Acórdãos TRL

Acórdão do Tribunal da Relação de Lisboa

Processo:	**2673/25.2T8OER.L1-2**
Relator:	**FERNANDO CAETANO BESTEIRO**
Descritores:	**HOMEBANKING** **PAGAMENTO ELECTRÓNICO** **AUTENTICAÇÃO** **UTILIZADOR** **NEGLIGÊNCIA GROSSEIRA** **ÓNUS DA PROVA**
Nº do Documento:	**RL**
Data do Acordão:	**08-10-2026**
Votação:	**UNANIMIDADE**
Texto Integral:	**S**
Texto Parcial:	**N**
Meio Processual:	**APELAÇÃO**
Decisão:	**IMPROCEDENTE**
Sumário:	**SUMÁRIO (art. 663º, n.º7, do CPC):** **I. A rejeição total ou parcial do recurso respeitante à impugnação da decisão de facto deve verificar-se quando ocorre falta de especificação, nas conclusões, dos concretos pontos de facto que o recorrente considera incorretamente julgados.** **II. Em situações, como a invocada pela Autora, em que ocorram prejuízos decorrentes de operações não autorizadas, de modo voluntário e consciente, pelo utilizador antes da sua notificação ao banco que disponibiliza o serviço ou instrumento de pagamento por meios electrónicos, que decorram de negligência grosseira do utilizador, ou ordenante, cabe a este suportar os danos resultantes de tais operações.** **Por força do disposto no art. 113º, n.º3, do RJSPME, recai sobre o banco o ónus de provar que a operação de pagamento foi devidamente autenticada, que o cliente contribuiu para a ocorrência dos prejuízos dela decorrentes em violação de obrigações a que estava sujeito por força do art. 110º do mesmo regime e que tal se verificou a título de negligência grosseira**
Decisão Texto Parcial:	
Decisão Texto Integral:	**I.** **AA, com o NIF …, intentou, contra Caixa Geral de Depósitos, SA, com o NIPC 500 960 046, a presente acção declarativa com processo comum peticionando a condenação desta no pagamento:** **a. Da quantia de € 7 290,00, acrescida de juros de mora, vencidos e vincendos, a contar da citação até efectivo e integral pagamento, correspondente ao valor total de que foi desapossada;** **b. Da quantia de € 100,00, acrescida de juros de mora vencidos e vincendos, a título de compensação pela privação do uso dos valores de que foi desapossada.** **Alega, em síntese, que:** **- É titular da conta de depósito à ordem n.º ... na Ré há cerca de**

21 anos, onde recebe os lucros provenientes do seu trabalho, bem como de uma conta a prazo, onde coloca determinados montantes;

- Em 20-01-2025, a Autora foi vítima de um crime de burla, ficando lesada em € 6 000,00, retirados da sua conta a prazo, e em € 1 290,00, removidos da sua conta à ordem, no total de € 7 290,00, por negligência, culpa e falta de cuidado da Ré;

- Pelas 16H43, a Autora recebeu uma *sms* do n.º de telefone oficial da Ré (que ficou armazenada na mesma caixa de *sms's* recebidas que as antigas enviadas pela Ré), dizendo "*um novo (Samsung Galaxy A40s) foi associado ao seu contrato pelas 16:41h. Se desconhece aceda: https://cgd-retornar.com*", tendo a Autora contactado a Ré para o seu n.º oficial, sem sucesso;

- A Autora clicou no referido *link* e recebeu uma chamada do número de telefone oficial da Ré, que atendeu, tendo sido informada de que estava a falar com um assistente da Ré (que sabia todos os seus dados) e que estariam a tentar fazer uma transferência da sua conta bancária, ao que a Autora respondeu que não tinha autorizado tal transferência, tendo o alegado assistente indicado que iria impedir a operação, necessitando de um código que a Autora iria receber por *sms*;

- A Autora recusou-se a fornecer o código, tendo aceitado digitá-lo no teclado do seu telemóvel, o que fez, e tendo entrado na *app* "Caixa directa" e clicado numa notificação, que o alegado assistente indicou que seria para cancelar a operação, sendo que, nesse momento, perdeu o acesso à *app*, terminando-se a chamada, e perdendo a Autora os montantes acima indicados;

- A Autora contactou a Ré, que a informou de que teria sido vítima de um crime de burla, e recomendou que fizesse participação criminal, o que a Autora fez, dando origem ao NUIPC n.º 000110/25.1PEOER, e se dirigisse a um balcão da Ré, o que também realizou;

- Porém, a Ré não ressarciu a Autora dos valores de que foi desapossada;

- Por tudo o exposto, a Autora entende ter direito às quantias peticionadas, uma vez que os bancos devem reembolsar o ordenante do montante das transferências não autorizadas, que a Ré não cancelou a transferência em causa no momento em que teve conhecimento da mesma, e que não possui sistema mínimo de segurança informática, devendo ser responsabilizada ao abrigo dos arts. 406.º do Código Civil, 103.º, 104.º, 106.º, n.º 5, 114.º, n.º 1, 135.º do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica e 73.º do Regime Geral das Instituições de

Crédito e Sociedades Financeiras.

*****

A Ré, a 12-09-2025, apresentou contestação, pugnando pela improcedência da acção.

Além de impugnar factualidade invocada na petição inicial, alegou, em síntese, que:

- A Autora foi vítima de *spoofing* - um dos ciberataques para os quais a Ré alerta especificamente no seu site - por sua própria negligência, ao ter carregado no *link* em causa e facultado os códigos de acesso a terceiro, assim autorizando a aludida transferência, inexistindo qualquer problema, avaria ou ataque cibernético ao sistema informático da Ré;

- A actuação da Autora consubstancia negligência grosseira, o que afasta a responsabilidade da Ré pelos movimentos por aquela indicados.

*****

A Autora respondeu a 19-09-2025, refutando ter actuado com negligência grosseira e reiterando a responsabilidade da Ré invocada na petição inicial (cf. despacho de 28-10-2025 que admitiu o articulado em referência).

*****

A 26-01-2026, foi proferido despacho onde, além do mais:

a. Se fixou o valor da causa em € 7 790,00;

b. Se saneou tabelarmente o processo;

c. Se fixou o objecto do litígio;

d. Se enunciaram os temas da prova.

*****

A audiência final realizou-se a 22-04-2026.

A 29-05-2026, foi proferida sentença que julgou a acção integralmente improcedente e, em consequência, absolveu a Ré de todos os pedidos contra si formulados nos autos.

