# A EXECUÇÃO INCORRETA E NÃO AUTORIZADA DE ORDENS DE PAGAMENTO

Nuno Tomás Cardoso

**Resumo:** O novo regime jurídico dos serviços de pagamento e moeda eletrónica e a execução incorreta e não autorizada de ordens e operações de pagamento.

**Palavras-chave:** Operações de pagamento; execução incorreta; execução não autorizada; responsabilidade civil.



## INTRODUÇÃO

O comércio jurídico eletrónico é uma realidade incontornável dos nossos dias, permitindo a aquisição e pagamento à distância de bens e serviços de consumo nas várias plataformas digitais, nacionais ou estrangeiras.

Os serviços de pagamento à distância vieram introduzir novas regulamentações jurídicas, que se vieram juntar às regras jurídicas que tradicionalmente regulavam os vários aspetos da relação jurídica bancária.

De entre essas instituições jurídicas avulta o regime jurídico dos serviços de pagamento e a responsabilidade pela sua execução incorreta e não autorizada.

Procura-se, deste modo, analisar de forma simples e sucinta o regime jurídico dos serviços de pagamento eletrónicos e o modo como se concretiza a responsabilidade jurídica pela sua execução incorreta e não autorizada, de modo a estimular o jurista à sua aplicação ou invocação perante os litígios submetidos em tribunal.

## I. O QUADRO LEGAL

### 1. Breve história

O primeiro regime jurídico de serviços de pagamento, doravante RJSP, surgiu na sequência da transposição para a ordem jurídica interna da primeira Diretiva dos Serviços de pagamento, a Diretiva 2007/64/CE, também referida como DSP1, a qual procurou promover uma uniformização do regime legal aplicável à prestação de serviços de pagamento bancários no mercado interno da União Europeia, aumentando a transparência das condições aplicáveis aos serviços de pagamento, definindo os requisitos de informação aplicáveis, os direitos dos utilizadores e as obrigações dos prestadores dos serviços de pagamento.

A Diretiva 2007/64/CE foi transposta para a ordem jurídica nacional através do Decreto-Lei n.º 317/2009, de 30 de outubro, que aprovou o regime jurídico dos serviços de pagamento, o qual foi por sua vez alterado pelo Decreto-Lei n.º 242/2012, de 7 de novembro, que para além de alterar o regime jurídico dos serviços de pagamento, passou também a regular o regime jurídico da moeda eletrónica, efetuando ainda a transposição da Diretiva n.º 2009/110/CE vigente a esse respeito.

Posteriormente, o regime jurídico dos serviços de pagamento foi revisto pela Diretiva (EU) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro, também designada por DSP2.

As revisões introduzidas pela Diretiva procuraram responder a uma acrescida preocupação com a proteção e segurança dos consumidores, bem como com a segurança dos pagamentos efetuados por via eletrónica, com vista a regular a realidade dinâmica dos meios de pagamento gerada pela emergência de novas aplicações informáticas, utilizadas por via da disseminação de modernos modelos de aparelhos de comunicações integrados por processadores informáticos, como computadores portáteis e telefones inteligentes (*smartphones*).

O legislador português transpôs o conteúdo do diploma para o ordenamento jurídico nacional pelo Decreto-Lei n.º 91/2018, de 12 de novembro, doravante designado de RJSPME, seguindo de perto o sistema da Diretiva, organizando o diploma em oito títulos, com um sistema denso de definições que se desdobra para além da ordem das letras do alfabeto, apelando a um esforço do intérprete, para coadunar as suas definições.

Da leitura do preâmbulo do RJSPME revisto resulta a manutenção de muitas das soluções já vigentes no anterior regime, com desenvolvimento de algumas soluções, como sucede no caso do reforço dos deveres de informação pré-contratual e contratual dos utilizadores dos serviços de pagamento, em conjugação com o Decreto-Lei n.º 95/2006, de 29 de maio, que estabeleceu o regime jurídico aplicável aos contratos à distância relativos a serviços financeiros celebrados com consumidores.

A grande inovação do novo regime veio assentar na introdução de um conceito de *"autenticação forte"* para os serviços de pagamento à distância, cuja aplicação é incentivada pelo legislador, sob pena de agravamento da responsa-

bilidade do prestador de serviços que não a exige no acesso aos seus serviços, de forma a proteger a confidencialidade e segurança dos pagamentos.

São ainda regulados os vários aspetos relativos à responsabilidade pelas operações incorretamente executadas e não autorizadas e o modo de a concretizar perante os prestadores de serviços, bem como o respetivo ónus da prova, os quais cumpre analisar no presente artigo.

## II. DA RELAÇÃO JURÍDICA

### 1. Da relação jurídica bancária

O regime jurídico dos serviços de pagamento enquadra-se no regime geral da relação jurídica bancária tradicional.

A relação jurídica bancária comum ou tradicional inicia-se através de um contrato de abertura de conta bancária, o qual é denominado *"contrato bancário matriz"*[1]. Este contrato base é aquele por intermédio do qual se vão desenvolver as relações jurídicas e comerciais entre o cliente e o Banco, aqui se incluindo outros contratos associados, instrumentais à concretização da relação comercial, cujas modalidades se encontram regulados pelo Decreto-Lei n.º 430/91, de 2 de novembro, com as alterações do Decreto-Lei n.º 88/2008, de 29 de maio.

O contrato de abertura de conta bancária é qualificado como um contrato de depósito irregular, previsto nos arts. 1205.º e 1206.º do Cód. Civil, por intermédio do qual o cliente confia dinheiro ao Banco, para a sua guarda, o qual, na qualidade de coisa fungível, será adquirido pelo Banco, que ficará depois obrigado a restituí-lo, logo que solicitado para o efeito.

Na jurisprudência nacional têm existido duas correntes[2], uma primeira que considera o depósito bancário como um depósito irregular e uma segunda que o considera como um contrato inominado, o que assume relevância para efeitos de aplicação subsidiária de normas.

Ao contrato de depósito bancário são também associados outros contratos instrumentais para a concretização das operações bancárias, o que é denominado giro bancário. Este conceito é definido pela doutrina[3], como *"o conjunto de operações escriturais de transferência de fundos, realizadas por um banqueiro, a pedido do seu cliente ou a favor dele"*, aqui se incluindo as transferências bancárias, ou outros atos de execução da ordem do cliente.

Este giro bancário é suportado por um conjunto de serviços, como a realização de serviços bancários ao balcão e à distância, disponibilização de cartões de crédito, operações de débito-direto, designadamente, pela *internet*, através

---

1 Antunes, José A. Engrácia, *Direito dos Contratos Comerciais*, Almedina, abril 2011, p. 484.

2 Oliveira, Fernando Baptista, *Contratos Privados – Das Noções à Prática Judicial*, Vol. II, Coimbra Editora, 1.ª Edição, 2014, p. 346.

3 Cordeiro, António Menezes, *Manual de Direito Bancário*, Almedina, Coimbra, 1.ª Reimpressão, novembro 1999, p. 494.

de serviços de pagamento e transferência, onde vem agora assumir expressa autonomia o contrato-quadro de prestação de serviços de pagamento (art. 2.º, alínea i) do RJSPME).

## 2. Do contrato-quadro

Antes da entrada em vigor do Decreto-Lei n.º 317/2009, de 30 de outubro, inexistia regulamentação jurídica específica sobre os serviços de pagamento eletrónicos, sendo as questões suscitadas no âmbito deste regime apreciadas no âmbito geral das normas do contrato de mútuo e de depósito.

A jurisprudência, em virtude da ausência dessa regulamentação jurídica específica, começou por considerar o denominado *"contrato de utilização de instrumentos de pagamento"*[4] como acessório ou instrumental em relação ao contrato de depósito bancário, o que se revelaria não só pela função do contrato, mas também pelo seu destino, que se encontrava ligado aos contratos anteriores. Neste sentido, o Ac. STJ de 15.05.2007[5], lavrado num período cronológico em que ainda não tinha sido emitida a primeira Diretiva em matéria de serviços de pagamento, a DSP1.

Posteriormente, começou a definir-se este contrato como um contrato autónomo relativamente ao contrário bancário matriz, apesar de se salientar a inexistência de regulamentação jurídica deste tipo de serviços. Neste sentido, o Ac. STJ de 15.10.2009[6].

O panorama alterou-se após a entrada em vigor do DSP1, sendo que atualmente a jurisprudência, v.g., o Ac. TRP de 14.07.2020[7], considera o contrato de utilização de instrumentos de pagamento como autónomo em relação ao contrato bancário matriz e sujeito até ao seu próprio contrato quadro ou matriz.

Assim, para a utilização dos serviços de pagamento passou a estar previsto um contrato-quadro, assim designado na lei (art. 2.º, alínea i) do RJSPME), o qual irá regular o modo e meios através dos quais o serviço de pagamento se realizará, designadamente, cartão de crédito ou serviços da banca *online* (*home banking*).

Podemos, então, afirmar que a autonomia do contrato de utilização de serviços de pagamento resulta agora de previsão legal expressa (art. 2.º, alínea i) do RJSPME). Porém, enquanto para uma parte da doutrina, como Francisco Correia[8], as operações singulares de pagamento *"devem qualificar-se como actos de execução do contrato inicial e não como novos contratos"*, para outra

---

4 Lima, Raquel Sofia Ribeiro, «A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na jurisprudência portuguesa», em *Revista Eletrónica de Direito da Faculdade de Direito da Universidade do Porto*, outubro de 2016, n.º 3, p. 8, disponível em https://cije.up.pt/pt/red/edicoesanteriores/2016-nordm-3/a-responsabilidade-pela-utilizacao-abusiva-on-line-de-instrumentos-de-pagamentoeletronico-na-jurisprudencia-portuguesa/.

5 Ac. STJ de 17.05.2007, relatado por Oliveira Rocha e disponível em http://www.dgsi.pt.

6 Ac. STJ de 15.10.2009, relatado por Alberto Sobrinho e disponível em http://www.dgsi.pt.

7 Ac. TRP de 14.07.2020, relatado por Fernando Baptista e disponível em http://www.dgsi.pt.

8 Correia, Francisco Mendes, «Operações não autorizadas e o regime jurídico dos serviços de pagamento e moeda eletrónica», em *Revista de Direito Civil*, Ano II (2017), Número 3, p. 705.

parte da doutrina, como Maria Raquel Guimarães[9], cada operação será um novo contrato de utilização de instrumento de pagamento, emitido com base no contrato-quadro de emissão de instrumento de pagamento.

