jurisprudência.pt

Tribunal da Relação de Guimarães
Processo nº 237/23.4T8VRM.G1

Relator: ALEXANDRA ROLIM MENDES
Sessão: 02 Outubro 2025
Número: RG
Votação: UNANIMIDADE
Meio Processual: APELAÇÃO
Decisão: APELAÇÃO IMPROCEDENTE

HOMEBANKING

RESPONSABILIDADE DO PRESTADOR DE SERVIÇOS DE PAGAMENTO

REJEIÇÃO DA IMPUGNAÇÃO DA MATÉRIA DE FACTO

Sumário

- As operações efetuadas através do serviço de “homebanking”, quando consistem na movimentação de contas a prazo e transferências de fundos, regem-se pelo Regime Jurídico dos Sistemas de Pagamento e da Moeda Eletrónica (RJSPME) (DL 91/2028, de 12 de novembro, que transpôs para o ordenamento jurídico nacional a Diretiva (EU) 2015/2366 do Parlamento e do Conselho, de 25 de novembro de 2015.
- É ao Banco, como prestador do serviço de pagamento, que, caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, cabe o ónus de provar que a operação de pagamento foi autenticada, devidamente registada e contabilizada e não decorreu de qualquer avaria técnica ou de qualquer outra deficiência do serviço prestado pelo prestador de serviços de pagamento, cabendo-lhe ainda demonstrar que houve negligência grosseira do ordenante na utilização dos serviços disponibilizados (arts. 113º e 115º, nº 3, do RJSPME).
- Contudo, a responsabilidade do prestador de serviços de pagamento é afastada caso haja da parte do utilizador dos serviços de pagamento uma atuação fraudulenta ou o incumprimento deliberado de uma ou mais das obrigações previstas no art. 110º do RJSPME.
- Provando-se que a A. carregou num link inserido numa SMS enviada por um

remetente desconhecido e através desse link entrou numa página semelhante à do seu banco, fornecendo as suas credenciais de segurança, violando as normas contratuais e legais sobre a utilização dos camais digitais e à revelia dos alertas de segurança emitidos pelo seu banco, agiu de forma incauta, não demonstrando a prudência e diligência que nas circunstâncias do caso empregaria um bom homem/mulher médio(a) para evitar ser vítima de fraudes.
- Tem assim, a A. de suportar as perdas resultantes das 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, tal como dispõe o art. 115º, nº 4, do RJSPME.

Texto Integral

Acordam no Tribunal da Relação de Guimarães

Relatório:

AA intentou a presente ação de processo comum contra o Banco 1..., S.A., peticionando que seja o Réu condenado a pagar a quantia de 9.860€(nove mil, oitocentos e sessenta euros) correspondente ao montante fraudulentamente retirado da sua conta, acrescido de juros moratórios até pagamento integral e efetivo.

Para tanto, alegou, em síntese, que é cliente do Banco Réu, sendo titular de uma conta de depósito à ordem e utilizando a aplicação do Réu "X...".
No dia 25.10.2021 recebeu duas mensagens no seu telemóvel de um remetente "..." que indicava que para evitar o bloqueio da conta deveria efetuar uma adesão de segurança obrigatória, indicando a hiperligação de um site onde o deveria fazer.
A Autora clicou no link indicado, tendo sido direcionada para um sítio em tudo idêntico ao da Ré, onde lhe foram solicitados alguns dados (nomeadamente o n.º de adesão e algumas coordenadas do cartão matriz), que a Autora forneceu, acreditando que estava no site do Réu.
Alguns dias depois apercebeu-se que tinha sido efetuada uma transferência da sua conta no valor de 9.860,00€ para uma conta titulada por terceiros, e que teria sido vítima de phishing, tendo o Banco Réu informado que não seria responsável pelo valor em causa, porquanto teria sido a Autora a entregar as respetivas matrizes que possibilitaram a transferência, aconselhando que

fosse apresentada queixa-crime.
Acrescenta que confiava no sistema do banco e que o mesmo seria à prova de ataques, imputando ao Banco Réu a obrigação de assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao seu utilizador, devendo proporcionar um sistema de segurança eficaz e impeditivo de utilização abusiva por parte de terceiros.
Defende, ainda, que a sua atuação não deve ser objeto de juízo de censura e, quanto muito, ser entendido como inconsciência leve, sendo o Réu, nos termos do artigo responsável pelo reembolso da quantia objeto da operação não autorizada.