*****

Inconformada, a 30-06-2025, a Autora interpôs recurso da decisão mencionada, que culminou com as seguintes conclusões (transcrição):

1. A Sentença recorrida julgou improcedente a ação, por

entender que a Autora atuou com negligência grosseira ao facultar credenciais e códigos no contexto da fraude sofrida.

2. Está provado que a Autora foi vítima de um esquema articulado de phishing, spoofing e vishing, com utilização aparente do número oficial da Ré e inserção das mensagens fraudulentas no mesmo histórico das SMS genuínas da CGD.

3. A Autora NÃO verbalizou, em momento algum, nenhum código, apenas digitou no teclado numérico do seu telemóvel, não tendo tampouco facultado dados pessoais (foram os próprios burlões que lhe disseram os seus dados – já os tinham);

4. Está igualmente provado que a Autora tentou contactar a Ré através do número oficial antes de aderir plenamente às instruções recebidas, o que revela cautela inicial e não leviandade acrítica.

5. A Autora, conforme indicado pelas diretrizes da Ré, contactou-a, de imediato, mas a Ré não atendeu (se tivesse atendido, toda esta situação era evitada).

6. A Ré não atendeu a Autora, que telefonou várias vezes.

7. Nos termos do artigo 113.º do RJSPME, competia à Ré provar não apenas que a operação foi autenticada e registada, mas também que a Autora atuou com fraude, dolo ou negligência grosseira.

8. A prova da mera utilização formalmente correta das credenciais e dos fatores de autenticação não basta, por si só, para demonstrar autorização da operação nem negligência grosseira do utilizador.

9. A sentença recorrida esvaziou o alcance do artigo 113.º, n.ºs 3 e 4, do RJSPME, convertendo em prova bastante de culpa agravada aquilo que a lei expressamente considera insuficiente quando isoladamente valorado.

10. A negligência grosseira exige um erro imperdoável, desatenção inexplicável ou incúria indesculpável, apreciados em face das circunstâncias concretas do caso.

11. As circunstâncias concretas dos autos — nomeadamente o spoofing do número da Ré, a integração das SMS na mesma caixa das comunicações autênticas, a mensagem indicando "chamada oficial" e a narrativa de bloqueio de uma operação pendente — afastam a ideia de comportamento grosseiramente censurável da Autora.

12. Os alertas genéricos de segurança disponibilizados no site e na aplicação da Ré não bastam, por si sós, para fundar um juízo

automático de negligência grosseira sobre qualquer cliente vítima de fraude sofisticada (até porque não explicam que as mensagens das quais devemos desconfiar, chegarão dentro da própria caixa de mensagens CGD).

13. A Ré não demonstrou ter adotado mecanismos suficientes e proporcionados de monitorização e prevenção de operações anómalas, designadamente perante a transferência global de 7.290,00 euros, precedida de levantamento de depósito a prazo e esvaziamento quase total das contas da Autora.

14. A Ré tendo ao seu dispor mecanismos para bloquear as verbas que saíram indevidamente da conta da Autora, optou por não o fazer;

15. A Ré não demonstrou a suficiência material do seu sistema de autenticação forte face ao risco concreto de fraude remota nem a adoção de verificação adicional autónoma e segura compatível com o perfil manifestamente atípico da operação.

16. A transferência do montante (praticamente total) da conta da Autora, algo que não é comum no seu histórico de cliente (por nunca ter ocorrido), deveria ter despertado um alerta de segurança na Ré, mas como aqui se verifica, não há qualquer segurança no que diz respeito à Ré.

17. O cartão matriz da Autora (fornecido pela Ré), estava caducado.

18. Nos termos do artigo 114.º, n.º 1, do RJSPME, subsiste o dever de reembolso imediato da operação de pagamento não autorizada, não tendo sido validamente afastado pela Ré.

19. A decisão recorrida viola os artigos 103.º, 104.º, 110.º, 111.º, 113.º, 114.º e 115.º do RJSPME, bem como os artigos 406.º, 762.º, 798.º e 799.º do Código Civil e o artigo 73.º do RGICSF.

20. Deve, por isso, a douta Sentença ser revogada e substituída por decisão que condene a Ré no pagamento à Autora da quantia de 7.290,00 euros, acrescida de juros de mora e demais quantias peticionadas.

*****

A Ré apresentou resposta a 07-03-2025, onde, além de concluir pela improcedência do recurso, alegou que a impugnação da decisão sobre a matéria de facto deve ser rejeitada por a Recorrente, nas conclusões, não indicar os concretos pontos da matéria de facto que considera incorrectamente julgados.

*****

A 07-09-2026, o recurso foi admitido, como apelação, com subida nos próprios autos e efeito devolutivo, o que não foi alterado neste Tribunal.

*****

II.

1.

As conclusões da alegação do recorrente delimitam o objeto do recurso, sem prejuízo da ampliação deste a requerimento do recorrido (arts. 635º, n.º4, 636º e 639º, n.º1 e 2 do CPC). Não é, assim, possível conhecer de questões nelas não contidas, salvo se forem do conhecimento oficioso (art. 608º, n.º2, parte final, *ex vi* do art. 663º, n.º2, parte final, ambos do CPC).

Também não é possível conhecer de questões novas – isto é, de questões que não tenham sido objeto de apreciação na decisão recorrida –, uma vez que os recursos são meros meios de impugnação de prévias decisões judiciais, destinando-se, por natureza, à sua reapreciação e consequente alteração e/ou revogação.

Tendo isto presente, no caso, atendendo às conclusões transcritas, a intervenção deste Tribunal de recurso é circunscrita às seguintes questões, considerando a sua dependência:

1. Saber se, na sentença recorrida, ocorre erro de julgamento quanto à factualidade referida pela Recorrente, devendo, previamente, aferir-se da admissibilidade da impugnação da decisão sobre a matéria de facto;

2. Saber se, na sentença impugnada, ocorre erro de julgamento no que respeita à improcedência da pretensão da Autora.

*****

2.

Na sentença impugnada, foi dada como provada a seguinte factualidade:

1. A Autora é titular de uma conta bancária "à ordem" na instituição da Ré, com o n.º de conta CGD ... e n.º de cliente ....

2. Para além da conta bancária descrita em 1., a Autora possui uma conta bancária "a prazo" na instituição da Ré.

3. A Autora e a Ré celebraram um acordo denominado "contrato n.º 394434", cujas "condições gerais" se dão por integralmente reproduzidas, respeitante à utilização, por parte da Autora, da aplicação "Caixa directa" da Ré.