Somos por perfilhar a interpretação sustentada por Francisco Correia, por ser aquela que, em nosso entender, melhor se integra na natureza do contrato--quadro e no propósito da relação jurídica bancária, apenas podendo a operação ser considerada num novo contrato no caso das operações de pagamento isoladas, isto é, que não estão enquadradas no âmbito de um contrato-quadro celebrado com um prestador de serviços de pagamento.

Com efeito, a utilização de serviços de pagamento com carácter isolado, de uma forma única, sem estar enquadrada em qualquer espécie de contrato, também não deixa de ficar sujeita à disciplina do diploma que regula os serviços de pagamento (art. 76.º do RJSPME), o que nos leva à próxima questão sobre a natureza do diploma.

Deste modo, teremos apenas dois contratos base, o da relação jurídica bancária tradicional e o contrato-quadro dos meios de pagamento, sendo o ato que origina a obrigação de pagamento uma mera execução dos dois anteriores e não um contrato com autonomia específica.

Na verdade, o ato que gera a obrigação de pagamento poderá ser qualificado como um contrato, mas apenas na sua vertente externa, na medida em que é celebrado entre utilizador dos serviços de pagamento – designado na lei como ordenante – e o beneficiário do serviço de pagamento, destinatário final da quantia ou preço. Esse, sim, já será um contrato autónomo, assumindo aqui o serviço de pagamento um carácter meramente instrumental.

### 3. Natureza imperativa

O regime jurídico de serviços de pagamento e da moeda eletrónica previsto no Decreto-Lei n.º 91/2018, de 12 de novembro (RJPME), tem carácter obrigatório e geral, aplicando-se às microempresas do mesmo modo que aos consumidores[10], embora sempre que o utilizador de serviços de pagamento não seja um consumidor, como por exemplo uma empresa, ou um profissional liberal, as partes podem, no clausulado do contrato-quadro em que acorda na prestação de serviços afastar, no todo ou em parte, algumas das normas previstas no presente capítulo (art. 76.º, n.ºs 2 e 3 do RJSPME).

O conteúdo e amplitude da obrigação de informação variam consoante nos encontremos perante uma operação de pagamento de carácter isolado (art. 83.º

---

9 Guimarães, Maria Raquel, *O Contrato-Quadro no Âmbito da Utilização de Meios de Pagamento Eletrónicos*, abril 2011, Coimbra Editora/Wolters Kluver, p. 507.

10 Nos termos do art. 2.º, alínea f) do RJSP, *"«consumidor» é uma pessoa singular que atua, nos contratos de serviços de pagamento e nos contratos celebrados com os emitentes de moeda eletrónica abrangidos pelo presente Regime Jurídico, com objetivos alheios às suas atividades comerciais, empresariais ou profissionais."*.

do RSJPME), ou perante uma operação de pagamento no âmbito de um contrato-quadro (arts. 90.º e 91.º do RJSPME), caso em que muitas das obrigações de informação já se encontram comunicadas e prestadas por via contratual.

A informação pré-contratual tem de ser prestada em suporte de papel ou qualquer outro relativamente ao suporte duradouro, que permita a sua disponibilização quando expressamente solicitado pelo utilizador, devendo ser fornecido mesmo quando o contrato é celebrado à distância (arts. 83.º, n.ºs 2 e 3 e 90.º, n.ºs 2 e 3 do RJSPME).

O ónus do cumprimento da informação prévia recai sobre o prestador de serviços (art. 80.º do RJSPME), assumindo também relevância o disposto no Decreto-Lei n.º 446/85, de 25 de outubro, com as sucessivas alterações, que aprovou o regime jurídico das cláusulas contratuais gerais (RJCCG), na medida em que os prestadores de serviços são usualmente entidades bancárias que apresentam os contratos de forma predisposta e pré-elaborada, pelo que ao ónus de informação do RJSP acrescerá o ónus de informação do regime das cláusulas contratuais gerais (art. 6.º do RJCCG), recaindo sobre a entidade prestadora de serviços, o ónus de comunicação efetiva (art. 5.º, n.º 3 do RJCCG).

O carácter injuntivo do RJSPME assume relevância no âmbito da validade das cláusulas contratuais estabelecidas entre as partes, o que é especialmente importante tendo em conta que o contrato-quadro será geralmente um contrato de adesão, em que uma das partes, em regra o banco, no dizer de Menezes Cordeiro[11], irá predispor o conteúdo do mesmo de forma genérica, rígida e não negociável, com vista a permitir a rapidez das operações.

A falta do cumprimento deste dever de informação, apesar de não vir expressamente regulado, implicará que as cláusulas não comunicadas se considerem excluídas do contrato, aplicando-se o regime civil subsidiário, com recurso, se necessário, às regras integração do negócio jurídico (art. 9.º, n.º 1 do RJCCG), o que terá relevância em termos de consequência da imputação das operações.

Por outro lado, serão nulas todas as cláusulas do contrato-quadro que se oponham às normas imperativas previstas no RJSPME (art. 294.º do Cód. Civil), designadamente, na parte em que preveem a distribuição do ónus da prova ou risco adveniente das operações, v.g., o Ac. TRL de 21.12.2017[12], já citado acima, onde se decidiu que *"são nulas e devem ser excluídas das Condições Gerais do contrato de utilização do serviço Caixadirecta on-line a que aludem os autos, por alterarem as regras de distribuição do risco e modificarem os critérios de repartição do ónus da prova (cf. artigos 12.º, 20.º e 21.º, alíneas f) e g) do Dec.Lei n.º 446/85, de 25 de Outubro), as cláusulas 9, 10 e 11 das referidas Condições Gerais, ao estabelecerem a presunção de que as operações bancárias realizadas fraudulentamente por terceiro foram consentidas e autorizadas pelo cliente."*.

---

11 Cordeiro, António Menezes, *Manual de Direito Bancário*, Almedina, Coimbra, 1.ª Reimpressão, novembro 1999, p. 444.

12 Ac. TRL de 21.12.2017, relatado por Manuel Rodrigues e disponível em http://www.dgsi.pt.

## 4. Operações abrangidas

A primeira versão do regime jurídico de serviços de pagamento previsto pelo Decreto-Lei n.º 317/2009, de 30 de outubro, aplicava-se apenas aos pagamentos dentro da União Europeia, no que significava que os ordenantes iniciais e os beneficiários finais das operações de pagamento teriam de ser comerciantes ou cidadãos, fisicamente situados dentro do espaço da União Europeia.

O novo regime do Decreto-Lei n.º 91/2018, de 12 de novembro, mantém a aplicação às operações de pagamento efetuadas na moeda de um estado membro e situadas na União Europeia, mas aplica-se agora, também às parcelas de pagamento efetuadas em Portugal em qualquer moeda, independentemente da moeda da transação, e mesmo que um dos prestadores de serviços de pagamento esteja situado em Portugal e outro fora da União Europeia (art. 3.º, n.º 3, alínea c) do RJSPME).

São, deste modo, aplicáveis às operações de pagamento, para fora da União Europeia, as disposições relativas à transparência e deveres de informação e esclarecimento, a cargo dos prestadores de serviços de pagamento com os seus clientes.

Assim, por exemplo, um cliente português coloca uma ordem de pagamento de serviços junto do seu banco em Portugal, para uma conta aberta num banco em Angola, sendo o regime jurídico dos serviços de pagamento aplicável à parcela da ordem executada em Portugal, pelo que a entidade prestadora dos serviços de pagamento em Portugal deverá informar o ordenante de qual a data prevista de realização da operação (data-valor) e a data em que o montante será creditado na conta de destino (data de disponibilização), a fim de permitir o adequado cumprimento da obrigação pecuniária.

O regime jurídico de serviços de pagamento, tem, contudo, exclusões, não se aplicando totalmente aos pagamentos em numerário sem intermediação bancária, bem como aos pagamentos através de cheque, vales ou ordens postais bem como aos levantamentos em numerário através de caixas automáticas (art. 5.º, n.º 1, alíneas a), g) e o) do RJSPME).

O regime é, porém, aplicável à fixação da data-valor dos pagamentos em dinheiro, como se verá adiante (art. 126.º do RJSPME).

Com efeito, o regime jurídico dos serviços de pagamento, não derrogou as convenções internacionais, como a Lei Uniforme dos Cheque, ou a Lei Uniforme de Letras e Livranças (LULL), pelo que as mesmas continuarão aplicáveis a esses tipos de pagamento.

## 5. As modalidades de serviços de pagamento

O objeto do regime jurídico dos serviços de pagamento é definir as várias modalidades de serviços de pagamento, os quais consistem em todos os serviços que permitam depositar ou levantar numerário de uma conta, e todas as operações necessárias à gestão dessa conta, aqui se incluindo a execução de

operações de pagamento, como os débitos diretos ou através de um cartão de pagamento (art. 4.º, alíneas a), b) e c) do RJSPME).

O Decreto-Lei n.º 91/2018, de 12 de novembro, veio inovar no campo dos serviços admissíveis, prevendo a existência de dois novos serviços de pagamento: os serviços de informação sobre contas e os serviços de iniciação de pagamento (art. 4.º, alíneas g) e h) do RJSPME).

Os serviços de informação sobre contas (*Account Information Serviçe*) visam permitir a reunião de informação sobre várias contas bancárias, mesmo que de bancos de diferentes Estados Membros, numa única aplicação digital para computador ou telemóvel com processador (*smartphone*) ou página *internet*, que agrega várias contas de pagamento em diferentes instituições e permite uma visão global da situação financeira.

O serviço de iniciação de pagamentos (*Payment Initiation Service*) visa permitir a realização de uma operação de pagamento em ambiente digital (*online*), sem que o ordenante tenha de agir diretamente com o prestador de serviços de pagamento (Banco) no qual a conta está domiciliada, permitindo assegurar a confidencialidade e segurança.

Nestes casos, será o prestador de serviços de iniciação de pagamento a aceder, em nome do cliente, à conta bancária do ordenante e a iniciar a operação de pagamento junto do prestador de serviços de pagamento do beneficiário.