*
O Banco Réu contestou na qual, em síntese, sustentou que a 23/09/2016 a Autora solicitou a adesão aos canais digitais, tendo-lhe sido entregues diversos códigos e coordenadas de segurança, pessoais e intransmissíveis - o que a Autora não podia ignorar, sendo que esta também não poderia ter considerado que as mensagens que recebeu no seu telemóvel eram legítimas.
Defende, pois, que existiu uma atuação gravemente negligente da parte da Autora.
Requereu a improcedência do pedido.
*

Realizou-se o julgamento na sequência do qual foi proferida sentença que julgou a ação **improcedente.**
*
Inconformada veio a Autora recorrer formulando as seguintes **Conclusões**:

I- A Autora, após ter recebido duas mensagens fraudulentas de alerta de bloqueio da conta, que tudo indicavam ter sido enviadas pela Ré, clicou na hiperligação que ali constava.
II- Tendo sido encaminhada para um site visualmente idêntico ao da Ré, onde introduziu o seu número de adesão e algumas combinações do seu cartão matriz.
III- Na convicção séria de que estaria a interagir com a Ré e sem qualquer consciência de que estaria a autorizar qualquer tipo de operação (transferência bancária ou outra).
IV- A Autora nunca recebeu qualquer código de validação por SMS, nem teve conhecimento da sua existência, conforme declarou de forma coerente em audiência de julgamento e demonstrado pelo facto de ter mostrado todas as mensagens à GNR aquando da apresentação de queixa-crime e ao balcão da

Ré, junto de um funcionário da mesma.
V- A Ré não fez prova inequívoca e suficiente, sobretudo, documental, do envio e, muito menos, da receção de tais códigos pela Autora.
VI- A Ré não provou o cumprimento dos deveres preventivos que lhe cabiam ao abrigo do artigo 111.º do DL 91/2018, nomeadamente a garantia de autenticação forte do cliente e monitorização e deteção de padrões anómalos e bloqueio preventivo de operações de risco elevado.
VII- A Autora não foi alertada nem instruída de forma clara, eficaz e atempada quanto aos riscos de utilização da aplicação, nomeadamente de phishing ou qualquer outra atividade fraudulenta, nem à data dos factos existiam alertas visíveis ou ativos na aplicação que usava (X...), nem lhe foram explicadas medidas de autoproteção aquando da adesão.
VIII- A Autora utilizava poucas vezes, senão raramente, a aplicação e para operações muito simples (ver saldo; carregar telemóvel e pequenas transferências esporádicas).
IX- A Douta sentença julga o comportamento da Autora com base num utilizador bancário "idealizado" quando, na verdade, o ordenamento jurídico protege o consumidor real, médio e falível.
X- A Ré só não seria responsabilizada pelas perdas sofridas pela Autora, decorrentes de operações fraudulentas sobre a sua conta no âmbito do Homebanking se alegar e provar que o dano resultou de atuação doloso ou grosseiramente negligente do utilizador do serviço.
XI- Não se pode entender sem mais que age de forma grosseiramente negligente o utilizador da conta bancária que, no âmbito do homebanking, fornece os seus dados confidenciais na sequencia do recebimento de um SMS que contem indicações de ser proveniente da respetiva entidade bancária e/ou o facto de a página web a que de depois acede apresentar ser dessa entidade bancária, por se mostrar idêntica à sua página oficial.
XII- A atuação da Autora, ainda que esta tenha fornecido os seus dados a terceiro, não revela dolo nem negligência grosseira, mas tão só uma confiança comum e compreensível num sistema que deveria garantir-lhe segurança — não se tratando de erro imperdoável, mas de reação humana a um engano sofisticado
XIII- Apesar de a Ré ter o ónus da prova de que a Autora agiu com dolo ou negligência grosseira, esta não o conseguiu provar.
XIV- Devendo ser a Douta Sentença ser revogada e ser o pedido da Autora julgado procedente, condenando a Ré no pagamento da quantia de 9.860,00€ acrescidos de juros de mora contados desde a citação até efetivo e integral pagamento.

