Processo: 2773/2022
Demandante:
Demandada:

Resumo: 1. O Decreto-lei nº 91/2018 de 12 de novembro aprovou o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RJSPME), transpondo para a ordem jurídica interna a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa a serviços de pagamento no mercado interno (também designada de DSP2);
2. São obrigações do utilizador de serviços de pagamento (SP): a utilização do instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização, adoção de todas as medidas razoáveis para preservar a segurança das suas credenciais de segurança personalizadas e a comunicação, logo que tenha conhecimento dos factos e sem atraso injustificado, ao prestador de serviços de pagamento ou à entidade designada por este último, da perda, do furto, do roubo, da apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento (artº 110º);
3. Uma operação de pagamento só é considerada autorizada se o ordenante tiver dado o seu consentimento, e a responsabilidade por operações não autorizadas é do prestador de serviços de pagamento, que deve reembolsar o ordenante - exceto em casos de fraude ou negligência grosseira (artº 111º, nº 3, 114º, 115º, 1 a 4);
4. No caso de operações de pagamento não autorizadas, o utilizador só pode ser obrigado a suportar as perdas até ao montante de €50 – exceto se existir fraude ou negligência grosseira (artº 115, nº 3 e 4).
5. A omissão um especial dever de atenção e cuidado na verificação de mensagens recebidas para efetuar login na conta bancária on line (homebanking), permitindo uma operação de pagamento não solicitada, nem autorizada, constitui negligência grosseira e o incumprimento dos deveres que estão subjacentes à utilização dos serviços de pagamento.

A – Relatório

1. Reclamação da Demandante e posição da Demandada

1.1. A Demandante formalizou em 24 de outubro de 2022, junto do Triave/Tribunal Arbitral de Consumo, reclamação contra a Demandada nos termos da qual peticiona a condenação desta

- no crédito de €450 na sua conta
- na celeridade de resolução das solicitações relativas a anulação de transferências

Alega,
No dia 22.09.2022, ao aceder ao *site* do inseriu um código que rececionou por SMS e, por duas vezes, deu erro
À terceira tentativa conseguiu aceder e constatou que tinha sido efetuada uma transferência, no valor de €450, para uma conta estrangeira associada a uma pessoa que desconhece
Todos os SMS que recebeu por parte do cartão universo têm o mesmo remetente
Solicitou, de imediato, o cancelamento da transferência, mas a Universo informou que só podia analisar o processo depois do valor a transferência deixar de estar cativa
O que muito a indignou porque bastaria cancelar a transferência e o assunto seria resolvido

No dia 23.09.2022, a Reclamada pediu o envio de informação adicional, o que fez, indicando que após a receção da documentação iria proceder a um reembolso no no prazo de 24h, o que não veio a acontecer
Já apresentou reclamação junto do – e, aguarda resposta
O valor já não está cativo, levando a crer que a transferência vai ser realizada, contrariamente às suas insistências, por escrito e por telefone

Juntou ao processo e com a reclamação: cópia das mensagens (SMS) recebidas, cópia dos movimentos do cartão, comunicações trocadas no âmbito da reclamação com a Demandada e o (10 documentos)

1.2. A Demandada respondeu nos seguintes termos:

- É responsável pela emissão e concessão de crédito associado a operações de pagamento
- Em causa, a transferência realizada no dia 22.09.2022, no valor de €450 para a beneficiária , com o IBAN
- Após a comunicação da Reclamante, à linha de apoio, de que havia efetivamente validado uma transação (transferência indevidamente autorizada), foi iniciado processo interno de averiguação e apurado que a Reclamante, devidamente conhecedora do teor da mensagem recebida através de validação com a utilização de sistema de segurança (código enviada para o seu numero de telemóvel, efetuou uma ordem de pagamento com a respetiva validação, tendo sido executada a operação de pagamento (transferência)
- a mensagem: "*Utilize o seguinte código de autorização para executar a operação de transferência no valor de 450 euros para o Nunca forneça este código em transações/pedidos não iniciados por si*"
- Ora, se a Reclamante estaria a tentar efetuar login na sua área de cliente *on line* ( ), não era sua intenção realizar/autorizar uma transferência com o valor e destinatário específicos
- De acordo com o artº 110º, nº 1 do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RJSPME), o utilizador de serviços de pagamento com direito a utilizar um instrumento de pagamento deve-o utilizar conforme as condições que regem a sua emissão e utilização,
- ao subscrever o Acordo de Prestação de Serviços de Pagamento e da Moeda Eletrónica (adesão ao), aderiu às Condições Gerais e Condições Particulares que se obriga a cumprir, as quais regulam os serviços prestados e a concessão de crédito pelo
- é responsável por garantir a segurança e confidencialidade do PIN, Códigos de Acesso, do Código bem como dos números e demais elementos identificativos dos Cartões, obrigando-se a diligentemente a tomar todas e as adequadas providências à prevenção da sua apropriação por terceiros
- No caso, a Reclamante não tomou as diligencias necessárias para salvaguarda da alegada utilização abusiva do seu instrumento de pagamento os canais digitais ( ), e conforme o previsto no artº 115º, nº 3 do RJSPME, o ordenante suporta todas as perdas resultantes de operações de pagamento não autorizadas, se aquelas forem devidas a atuação fraudulenta ou ao incumprimento deliberado de uma