As entidades prestadoras de serviços de pagamento passam a deixar de poder ser apenas as instituições bancárias, para passarem a poder ser outras, embora limitadas àquelas que se encontrem previstas no art. 11.º, n.º 1, alínea a) do RSJPME, sendo proibida a prestação a título profissional de serviços de pagamento, por parte de entidades não incluídas nestas alíneas, nisso consistindo o princípio da exclusividade (art. 11.º do RJSPME).

As entidades gestoras podem visar a prestação de um ou mais serviços de pagamento previstos na lei, caso em que poderão assumir a designação de instituições de pagamento (arts. 11.º, n.º 5 e 13.º, n.º 1 do RJSPME).

A constituição de instituições de pagamento depende de autorização a conceder, caso a caso, pelo Banco de Portugal, estando dependente de várias condições gerais (art. 18.º, n.ºs 1 e 2 do RJSP), de liquidez e solvabilidade (art. 48.º do RJSPME) e encontrando-se sujeitas a registo junto do Banco de Portugal (art. 34.º, n.º 1 do RJSPME) e fiscalização pela mesma entidade.

O Banco de Portugal estabeleceu, no Aviso n.º 2/2021[13], os avisos aplicáveis às instituições de pagamento e de moeda eletrónica e a sua aplicação no tempo.

[13] Aviso do Banco de Portugal n.º 2/2021, de 30 de Março, disponível em http://www.bportugal.pt/aviso/all.

## III. AS OBRIGAÇÕES DAS INSTITUIÇÕES DE PAGAMENTO

### 1. Obrigações internas

O regime jurídico dos serviços de pagamento veio estabelecer várias obrigações genéricas de organização interna de atividade a cargo das instituições de pagamento, as quais assumem relevância, em nosso entender, como normas de conduta no decurso da prossecução da atividade económica das mesmas, e que se distinguem dos deveres concretos, que se colocam a propósito da execução do programa contratual e de cada uma das ordens de pagamento.

Tais normas vêm acrescer, no caso dos bancos, às que já resultam do seu quadro de atividade, previstas pelo Decreto-Lei n.º 298/92, de 31 de dezembro, que aprovou o regime geral das instituições de crédito e sociedades financeiras, com a suas sucessivas alterações, abreviadamente designado RJICSF, designadamente, no seu art. 90.º-A (Registos e Arquivo), art. 90.º-B (conceção de produtos), art. 90.º-C (comercialização de produtos) e art. 90.º-D (monitorização de produtos).

As obrigações constantes do RJSPME são essencialmente quatro:

A primeira obrigação é a obrigação de controlo do *controlo do risco operacional e de segurança*, que obriga estas instituições a estabelecer um quadro de medidas de mitigação de incidentes e mecanismos de controlo adequado para gerir os riscos operacionais e de segurança dos serviços de pagamento por si prestados, fornecendo anualmente ao Banco de Portugal uma avaliação dos riscos de atividade e mecanismos de controlo adotados (art. 70.º, n.º 3 do RJSPME).

A segunda obrigação consiste em adotar medidas de segurança suficientes para proteger a *confidencialidade e a integridade das credenciais de segurança personalizada dos utilizadores* dos serviços de pagamento (art. 104.º, n.º 3 do RJSPME). Esta obrigação, ainda que de carácter indeterminada, aproxima-se bastante de um dever, o qual existirá simultaneamente, em concreto, a propósito de cada instrumento de pagamento emitido para cumprimento de ordem de pagamento.

A terceira obrigação consiste na *manutenção de registos de atividades, serviços e operações,* que permitam a todo o tempo, a verificação do cumprimento dos deveres a que estão obrigados nos termos do presente regime, estando obrigados disponibilizar ao Banco de Portugal as comunicações trocadas com os utilizadores dos serviços de pagamento, seja por formato escrito ou gravação de conversa telefónica (art. 73.º, n.ºs 1, 3 e 4 do RJSPME).

A quarta obrigação é a *proibição genérica de prestação de serviços a entidades sediadas em ordenamentos jurídicos offshore considerados não cooperantes ou de beneficiário último desconhecido*, sem prejuízo de deverem proceder ao registo das operações de serviços de pagamento, que tenham como beneficiário pessoa singular ou coletiva situada em ordenamento jurídico *offshore* (art. 74.º do RJSP e art. 118.º-A do Decreto-Lei n.º 298/92, que aprovou o regime geral das instituições de crédito e sociedades financeiras – RGICSF). Neste sentido, é autorizado o tratamento de dados pessoais pelos sistemas de pagamento e

pelos prestadores de serviços de pagamento, na medida em que se mostrar necessário à salvaguarda da prevenção da investigação e deteção de fraude em matéria de pagamentos (art. 136.º, n.º 1 do RJPS).

## 2. Obrigações externas

As obrigações externas das instituições de pagamento colocam-se perante os clientes que com elas celebram contratos, e no âmbito da execução das ordens e operações de pagamento em concreto, constituindo deveres com conteúdo legal, cuja violação e inobservância serão fonte de responsabilidade civil contratual.

Assim, no âmbito da sua atividade de operações de pagamento, surpreendem-se os seguintes deveres:

– *Dever de assegurar a acessibilidade reservada do instrumento de pagamento*, pelo que só o autor da ordem poderá aceder ao mesmo, correndo o risco do envio do instrumento de pagamento, por conta do prestador de serviço de pagamento (art. 111.º, n.º 1, alínea a) e n.º 3 do RJSPME), que nessa medida deverá adotar mecanismos seguros de transmissão do mesmo.

Este dever apresenta relevância em dois aspetos:

O primeiro diz respeito à entrega do instrumento, o qual, pese embora considerado acessório pela doutrina[14], originou no passado, na ausência de regulamentação específica, várias questões a propósito do envio de cartões físicos via postal, levando à criação de vária jurisprudência sobre quem recaía a responsabilidade pela entrega do instrumento de pagamento, tendo-se concluído que tal risco recaía sobre a instituição de pagamento, o que conheceu agora letra de lei, apesar de já existirem recomendações, com cerca de vinte anos, nesse sentido, pelo Banco de Portugal[15], que recomendava que não fossem enviados cartões prontos a utilizar.

Atualmente, a questão da entrega do instrumento deverá ser colocada no âmbito do envio digital do instrumento de pagamento, devendo a entidade prestadora de serviços de pagamento enviar o instrumento de pagamento apenas para o correio eletrónico identificado como sendo do ordenante, ou para o número telefónico associado, devendo o sistema do banco poder reconhecer se o número telefónico se encontra inserido num IMEI validado, pois o mesmo cartão num telemóvel diferente, poderá ser sinal de intromissão não autorizada, que cumpre detetar, sob pena de imputação da operação não autorizada à entidade prestadora de serviços de pagamento.

---

14 Lima, Raquel Sofia Ribeiro, ob. cit., p. 18.

15 Aviso do Banco de Portugal n.º 11/2001, de 20 de novembro, disponível em http://www.bportugal.pt/aviso/all.

O segundo aspeto, e o mais relevante, implica que os riscos de acessibilidade derivados da utilização normal do instrumento de pagamento correm por conta da entidade gestora dos serviços de pagamento, sendo esta que suporta dos riscos de uma operação não autorizada, que tenha origem na intromissão no instrumento de pagamento do cliente.

– *Dever de abstenção de envio de instrumentos de pagamentos não solicitados*, isto é, sem que seja colocada uma ordem de pagamento, salvo nos casos de necessidade de substituição do instrumento de pagamento anterior (art. 111.º, n.º 1, alínea b) do RJSPME). Este dever está em linha com o dever de proteção económica dos consumidores (art. 9.º, n.º 4 da Lei n.º 24/96, de 31 de julho, que aprovou a Lei de Defesa dos Consumidores[16]) contra a venda forçada de produtos ou serviços não previamente solicitados.
– *Dever de garantir, a todo o momento, meios apropriados para comunicar operações fraudulentas ou solicitar o desbloqueio*, sob pena de o ordenante não ficar obrigado a suportar as consequências financeiras resultantes da utilização desse sistema de pagamento, salvo caso utilização fraudulenta (arts. 111.º, n.º 1, alínea c) e 115.º, n.º 8 do RJSPME). Este dever é relevante, na medida em que o utilizador de serviços de pagamento, tem o dever de comunicar, sem atraso injustificado, ao prestador de serviços de pagamento ou entidade por aquele indicada, da perda, furto, roubo, apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento (art. 110.º, n.º 1, alínea b) do RJSPME).

O dever de comunicação do utilizador de serviços é importante, na medida em que só após a comunicação de operação não autorizada o utilizador deixará de suportar quaisquer consequências financeiras resultantes da utilização de um sistema de pagamento perdido, furtado, roubado ou abusivamente apropriado (art. 115.º, n.º 7 do RJSPME). A entidade prestadora de serviços de pagamento deverá, assim, garantir, a todo o momento, os meios apropriados para comunicar as operações fraudulentas, sob pena de poder começar a responder em momento anterior ao comunicado.

– *Dever de facultar ao utilizador dos serviços de pagamento, a pedido deste, os meios necessários para fazer prova, durante 18 meses, de que efetuou a comunicação de furto, roubo, apropriação abusiva, ou qualquer utilização não autorizada do instrumento de pagamento* (art. 111.º, n.º 1, alínea d) do RJSPME). Este dever assume um carácter

---

16 Art. 9.º, n.º 4 da Lei n.º 24/96, de 31 de julho: *"O consumidor não fica obrigado ao pagamento de bens ou serviços que não tenha prévia e expressamente encomendado ou solicitado, ou que não constitua cumprimento de contrato válido, não lhe cabendo, do mesmo modo, o encargo da sua devolução ou compensação, nem a responsabilidade de duração média normal dos produtos fornecidos."*.

conservatório, por forma a garantir que durante determinado período de tempo, fica registada a comunicação efetuada, o que poderá ter relevância no caso de existir inquérito criminal sob a conduta do utilizador, o qual terá uma duração não inferior àquele período de tempo, assegurando-se assim a fidedignidade das datas das comunicações, o que terá relevância para responsabilidade civil futura.