Termos em que,
E nos demais de Direito que aqui concretamente sejam aplicáveis, se requer a V/Exa. que se proceda à alteração da sentença proferida nestes autos e seja a RÉ condenada a pagar à Autora as quantias peticionadas.
*
O Réu apresentou contra-alegações pedindo a rejeição do recurso de impugnação da matéria de facto por falta de requisitos legais e pronunciando-se no sentido da improcedência do recurso e confirmação da decisão recorrida.
*
Questões a decidir:

- Verificar se é admissível o recurso de impugnação da matéria de facto;
- Caso tal recurso seja admissível, analisar se a prova produzida permite retirar as conclusões de facto expostas na sentença recorrida;
- Verificar se a apropriação de quantias da conta da A. ocorreu ou não por culpa desta.
*
Nada obstando ao conhecimento do objeto do recurso, cumpre apreciar e decidir.

Os factos considerados provados na 1ª instância foram os seguintes:

1. A Autora é titular de uma conta de depósito sediada no Banco Réu identificada com o n.º ...10.
2. No dia 23.09.2016, a Autora solicitou a adesão aos canais digitais (nomeadamente à aplicação de homebankig “X...”), a que foi atribuído o n.º ...02 e associado o número de telemóvel para segurança adicional ...98, pertencente à Autora,
3. (...) na sequência da adesão foram entregues à Autora um PIN e um cartão matriz, elementos pessoais e de segurança para efetuar operações na aplicação.
4. No dia 25.10.2021, pelas 11:43h, a Autora recebeu uma mensagem no seu telemóvel ...98, proveniente de um remetente com a designação “...”, com o seguinte conteúdo:
“X...: Evite o Bloqueio da conta.
Efetue Adesão de Segurança Obrigatória
Acesse: .../”.
5. No mesmo dia, pelas 15:27 horas, a Autora recebeu nova mensagem do mesmo remetente, com o seguinte conteúdo:

“Banco 1...: Evite o Bloqueio da Conta.
Efetue Adesão de Segurança Obrigatória
Acesse: ...”
6. A Autora, acreditando que as mensagens eram remetidas pelo Banco Réu, clicou na hiperligação constante da última mensagem, sendo direcionada para um sítio da internet, onde a Autora, acreditando tratar-se do sítio do Banco Réu, inseriu o seu PIN de acesso à aplicação X..., as coordenadas do cartão matriz que foram solicitadas,
7. (...) bem como os códigos que recebeu por sms no seu telemóvel.
8. Nessa sequência, foram registadas as seguintes operações:
- às 18:49, foi ativada a funcionalidade “autorização por notificação push”, que permitia substituir a disponibilização de códigos de autenticação enviados por mensagem SMS pela disponibilização desses mesmos códigos usando as notificações aplicacionais nos smartphones, habitualmente designadas por “push notifications”.
- para a ativação desta funcionalidade, foi efetuada a autenticação forte por via da inserção de três matrizes do cartão e “one time password” de seis dígitos enviada para o número de telemóvel que a Autora tem associado ao sistema de segurança adicional (...98), tendo a Autora recebeu a seguinte mensagem de texto:
“ATENÇÃO: NÃO DIVULGUE ESTE CÓDIGO A TERCEIROS, NEM ATRAVÉS DE CHAMADAS TELEFÓNICAS. Ativar autorizacoes. Código SMS XXXXXX.”
- às 18:50, foi ativada a funcionalidade “deixar cartão matriz em casa”, para a qual foi pedido novo código enviado para o número de telemóvel da Autora e três posições do cartão matriz;
- às 18:51 foi realizada uma transferência no montante de 9.860,00€ da conta DO da Autora para a conta com o IBAN ...23, titulada por BB, tendo sido efetuada com a inserção do PIN e autenticação forte por via de one time password enviada para o equipamento autorizado.
9. A 08.11.2021 a Autora deslocou-se ao balcão do Banco Réu em ... por não conseguir aceder à aplicação X... a partir do seu telemóvel, tendo sido informada do saldo da sua conta e da transferência referida em 8,
10. (...) que não tinha efetuada ou autorizada pela Autora.
11. Perante o conhecimento de que a Autora não reconhecia a transferência efetuada, o Banco Réu de imediato procedeu à anulação dos canais digitais e aconselhou a Autora a apresentar queixa, colaborando com a mesma na obtenção dos documentos para o efeito.
12. Ainda no dia 08.11.2021 a Autora apresentou queixa crime.
13. O Banco Réu tem alertas com medidas de segurança para que os clientes previnam a ocorrência de práticas fraudulentas.