ou mais obrigações previstas no artº 110º, caso em que não são aplicáveis os limites referidos no nº 1

- Pelo que, não pode assumir o valor em dívida decorrente de transação indevidamente autorizada, pelo facto de não terem sido tomadas todas as medidas preventivas e necessárias para salvaguarda de utilização indevida de pagamento

Juntou, informação da conta e da transferência efetuada

1.3. Em julgamento, a Demandante requereu a junção de cópia das mensagens recebidas e a Demandada exemplos de *e-mails, SMS* de *phishing*, *sites* fraudulentos, registo do domínio " e cópia da queixa-crime apresentada no DIAP.

B – Saneador

A Lei 144/2015 de 8 de setembro transpôs para a ordem jurídica nacional a Diretiva 2013/11/UE do Parlamento Europeu e do Conselho de 21 de maio, sobre a resolução alternativa de litígios de consumo (RAL), e estabeleceu os princípios e regras a que deve obedecer o funcionamento das entidades de resolução alternativa de litígios e o respetivo enquadramento jurídico (artº1º).

Assim, a Lei RAL é aplicável aos procedimentos quando os mesmos sejam iniciados por consumidor contra um fornecedor de bens ou prestador de serviços e respeitem a obrigações contratuais resultantes de contratos de compra e venda ou de prestação de serviços, celebrados ou prestados a consumidores residentes em Portugal.

O Centro de Arbitragem de Conflitos de Consumo do Vale do Ave/Tribunal Arbitral, faz parte integrante da Rede de Arbitragem de Consumo, sendo um meio de resolução alternativa de litígios, promove a resolução de conflitos de consumo relativos à prestação de serviços no seu âmbito geográfico (tudo como decorre do seu Regulamento – artºs 1º a 5º).

Assim, este tribunal é material e territorialmente competente, uma vez que está em causa um processo de conflito de consumo, iniciado por consumidor, decorrente da celebração de um contrato e da prestação de serviços de profissional (no caso, pessoa coletiva), na área de residência da Demandante, na Trofa.

A toda a causa é atribuído um valor certo que representa a utilidade económica imediata do pedido e que determina, nomeadamente, a competência do tribunal (nºs 1 e 2 do artº 296º do CPC).

Para a determinação do valor da causa, deve atender-se ao momento em que a ação é proposta (nº 1 do artº 299º do CPC), sendo certo que o valor deve ser fixado no despacho saneador, sem prejuízo do dever da sua indicação pelas partes (nº 1 do artº 306º).

Para definição do valor do processo, é relevante a utilidade que o Demandante pretende obter, em função da causa de pedir e do pedido formulado, o que corresponde, no caso em apreço, ao montante do pedido (cfr. nº1 do artº 297º).

O valor do processo é, pois, de €450 (quatrocentos e cinquenta euros), o que se enquadra no âmbito da competência do Tribunal (nº 1 do artº 6º do Regulamento do TRIAVE).

Nos termos dos nº 2 e 3 do artº 14º da Lei 24/96 de 31 de julho (na redação da Lei nº 63/2019 de 16 de agosto), os conflitos de consumo de reduzido valor económico (até €5.000) estão sujeitos à arbitragem necessária quando, por opção expressa dos consumidores, sejam submetidos à apreciação do tribunal arbitral adstrito aos centros de arbitragem de conflitos de consumo legalmente autorizados (cf. ainda, nº 1 do artº 10º do Regulamento).

Ainda, de acordo com o Regulamento do TRIAVE (artº 19º), aplicam-se a este processo, subsidiariamente e com as necessárias adaptações, a Lei da Arbitragem Voluntária e o Código de Processo Civil (1ª parte do nº 1 do artº 39º da Lei 63/2011 de 14 de dezembro).