4. Através do acordo descrito em 3., a Autora e a Ré acordaram que o acesso à aplicação "Caixa directa" é feito através da introdução de elementos de identificação da Autora, definidos pela Ré ou pela Autora, e que a realização das operações bancárias poderá depender da introdução de elementos de validação adicionais definidos pela Ré, consoante o seu montante e tipo.

5. Através do acordo descrito em 4., a Autora e a Ré acordaram que as operações realizadas através da aplicação "Caixa directa" consideram-se autorizadas pela Autora quando tenham sido introduzidos os referidos elementos de identificação e, nos casos solicitados pela Ré, os elementos de validação adicionais, sendo da sua responsabilidade, a não ser que a Autora comunicasse qualquer situação prévia de utilização não autorizada da aplicação "Caixa directa" por terceiro.

6. A Autora é prestadora de serviços, auferindo uma quantia mensal que oscila entre os € 760,00 e € 819,00.

7. A Autora recebia os lucros provenientes da sua atividade na conta bancária descrita em 1..

8. Em 20-01-2025, pelas 16H43, a Autora recebeu uma mensagem *sms* no seu telemóvel, proveniente do mesmo servidor utilizado pela Ré e constante da mesma caixa de mensagens que as mensagens anteriormente remetidas pela Ré, com o seguinte texto: «*Um novo (Samsung Galaxy A40s) foi associado ao seu contrato pelas 16:41. Se desconhece, aceda: https://cgd-retornar.com*».

9. Como consequência, a Autora acedeu à sua aplicação "Caixa direta online" para verificar se a Ré tinha associado algum telefone à sua conta bancária e contactou telefonicamente a Ré para o n.º ..., sem sucesso.

10. Em acto contínuo, a Autora clicou no *link* que lhe foi disponibilizado na referida *sms* e forneceu os seus dados do "Caixa directa" (n.º de contrato, código de acesso e n.º de telemóvel).

11. De seguida, a Autora recebeu uma chamada telefónica, que se apresentava com o n.º ..., e que a Autora atendeu, tendo um terceiro se apresentado como assistente da Ré, chamado BB.

12. No decurso da chamada telefónica descrita em 11., o terceiro indicou à Autora que entrava em contacto para a ajudar e informou que alguém estaria a tentar fazer uma transferência bancária da sua conta bancária para outra conta bancária.

13. Acto contínuo, a Autora indicou ao terceiro que não havia

realizado a transferência bancária em causa, tendo o terceiro referido que iria impedir a operação bancária descrita, sendo necessário que a Autora lhe facultasse um código que iria receber, por parte da Ré, por *sms.*

14. Em simultâneo, pelas 17H00 desse mesmo dia, a Autora recebeu uma *sms* enviada pelo sistema da Ré na sua caixa telefónica de mensagens, constante da mesma caixa de mensagens que a *sms* descrita em 8. e que as *sms's* anteriormente remetidas pela Ré, com o seguinte teor: «*NUNCA PARTILHE ESTE CODIGO COM NINGUEM. Para confirmar o seu acesso ao Caixadirecta introduza o código 378857. CASO NAO TENHA ACEDIDO, CONTACTE-NOS DE IMEDIATO*!».

15. Pelas 17H01 desse mesmo dia, a Autora recebeu uma *sms* enviada pelo sistema da Ré na sua caixa telefónica de mensagens, constante da mesma caixa de mensagens que a *sms* descrita em 8. e que as *sms's* anteriormente remetidas pela Ré, com o seguinte teor: «*Caixadirecta – Para confirmar o envio de mensagem, introduza o código 615996.*».

16. Pelas 17H05, a Autora recebeu uma *sms* na sua caixa telefónica de mensagens, constante da mesma caixa de mensagens que a *sms* descrita em 8. e que as *sms's* anteriormente remetidas pela Ré, com o seguinte teor: «*Encontra-se numa chamada oficial com BB. Para bloquear a operacao pendente, siga os passos indicados*» e recebeu, na mesma caixa de mensagens e em simultâneo, uma *sms* enviada pelo sistema da Ré com o teor «*NUNCA PARTILHE ESTE CODIGO COM NINGUEM. Para confirmar a transferência para a conta ... no valor de 7.290,00 EUR, introduza o código 378910.*».

17. Pelas 17H11, a Autora recebeu uma *sms* enviada pelo sistema da Ré na sua caixa telefónica de mensagens, constante da mesma caixa de mensagens que a *sms* descrita em 8. e que as *sms's* anteriormente remetidas pela Ré, com o seguinte teor: «*Para confirmar Alteracao de código de acesso, introduza o código 780916.*»

18. Durante o decurso da chamada descrita em 11., a Autora forneceu ao terceiro os códigos recebidos por *sms* no seu telemóvel, e acima descritos.

19. Durante o decurso da chamada descrita em 11., a Autora entrou na sua aplicação "Caixa directa" através do seu telemóvel e clicou numa notificação que possuía o texto "sim", seguindo as instruções do terceiro, que referiu que esse seria o último passo para impedir a operação bancária em causa.

20. Nesse momento, a Autora ficou sem acesso à aplicação "Caixa

directa" e, em simultâneo, a chamada telefónica descrita em 11. terminou.

21. Como consequência do descrito em 10. a 19., foram transferidos das contas bancárias da Autora descritas em 1. e 2. os seguintes montantes, ficando a Autora com € 7,38 de saldo disponível:

a) € 6 000,00 retirados da conta bancária "à ordem";

b) € 1 290,00 retirados da conta bancária "a prazo".

22. Cerca de 20 (vinte) minutos após a realização da transferência bancária descrita em 21., os montantes em causa foram dissipados da conta bancária para onde foram transferidos.

23. Cerca de 30 (trinta) minutos após o fim da chamada telefónica descrita em 11., a Autora realizou uma chamada telefónica para a Ré, dando conta da mensagem recebida, do teor da chamada telefónica anterior, e da falta de acesso à sua "Caixa direta" ao assistente da Ré que a atendeu, tendo este informado que, em suma, provavelmente teria sido vítima de uma "burla", que a equipa da Ré já tinha conhecimento do sucedido e iria iniciar procedimentos, que se deveria dirigir a um balcão da Ré com o comprovativo da transferência que não solicitou e pedir informação sobre a sua reversão, que a mesma teria de ser vista com a equipa especializada, bem como dirigir-se à Polícia de Segurança Pública (PSP) para apresentar queixa e retornar ao balcão para entregar a participação efectuada, que a situação foi relativamente rápida, mas que o dinheiro podia já ter sido todo retirado, ou não, da conta de destino, que tal teria de ser visto posteriormente, e que no dia seguinte saberia o que iria ser feito.