*
*
Factos considerados não provados na sentença recorrida:

- A Autora não foi informada nem recebeu qualquer alerta de possíveis ataques, burlas, fraudes ou possibilidade de furto das suas informações pessoais ou dados de acesso.
*
*
Do recurso de impugnação da matéria de facto:

O art. 640 do C. P. Civil, exige a quem pretende impugnar a decisão quanto à fixação dos factos na sentença, que tome posição específica sobre os motivos da discordância, indicando os pontos de facto que pretende impugnar, os concretos meios de prova que impugnam decisão diversa e a decisão que entende ser a correta.

No caso, embora, a Recorrente cumpra estes ónus no "corpo" das alegações de recurso, considerando que os pontos 7,8 e 13 da matéria de facto provada se encontram incorretamente julgados, nas conclusões do recurso nada refere relativamente à sua discordância sobre a matéria de facto considerada provada e/ou não provada.

Ora, decorre do disposto no art. 639º do C. P. Civil que as conclusões das alegações definem o objeto do recurso.

Diz-nos Abrantes Geraldes (*in* Recursos no Novo Código de Processo Civil, 3ª ed., págs. 95) que em resultado do que consta do art. 639º, nº 1 do C. P. Civil, as *conclusões* delimitam a área de intervenção do tribunal *ad quem,* exercendo uma função semelhante à do pedido na petição inicial, ou à das exceções na contestação.

Decorre ainda do art. 635º, nº 4 que nas conclusões da alegação pode o recorrente restringir expressa ou tacitamente o objeto inicial do recurso.

Ora, a declaração é tácita quando se deduz de facto que com toda a probabilidade a revelam (v. art. 217º do C. Civil, por via do art. 295º do mesmo Código).

Refere o mencionado Autor, na mesma obra que, a restrição pode ser tácita

em resultado da falta de correspondência entre a motivação e as conclusões.

Como se refere no Acórdão do STJ de 6/6/2018 (*in* www.dgsi.pt), são as conclusões que delimitam o objeto do recurso, não podendo o Tribunal "*ad quem*" conhecer de questão que delas não conste. Se o recorrente, ao explanar e ao desenvolver os fundamentos da sua alegação, impugnar a decisão proferida na 1ª instância sobre a matéria de facto, pugnando pela sua alteração/modificação, mas omitindo nas conclusões qualquer referência e essa decisão e a essa impugnação, essa questão não faz parte do objeto do recurso".

Abrantes Geraldes (*in* ob. cit., pág. 131) refere que, as conclusões exercem ainda a importante função de delimitação do objeto do recurso (…) . Conforme ocorre com o pedido formulado na petição inicial, as conclusões do recurso devem corresponder à identificação clara e rigorosa daquilo que se pretende obter do Tribunal Superior, em contraposição com aquilo que foi decidido pelo tribunal *a quo.*"

Assim, no que respeita ao **recurso de impugnação da decisão da matéria de facto**, nada dizendo a Recorrente nas conclusões do seu recurso, sobre tal impugnação, nomeadamente, quais os pontos que considera incorretamente julgados, este Tribunal não pode conhecer dessa impugnação por a mesma não fazer parte do objeto do recurso, **rejeitando-se, pois, o recurso nessa parte**.
*
O Direito:

Da responsabilidade pelas transferências bancárias feitas a partir da conta da A., em 25/10/21:

Tendo em conta a matéria de facto provada, concluiu-se que entre A. e R. foi celebrado um "contrato de abertura de conta", no âmbito da prestação pelo segundo à primeira de serviços bancários.