– *Dever de impedir toda a utilização do instrumento de pagamento, após a comunicação de operação fraudulenta* (art. 111.º, n.º 1, alínea e) do RJSPME). O presente dever é um corolário do dever de assegurar a acessibilidade reservada do instrumento de pagamento, pelo que uma vez comunicada a violação desse acesso, é dever da entidade prestadora de serviços de pagamento impedir o acesso não autorizado.

Os referidos deveres estão a cargo da entidade prestadora de serviços de pagamento e devem ser observados em toda e qualquer operação de pagamento, sendo deveres conformadores da prestação a seu cargo, cujo incumprimento determinará, inevitavelmente, a sua responsabilidade civil, como acima se mencionou.

## IV. AS OBRIGAÇÕES DO UTILIZADOR

### 1. Os deveres do utilizador

O utilizador de serviços de pagamento não tem, à semelhança do que sucede com as entidades prestadoras de serviços de pagamento, obrigações genéricas que sobre ele recaiam, porém, não está isento de deveres, no âmbito da utilização concreta de instrumentos de pagamento emitidos, a sua solicitação.

Assim, e sem prejuízo de posteriormente se analisarem os aspetos jurídicos emergentes de uma ordem de pagamento, são de enunciar os seguintes deveres:

– *O dever de utilização adequado do instrumento de pagamento.* Este dever será cumprido de acordo com as instruções de segurança que regeram a sua emissão e regem a sua utilização (art. 110.º, n.º 1, alínea a) do RSJPME). As instruções de segurança são regras técnicas de autenticação que permitem ao prestador de serviços de pagamento verificar a identidade do utilizador do instrumento de pagamento, e não duvidar que os elementos constantes da ordem são dele provenientes, por se encontrarem validados com as credenciais de segurança personalizadas (art. 2.º, alínea c) do RJSPME), que apenas são conhecidas pelo utilizador (art. 111.º, n.º 1, alínea a) do RJSPME).

O utilizador dos serviços de pagamento deverá, deste modo, utilizar a diligência adequada, segundo o critério de um bom pai de família (art. 487.º, n.º 2 do Cód. Civil), por forma a não colocar em perigo a utilização do instrumento de pagamento emitido, evitando condutas de negligência ou desleixo na guarda das instruções de segurança que lhe permitem a autenticação, evitando a divulgação dos códigos e palavras chave de acesso, sob pena de a entidade prestadora de serviços de pagamento, não responder pelas perdas.

Este será o dever cuja discussão mais se colocará na prática, o que já vinha a suceder na primeira versão da DSP1, na medida em que à entidade prestadora de serviços de pagamento caberá alegar e provar o uso incorreto das instruções de segurança por parte do utilizador do sistema de pagamento, ou a negligência na guarda das instruções de segurança e autenticação.

No dizer de Raquel Guimarães[17], poderá até ser invocado incumprimento deliberado do utilizador, *"dependendo do 'esquema' concreto através do qual os dados do utilizador são obtidos e do seu grau de 'ingenuidade' ao facultar esses dados".*

Na verdade, apenas no caso de existir negligência leve do utilizador dos serviços, no uso dos instrumentos de segurança, caberá à entidade prestadora dos serviços de pagamento suportar o risco do prejuízo decorrente de operações não autorizadas, pois caso exista negligência grave ou grosseira, deverá ser responsabilizado o utilizador. Neste sentido, a jurisprudência[18] considerou recentemente que *"estando provado que a Autora transmitiu as credenciais de autenticação ao pai que as disponibilizou online em site e por meio não apurado, incluindo os números das coordenadas do cartão matriz e que "foi através do uso dessas credenciais de acesso que um sujeito cuja identificação não foi possível apurar atuou da forma descrita nas alíneas…" (para além de se ter, ainda, provado que "o sistema informático do réu não foi alvo por essa ocasião de um ataque informático), só a essa postura gravemente negligente da Autora se devem atribuir as consequências danosas no seu património, que, como tal, terá de suportar."*.

Será, então, no recorte prático de cada operação em causa que o presente dever será afirmado.

– *O dever de proteção das credenciais de segurança personalizadas* que lhe são disponibilizadas para a realização da operação por parte do prestador dos serviços de pagamento (art. 110.º, n.º 2 do RJSPME), não devendo ter qualquer comportamento imprudente que permita que terceiros possam tomar conhecimento das credenciais de segurança e apropriar-se das quantias objeto da operação de pagamento. Este dever encontra-se relacionado com o dever anteriormente exposto;

---

17 Guimarães, Maria Raquel, «A fraude no comércio eletrónico: o problema da repartição do risco por pagamentos fraudulentos», *Infrações Económicas e Financeiras: Estudos de Criminologia e Direito,* Coimbra Editora, 2013, p. 594.

18 Ac. TRP de 14.07.2020, relatado por Fernando Baptista e disponível em http://www.dgsi.pt.

– *O dever de comunicação, sem atraso injustificado*, ao prestador de serviços de pagamento ou entidade por aquele indicada, da perda, furto, roubo, apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento (art. 110.º, n.º 1, alínea b) do RJSP).

Após a realização desta comunicação, o ordenante não suportará quaisquer consequências financeiras resultantes da utilização de um sistema de pagamento perdido, furtado, roubado ou abusivamente apropriado, salvo no caso de atuação fraudulenta (art. 115.º, n.º 7 do RJSP).

Os deveres em causa devem ser observados em toda e qualquer operação de pagamento, sendo conformadores da prestação, cujo incumprimento poderá determinar a exclusão da responsabilidade civil do prestador de serviços de pagamento, por operações não autorizadas.

## V. DAS OPERAÇÕES DE PAGAMENTO

### 1. A instrução de pagamento

O RJSPME regula o modo de emissão das ordens de pagamento, estabelecendo um elaborado sistema de definições, que cumpre elucidar.

O primeiro ponto chave da ordem de pagamento é o seu autor, que a lei define como o utilizador, e que será a pessoa singular ou coletiva, que utiliza o serviço de pagamento, a título de ordenante ou de beneficiário, ou até em ambas as qualidades (art. 2.º, alínea eee) do RJSPME).

O ordenante é definido por sua vez, como a 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, alínea mm) do RJSPME).

O segundo ponto chave é própria ordem de pagamento, a qual surge definida como a 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, alínea ll) do RJSPME).

A operação de pagamento é definida como o ato praticado 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, alínea ii) do RJSPME).

Para a concretização material da operação de pagamento, o ordenante carecerá de utilizar um instrumento de pagamento, o qual consiste, por sua vez, num conjunto de procedimentos de autenticação acordados entre o utilizador e o prestador de serviços de pagamento (art. 2.º, alínea aa) do RJSPME), regra geral, através de uma aplicação informática, que poderá estar alojada num cartão, telemóvel, computador ou outro dispositivo tecnológico (art. 2.º, alínea bb) do RJSPME).

O utilizador deverá concretizar, na ordem de pagamento, os elementos essenciais da operação a ordenar – *nisto consistindo a sua instrução* –, a fim de tornar a sua declaração perfeita, na medida em que ocorrendo a mesma, as mais das vezes, em formulário digital, não haverá lugar à aplicação da doutrina da impressão do destinatário, consagrada no art. 236.º do Cód. Civil, pelo que terá de haver correspondência entre a instrução pretendida pelo ordenante e os dados inscritos no formulário digital.

No âmbito desta instrução, o utilizador do serviço de pagamento deve indicar um identificador único, o qual consiste numa combinação de letras, números ou símbolos fornecidos pelos prestadores de serviços de pagamento para identificar outro utilizador ou a conta destino, tendo em vista uma operação de pagamento (art. 2.º, alínea z) do RJSPME).

O RJSPME não prevê a possibilidade de correção de lapsos na ordem de pagamento após a sua validação e envio ao prestador de serviços de pagamento do ordenante, mas caso os dados inseridos não permitam realizar a operação, poderá ser recusada a execução da ordem, devendo nesse caso a entidade prestadora de serviços comunicar ao ordenante o procedimento a seguir para retificar os erros factuais que tenham conduzido a essa recusa (art. 120.º, n.ºs 2 e 5 do RJSPME), o que não se confunde com a retificação a cargo do prestador de serviços (arts. 130.º e 131.º do RJSMPE).

O RJSPME dispõe ainda que antes da realização de qualquer operação de pagamento, deve pela entidade prestadora de serviços de pagamento ser prestada informação obrigatória sobre a mesma, a qual permitirá ao utilizador acompanhar a execução da ordem.

A obrigação de informação pode, por acordo entre o utilizador e a entidade prestadora de serviços de pagamento, ser dispensada nas operações de pagamento de baixo valor, que não excedam € 30,00 ou tenham um limite de despesas ou fundos até € 150,00, ou que sejam provenientes de instrumentos pré-pagos até ao valor de € 250,00, como por exemplo sucede nos cartões porta-moedas eletrónicos (art. 81.º do RJSPME).

Assim, após a emissão da ordem de pagamento, e caso exista saldo credor a favor do utilizador, deverá ser comunicada a confirmação da receção da ordem (iniciação) com a sua referência e montante (art. 85.º do RJSPME).

Seguidamente, exige-se a verificação dos elementos da ordem (confirmação), como seja a data de receção e montante de encargos associados (art. 87.º do RJSPME), aqui se situando o momento do consentimento para autorização da operação (art. 103.º, n.ºs 1 e 2 do RJSPME) prestado pela via digital.

Após a execução da ordem, a entidade prestadora de serviços de pagamento deve prestar informação sobre a data efetiva de realização da operação, isto é, a data em que a quantia transferida ou paga estará disponível para o beneficiário da operação (data-valor), devendo ainda indicar o montante e encargos da operação, com uma referência identificativa da mesma (art. 88.º do RJSPME), o que terá relevância para rastrear a mesma.

Após a autenticação forte da operação, o prestador de serviços de pagamento que gere a conta não poderá recusar a execução de uma ordem de pagamento autorizada (art. 120.º, n.º 1 do RJSPME).

A ordem de pagamento emitida, após ter sido recebida pelo prestador de serviços de pagamento, tem carácter irrevogável (art. 103.º, n.º 6 do RJSPME), só podendo ser revogada se existir acordo entre o utilizador e o prestador de serviços de pagamento em causa (art. 121.º, n.ºs 1 e 5 do RJSPME).