24. Em consequência do descrito em 23., nessa mesma noite, pelas 22H00, a Autora deslocou-se à esquadra da PSP de Carnaxide, tendo realizado a respetiva participação, que deu origem ao NUIPC n.º 000110/25.1PEOER.

25. No dia 20-01-2025, não foi registada qualquer avaria, anomalia ou deficiência técnica no sistema informático da Ré, que tenha afetado a transferência bancária descrita em 21..

26. Em consequência do descrito em 23., na manhã seguinte, a Autora dirigiu-se ao balcão da Ré, sito em Algés.

27. A Autora recorreu a família e a amigos para proceder ao pagamento das suas despesas de alimentação e habitação.

28. Há mais de 15 (quinze) anos que a Ré divulga, no seu *site* oficial, que os utilizadores do serviço "Caixa directa" não devem clicar em *link's* e fornecer os seus dados, bem como que, em caso algum, a Ré pede aos seus clientes os seus códigos/credenciais de

segurança, seja para que finalidade for.

29. No seu *site* "Caixa directa web", a Ré possui diversas recomendações de segurança, alerta especificamente para a técnica de ciberataque de *spoofing,* refere a necessidade de conferir que os dados da operação recebidos por *sms* estão correctos antes de inserir o código recebido no telemóvel e, caso seja detectada alguma anomalia, não deve ser confirmada a operação nem prosseguida a utilização dos serviços *internet banking* para particulares e/ou empresas, apresentando um exemplo de *sms* fraudulento com o texto «*Ativou a aplicação Autenticacao.gov no novo dispositivo Samsung Galaxy A40s. Se não reconhece, va de imediato a https://cmd-encerrar.com*».

30. Na aplicação "Caixa directa", a Ré possui informações com recomendações de segurança, informando «*A Caixa não envia SMS com links*», «*Não forneça dados do cartão matriz nem o código SMS Token*», «*Nunca valide uma operação que não solicitou.*», «*A Caixa não envia emails com links ou a solicitar dados», «Não responda, não clique em links, não abra ficheiros*», e envia mensagens aos seus clientes alertando para a realização de chamadas telefónicas e envio de mensagens em nome da "Caixa", de fraude, *phising sms* e telefonemas falsificados, com as recomendações «*desconfie sempre de mensagens/chamadas que não solicitou*» e «*nunca forneça dados confidenciais e bancários em resposta a mensagens (ex SMS, e-mail) ou telefonemas fraudulentos, mesmo que possam parecer ter origem na CGD.*».

*****

Na decisão recorrida, foi dado como não provado que:

i. No momento descrito em 8., a *sms* recebida pela Autora foi enviada através do número de telemóvel oficial da Ré.

ii. No momento descrito em 10., o *link* em que a Autora clicou não chegou a ser direccionado para nenhuma página online.

iii. No momento descrito em 11., o terceiro tinha conhecimento dos dados da Autora porque entrou no sistema informático da Ré, apropriando-se assim dos mesmos.

iv. No momento descrito em 19., a notificação em que a Autora clicou apareceu como "cancelar operação".

v. As transferências bancárias do valor descrito em 21. carecem da utilização do cartão matriz conferido pela Ré.

vi. Em 30-01-2025, a Ré enviou uma carta à Autora endereçada à sua morada, informando que foi efectuado o pedido de devolução do montante transferido da sua conta bancária, e que o reembolso foi recusado, tendo-se concluído pela ausência de

elementos que permitam responsabilizar a Ré, por as operações terem exigido a correcta utilização dos meios de pagamento e terem sido regularmente autenticadas, registadas e contabilizadas, não podendo a Ré proceder ao reembolso.

*****

3.

Passando ao conhecimento da primeira questão acima enunciada, atinente a saber se, na sentença recorrida, ocorre erro de julgamento quanto à factualidade referida pela Recorrente.

Na resposta ao recurso, a Ré defende a rejeição da impugnação da decisão sobre a matéria de facto, invocando, como seu fundamento, a ausência de identificação dos concretos pontos da matéria de facto que a Recorrente entende terem sido incorrectamente julgados.

Cumpre, pois, conhecer da rejeição aludida.

Importa reter que, o art. 640º do CPC preceitua que:

"1. Quando seja impugnada a decisão sobre a matéria de facto, deve o recorrente obrigatoriamente especificar, sob pena de rejeição:

a) Os concretos pontos de facto que considera incorretamente julgados;

b) Os concretos meios probatórios, constantes do processo ou de registo ou gravação nele realizada, que impunham decisão sobre os pontos da matéria de facto impugnados diversa da recorrida;

c) A decisão que, no seu entender, deve ser proferida sobre as questões de facto impugnadas.

2 - No caso previsto na alínea b) do número anterior, observa-se o seguinte:

a) Quando os meios probatórios invocados como fundamento do erro na apreciação das provas tenham sido gravados, incumbe ao recorrente, sob pena de imediata rejeição do recurso na respetiva parte, indicar com exatidão as passagens da gravação em que se funda o seu recurso, sem prejuízo de poder proceder à transcrição dos excertos que considere relevantes".

Por força do aludido normativo, o recorrente, na impugnação da matéria de facto, tem um triplo ónus que, não sendo cumprido, importa a rejeição do recurso da decisão de facto:

1. Deve concretizar os factos que impugna;

2. Deve indicar os concretos meios de prova que justificam a impugnação e impõem uma decisão diversa e, caso tenha havido gravação daqueles, deve indicar as passagens da gravação em que funda a sua discordância;

3. Deve especificar a decisão que entende dever ser proferida quanto à factualidade que impugna.

Segundo Abrantes Geraldes (Recursos no Novo Código de Processo Civil, 7ª edição, 2022, Almedina, Coimbra, p. 194-195), em anotação ao referido artigo 640.º, com a reforma processual-civil de 2013 "foram recusadas soluções maximalistas que pudessem reconduzir-nos a uma *repetição dos julgamentos*, tal como foi rejeitada a admissibilidade de *recurso genéricos* contra a errada decisão da matéria de facto, tendo o legislador optado por restringir a possibilidade de revisão de concretas questões relativamente às quais sejam manifestadas e concretizadas divergências por parte do recorrente".