Não foram deduzidas exceções.
As partes têm personalidade jurídica e são capazes.
Cumpre apreciar e decidir.

C – Delimitação do objeto do Litígio

Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RJSPME) e a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho dos Serviços de pagamento (DSP2)

- ✓ Direitos e Deveres do Ordenante e Responsabilidade do Prestador dos Serviços de Pagamento (SPS).
- ✓ Responsabilidade pela execução de operações de pagamento não autorizadas, nomeadamente no caso de culpa grosseira do Ordenante
- ✓ Reembolso do montante da operação e (i)revogabilidade da ordem de pagamento.

D – Fundamentos, com interesse para a decisão da causa

I - Factos provados:

I. A aqui Demandada, é uma Instituição de Moeda Eletrónica e responsável pela emissão e concessão de crédito associado a operações de pagamento do
II. A Demandante subscreveu o aderiu ao e às respetivas Condições Gerais e Particulares de utilização;
III. A Demandante acede regularmente à sua conta do utilizando para o efeito um código, pessoal e pré-definido, pelo qual deve zelar acautelando a sua apropriação por terceiros;
IV. No dia 22 de setembro de 2022, ao aceder ao *site* do a Demandante recebeu uma mensagem, *"utilize o seguinte código de autorizaçã para executar a operação Transferência no valor de 450 euros para o IBAN* , o que fez;
V. A Demandante de seguida e ao aceder ao *site* do utilizou o código referido na SMS (IV);
VI. A Demandante quando entrou no *site* constatou que havia sido feita uma transferência de €450, para uma conta estrangeira associada a uma pessoa que desconhece, o que não pretendia;
VII. A Demandante reclamou, de imediato, junto dos serviços de apoio da Demandada que declinou a sua responsabilidade, após análise da situação, com base na falta de garantia

de segurança e confidencialidade do PIN, Códigos de Acesso, do Código OPT, dos números e demais elementos identificativos dos Cartões e falta das diligencias necessárias para salvaguarda da utilização abusiva do seu instrumento de pagamento designadamente os canais digitais ( );

VIII. A Demandante reclamou para o mas, ainda, não obteve resposta;

IX. Do extrato da conta do a Demandante consta uma transferência de €450 para , pessoa que desconhece;

X. A Demandada foi alvo de ataque informático e, desse facto, e na qualidade de emissora e concedente de crédito associada a operações de pagamento do " ", apresentou queixa no DIAP, em 28.12.2022.

II - Factos não provados

Com relevância para a decisão, foi identificado o seguinte facto não provado:

I. Não se provou o atraso da Demandada no tratamento da reclamação da Demandante.

E – Da fundamentação de facto

Os factos considerados como provados foram alegados pelas partes e não foram impugnados.
Ainda, os factos referidos de III a VI, VIII, IX e X foram alegados pelas partes e constam dos documentos juntos ao processo.
A Demandante relatou em julgamento a sucessão de mensagens recebidas no dia 22 de setembro, designadamente o SMS em questão e pelo qual deu autorização para transferência da quantia em causa.
Relatou que introduziu o código sem que tivesse consciência de ter autorizado uma transferência.
Por seu turno, a Demandada referiu que o foi alvo de ataque informático, tendo junto informação nomeadamente, exemplos de mails, SMS, de *phising*, a lista dos *sites* fraudulentos que compraram a palavra entre julho e setembro, *prints* google de busca de *sites* de cópias, e queixa-crime que deu entrada no DIAP (denuncia contra desconhecidos).

Quanto ao alegado atraso ou falta de celeridade no tratamento da reclamação, a Demandante não carreou factos que o tivessem demonstrado.

Não foram apresentadas testemunhas.

O tribunal ouviu as partes e atendeu às suas declarações em conformidade com o princípio da cooperação, consagrado no CPC (artº 7º), ao abrigo do qual o juiz pode ouvir as partes e os seus representantes ou mandatários, convidando-os a fornecer esclarecimentos sobre a matéria de facto ou de direito que se afigurem pertinentes.

Ora, às partes cabe alegar os factos essenciais que constituem a causa de pedir e aqueles em que se baseiam as exceções invocadas (artº 5º, nº 1 do CPC) sendo, ainda, considerados pelo juiz os factos instrumentais (os que resultem da instrução da causa), e os factos complementares (os que resultem como complemento ou concretização dos que as partes hajam alegado e resultem da instrução da causa, desde que sobre eles tenham tido a possibilidade de se pronunciar).