Caso não exista esse acordo, apenas nos casos de a ordem ter sido dada com prazo futuro, no máximo, de quatro dias úteis (art. 123.º, n.º 1 do RJPME), é que o utilizador dos serviços de pagamento poderá, até ao final do dia útil anterior à data acordada, revogar a ordem de pagamento (art. 121.º, n.º 4 do RJSPME).

A lei prevê ainda, desde que convencionado no contrato-quadro, o bloqueio da ordem de pagamento, no caso de objetivamente estar em causa a segurança do instrumento de pagamento, a suspeita não autorizada ou fraudulenta do uso desse instrumento, ou no caso de existir uma linha de crédito associada, o risco de ultrapassagem desses limites (art. 108.º, n.º 2 do RJSPME).

A norma é algo equívoca, na medida em que o prestador de serviços de pagamento poderá, à margem do contrato, impedir o acesso do utilizador aos serviços de pagamento, caso existam motivos objetivamente comprovados, relacionados com o acesso não autorizado à conta de pagamento ou com a iniciação fraudulenta e não autorizada de uma operação de pagamento (art. 109.º, n.º 1 do RJSPME).

O utilizador deverá ser informado da recusa com estes motivos (art. 109.º, n.º 2 do RJSPME), e o incidente deverá ser comunicado ao Banco de Portugal, com os pormenores relevantes, sem prejuízo da competência das autoridades judiciais (art. 109.º, n.ºs 5 e 6 do RJSPME).

## 2. Da autenticação forte

A previsão da autenticação forte foi uma inovação criada pela DSP2, e passa a estar disponível sempre que o cliente acede via remota (*online*) à sua conta de pagamento, inicia uma operação de pagamento eletrónico, ou realiza uma ação através de um canal remoto, que possa envolver o risco de fraude no pagamento ou abusos (art. 104.º, n.º 1, alíneas a), b) e c) do RJSPME).

A noção de autenticação forte é expressamente definida na lei como uma autenticação baseada na utilização de dois ou mais elementos, independentes entre si, na medida em que a violação de um deles não possa comprometer o outro (art. 2.º, alínea d) do RJSPME).

A noção de autenticação fraca é definida por exclusão de partes.

A autenticação forte assume essa designação pela combinação de vários elementos, que até então poderiam ser utilizados isoladamente, mas que agora surgem todos englobados na mesma operação, detendo as seguintes características:

– *Conhecimento*, isto é, algo que só o utilizador conhece, como seja o caso de uma palavra-passe formada por elementos pessoais ou familiares;
– *Posse,* isto é, algo que só o utilizador possui, como o IMEI de um telemóvel;
– *Inerência*, isto é, algo inerente e não dissociável do utilizador e que o identifica, como uma impressão digital, reconhecimento de voz, ou retina.

Nas operações de pagamento digital ou iniciadas através de um serviço de iniciação de pagamento, a autenticação forte deve incluir um elemento que associe de forma dinâmica a operação em causa a um montante e beneficiário específico, como seja, por exemplo, um código única e isoladamente gerado para o telemóvel do ordenante (art. 104.º, n.º 2 do RJSPME).

De salientar que a entidade prestadora de serviços de pagamento deve adotar as medidas suficientes para proteger a confidencialidade e integridade das credenciais de segurança personalizadas dos utilizadores do serviço de pagamento (art. 104.º, n.º 3 do RJSPME), o que é consentâneo com a obrigação de proteção da confidencialidade e integridade das credenciais de segurança personalizada dos utilizadores (art. 104.º, n.º 3 do RJSPME) e com o dever concreto de acessibilidade reservada do instrumento de pagamento em cada operação de pagamento (art. 111.º, n.º 1, alínea a) e n.º 3 do RJSPME).

Entre os meios de autenticação forte podem ser utilizados os meios de autenticação eletrónica disponibilizados pelo Estado Português, no âmbito da utilização eletrónica do cartão do cidadão, criado pela Lei n.º 7/2007, de 5 de fevereiro, com as alterações da Lei n.º 37/2014, de 26 de junho, que criou a chave móvel digital, e pela Lei n.º 32/2017, de 1 de junho, que reviu ambos os diplomas assinalados.

O cidadão será responsável pela utilização segura da sua palavra-passe, bem como do telemóvel e do endereço de correio associado (art. 3.º, n.º 3 da Lei n.º 37/2014, de 26 de junho), embora o Estado também se responsabilize pelas garantias de segurança (art. 42.º da Lei n.º 7/2007, de 5 de fevereiro).

## 3. Da data-valor

A ordem de pagamento, visando cumprir uma obrigação pecuniária, carece de ter um prazo que sirva de referência para o cumprimento e uma data de disponibilização dos fundos junto do beneficiário, o que é usualmente designado como data-valor.

A data-valor assume relevância no âmbito do movimento de depósitos à ordem e transferências efetuadas em euros, sendo juridicamente regulada pelo Decreto-Lei n.º 18/2007, de 22 de janeiro, abreviadamente designado como regime jurídico da data-valor (RJDV).

O referido diploma foi, contudo, parcialmente revogado pelo Decreto-Lei n.º 317/2009, de 30 de outubro, que transpôs para a ordem jurídica nacional a DSP1, embora na parte que continue em vigor contenha alguns conceitos essenciais.

A data-valor surge definida como a data a partir da qual a transferência ou o depósito se tornam efetivos, passíveis de ser movimentados pelo beneficiário, e se inicia a eventual contagem de juros decorrentes dos saldos credores ou devedores das contas de depósito (art. 3.º, alínea d) do RJDV). O dia útil será o período do dia em que a instituição se encontra aberta ao público, o horário normal de funcionamento (art. 3.º, alínea f) do RJDV). A data de disponibilização será o momento a partir do qual o titular pode livremente proceder à movimentação dos fundos depositados na sua conta de depósitos, sem estar sujeito ao pagamento de juros pela mobilização desses fundos (art. 3.º, alínea e) do RJDV).

No âmbito do RJSPME, uma vez recebida a ordem de pagamento, o prestador de serviços de pagamento do ordenante deve garantir que o montante da operação seja creditado na conta de pagamento do beneficiário até final do primeiro dia útil seguinte, embora tal prazo possa ser acrescido de um dia, no caso das operações de pagamento emitidas com ordem que tenha base em suporte de papel, via de regra ordenadas ao balcão (art. 124.º, n.ºs 1 e 2 do RJSPME).

Caso a ordem seja de transferência entre contas situadas no mesmo prestador de serviços de pagamento, os fundos serão creditados nas contas do beneficiário no próprio dia, com a mesma data-valor e data de disponibilização (art. 127.º do RJSPME).

A data-valor atribuída ao crédito na conta de pagamento do beneficiário deve ser, no máximo, o dia útil em que o montante da operação de pagamento é creditado na conta do prestador de serviços de pagamento do beneficiário (art. 128.º do RJSPME), na medida em que o novo regime dos serviços de pagamento veio permitir esta nova realidade de uma instituição intermediária processadora do pagamento.

No caso de depósito presencial de numerário numa conta para realização de um pagamento, a data-valor poderá ser uma de duas:

– No caso do depositante consumidor, definido como o utilizador que emite ordens com objetivos alheios às suas atividades comerciais, empresariais ou profissionais (art. 2.º, alínea f) do RJSPME), o prestador de serviços de pagamento deve assegurar que o montante seja disponibilizado imediatamente após a receção dos fundos e com data-valor coincidente com esse momento (art. 126.º, n.º 1 do RJSPME).
– No caso de depositante profissional, o montante deve ser disponibilizado, o mais tardar, no dia útil seguinte (art. 126.º, n.º 2 do RJSPME).

Se o depósito de numerário não for presencial, como sucede nos terminais automáticos multibanco ou cofre externo, ou outros meios de recolha de valores que não tenham possibilidade de verificação imediata da quantidade e autenticidade dos valores, os mesmos consideram-se recebidos no dia útil seguinte ao

momento do depósito, devendo essa data ser comunicada ao depositante (art. 126.º, n.ºs 3 e 4 do RJSP).

A falta de comunicação por parte do prestador de serviços de pagamento implicará que o prestador de serviços de pagamento fique obrigado a assegurar uma atribuição de uma data valor à operação anterior à da disponibilização dos fundos (art. 126.º, n.º 5 do RJSP).

No caso de depósitos através de cheques, normalizados ou visados, a definição da data-valor continua a ser dada pelo art. 5.º do Decreto-Lei n.º 15/2007, de 22 de janeiro.

## VI. DAS OPERAÇÕES INCORRECTAMENTE EXECUTADAS

### 1. Da obrigação de execução correcta

A emissão de uma ordem de pagamento pelo ordenante gera no prestador de serviços de pagamento uma obrigação de execução correta da ordem.

A ordem de pagamento surge definida como a instrução dada por um ordenante ou por um beneficiário ao seu prestador de serviços de pagamento requerendo a execução de uma operação de pagamento, a favor de um beneficiário, designado pelo identificador único, a qual é concretizada através de instrumento de pagamento.

Deste modo, se uma ordem de pagamento for executada em conformidade com o identificador único, considera-se que foi executada corretamente no que diz respeito ao beneficiário especificado no identificador único (art. 129.º, n.º 1 do RJSPME).

O utilizador dos serviços de pagamento, quando tenha conhecimento de que a ordem não foi executada como previsto, deve, sem atraso injustificado, e dentro de um prazo nunca superior a 13 meses a contar da data do débito, efetuar uma reclamação ao prestador de serviços de pagamento (art. 112.º, n.º 1 do RJSPM).

A falta de prestação de informação pré-contratual, bem como antes e após a colocação da ordem de pagamento, sobre os elementos da mesma, implica que não exista prazo para a realização da reclamação (art. 112.º, n.º 2 do RJSPME).

Caso exista intervenção de um prestador de serviços de iniciação de pagamento, a reclamação deverá ser efetuada ao prestador de serviços de pagamento que gere a conta (art. 112.º, n.º 3 do RJSPME).

Após a reclamação, o prestador de serviços de pagamento do ordenante (art. 130.º, n.º 7 do RJSPME) ou do beneficiário (art. 131.º, n.º 11 do RJSPME) devem envidar imediatamente esforços para rastrear a operação de pagamento, e comunicar ao ordenante ou ao beneficiário os resultados obtidos.