"A rejeição total ou parcial do recurso respeitante à impugnação da decisão de facto deve verificar-se em algumas das seguintes situações: (…)

a) Falta de *conclusões* sobre a impugnação da decisão da matéria de facto (arts. 635.º, n.º 4, e 641.º, n.º 2, al. b)); (…)

b) Falta de especificação, nas *conclusões*, dos *concretos pontos de facto* que o recorrente considera incorretamente julgados (art. 640.º, n.º 1, al. a)); (…)

c) Falta de especificação, *na motivação, dos concretos meios probatórios* constantes do processo ou nele registados (v.g. documentos, relatórios periciais, registo escrito, etc.); (…)

d) Falta de indicação exata, *na motivação,* das *passagens da gravação em que o recorrente* se funda; (…)

e) Falta de posição expressa, na *motivação*, sobre o *resultado pretendido* relativamente a cada segmento da impugnação.

(…) As referidas exigências devem ser apreciadas à luz de um *critério de rigor*. Trata-se, afinal, de uma decorrência do princípio da autorresponsabilidade das partes, impedindo que a impugnação da decisão da matéria de facto se transforme numa mera manifestação de inconsequente inconformismo (…)» (obra citada, p. 200-202).

Em idêntico sentido, Lebre de Freitas, Ribeiro Mendes e Isabel Alexandre (Código de Processo Civil Anotado, vol. 2.º, 2022, Coimbra Editora, p. 97 e 98, em anotação ao referido artigo 640.º do CPC, referem que "vê-se que o recorrente é destinatário de exigentes ónus legais, na medida em que está obrigado a indicar

sempre os concretos pontos de facto que considera terem sido incorretamente julgados, indicando-os na fundamentação da alegação e sintetizando-os nas conclusões, bem como a identificar os concretos meios de prova, constantes do processo ou que tenham sido registados, que, do seu ponto de vista, impunham decisão diversa da recorrida (cf. art. 662, n.º1). Tem assim o recorrente, sob cominação da rejeição do recurso na parte em que estes ónus não tenham sido observados, de demonstrar o erro na fixação dos factos materiais em causa, resultante da formação de uma convicção assente num erro na apreciação das provas que ao juiz cabe livremente apreciar (art. 607, n.º 4 e 5), recorrendo às presunções judiciais concretamente mais adequadas, de acordo com as regras da experiência (…). Tem, por isso, também o recorrente o ónus de indicar ao tribunal "a decisão que, no seu entender, deve ser proferida sobre as questões de factos impugnadas".

"(…) Não ficam por aqui os ónus das partes".

"A gravação da produção de prova (…) tem como consequência, de acordo com o n.º 2, que o recorrente (…) tem de indicar com exatidão as passagens da gravação em que se funda, sem prejuízo de poder proceder à sua transcrição. Se não o fizer, o recurso é rejeitado (…)".

Como se refere no acórdão do STJ de 08-02-2024, processo n.º 7146/20.7T8PRT.P1.S1 (acessível em dgsi.pt), a "rejeição do recurso respeitante à impugnação da decisão da matéria de facto apenas deve verificar-se quando falte nas conclusões a referência à impugnação da decisão sobre a matéria de facto, através da referência aos «concretos pontos de facto» que se considerem incorretamente julgados (alínea a) do n.º 1 do artigo 640.º), sendo de admitir que as restantes exigências (alíneas b) e c) do n.º 1 do artigo. 640.º), em articulação com o respetivo n.º 2, sejam cumpridas no corpo das alegações".

Atentando nas conclusões do recurso, constata-se que nas mesmas não consta qualquer referência aos concretos enunciados de facto que a Recorrente considera incorrectamente julgados.

Ora, como se referiu, a falta de especificação, nas conclusões, dos concretos pontos de facto que a Recorrente considera incorrectamente julgados constitui fundamento para a rejeição da impugnação da decisão sobre a matéria de facto.

Face ao referido, rejeita-se a impugnação da decisão sobre a matéria de facto.

*****

4.

Passando ao conhecimento da segunda questão acima enunciada, que se reconduz a saber se, na sentença recorrida, ocorre erro de julgamento no que respeita à improcedência da pretensão da Autora.

Alega a Autora / Recorrente que, nas contas bancárias junto da Ré / Recorrida de que é titular, ocorreu uma operação de movimento a débito, no montante total de € 7 290,00, por si não autorizada de modo intencional e consciente, realizada por intermédio do serviço de *home banking* da Ré, antes da notificação a esta, e que da mesma ocorreram danos na sua esfera patrimonial, cujo ressarcimento incumbe à Ré.

Na sentença recorrida, afastou-se a responsabilidade da Ré pelos danos decorrentes da aludida operação por a Autora ter actuado com negligência grosseira, o que esta refuta.

Para a economia da presente decisão, releva que, na esteira do referido no acórdão desta Secção de 13-03-2025, proferido no processo n.º 11019/23.3T8SNT.L1 (acessível em dgsi.pt), a relação jurídica entre as partes que cumpre analisar tem a sua origem num *contrato de abertura de conta* (também designado por *contrato de conta bancária* – José A. Engrácia Antunes, *Direito dos Contratos Comerciais*, Almedina, 2009, pp. 483 e ss.), gerador de uma relação jurídica bancária, que se traduz "*num contrato celebrado entre um banco (a ré) e um seu cliente (a autora) que enquadra e disciplina uma relação duradoura entre as partes e no âmbito do qual irão surgir outros contratos que implicam existência e movimentação de fundos (na maioria dos casos haverá, pelo menos, um contrato de depósito bancário, podendo também existir, apenas ou cumulativamente, um contrato de conta-corrente bancária ou uma de várias espécies de contratos de crédito)*", com as características de um contrato-quadro.

É frequente surgir, no âmbito da relação jurídica bancária, como acessório do contrato de abertura de conta que lhe deu origem, um outro contrato usualmente designado por *contrato de home banking*, *online banking*, *internet banking*, *e-banking*, banca ao domicílio, banca eletrónica ou banco *online*. Este contrato respeita a um sistema de canais digitais disponibilizado pelo banco via Internet que permite aos clientes obter informações sobre a sua conta bancária, efectuar transferências e pagamentos, além de outras operações bancárias, que tradicionalmente apenas eram feitas "ao balcão", nos espaços físicos de agências e sucursais (veja-se, no mesmo sentido, também o acórdão do TRP de 14-07-2020, processo n.º 22 158/17.0T8PRT.P1, acessível em dgsi.pt).