Ainda, são atendíveis, os factos notórios, aqueles que o tribunal toma conhecimento em virtude do exercício das suas funções (tudo conforme o previsto no artº 5º, nºs 1 e 2, do CPC).

F - Da fundamentação de Direito

1. **Enquadramento legal – Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RJSPME), e a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho dos Serviços de pagamento (DSP2)**

A Reclamante subscreveu o Acordo de Prestação de Serviços de Pagamento e da Moeda Eletrónica, aderiu ao e às respetivas Condições Gerais e Particulares de utilização o que configura a subscrição de um contrato abrangido pelo Regime das Clausulas Contratuais Gerais – Decreto-Lei nº 446/85 de 25 de outubro.

Cumpre à Demandada, conforme o regime aplicável, o ónus da alegação e prova da comunicação do respetivo conteúdo, de acordo com o disposto no artº 5º.
Ora, a Demandante não reclamou, em momento algum do processo, nem a subscrição do dito Acordo, nem o conhecimento das clausulas contratuais relativas à utilização do

Foi, então, celebrado um contrato de prestação de serviços por meios eletrónicos à luz do disposto no Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica – Decreto-Lei nº 91/2018 de 12 de novembro.
Este diploma veio, ainda, transpor para o ordenamento jurídico nacional a Diretiva (EU) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro, relativa aos serviços de pagamento no mercado Interno (também designada de DSP2), e que contempla os pagamentos realizados em linha e através de telemóveis inteligentes.

Como resulta da comunicação do Banco de Portugal, *"o novo RJSPME passa a ser o elemento central na prestação de serviços de pagamento em Portugal, impactando não só na forma como os prestadores de serviços de pagamento disponibilizam os seus serviços, mas também no modo como particulares, empresas e Administração Pública efetuam pagamentos no seu dia-a-dia.*

O Decreto-Lei introduz um conjunto de alterações na prestação de serviços de pagamento em Portugal, sendo de destacar a sua aplicação a mais operações de pagamento, a criação e regulação de novos tipos de serviços de pagamento, a definição de um conjunto de requisitos de segurança a respeitar na execução de operações de pagamento e a imposição, aos prestadores de serviços de pagamento, de maiores responsabilidades na execução de operações de pagamento não autorizadas.

Com a publicação do novo RJSPME pretende-se promover um mercado de pagamentos mais inovador, competitivo e seguro."

Estão consagradas regras tendo em vista a proteção dos utilizadores, no quadro do desenvolvimento do comércio eletrónico, deveres de informação pré-contratual e contratual destinados a garantir a transparência das condições, direitos e obrigações na prestação e utilização de serviços de pagamento.

Recorde-se que no caso concreto, e como ficou provado, a Demandante inadvertidamente inseriu os dados recebidos por *SMS* (formato habitual e acordado para proceder a movimentações bancárias), do que resultou a transferência de €450 para a conta bancária de um terceiro, o que, de facto, não pretendia.

Não está, pois, em causa a verificação (ou não) da imposição de clausulas desconhecidas por parte da Demandada, ou mesmo da existência de uma autenticação forte do cliente (artº 104º).

Vamos analisar a questão sob a vertente do consentimento ou autorização de pagamento (artº. 103º), as obrigações decorrentes da utilização dos serviços de pagamento (artº 110º), responsabilidades associadas, designadamente quanto ao reembolso (artºs 111º a 115º), revogação do consentimento (artº 121º).

Posto isto,
De acordo com as definições assentes, considera-se (artº 2º):
a) *«Aceitação de operações de pagamento» um serviço de pagamento contratado entre um prestador de serviços de pagamento e um beneficiário para aceitar e processar operações de pagamento, que dê origem a uma transferência de fundos para o beneficiário;*

b) «Agente» uma pessoa singular ou coletiva que presta serviços de pagamento em nome de uma instituição de pagamento ou de uma instituição de moeda eletrónica;

c) «Autenticação» um procedimento que permite ao prestador de serviços de pagamento 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;

d) «Autenticação forte do cliente» uma autenticação baseada na utilização de dois ou mais elementos pertencentes às categorias conhecimento (algo que só o utilizador conhece), posse (algo que só o utilizador possui) e inerência (algo que o utilizador é), os quais são independentes, na medida em que a violação de um deles não compromete a fiabilidade dos outros, e que é concebida de modo a proteger a confidencialidade dos dados de autenticação;
...
f) «Consumidor» 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;
...
ii) «Operação de pagamento» o 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;

De acordo com o artº 103º, uma operação de pagamento ou um conjunto de operações de pagamento, só se consideram autorizados se o ordenante consentir na sua execução, que (salvo acordo em contrário), deve ser dada previamente à execução da operação, e sob a forma acordada entre o ordenante e o respetivo prestador do serviço de pagamento.
Na falta do consentimento, considera-se que a operação de pagamento não foi autorizada.