Mencionam-se aqui serviços de pagamento do beneficiário, na medida em que, no comércio jurídico é, por vezes, a entidade prestadora de um serviço onde é disponibilizado um meio de pagamento eletrónico que solicita uma autorização prévia de débito eletrónico.

São os casos em que há uma operação autorizada, mas a mesma não especifica o montante exato da operação, ou em que o montante da operação excede o montante que o ordenante poderia razoavelmente esperar, com base no seu perfil de despesas anterior, nos termos do seu contrato-quadro e nas circunstâncias específicas do caso (art. 117.º, n.º 1 do RJSPME).

Neste caso é possível solicitar o reembolso, ao prestador de serviços, embora caiba ao ordenante o ónus de provar a discrepância da operação (art. 117.º, n.º 3 do RJSPME).

Podemos então afirmar que na economia da DSP2, o reconhecimento de uma operação incorretamente executada confere direito a uma retificação com vista ao reembolso, a qual deverá ser efetuada pelo prestador de serviços de pagamento do ordenante (art. 130.º, n.º 1 do RJSPME) ou do beneficiário (art. 131.º, n.º 1 do RJSPME), consoante aquele que tenha emitido a ordem de pagamento e o tipo de incorreção em causa.

A entidade prestadora de serviços de pagamento poderá, assim, ser responsabilizada pela operação incorretamente executada, não só do ponto de vista contratual (art. 798.º do Cód. Civil), mas do ponto de vista extracontratual, uma vez que se trata de uma obrigação prevista na lei (art. 483.º do Cód. Civil).

Por esse motivo, dispõe o RJSPME que as entidades prestadoras de serviços de pagamento são ainda responsáveis pelo pagamento de quaisquer encargos cuja responsabilidade lhes caiba e por quaisquer juros a que estejam sujeitos os utilizadores do serviço de pagamento (arts. 130.º, n.º 9 e 131.º, n.º 12 do RJSPME).

Porém, haverá casos em que a execução errada se deve à incorreta introdução de dados.

Assim, quando o identificador único fornecido pelo ordenante está incorreto, o prestador de serviços de pagamento do ordenante não é responsável pela não execução ou pela execução incorreta da ordem de pagamento (art. 129.º, n.º 2 do RJSPME), embora deva, no âmbito de uma obrigação qualificada como de meios, proceder aos esforços razoáveis para recuperar os fundos envolvidos na operação, se necessário com a colaboração do prestador de serviços de pagamento do beneficiário, o qual deverá prestar todas as informações relevantes (art. 129.º, n.º 3 do RJSPME), podendo cobrar pelo serviço de recuperação (art. 129.º, n.º 5 do RJSPME).

Se a recuperação dos fundos não se mostrar possível, o autor da ordem com o número incorreto poderá efetuar uma solicitação por escrito ao seu prestador de serviços, com vista ao fornecimento das informações necessárias, que possibilitem a instauração de ação judicial (art. 129.º, n.º 4 do RJSP).

Na escolha da ação judicial a propor, cumprirá distinguir consoante a qualidade do destinatário final que acabou por erradamente ser destinatário da quantia incorretamente paga ou transferida, no sentido de saber se o mesmo é um terceiro alheio ao ordenante ou uma pessoa das suas relações jurídicas.

Na verdade, sendo um terceiro alheio ao ordenante, o fundamento será, em regra, o enriquecimento sem causa, na medida em que inexistirá, em princípio, qualquer relação – causa justificativa – que fundamente a deslocação de fundos entre as contas (art. 473.º do Cód. Civil).

Porém, caso o destinatário final da quantia seja um credor do ordenante, poderá colocar-se a questão de saber se ao mesmo será lícito reter a quantia (art. 754.º do Cód. Civil). Neste conspecto, segundo Francisco Correia[19], o beneficiário da operação incorreta não poderá reter a prestação, ainda que seja credor do ordenante, porquanto nos termos do art. 114.º, n.º 1 do RJSPME (anterior art. 71.º, n.º 1), *"o carácter não autorizado da operação deve estender-se a todos os momentos da sua execução"*, continuando nessa medida a não existir causa justificativa para o enriquecimento por prestação, pelo que o fundamento da restituição deverá continuar a ser o enriquecimento sem causa (art. 473.º do Cód. Civil).

Os casos mais comuns em que a operação poderá não ser corretamente executada são três:

– A execução parcial da ordem de pagamento, por exemplo, por negligência do gestor de conta na transferência do montante integral, porque omitiu o ato ou deduziu as despesas da operação antecipadamente, sem informar o ordenante que a conta não tinha saldo credor que permitisse a realização da operação, o que confere o direito ao reembolso da parte do montante da operação de pagamento não executada (art. 130.º, n.º 3 do RJSPME), podendo significar que a entidade prestadora dos serviços de pagamento tenha de efetuar a ordem gratuitamente, restituindo as despesas.
– A execução incorreta da ordem de pagamento, por exemplo, por pagamento a beneficiário distinto do indicado, a qual confere o direito ao reembolso do montante da operação de pagamento, consagrando-se a reposição da conta de pagamento debitada, na situação em que estaria se não tivesse ocorrido a execução incorreta da operação de pagamento. A reposição poderá ser efetuada pelo prestador de serviços de pagamento do ordenante (art. 130.º, n.º 3, parte final, do RJSPME) ou pelo prestador de serviços de pagamento do beneficiário (art. 130.º, n.º 5 do RJSPME), consoante a fase da operação em que o erro se tenha verificado.
– A execução tardia, por exemplo, por falta de pagamento na data-valor prevista ou indicada na confirmação do instrumento de pagamento, confere, respetivamente:
    i) No caso dos serviços de pagamento do ordenante, o direito a que este prestador de serviços peça ao prestador de serviços da conta do beneficiário para que, atuando em seu nome, proceda ao crédito na conta de pagamento do beneficiário em data que não seja posterior à que seria atribuída caso a operação tivesse sido corretamente efetuada (art. 130.º, n.º 8 do RJSPME).

---

[19] Correia, Francisco Mendes, «Operações não autorizadas e o regime jurídico dos serviços de pagamento e de moeda eletrónica», *Revista de Direito Civil*, Ano II (2017), n.º 3, Almedina, p. 713.

ii) No caso dos serviços de pagamento do beneficiário, a transmissão tardia da ordem de pagamento recebida implica que a data-valor do crédito na conta de pagamento do beneficiário não pode ser posterior à data-valor que teria sido atribuída caso a operação tivesse sido corretamente executada (art. 131.º, n.º 3 do RJSP).

Os direitos acima conferidos não prejudicam o direito a indemnização suplementar, nos termos da legislação aplicável ao contrato celebrado (art. 133.º do RJSP), nem o exercício do direito de regresso entre prestadores (art. 134.º RJSPME), uma vez que a execução incorreta deriva de conduta destes.

## VII. DAS OPERAÇÕES NÃO AUTORIZADAS

### 1. Noção e tipos de responsabilidade

Uma operação de pagamento não autorizada é aquela a que o utilizador não tenha dado o consentimento à sua execução, como seja o caso de operações efetuadas através de um instrumento de pagamento perdido, furtado ou abusivamente apropriado.

A operação de pagamento não autorizada não se confunde com uma operação de pagamento não executada, incorretamente executada ou tardiamente realizada, cuja ocorrência pode conferir direito a retificação na sequência de uma reclamação (art. 112.º do RJSPME) e cujo regime segue o disposto nos arts. 130.º e segs. do RJSPME e que acima analisámos.

O regime jurídico de serviços de pagamento prevê três tipos de responsabilidade civil para regular as operações não autorizadas:

– Responsabilidade contratual do prestador de serviços de pagamento ou de iniciação do pagamento, quando a operação não autorizada e sua execução se fique a dever a factos imputáveis ao prestador a título censurável, sendo aplicável a responsabilidade civil contratual (art. 798.º do Cód. Civil), com as especificidades constantes do regime jurídico dos serviços de pagamento, prevista no art. 115.º, n.ºs 7 e 8 do RJSPME;
– Responsabilidade objetiva do prestador de serviços de pagamento ou de iniciação do pagamento, quando a operação não autorizada e a sua execução são imputáveis a terceiro a título censurável, pois independentemente da responsabilidade civil contra o terceiro, nos termos do regime jurídico dos serviços de pagamento, o prestador de serviços de pagamento está obrigado a repor a conta no estado em que estaria antes da realização da operação, suportando as perdas daí decorrentes, nos termos do art. 114.º, n.º 1 do RJSPME;
– Responsabilidade contratual do utilizador, quando a operação não autorizada se deva a factos imputáveis a título censurável ao utiliza-

dor, aplicando-se o art. 798.º do Cód. Civil e os limites de imputação previstos no art. 115.º do RJSPME.

## 2. Operações imputáveis ao prestador de serviços

A responsabilidade do prestador de serviços de pagamento ou de iniciação do pagamento por uma operação não autorizada ocorre, em regra, em três casos.

O primeiro caso sucede quando o prestador de serviços recebe do ordenante a comunicação, dentro do prazo de 13 meses (art. 112.º, n.º 1 do RJSPME), da existência de uma operação não autorizada, com origem em furto, perda ou apropriação abusiva, a que alude o art. 110.º, n.º 1, alínea b) do RJSPME.

Nestes casos, após a comunicação da operação não autorizada, a entidade prestadora de serviços de pagamento deverá bloquear o instrumento de pagamento, para impedir a sua utilização abusiva por terceiro.

Caso o prestador de serviços de pagamento ou de iniciação de serviços de pagamento não bloqueie imediatamente o instrumento de pagamento, o mesmo será responsável por todos os pagamentos não autorizados após o momento temporal da referida comunicação (art. 115.º, n.º 7 do RJSPME), sendo o primeiro caso de responsabilidade por operações não autorizadas imputável ao prestador de serviços de pagamento ou de iniciação do serviço de pagamento.

A fundamentação da referida responsabilidade tem previsão legal expressa e baseia-se no dever de impedir a utilização do instrumento de pagamento, logo que a comunicação seja efetuada (art. 111.º, n.º 1, alínea e) do RJSPME), a qual é independente do grau de culpa que o utilizador possa ter na operação não autorizada.