Como se menciona no aludido acórdão desta Secção de 13-03-2025, o "contrato de *homebanking* é um contrato acessório

do de conta bancária e que regula os direitos e deveres das partes no acesso e movimentação da(s) conta(s) bancária(s) pelo cliente bancário através de canais digitais disponibilizados pelo banco. Apesar de a lei não lhe atribuir um nome nem um conjunto concentrado de regras que o visem em exclusivo, é já um tipo social bem reconhecido na comunidade jurídica, e na sociedade em geral, por força da sua frequente e generalizada repetição na prática bancária, e pelo sequente tratamento que tem na doutrina – v.g., além dos textos supra citados, Calvão da Silva, «Conta corrente bancária, operação não autorizada e responsabilidade civil, STJ, Acórdão de 18 de dezembro de 2013», *Revista de Legislação e de Jurisprudência*, Ano 144, n.º 3991 (mar.-abr. 2015), pp. 290-326, Bruno Silva Palhão, «Os serviços de pagamento e as operações não autorizadas», *Cadernos de Direito Privado*, n.º 65 (jan.-mar. 2019), pp. 3-17, Hugo Luz dos Santos, «Plaidoyer por uma "distribuição dinâmica do ónus da prova" e pela "teoria das esferas de risco" à luz do recente Acórdão do Supremo Tribunal de Justiça, de 18/12/2013 , o (admirável) "mundo novo" no homebanking?», *O Direito*, Ano 147, n.º 3 (2015), pp.715-743 –, e na jurisprudência (v.g., Ac. STJ de 23/01/2024, proc. 379/21.0T8FAR.E1.S1, Cons. Nelson Borges Carneiro).

Apesar de atípico, o referido contrato de home banking encontra-se regulado pelo Regime Jurídico dos Serviços de Pagamento e da Moeda Electrónica (RJSPME), aprovado pelo DL n.º 91/2018, de 12-11 (com as alterações operadas pelo DL n.º 66/2023, de 08-08, Lei n.º 82/2023, de 29-12, e Lei n.º 1/2025, de 06-01, vigentes à data dos factos em apreço), quando, no âmbito da sua execução, seja utilizado um serviço de pagamento convencionado entre as partes, sendo certo que este não inclui necessariamente tal tipo contratual, que pode abranger apenas um âmbito mais restricto, designadamente, atinente a consulta de dados e transferências entre contas do mesmo titular.

No caso dos autos, no âmbito das relações constituídas pelos contratos de abertura de conta a que respeitam os pontos 1 e 2 da matéria de facto provada, por força de um contrato de home *banking* celebrado entre as partes, a que respeitam os pontos 3 a 5 da matéria de facto provada, a Ré, banco, disponibilizou a possibilidade de a Autora, utilizador, lhe dar ordens de mobilização dos fundos depositados em tal conta, sendo que a mesma tem o direito de exigir da ré a execução das ordens que lhe dá por via da plataforma electrónica.

Em situações, como a invocada pela Autora, em que ocorram prejuízos decorrentes de operações não autorizadas, de modo voluntário e consciente, pelo utilizador antes da sua notificação ao banco que disponibiliza o serviço ou instrumento de

pagamento por meios electrónicos, o comportamento daquele tem relevância determinante no apuro da responsabilidade pelos mesmos, como salienta Carolina França Barreira, '*Home banking*: A repartição dos prejuízos decorrentes de fraude informática', in Revista Electrónica de Direito, Outubro 2015, nº 3, Faculdade de Direito da Universidade do Porto, p. 47 (acessível em www.cije.up.pt/revistared).

Como se refere no acórdão do TRP de 18-04-2023, processo n.º 16900/21.1T8PRT. P1 (acessível em dgsi.pt), "*nas situações não imputáveis a título de negligência grave ao utilizador do serviço (a pessoa singular ou colectiva que utiliza o serviço de pagamento a título de ordenante – alínea eee) do art. 2º do 'Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica', aprovado pelo DL 91/2018, de 12/11), é o banco (o prestador do serviço) quem deve arcar com os prejuízos que excedam o valor de 50,00€ (arts. 114º e 115º, nº 1 do RJSPME) decorrentes de operações de pagamento não autorizadas, pois é a este que cabe suportar o risco do sistema informático que sustenta o serviço de home banking não ser seguro e permitir a intromissão de terceiros; a responsabilidade do utilizador do serviço (ordenante da operação) é, nestas situações, limitada ou circunscrita ao referido montante (50,00€), arcando o banco com os prejuízos excedentes, por lhe caber suportar o risco do sistema informático que sustenta o serviço do home banking não ser seguro e permitir a intromissão de terceiros*".

Por sua vez, nos casos de negligência grosseira do utilizador, ou ordenante, cabe a este suportar os danos 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 € 50,00, como decorre do art. 115º, nº 4 do RJSPME.

O banco, ou prestador do serviço, suporta os prejuízos causados pelas debilidades dos sistemas de pagamento que disponibiliza aos seus clientes sempre que as perdas não sejam decorrentes de negligência grosseira destes.

Por força do disposto no art. 113º, n.º3, do RJSPME, na aludida versão, recai sobre o banco o ónus de provar que a operação de pagamento foi devidamente autenticada, que o cliente contribuiu para a ocorrência dos prejuízos dela decorrentes em violação de obrigações a que estava sujeito por força do art. 110º do mesmo regime e que tal se verificou a título de negligência grosseira (veja-se, no mesmo sentido, Carolina França Barreira, obra citada, p. 37, 62-63, bem como os acórdãos do TRP de 18-04-2023 e do TRG de 13-07-2026, processo n.º 2918/25.9T8GMR.G1, acima mencionados).

Cumprido o ónus de prova referido por parte do banco,

prestador de serviços, o utilizador deverá suportar a totalidade dos prejuízos.

O conceito de negligência grosseira deve ser encontrado na disciplina geral do direito civil, posto que não se mostra densificado no RJSPME, como salienta Carolina França Barreira (obra citada, p. 50).

Tratando-se de violação de deveres contratuais, a negligência grosseira em referência deve ser aferida nos termos aplicáveis à responsabilidade civil, designadamente, à luz dos arts. 799º, n.º 2, e 487º, n.º 2 do Cód. Civil, com apelo à "*comparação entre o comportamento concretamente adoptado pelo agente e o que seria observado nas mesmas circunstâncias de facto por um utilizador do serviço de pagamento normalmente informado, diligente e cuidadoso, pois este é o padrão referencial ou parâmetro de aferição a considerar para apurar do grau de reprovação ou censura de que é merecedor a conduta do utilizador (o grau de reprovação ou de censura será tanto maior quanto mais ampla for a possibilidade de a pessoa ter agido de outro modo), donde resulta 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*" (acórdão do TRP de 18-04-2023, acima referido, que se segue de perto).