Ora, nestes termos, a Demandante consentiu na operação, uma vez que introduziu os códigos que recebeu e os utilizou como acordado.

Porém, o consentimento pode ser retirado pelo ordenante em qualquer momento e conforme o acordado, entre o ordenante e o prestador de serviços de pagamento envolvidos, mas nunca depois do momento de irrevogabilidade estabelecido nos termos do artigo 121.º

Considera o artº 121º que uma ordem de pagamento não pode ser revogada pelo utilizador de serviços de pagamento após a sua receção pelo prestador de serviços.
Excetuam-se os casos previstos nos nº 3 a 7, aqui não enquadráveis (como débito direto e acordo da data de pagamento/do beneficiário).

Por seu turno, o artº 110º prevê as obrigações do utilizador, associadas a instrumentos de pagamento, a saber

a) Utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização,
b) tomar todas as medidas razoáveis, em especial logo que receber um instrumento de pagamento, para preservar a segurança das suas credenciais de segurança personalizadas
c) 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.

Prevê o diploma e associado às obrigações do prestador de serviços (artº 111º), que o risco inerente ao envio ao utilizador de serviços de pagamento de um instrumento de pagamento e das respetivas credenciais de segurança personalizadas, recai sobre o prestador do serviço de pagamento (nº 3).

Pelo que, o ordenante que se confronte com a execução não consentida de uma operação de pagamento terá de comunicar ao Prestador de Serviço de Pagamento, a utilização não autorizada do instrumento de pagamento, devendo fazê-lo no prazo máximo de 13 meses contados desde a data do débito, sob pena de caducidade (artº 112º, nº 1).

Nestes termos, compete ao Prestador de Serviço de Pagamento, depois de receber a comunicação, ou de conhecer a natureza não autorizada da operação por qualquer via, o imediato bloqueio do instrumento de pagamento utilizado e o reembolso ao ordenante da operação de pagamento não autorizada, devendo fazê-lo até ao final do primeiro dia útil seguinte àquele em que tiver tido conhecimento sobre a operação.

Este é o regime-regra, que assenta no dever jurídico de o Prestador de Serviço de Pagamento de repor a conta de pagamento do ordenante na situação em que ela estaria se a operação de pagamento não autorizada nunca tivesse sido executada.

No entanto, o Prestador de Serviço de Pagamento não é obrigado a reembolsar o ordenante se tiver motivos razoáveis para suspeitar de uma atuação fraudulenta, caso em que deverá investigar o sucedido e comunicar, de imediato, o assunto às autoridades competentes – tudo conforme o previsto nos artºs 114º e 115º.

Resta-nos verificar que, no caso em apreço, o Prestador de Serviço de Pagamento não invocou a existência de fraude, mas a falta de prevenção necessária para a salvaguarda de utilização indevida do instrumento de pagamento (violação dos deveres de cuidado e prevenção pelo ordenante) – o que se provou.

E, não se apurou, nem provou, o incumprimento ou qualquer ação do Prestador de Serviço de Pagamento.

Vejamos, agora, o disposto no Código Civil, quanto à responsabilidade civil contratual.

Cabe ao credor a prova dos factos constitutivos do seu direito (nº 1 do artº 342º) - o que a Demandante fez mediante a prova da transferência que, na verdade, não pretendia efetuar, e a comunicação do sucedido ao Prestador de Serviço de Pagamento.

Dispõe o artº 798º, que o devedor que falta culposamente ao cumprimento da sua obrigação, é responsável pelo prejuízo que causa ao credor, cabendo-lhe ainda provar (sendo o caso), que a falta de cumprimento ou o cumprimento da obrigação não procede de culpa sua (nº 1 do artº 799º).
Assim, compete, agora, ao devedor, afastar a sua responsabilidade designadamente mediante a prova de que a operação foi devidamente autenticada e não foi afetada por qualquer avaria técnica ou deficiência do serviço.