O segundo caso previsto de responsabilidade do prestador de serviços de pagamento ou de iniciação de serviços de pagamento pela operação não autorizada, será o caso de o prestador não ter fornecido ou implementado os meios apropriados para notificar a perda, roubo, apropriação abusiva, ou utilização não autorizada, pois, nesses casos, o ordenante não ficará obrigado a suportar as consequências financeiras resultantes da utilização desse instrumento de pagamento (art. 115.º, n.º 8 do RJSPME).

A referida responsabilidade tem novamente previsão legal expressa, e baseia-se no dever previsto no art. 111.º, n.º 1, alínea c) do RJSPME, o qual é suscetível de se verificar por um conjunto das mais variadas razões: por exemplo, o servidor da página *internet* do prestador de serviços não se encontra *online* durante 24 horas ou ao fim-de-semana, impedindo a atempada realização da comunicação.

Em qualquer um destes dois casos em que se verifique a responsabilidade da entidade prestadora de serviços, a mesma deverá proceder ao reembolso imediato da quantia envolvida na operação não autorizada (art. 114.º, n.º 1 do RJSPME), repondo ainda a conta de pagamento debitada no estado em que estaria caso a operação não autorizada não tivesse sido efetuada (art. 114.º, n.º 4 do RJSPME), independentemente do montante em causa.

Caso a mesma não proceda de imediato às referidas medidas, ficará obrigada a suportar juros moratórios, acrescidos de 10 pontos percentuais, contados desde a data da operação não autorizada até à data do reembolso efetivo (art. 114.º, n.º 10 do RJSPME).

Note-se que, neste caso, não será lícito à entidade prestadora de serviços de pagamento e de iniciação de pagamento retardar o reembolso com fundamento na suspeita de atuação fraudulenta seja do utilizador, seja de terceiro.

O mecanismo da reposição ou do reembolso imediato não prejudica o direito a indemnização suplementar a que possa haver lugar (art. 114.º, n.º 10, *in fine*, do RJSPME), designadamente, no dizer de Francisco Correia[20], por outros danos que possam ter lugar.

O terceiro caso será o caso geral da violação de qualquer dever contratual a que o prestador de serviços de pagamento ou de iniciação de pagamento se encontre adstrito, o qual originará o dever de proceder à indemnização por quaisquer danos causados (art. 798.º do Cód. Civil), como seja, por exemplo, o dever de não enviar instrumentos de pagamentos não utilizados, ou de não aceitar ordens de pagamentos vindas de dispositivos não reconhecidos, ou que não passem os testes de autenticação.

### 3. Operações imputáveis a terceiro

A operação não autorizada imputável a terceiro é aquela em cuja realização teve intervenção um terceiro a título censurável e pela qual é o mesmo responsável em primeira linha, quer perante o utilizador, quer perante o prestador de serviços de pagamento e de iniciação de pagamento (art. 483.º do Cód. Civil).

Porém, no dizer de Francisco Correia[21], encontra-se previsto no regime jurídico dos serviços de pagamento e moeda eletrónica um regime de responsabilidade civil que deve ser enquadrado na responsabilidade objetiva ou pelo risco, pois independentemente da responsabilidade do terceiro, a entidade prestadora de serviços de pagamento encontra-se obrigada a reembolsar imediatamente o utilizador do montante da operação de pagamento não autorizada, ou ainda a repor a conta no estado em que se encontrava (art. 114.º, n.º 1 do RJSPME).

Assim, no dizer deste Autor, nos casos de responsabilidade de terceiro, a lei prevê um caso de imputação da responsabilidade ao banco sem que seja necessário um juízo de licitude, isto é, ocorrendo uma imputação objetiva que opera no âmbito dos riscos próprios da atividade dos serviços de pagamento eletrónico, cuja esfera de danos é delimitada pela previsão legal do art. 114.º, n.º 1 do RJSPME, bastando, para o efeito, que a operação não autorizada não seja imputável ao utilizador.

---

20 Correia, Francisco Mendes, ob. cit., p. 711.
21 Correia, Francisco Mendes, ob. cit., p. 718.

A jurisprudência que resolve os litígios com recurso ao RJSPME e não ao art. 796.º do Cód. Civil, ainda que sem expressamente mencionar tal tipo de imputação, resolve os litígios nesse sentido. Com efeito, o Ac. TRL de 21.12.2017[22] dispõe que *"Se o banco réu não demonstrou, como era seu ónus, que o utilizador teve qualquer comportamento suscetível de por em causa a segurança do sistema, desconhecendo-se o modo como os terceiros lograram obter as chaves de segurança (número do contrato, código de acesso (password) e combinação de três números dos 64 possíveis do cartão matriz), tem o mesmo a obrigação de reembolsar imediatamente o ordenante do montante da operação de pagamento não autorizada (…)".*

Deste modo, parece aqui inferir-se uma responsabilidade objetiva, assente nos riscos próprios da atividade.

O reembolso automático conhece, contudo, uma exceção, nos casos em que o prestador de serviços de pagamento ou de iniciação de serviços de pagamento tiver motivos razoáveis para suspeitar de atuação fraudulenta do utilizador e comunicar por escrito esses fundamentos às autoridades judiciárias, nos termos da lei penal e de processo penal (art. 114.º, n.ºs 2 e 6 do RJSPME), o que pressupõe suspeitas da prática de crime e não de mero ilícito civil, caso em que não será obrigado ao reembolso.

O utilizador surge na lei designado como ordenante, embora o utilizador nos casos de operações não autorizadas não tenha propriamente dado uma instrução que origine um instrumento de pagamento, dado que, em regra, nos encontramos perante uma operação não autorizada, à sua revelia.

Por conseguinte, a atuação fraudulenta aqui mencionada não corresponde a comportamento negligente, ainda que grosseiro, do utilizador, mas sim a atuação dolosa da parte do utilizador dos serviços de pagamento, na medida em que apenas essa dá lugar à prática de crime previsto na lei penal.

Neste sentido, o Ac. TRL de 21.12.2017[23], onde se expendeu que a: *"(…) Recorrente fez prova de que as operações foram regularmente efetuadas através do seu sistema informático e com fornecimento das correspondentes credenciais de segurança bem como que o sistema informático se encontrava a funcionar sem avaria ou deficiência.*

*Contudo, não fez prova de que na causa da fraude esteve uma conduta dolosa ou sequer negligente dos Autores. Não se tendo provado como foi obtido o acesso às credenciais de segurança utilizadas na autenticação das operações em causa (o que permanece desconhecido), não se pode estabelecer um nexo de causalidade entre a conduta dos Autores e a realização das operações; sendo que esse nexo de causalidade é pressuposto da relevância do comportamento doloso ou negligente."*

Quando não tenham sido detetados motivos razoáveis que constituam fundamento válido de suspeita de fraude, ou essa suspeita não tenha sido comuni-

---

22 Ac. TRL de 21.12.2017, relatado por Manuel Rodrigues e disponível em http://www.dgsi.pt.

23 Ac. TRL de 21.12.2017, relatado por Manuel Rodrigues e disponível em http://www.dgsi.pt.

cada, por escrito, à autoridade judiciária nos termos da lei penal e de processo penal, são devidos ao utilizador juros moratórios, contados desde a data em que o utilizador dos serviços de pagamento comunicou a negação da mesma, até à data de reembolso efetivo (art. 114.º, n.º 10 do RJSPME).

### 4. Operações imputáveis ao utilizador

Uma vez perante uma operação não autorizada, o utilizador tem o dever de comunicar, sem atraso injustificado, ao prestador de serviços de pagamento, de iniciação de serviços de pagamento ou à entidade por aquele indicada, da ocorrência de perda, furto, roubo, apropriação abusiva ou qualquer outra utilização não autorizada do instrumento de pagamento (art. 110.º, n.º 1, alínea b) do RJSPME), a qual não poderá cobrar qualquer taxa pelo serviço, que deverá ser assegurado gratuitamente (art. 111.º, n.º 2 do RJSPME).

Após a comunicação, o ordenante não suportará quaisquer consequências financeiras resultantes da utilização de um sistema de pagamento perdido, furtado, roubado ou abusivamente apropriado, salvo no caso de atuação fraudulenta da sua parte (art. 115.º, n.º 7 do RJSPME).

A noção de atraso injustificado, sendo um conceito indeterminado, implicará que possa aqui assumir relevância a autonomia e vontade das partes (art. 405.º do Cód. Civil), para definir a antecedência mínima de comunicação, sendo, porém, nulas as cláusulas que alterem o risco a cargo dos contratantes, designadamente, a cargo dos prestadores de serviços de pagamento (art. 21.º, alínea f) do RJCCG).

Logo que um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, incumbe ao respetivo prestador do serviço de pagamento ou de iniciação de serviços de pagamento fornecer prova de que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência do serviço prestado pelo prestador de serviços de pagamento (art. 113.º, n.ºs 1 e 2 do RJSPME).

Porém, a prova de que a operação foi corretamente introduzida no sistema não é, por si só, suficiente para provar que a operação de pagamento foi autorizada pelo utilizador, ou que este último agiu de forma fraudulenta, ou com negligência grosseira, por referência aos deveres do art. 110.º do RJSPME.

Esta noção de insuficiência da prova é una inovação do RJSPME, que visa precludir o incumprimento da obrigação de reembolso imediato por parte dos prestadores de serviços de pagamento.

Deste modo, o ónus da prova da totalidade da operação não autorizada recai sobre o prestador do serviço de pagamento ou de iniciação ao pagamento, a quem cabe também provar a ocorrência de comportamento negligente ou doloso do utilizador (neste sentido, o já citado Ac. TRL de 21.12.2017).