No decorrer dessa relação contratual, o Réu disponibilizou à A. um serviço de banco online, via Internet, que permite aos clientes obter informações sobre a sua conta, efetuar pagamentos, transferências e outras operações bancárias a que a A. aderiu, celebrando, assim, as partes um contrato acessório de *homebanking* (banco virtual).

Conforme se escreve no Acórdão do Supremo Tribunal de Justiça, de 23/01/24, proferido no processo 379/21.0T8FAR.E1.S1 (*in* www.dgsi.pt) "O contrato de "homebanking" celebrado entre a autora e banco réu é o acordo mediante qual o cliente adere a um serviço prestado pelo banco, que consiste na possibilidade de manter relações via internet, de forma a aceder a informações sobre produtos e serviços do banco; obter informações e realizar operações bancárias sobre contas de que a autora fosse titular e, realizar pagamentos, cobranças e operações de compra, venda, subscrição ou resgate sobre produtos ou serviços disponibilizados pelo banco.".

Como é sabido, para efeitos de utilização do "homebanking" os bancos fornecem aos clientes senhas de acesso e usam criptogafia (torna ilegíveis os dados para pessoas não autorizadas), autenticação em dois fatores, tokens (código temporário usado para verificar a identidade de um utilizador) e outros métodos para proteger as transações.

As operações efetuadas através do serviço de "homebanking", quando consistem na movimentação de contas a prazo e transferências de fundos, como as que estão em causa nos presentes autos, regem-se pelo Regime Jurídico dos Sistemas de Pagamento e da Moeda Eletrónica (RJSPME) (DL 91/2028, de 12 de novembro, que transpôs para o ordenamento jurídico nacional a Diretiva (EU) 2015/2366 do Parlamento e do Conselho, de 25 de novembro de 2015, alterado pela Lei 82/2023, de 29 de dezembro e pela Lei 1/2025, de 6 de janeiro).

Com efeito, o mencionado diploma legal, no seu art. 4º, enumera os serviços que se devem caracterizar como "serviços de pagamento", designadamente e com interesse para o caso em apreço, incluindo nos mesmos a "Execução de serviços de pagamento, incluindo a transferência de fundos depositada numa conta de pagamento aberta junto do prestador de serviços de pagamento do utilizador (…)" (v. alínea c) do preceito em causa).

De acordo com a alínea aa) do art. 2º do RJSPME, entende-se por "Instrumento de pagamento" "um dispositivo personalizado ou conjunto de procedimentos acordados entre o utilizador e o prestador de serviços de pagamento e a que o utilizador de serviços de pagamento recorra para emitir uma ordem de pagamento".

Por sua vez, tal como se refere na alínea f) da mesma norma, "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", tal como acontece com a A., que assim, deve ser qualificada como "Consumidora" para efeitos de aplicação do diploma acima mencionado.

Por outro lado, para os termos do diploma em causa o Banco Réu é um "Prestador de serviços de pagamento, por ser uma instituição de crédito com sede em Portugal (v. alínea pp) do art. 2º e art. 11º, nº 1 – a)).

Conforme decorre do nº 1, do art. 103º do RJSPME, uma operação de pagamento ou um conjunto de operações de pagamento só se consideram autorizados se o ordenante consentir na sua execução.

Do art. 110º do mesmo diploma, resulta que o utilizador dos serviços de pagamento deve utilizar o instrumento de pagamento de acordo com as regras que regem a sua emissão e utilização e comunicar, logo que tenha conhecimento dos factos e sem atraso injustificado, ao prestador de serviços de pagamento ou à entidade designada por este último, designadamente, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento.

É no, entanto, ao Banco, como prestador do serviço de pagamento, que, caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, cabe o ónus de provar que a operação de pagamento foi autenticada, devidamente registada e contabilizada e não decorreu de qualquer avaria técnica ou de qualquer outra deficiência do serviço prestado pelo prestador de serviços de pagamento, cabendo-lhe ainda demonstrar que houve negligência grosseira do ordenante na utilização dos serviços disponibilizados (arts. 113º e 115º, nº 3, do RJSPME).

Assim, é o banco que presta o serviço que tem de provar que a(s) transação (ões) que executou foi(ram) devidamente autorizada(s) pelo cliente, assumindo o risco por falhas ou problemas no sistema se não provar que a operação de pagamento não foi afetada por avaria técnica ou qualquer outra deficiência.