Neste caso, não só a utilização de *phishing*, que vem alegada é de conhecimento público, como a Demandada deu conhecimento ao Banco de Portugal e às autoridades.

Dispõe o artigo 114.º que, sem prejuízo dos caso de comunicação e retificação de operações de pagamento não autorizadas ou incorretamente autorizadas, conforme o artº 112º, aqui não aplicáveis, ***o prestador de serviços de pagamento do ordenante deve reembolsar imediatamente o ordenante do montante da operação de pagamento não autorizada após ter tido conhecimento da operação ou após esta lhe ter sido comunicada e, em todo o caso, o mais tardar até ao final do primeiro dia útil seguinte àquele conhecimento ou comunicação***. (sublinhado nosso).

Mas, *já* ***não está obrigado ao reembolso, no prazo previsto no número anterior 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.***
No entanto, (artº 115º) ***o ordenante pode ser obrigado a suportar as perdas relativas às operações de pagamento não autorizadas resultantes da utilização de um instrumento de pagamento perdido, furtado, roubado ou da apropriação abusiva de um instrumento de pagamento dentro do limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, até ao máximo de (euro) 50.***
Exceto, se
a) 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*
b) 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.

O ordenante (prossegue o nº 3 ao artº 115), suporta todas as perdas resultantes de operações de pagamento não autorizadas, se aquelas forem devidas a atuação fraudulenta ou ao incumprimento deliberado de uma ou mais das obrigações previstas no artigo 110.º, caso em que não são aplicáveis os limites referidos no n.º 1.

E, (nº 4), em caso de negligência grosseira do ordenante, este suporta as perdas resultantes de operações de pagamento não autorizadas até ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, ainda que superiores a (euro) 50.

Por último cumpre verificar a posição do onde se lê,

"iv. Repartição de responsabilidades no processamento de operações não autorizadas
Caso seja realizada na minha conta uma operação de pagamento não autorizada no montante de 123 euros, por exemplo na eventualidade de alguém tomar posse indevida de informação constante do meu cartão de crédito, apenas me será imputável um montante máximo de 50 euros.
O novo regime jurídico dos serviços de pagamento reforça as salvaguardas do utilizador de serviços de pagamento perante a execução de operações de pagamento não autorizadas:

1. *Diminui o montante máximo a suportar pelo utilizador numa operação de pagamento não autorizada, de 150 euros para 50 euros (exceto em casos de fraude ou negligência grosseira);*
2. *Desresponsabiliza os utilizadores no caso de operações online em que o prestador de serviços de pagamento não exija procedimentos de autenticação forte (a menos que o utilizador aja fraudulentamente).*

Em todo o caso, sempre que utilizadores dos serviços de pagamento identifiquem operações de pagamento não autorizadas, ou incorretamente executadas, deverão informar o mais rapidamente possível o seu prestador de serviços. A partir do momento em que o fizerem não deverão suportar quaisquer perdas adicionais resultantes da utilização não autorizada desse instrumento (salvo em caso de atuação fraudulenta ou de negligência grosseira da sua parte).

Aqui chegados, há que distinguir entre negligência leve (limita a responsabilidade do ordenante ao valor €50), ou grosseira (aplicável o nº 4 do artº 115º).

A negligência grosseira *(*)* assenta na violação de um dever objetivo de cuidado, e de previsibilidade da verificação do dano ou do perigo, de forma particularmente grave, tendo em conta o grau de inobservância do dever a que estava cometido o agente – o que foi, manifestamente, o caso.

Por último, relativamente à alegada falta de celeridade da Demandada na resolução das solicitações relativas a anulação de transferências.

Não se provou que a Demandada não tivesse diligenciado pelo tratamento da reclamação da Demandante.

Nem, ainda, que a atuação da Demandante, em face do disposto no nº 4 do artº 115º, supra, tivesse conduzido a um outro resultado, nomeadamente ao reembolso da quantia de €450, como era a pretensão da Demandante.

Pelo que, não pode prosseguir o pedido.

(*) Ac. do STJ nº 747/04.2 TTCBR.C1.S1, Ac. da TRP nº 212/10.9TTVNG.P1 e Ac. TRL nº 45/17.1PHSXL-3

G – Decisão

Termos em que se decide julgar a presente ação como não provada e, como tal, totalmente improcedente e se decide absolver a Demandada do pedido contra ela formulado pela Demandante

Notifiquem-se as partes da decisão.

Guimarães, 14 de fevereiro de 2023

A Juiz Árbitro

(Margarida Granwehr de Sousa)