As operações não autorizadas resultam as mais das vezes de introduções não autorizadas no sistema, as quais se podem integrar em vários tipos de conduta, tal como vieram definidos pela primeira vez no Ac. STJ de 18.12.2013[24]:

– O *phishing,* do inglês *fishing,* ou pesca, consiste numa fraude eletrónica por intermédio da qual se procede à remessa de mensagens de correio eletrónico não solicitado, com uma aparência de proveniência de uma instituição bancária, mediante a utilização de sinais distintivos semelhantes, mas sem suplantar as terminações dos nomes de domínio, em que o utilizador, com o pretexto ou *"isco"* de atualização de dados, ofertas comerciais ou até o pagamento de uma taxa, é persuadido a introduzir dados pessoais, como número de conta, número de cartão, número de contribuinte, ou palavra passe, que, uma vez obtidos, permitem o acesso não autorizado por terceiros à conta bancária. Trata-se da modalidade menos sofisticada de intromissão, em regra detetável pelos utilizadores mais experientes, por ter pequenos detalhes não coincidentes com as mensagens originais, tais como diferentes terminações de domínio.
– O *pharming,* ou cultivo, o qual consiste na remessa de mensagens de correio eletrónico não solicitadas, as quais contêm ficheiros ocultos ou *spyware*, que instalam programas nos sistemas informáticos dos utilizadores, alterando os arquivos do sistema e permitindo que sempre que o utilizador digite o endereço da página da sua instituição bancária, o mesmo seja na realidade dirigido a uma página clonada, idêntica à verdadeira, onde são introduzidos todos os dados necessários à concretização de uma operação, os quais são depois capturados por terceiros, para uso não autorizado. Trata-se de uma modalidade mais sofisticada de intromissão, não detetável mesmo pelos utilizadores mais experientes, por implicar uma pré-alteração do próprio sistema informático do utilizador, com alteração dos próprios nomes de domínio.

Afim ou instrumental do *pharming* é o *keylogging*, o qual consiste no uso de um programa invasivo oculto, que o sistema do utilizador contacta após uma visita de uma página não segura ou receção de um correio eletrónico não solicitado, que uma vez instalado regista tudo o que é digitado e que permite capturar senhas, números de cartão de crédito, entre outros, e que são depois utilizados por terceiros para fraude.

A entidade prestadora de serviços de pagamento ou de iniciação do pagamento, que retira utilidade económica da utilização em massa dos sistema de pagamento, tem a obrigação de assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao utilizador

[24] Ac. STJ de 18.12.2013, relatado por Ana Paula Boularot e disponível em http://www.dgsi.pt.

do serviço de pagamentos que tenha direito de utilizar o referido instrumento (art. 111.º, n.º 1, alínea a) do RJSPME, correspondente ao antigo art. 68.º, n.º 1, alínea a) do DSP1), designadamente, através do reconhecimento do IMEI ou do aparelho utilizado pelo ordenante, instituindo um sistema de controlo e autenticação, pelo que os riscos pela utilização normal do sistema correm por sua conta, devendo por isso suportar o prejuízo decorrente da operação não autorizada pelo cliente.

Por isso, no caso de não se demonstrar qualquer incumprimento do utilizador, e de o valor da ordem ser superior a € 50,00, o prestador de serviços deve reembolsar imediatamente o ordenante, após ter tido conhecimento da mesma ou de esta lhe ter sido comunicada, o mais tardar até ao final do primeiro dia útil seguinte, aquele conhecimento ou comunicação (art. 114.º, n.ºs 1 e 5 do RJSP), sob pena de contagem de juros (art. 114.º, n.º 10 do RJSPME).

No caso de prestador de serviços de iniciação de pagamento, prevê a lei a comunicação ao prestador de serviços que gere a conta, via de regra, o Banco, o qual também não ficará, deste modo, obrigado ao reembolso (art. 114.º, n.º 6 do RJSPM).

Só não ocorrerá reembolso imediato quando o prestador de serviços de pagamento comunicar por escrito, às autoridades judiciárias, nos termos da lei penal e do processo penal, que tem motivos razoáveis para suspeitar de atuação fraudulenta do próprio utilizador (art. 114.º, n.º 2 do RJSPME), embora não se exija aqui a apresentação formal de uma queixa-crime, podendo tratar-se do mero reporte de uma operação.

No âmbito da imputação de operações assume também relevância a atuação do ordenante com dolo ou mera culpa – negligência.

O dolo corresponde tradicionalmente à intenção do agente de praticar o facto e a negligência corresponde aos casos em que o agente não tinha essa intenção, mas o comportamento não deixa de ser censurável em virtude de ter omitido o dever objetivo de cuidado a que estava legalmente obrigado, para evitar a lesão de bens jurídicos.

Segundo Menezes Leitão[25], na negligência grosseira estaremos perante um caso de culpa grave, em que a conduta do agente só seria suscetível de ser realizada por uma pessoa especialmente negligente, uma vez que a grande maioria das pessoas não procederia desta forma, sendo uma espécie de negligência qualificada.

No caso da negligência simples estaremos perante um caso de culpa leve, em que a conduta do agente não seria suscetível de ser realizada por um homem médio, correspondente ao critério da culpa do bom pai de família (art. 487.º, n.º 2 do Cód. Civil).

O dever objetivo de cuidado aqui violado será o de utilização adequada do instrumento de pagamento (art. 110.º, n.º 1, alínea a) do RJSPME) e de proteção das credenciais de segurança (art. 110.º, n.º 2 do RJSPME).

---

[25] Leitão, Luís Manuel Teles de Menezes, *Direito das Obrigações*, Vol. I, 3.º Edição, Almedina, janeiro 2003, p. 318.

No caso de dolo e atuação fraudulenta do utilizador, com incumprimento deliberado das condições do sistema de pagamento, ou negligência grosseira do ordenante, este suporta todas as perdas decorrentes de operações de pagamento não autorizadas (art. 115.º, n.ºs 3 e 5 do RJSPME).

Assim, por exemplo, num caso de *pishing*, foi considerado existir negligência grosseira, no Ac. TRP de 25.11.2013[26], onde se expendeu que *"Age com culpa o utente que fornece todo o conteúdo do cartão matriz perante uma solicitação numa página idêntica à do banco, uma vez que contraria toda a lógica do sistema de segurança que não pode ser desconhecida do utilizador"*, o que implica que o utilizador suporte todo o dano da operação não autorizada.

No caso de a atuação do utilizador ser apenas de negligência leve, o utilizador pode ser obrigado a suportar as perdas de utilização de instrumento de pagamento perdido, furtado ou roubado, até ao máximo de € 50,00 (art. 115.º, n.º 1 do RJSPME), vigorando, quanto ao mais, a regra do reembolso imediato, salvo se o prestador de serviços de pagamento não exigir autenticação forte, caso em que não suportará nenhuma perda (art. 115.º, n.º 5 do RJSPME).

Num caso de negligência leve, *pharming*, analisado no Ac. TRP de 04.06.2019[27], o utilizador foi considerado isento de culpa, assim, *"Age sem qualquer culpa ou negligência o utilizador de conta bancária, que utilizando os serviços de homebanking prestados pelo banco, é vítima de um ataque informático, através da técnica de pharming, mediante a qual foram "revelados" inadvertidamente os dispositivos de segurança que haviam sido fornecidos pelo banco, e que de forma não concretamente apurada, originaram uma operação de transferência de fundos não autorizada da sua conta para terceiro, não autorizada."*.

O contexto da conduta do utilizador e os usos sociais poderão também ser relevantes para a definição do grau de culpa, por exemplo, no Ac. STJ de 14.12.2016[28] concluiu-se que

> *"Havendo quebra de segurança resultante da intromissão abusiva de terceiros, que lograram, por meio desconhecido, obter os dispositivos de segurança que permitiram o acesso às contas, não é adequado concluir ser aquela quebra imputável ao utilizador do serviço de pagamento apenas por ter este facultado os referidos dispositivos à contabilista, uma "auxiliar", sendo esta atuação conforme com a diligência de um homem médio e, por isso, razoável, inexistindo negligência grave".*

Convém também relembrar aqui o carácter imperativo da presente lei, a qual impede que sejam modificadas as regras de distribuição do risco (art. 76.º do RJSPME) através de cláusulas contratuais.

Por conseguinte, não será lícito à entidade prestadora dos serviços de pagamento aplicar cláusulas do contrato contrárias ao RJSPME, para evitar o reembolso imediato, sendo que, se o fizer, deverá o utilizador aferir de qual

---

26 Ac. TRG de 25.11.2013, relatado por Espinheira Baltar e disponível em http://www.dgsi.pt.
27 Ac. TRP de 04.06.2019, relatado por Alexandra Pelayo e disponível em http://www.dgsi.pt.
28 Ac. STJ de 14.12.2016, relatado por Pinto de Almeida e disponível em http://www.dgsi.pt.

a proporcionalidade ínsita nessas cláusulas, a fim de submeter as mesmas a apreciação judicial.

Pelo *supra* exposto, este será, em suma, o regime jurídico aplicável às operações de pagamento não autorizadas.

## CONCLUSÕES

1. O regime jurídico dos serviços de pagamento, pese embora a sua vigência na nossa ordem jurídica desde há, pelo menos, dez anos a esta parte, introduzido pela Lei n.º 317/2009, de 30 de outubro, tem vindo a ser pouco utilizado na nossa ordem jurídica como fundamento direto de resolução dos litígios surgidos em matéria de serviços de pagamento, assumindo o fundamento clássico da repartição do risco, previsto no art. 796.º do Cód. Civil, predominância na resolução dos mesmos.
2. A revisão efetuada ao diploma dos serviços de pagamento e moeda eletrónica pelo Decreto-Lei n.º 91/2018, de 12 de novembro, abreviadamente designado de RJSPME, veio consagrar soluções inovadoras no campo da responsabilidade dos prestadores de serviços de pagamento pelas operações não autorizadas e na autenticação forte das operações.
3. A definição dos deveres a cargo do utilizador e as obrigações internas e externas das entidades prestadoras de serviços de pagamento implicarão a alteração dos contratos de serviços bancários existentes no comércio jurídico e a prática dos serviços de pagamento, criando um novo paradigma de responsabilidade pela execução incorreta e não autorizada dos serviços de pagamento.
4. A consagração de um novo regime de suficiência do ónus da prova a cargo dos prestadores de serviços de pagamento, bem como de novos limites de operações suportadas, irá alterar a prática da imputação de operações não autorizadas, e a forma como são dirimidos os litígios, em rumo para um mercado único de serviços de pagamento.
5. A perceção do novo regime e das suas soluções mostra-se, deste modo, essencial quer para o cidadão na sua atividade do dia a dia, quer para o jurista na apreciação das questões que lhe são submetidas, com vista a uma aplicação mais direta e mais qualificada do regime.

Lisboa, 14 de junho de 2021