do ordenante não a exigir, a responsabilidade do ordenante é ainda mais restrita. Só suporta as perdas se tiver atuado fraudulentamente (art. 115.º, n.º 5, RSP)[28]. Claro está que o banco só a dispensará quando o risco for diminuto ou a operação de baixo valor.

Todavia, 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 (art. 105.º, n.º 6, RSP).

---

[27] Face ao art. 72.º do regime anterior (em parte coincidente com o atual 115.º RSP 2), M. Januário da Costa Gomes (*Contratos comerciais*, cit., p. 245) referia já que a norma regulava uma questão de risco.

[28] Situação distinta é se o beneficiário ou o seu prestador de serviços de pagamento não aceitar a autenticação forte do cliente, hipótese em que reembolsa os prejuízos financeiros causados ao prestador de serviços de pagamento do ordenante (art. 105.º, n.º 6, RSP).

VI. Cabe articular este regime com o dever de comunicar ao prestador de serviços de pagamento ou à entidade designada por este último a perda, o furto, o roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento (art. 110.º, n.º 1, al. *b)*, RSP). Depois desse momento — ou seja realizada a comunicação —, o utilizador dos serviços de pagamento deixa suportar quaisquer consequências financeiras resultantes da utilização de um instrumento de pagamento perdido, furtado, roubado ou abusivamente apropriado. O limite aqui é, também, o da sua atuação fraudulenta (art. 115.º, n.º 7, RSP).

VII. A análise que estamos a fazer assenta nas relações entre o prestador de serviços e o ordenante, deixando na sombra o terceiro que atuou ilicitamente ao retirar da conta do ordenante esses fundos. Claro está que atuou ilicitamente e responde sempre face ao titular da conta nos termos do art. 483.º, n.º 1 (para além da responsabilidade criminal), uma vez que lhe atinge um direito absoluto. Neste caso às somas pecuniárias. O titular da conta tem um crédito face ao banco, mas diz respeito a moeda escritural. Ao retirar esses fundos ilicitamente da sua conta, retira-lhe moeda escritural, que é meio de pagamento, mesmo face ao Estado[29]. Fundos esse que teria o direito de transformar em moeda legal, em termos garantidos pelo fundo de garantia dos depósitos e, em última instância, pelo próprio Estado.

Ao restituir essa quantia ao ordenante, o banco terá depois direito a reavê-la perante o autor do desvio.

Assim como o ordenante no montante da perda que lhe foi imposta, ao abrigo da responsabilidade civil extracontratual por factos ilícitos.

Contudo, e esse é em grande parte o ponto, esses créditos dificilmente podem obter satisfação, até porque se desconhecerá a identidade do terceiro. Por isso, na prática tudo se resolverá no âmbito das relações entre o ordenante e o prestador de serviços de pagamento e correspondente distribuição das perdas entre eles.

4.9. O afastamento da responsabilidade — casos de força maior

I. A responsabilidade prevista nos arts. 103.º a 134.º RSP não é aplicável em caso de circunstâncias anormais e imprevisíveis alheias à vontade da parte que as invoca, se as respetivas consequências não tivessem podido ser evitadas apesar de todos os esforços desenvolvidos. Consiste num caso de força maior: anormal, imprevisível e cujas consequências, pese embora o cumprimento das obrigações do banco — nos rigorosos e extensos termos em que a lei as impõem (p. ex., em caso de guerra) —, não podiam ter sido evitadas.

---

[29] Ver, desenvolvidamente sobre este ponto, M. Pestana de Vasconcelos, *Direito bancário*, cit., pp. 28, ss..

II. Não existe, igualmente, responsabilidade se o prestador de serviços de pagamento cumprir outras obrigações legais, nomeadamente, as relacionadas com a prevenção do branqueamento de capitais e de financiamento do terrorismo (art. 135.º RSP).

5. CONCLUSÕES

Do regime exposto é possível formular as seguintes conclusões, destacando os princípios que travejam a responsabilidade do banco nos casos de operações de pagamento não autorizadas (do maior relevo depois na interpretação das normas que compõem o regime).