Por ausência de outro critério legal, o padrão de conduta exigível ao utilizador do serviço deve ser definido tendo em conta o modelo de uma pessoa-tipo, um sujeito ideal, o tipo de homem médio ou normal, medianamente sagaz, prudente avisado e cuidadoso (fazendo reportar estas qualidades ao do utilizador do serviço em causa) que utiliza tais serviços.

Como refere Antunes Varela (Das Obrigações em Geral, vol. I, 9ª edição, 1996, Almedina, Coimbra, p. 596-597, nota 3), a referência, no art. 487º, n.º2, do CC, ao bom pai de família acentua mais a nota ética ou deontológica do bom cidadão do que o critério puramente estatístico do homem médio, não estando o julgador vinculado às práticas de desleixo, de desmazelo ou de incúria, que porventura se tenham generalizado no meio, se outra for a conduta exigível das pessoas de boa formação e são procedimento.

A negligência grosseira verificar-se-á 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, correspondendo ao erro imperdoável, à desatenção inexplicável e à incúria indesculpável, vistos em confronto com o comportamento do comum das pessoas, mesmo daquelas pouco diligentes – 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" (acórdão do TRP de 18-04-2023).

Salienta-se no acórdão do TRG de 13-07-2026, processo n.º 2918/25.9T8GMR.G1 (acessível em dgsi.pt), que a negligência grosseira que releva "*corresponde a uma actuação que se afasta não apenas do comportamento do homem médio diligente, mas inclusivamente do padrão mínimo de cuidado que poderia esperar-se de uma pessoa normalmente descuidada*".

Haverá, ainda, que ponderar as circunstâncias do caso concreto, sejam as que respeitam *às condições do agente, sejam as que desencadearam o seu comportamento que determinou a ocorrência do dano, só assim se podendo avaliar qual a diligência que, no caso, lhe eram exigíveis* (cf. acórdão desta Relação de 11-09-2025, processo n.º 451/24.5T8LSB.L1-2, que teve a concordância da Exmª Primeira Adjunta, acessível em dgsi.pt).

Do contrato de *home banking* emerge uma relação obrigacional complexa, geradora de deveres principais, acessórios e deveres laterais (Carolina França Barreira, obra citada, p. 17).

Por um lado, ao banco exige-se que assegure os mecanismos de segurança inerentes ao instrumento de pagamento que disponibiliza aos clientes, pois sobre si recai o dever de prestar um serviço eficaz e seguro, cabendo-lhe um reforçado dever de informar e elucidar os clientes dos casos de fraude e de intromissão de terceiros não autorizados nas operações que o sistema *home banking* permite e, assim, de elucidação dos perigos inerentes à utilização do serviço que se comprometeu a prestar (Carolina França Barreira , obra citada, p. 21 e ss.).

Por outro lado, sobre o utilizador do serviço impende um conjunto de deveres acessórios de conduta conexionados com a segurança do sistema.

Assim, além de dever tomar as medidas razoáveis para preservar a eficácia dos mecanismos de segurança personalizados

associados ao instrumento que utiliza (art. 110º, n.º 2, do RJSPME) e de comunicar ao banco prestador do serviço, sem atraso, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento (art. 110º, n.º1, al.b), do RJSPME), sobre o utilizador recaem deveres que respeitam à necessidade de se acautelar e proteger dos perigos de fraude para os quais seja alertado pelo banco, mormente por avisos, alertas e informações de segurança feitos no momento em que acede ao serviço na página do banco, logo depois de feito o registo inicial.

Nessa perspectiva, tem-se como dever acessório do cliente utilizador, em vista de utilizar, com segurança, o serviço que lhe é proporcionado, o de se manter ao corrente das variadas formas de fraude informática que vão surgindo e que o banco cuida de levar ao seu conhecimento em vista de que tome as cautelas devidas e adequadas e de as adoptar.

Importa atentar em que, como se assume no acórdão do TRG de 13-07-2026, processo n.º 2918/25.9T8GMR.G1 (acessível em dgsi.pt), "*a utilização regular dos instrumentos de pagamento pressupõe a observância das regras de segurança previamente comunicadas pelo prestador e a preservação da confidencialidade dos respetivos elementos de autenticação. Por isso, o n.º 2 do mesmo artigo [110º do RJSPME] dispõe expressamente que o utilizador deve tomar todas as medidas razoáveis para preservar a segurança das credenciais de segurança personalizadas que lhe foram atribuídas",* o que constitui *"um verdadeiro dever de diligência que deve ser aferido segundo o padrão objetivo do bom pai de família consagrado no art. 487/2 do Código Civil. O utilizador deve, por conseguinte, guardar os códigos de acesso, palavras-passe, elementos de autenticação e demais dispositivos de segurança de forma a impedir o respetivo conhecimento por terceiros, abstendo-se de os divulgar ou disponibilizar.*"

Em sede de situações como a em apreço, relevam os múltiplos mecanismos de fraude electrónica que têm vindo a verificar-se na utilização dos serviços de *home banking*.

Entre tais mecanismos, tem sido identificados os seguintes, segundo o acórdão do TRG de 1-07-2026, processo n.º 2918/25.9T8GMR.G1 (acessível em dgsi.pt):

a. *O phishing, que* se reconduz ao envio de comunicações electrónicas que aparentam provir da instituição financeira legítima, induzindo o utilizador a introduzir credenciais de autenticação numa página falsa que reproduz, com maior ou menor fidelidade, a aparência do sítio oficial do banco;

b. O *smishing,* que consiste na realização de um contacto fraudulento mediante mensagens SMS aparentemente

provenientes da instituição financeira;

c. O *vishing*, em que o contacto com o utilizador é efectuado por chamadas telefónicas, durante as quais o agente se apresenta como funcionário do banco ou de uma entidade pública;

d. O *spoofing*, em que o agente dissimula ou falsifica elementos identificativos das comunicações electrónicas, telefónicas ou digitais, fazendo-as surgir perante o utilizador como provenientes de uma fonte legítima, de forma a fazer surgir a comunicação como proveniente da entidade legítima com quem o utilizador habitualmente se relaciona, sendo este confrontado com mensagens, correios electrónicos ou chamadas que aparentam ter origem na instituição bancária com a qual mantém relação contratual;

e. O *pharming*, em que o sistema informático do utilizador é previamente comprometido através da instalação de programas maliciosos (*malware*), sendo subsequentemente redirecionado para páginas falsas mesmo quando introduz corretamente o endereço eletrónico autêntico da instituição financeira;

f. O SIM *swaping*, que se reconduz na obtenção fraudulenta de um duplicado do cartão SIM do utilizador, permitindo ao agente receber os códigos de autenticação enviados por SMS e concluir operações aparentemente validadas segundo os protocolos de autenticação forte.