Contudo, como resulta do que acima foi dito, a responsabilidade do prestador de serviços de pagamento é afastada caso haja da parte do utilizador dos serviços de pagamento uma atuação fraudulenta ou o incumprimento deliberado de uma ou mais das obrigações previstas no art. 110º acima

mencionado.

No caso, a A. recebeu no seu telemóvel duas mensagens enviadas de um remetente com a designação "...", com o seguinte conteúdo:
"X...: Evite o Bloqueio da conta.
Efetue Adesão de Segurança Obrigatória
Acesse: .../".

"Banco 1...: Evite o Bloqueio da Conta.
Efetue Adesão de Segurança Obrigatória
Acesse: ..."

Acreditando que as mensagens eram do Banco ora Réu, onde tinha conta bancária, a A. clicou na hiperligação constante de uma das referidas mensagens e foi direcionada para um sítio da internet, onde, acreditando tratar-se do sítio do Banco Réu, inseriu o seu PIN de acesso à aplicação X..., as coordenadas do cartão matriz que foram solicitadas, bem como os códigos que recebeu por SMS no seu telemóvel.

É manifesto que no caso em apreço a transferência ocorrida da conta da Autora foi devida a uma fraude informática, estando em causa uma situação de *smishing* (sms + *phishing*) que é uma variação do *phishing* (do inglês "pesca") mas em que a abordagem do utilizador acontece por SMS.
O *phishing*, ocorre quando o lesado recebe um email ou outra mensagem digital, como por exemplo um email, com um link e ao clicar neste é direcionado para um site falso.
No *phishing* ou no *smishing*, o utilizador entra no site falso por conta própria, ao carregar no link que lhe foi enviado (sobre as noções de *phishing* ou no *smishing,* consultar no sítio da internet do Centro Nacional de Cibersegurança (CNCS) o artigo "Boas Práticas contra o Pishing, o Smishing e o Vishing").

Vemos que na situação em análise as mensagens que continham os links que direcionavam o utilizador para um site falso, provinham de um remetente com a designação "..." e não com o nome do Banco, ora Réu. Por outro lado, as hiperligações contantes das mensagens eram diferentes.

Muitas vezes, como é sabido, os ciber criminosos recorrem a tecnologia que lhes permite mascarar o remetente das mensagens, aparecendo as mesmas como remetidas pela entidade legítima, no entanto, não foi isso que se passou no caso em apreço, em que a mensagem provinha de um remetente

desconhecido, o que deveria ter, desde logo, levantado suspeita de que a mensagem não era confiável.

Contudo, a A. sem atentar nesse facto, não só carregou no link, como forneceu a terceiros códigos de segurança e coordenadas do cartão matriz, com base nas quais, outrem conseguiu aceder e usar a sua conta bancária, sendo certo que, como resultou provado (facto 13.), o Banco Réu tem alertas com medidas de segurança para que os clientes previnam a ocorrência de práticas fraudulentas e, para além disso, na mensagem em que o Banco enviou à A. o código para autorização da operação, contém um alerta no sentido de que tal código não deve ser divulgado a terceiros (facto 8).

Ao receber a mensagem com um remetente desconhecido, deveria ter ligado para o seu banco, para confirmar se era daí que provinha a mensagem ou entrado no site do Banco, digitando o nome desta entidade na barra de endereços do navegador (por exemplo o Google Chrome) evitando, assim entrar em páginas falsas, permitindo o acesso de terceiros à sua conta bancária. Seria este o comportamento esperado de um utilizador medianamente cauteloso e diligente.

Na verdade, quer a comunicação social, quer, nomeadamente, as entidades bancárias, estão constantemente a alertar o público em geral e os respetivos utilizadores, em particular, para não carregarem em links enviados por entidades desconhecidas e não fornecerem códigos secretos ou dados pessoais a ninguém, alertando-os para aos riscos associados ao uso das tecnologias.

Deste modo, quem carrega num link inserido numa mensagem de texto que recebe no telemóvel, proveniente de um remetente desconhecido e a partir daí fornece os códigos confidenciais a terceiros, só de si se pode queixar, sem prejuízo, obviamente, da responsabilidade criminal a ser assacada ao agente criminoso (v. art. 221º, do C. Penal).