1. Cabe ao utilizador manter sistemas de segurança, de diversa natureza, *state of the art*, para impedir que a conta do utilizador dos serviços seja acedida por terceiros, sem a autorização deste. Como vimos, trata-se de uma verdadeira obrigação de resultado, próxima de uma obrigação de garantia.

A sua justificação económica é clara: o cliente paga diversas comissões, em crescendo, pela realização de operações de pagamento. O seu cerne, diríamos que um dos núcleos da contraprestação do banco pela comissão paga (que tem sempre nos termos da lei de ter como correspetivo um serviço efetivo por parte do banco — art. 3.º, al. *f)*, do Decreto-Lei n.º 58/2013 de de 8 de maio[30]), é que a segurança dos fundos que confia ao banco seja protegida.

Ela desdobra-se, ou tem consagração direta, nos deveres de assegurar a proteção das credenciais e na deteção de operação abusivas ou fraudulentos. Mas tem caráter geral, como se vê. As operações abusivas ou fraudulentas podem assumir configurações muito diversas e, num momento em que sistemas de inteligência artificial possam dar vantagem aos *hackers*, o banco tem de assegurar a proteção das contas.

Violado o sistema, salvo em casos bastante restritos, de força maior, responde.

A autentificação forte consiste num meio eficiente de proteção adicional. Mas não é inviolável. Nada é, aliás, como bem se pode constatar pela constante penetração dos mais sofisticados sistemas de segurança.

2. Face a uma operação não autorizada, cabe ao prestador do serviço a restituição do valor. Porém, nos casos específicos da utilização de um instrumento de pagamento perdido, furtado, roubado ou da apropriação abusiva de um instrumento de pagamento, a lei aloca essa perda ao cliente até ao montante de €50. Depois desse valor, a responsabilidade cabe ao banco, no que consiste numa verdadeira responsabilidade pelo risco.

Só há um afastamento da responsabilidade do banco no âmbito das operações indevidas em caso de fraude ou de atuação dolosa. No que consiste, aliás, numa simples aplicação de um princípio geral do direito, nos

30 Ver M. Pestana de Vasconcelos, *Direito bancário*, cit., pp. 403, ss..

termos do qual a fraude não pode beneficiar quem a pratica. Diga-se, ainda, que poderá haver aqui concomitantemente responsabilidade criminal.

Fora destas hipóteses, só uma atuação com negligência grosseira do utilizador do serviço afasta a responsabilidade do banco para além do valor de €50. É o próprio utilizador que compromete os sistemas de segurança, incumprindo deveres que sobre ele impedem no âmbito da relação bancária/pagamento.

Mas exige-se negligência grosseira, o que é um caso extremo. A simples negligência simples, a culpa leve, não afasta a responsabilidade do banco.

Ou seja: no âmbito de riscos que a lei faz recair sobre o banco (e que incluem todos aquele relativos à penetração do sistema de segurança por terceiro — quando não haja, claro, culpa da sua parte por não ter um sistema suficientemente eficiente) inclui-se mesmo aquele que decorre do risco de um comportamento ilícito e culposo do cliente que gerou a perda para além dos €50. Portanto: do dano decorrente de uma ação ilícita, por incumprimento das obrigações contratuais, e culposa do cliente. Que vai mesmo, se o banco não exigir uma autentificação forte, aos casos de negligência grosseira da sua contraparte.

3. Pode, assim, concluir-se, numa breve súmula, que a responsabilidade do banco é, no quadro do nosso sistema, excecionalmente intensa. E que o novo RSP deu passos mais largos nesse sentido.

O objetivo é claro: dado o relevo central dos sistemas de pagamentos na vida moderna e a fonte crescente de rendimentos que os prestadores de serviços deles retiram, visa-se estabelecer uma proteção máxima dos titulares das contas.

(Porto, 19 de outubro de 2019)