No caso em apreço, constata-se que, no dia 20-01-2025, ocorreu a movimentação, a débito, das contas tituladas pela Autora junto da Ré, no valor total de € 7 290,00, para crédito em conta do beneficiário, por via do contrato de *home banking* entre as mesmas celebrado, a que se referem os pontos 3 a 5 dos factos provados.

A operação referida verificou-se em consequência do fornecimento, pela Autora a terceiro, do número do contrato de *home banking* celebrado entre a mesma e a Ré, dos códigos de acesso à plataforma Caixa Directa, número de telemóvel associado ao aludido contrato, do código de confirmação da operação de transferência na aludida plataforma, do código de confirmação da alteração do código de acesso à plataforma referida e de clicar em "sim" numa notificação existente na aplicação Caixa Directa (cf. pontos 10-21 da matéria provada).

Releva, ainda, que a actuação da Autora referida foi precedida e mostra-se decorrente de a mesma aceder a um link que surgiu numa sms recebida no seu telemóvel (cf. ponto 8 da matéria de facto dada como provada).

Da matéria de facto dada como provada resulta evidenciado que

a operação de pagamento invocada pela Autora foi devidamente autenticada, mediante a inserção do código de autenticação forte (Token) que foi enviado, por sms pela ré, e que a Autora forneceu ao terceiro mencionado, após lhe comunicado as credenciais de acesso à plataforma de *home banking*.

Considerando que está demonstrado que o serviço da Ré não sofreu qualquer avaria, anomalia ou deficiência técnica que tenha afectado a transferência mencionada (cf. ponto 25 da matéria de facto provada), cumpre, atentando no referido acima, apurar se a actuação da Autora contribuiu para a realização da aludida operação, em violação de obrigações a que estava sujeita por força do art. 110º do RJSPME e que tal se verificou a título de negligência grosseira.

O contributo da Autora para a realização da operação em referência decorre da comunicação, pela mesma a terceiro, desde logo, dos códigos de acesso à plataforma Caixa Directa e de autenticação forte (Token) que foi enviado, por sms, pela Ré, bem como do número de telemóvel associado ao contrato de *home banking*.

A actuação da autora ocorre após ter deparado com uma sms no seu telemóvel de associação ao contrato de *home banking* de um novo aparelho e da indicação de um link para aceder no caso de desconhecer tal associação, a que a mesma acedeu.

Ora, o comum dos utilizadores dos serviços de *home banking*, mesmo o menos diligente, ter-se-ia abstido de prosseguir a operação quando se deparou com a mensagem referida, não acedendo ao link nela constante.

Por menos diligente e cauteloso que seja o comum dos utilizadores do serviço prestado pela Ré, haverá que reconhecer-se que mensagem mencionada permitiu à Autora ficar alerta e suspeitar que a mesma era fraudulenta, posto que claramente contrária aos procedimentos utilizados pelas instituições bancárias, como a Ré.

A alerta e a suspeita mencionada mostrar-se-iam incrementados com a solicitação da indicação de códigos de acesso à plataforma Caixa Directa e de autenticação forte (Token) ou quaisquer outros.

Importa reter que a Ré, à data dos factos em apreço, nos sites oficial e da Caixa Directa e na aplicação com a mesma designação, tinha disponibilizado alertas aos clientes sobre mensagens com indicação de sites, cujo acesso não deve ser realizado, e para o pedido indevido de códigos fornecidos pela Ré no âmbito do serviço de *home banking* (cf. pontos 28 a 30), o que

vai ao encontro das mais elementares regras de prudência de um normal utilizador de tal serviço.

Entende-se, pois, que se impunha à Autora que se tivesse abstido de aceder ao site indicado na mensagem mencionada e de fornecer os códigos a que se fez referência.

A displicência e falta de cuidado evidenciada pela actuação da Autora, como utilizadora, constitui um desrespeito elementar de regras de cuidado e prudência associadas à necessidade de acautelar a ocorrência de fraude informática, que se lhe impunham por força do disposto no art. 110º, n.º2, do RJSPME, para cuja observância foi alertada pela Ré e para o que qualquer utilizador está fortemente avisado.

À Autora impunha-se, claramente, a adopção de um comportamento diverso do verificado, adequado a prevenir a realização da operação mencionada e os consequentes danos, designadamente, não acedendo ao site mencionado nem fornecendo qualquer um dos códigos aludidos.

O grau de inconsideração ou descuido evidenciado pela Autora atinge o patamar mais elevado, posto que se traduz na omissão de elementares deveres de cuidado e diligência, que se impunham nas circunstâncias em que actuou, posto que plena e facilmente apreensíveis.

Entende-se, face ao exposto, como se assume na decisão recorrida, que a operação de débito efectuada nas suas contas referida no acervo provado é imputável à Autora, a título de negligência grosseira.

Considerando o disposto no art. 115º, nº 4 do RJSPME, na versão acima referida, e ao supra referido, forçoso se mostra concluir que a Ré não é responsável pelos danos sofridos em consequência da operação alegada e demonstradas nos autos, cabendo à Autora, cliente utilizador do serviço de *home banking*, suportá-los.

O recurso mostra-se, face ao referido, improcedente e a sentença recorrida deve ser confirmada.

*****

5.

Considerando a improcedência do recurso, a recorrente deverá suportar as respectivas custas (art. 527º, n.º1 e 2 do CPC), sem prejuízo do decidido sobre apoio judiciário.

*****

III.

Em face do exposto, acordam os Juízes Desembargadores que compõem o Colectivo desta 2ª Secção em julgar o recurso interposto pela autora improcedente e, em consequência, confirmar a sentença recorrida.

Custas do recurso pela autora, sem prejuízo do decidido sobre apoio judiciário.

Notifique.

*****

Lisboa, 08 de Outubro de 2026.

Os Juízes Desembargadores,

Fernando Caetano Besteiro **(relator).**

Rute Sobral **(1.ª adjunta).**

Ana Cristina Clemente **(2.ª adjunta).**