Acresce que a A., uma técnica de serviço social, com uma com formação superior mínima de licenciatura deveria agir com maior cautela diante de situações digitais suspeitas, especialmente quando contêm links, pois é do conhecimento de qualquer homem/mulher médio/média que clicar em links sem verificar a autenticidade dos remetentes, expõe a pessoa a golpes como o *phishing* e o *smishing*, que podem comprometer dados pessoais e profissionais e permitir o acesso a contas bancárias.

Com efeito, eram-lhe exigíveis cautelas e zelo que nas circunstâncias do caso empregaria um bom homem/mulher médio(a) (v. art. 487º, nº 2, do C. Civil).

Assim, atendendo ao comportamento adotado pela A. e aquele que seria observado em iguais circunstâncias por um utilizador de serviço normalmente informado, diligente e cuidadoso, temos de qualificar a conduta da A. como grosseiramente negligente "em que a conduta do agente só seria susceptível de ser realizada por uma pessoa especialmente negligente, uma vez que a grande maioria das pessoas não procederia da mesma forma". (Menezes Leitão *in* Direito das Obrigações, vol. I, 14ª ed., pág. 313).

No Acórdão da Relação do Porto de 18/04/23, proferido no processo 16900/21.1T8PRT.P1 (*in* www.dgsi.pt), diz-se que "A culpa grosseira ocorrerá quando a omissão do dever de cuidado em que a negligência se traduz revelar que o comportamento observado se afastou do (contraria o) grau de diligência minimamente exigível e da observância de deveres de cuidado (resultantes da relação jurídica) ostensivamente evidentes, patentes e manifestos, traduzindo desconsideração do proceder expectável a qualquer comum utilizador do serviço de pagamento minimamente cuidadoso, apresentando-se como altamente reprovável à luz do mais elementar senso comum, revelando desconformidade com todos os padrões de referência.
A negligência grosseira será de afirmar, assim, quando o grau de reprovação ultrapassar a mera censura que merece a simples imprudência, irreflexão ou o impulso leviano, alcançando um mais alto grau de desleixo e incúria, decorrendo da inobservância das mais elementares regras de prudência e da não adopção do esforço e diligência minimamente exigíveis, nas circunstâncias concretas…comportamento que nunca por nunca seria adoptado pela generalidade dos utilizadores do serviço de pagamento colocados perante as concretas circunstâncias que se apresentaram ao agente, pois que a diligência e cuidados exigíveis no caso os levariam a abster-se de o adoptar e/ou prosseguir.".

Concluiu-se, pois, que a atuação da A., ora Recorrente, infringiu as suas obrigações de utilizadora do serviço, fazendo do mesmo um uso indevido, pelo que a sua conduta se subsume ao disposto na al. a), do nº 1, do art. 110º, do DL 91/2018, sendo certo que do lado do Banco Réu a transação bancária ocorreu de forma regular, executando uma operação bancária autorizada pela Autora (arts. 103º, nº 1 a 3 e 104º do RJSPME), transação essa que, nos termos do disposto nos art. 120º do RJSPME, não pode podia recusar.

A A. ao carregar num link inserido numa sms enviada por um remetente desconhecido e ao fornecer as sua credenciais de segurança, violando as normas contratuais e legais sobre a utilização dos camais digitais e à revelia dos alertas de segurança emitidos pelo seu Banco, agiu de forma incauta, não demonstrando a prudência e diligência que lhe seriam exigíveis para evitar ser vítima de fraudes.

Tem assim, a A. de suportar as perdas resultantes das 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, tal como dispõe o art. 115º, nº 4, do RJSPME.

Confirma-se, desta forma, a decisão recorrida.
*
*
DECISÃO:

Pelo exposto, acorda-se nesta secção cível do Tribunal da Relação de Guimarães em julgar improcedente a apelação, confirmando a decisão recorrida.
Custas a cargo da Apelante (art. 527º, nºs 1 e 2, do C. P. Civil)..
*
*
Guimarães, 2 de outubro de 2025

Alexandra Rolim Mendes
António Beça Pereira
Ana Cristina Duarte