Acórdão do Tribunal da Relação de Guimarães

Processo: 1284/24.4T8BRG.G1
Relator: FERNANDA PROENÇA FERNANDES
Descritores: RESPONSABILIDADE CIVIL BANCÁRIA
HOMEBANKING
CULPA DO LESADO
ÓNUS DA PROVA
Nº do Documento: RG
Data do Acordão: 02-04-2025
Votação: UNANIMIDADE
Texto Integral: S
Meio Processual: APELAÇÃO
Decisão: APELAÇÃO PROCEDENTE
Indicações Eventuais: 3.ª SECÇÃO CÍVEL

Sumário:

No âmbito do homebanking, a entidade bancária só não será responsabilizada pelas perdas sofridas pelo cliente, decorrentes de operações fraudulentas sobre a conta deste, se alegar e provar que o dano resultou de actuação dolosa ou grosseiramente negligente do utilizador do serviço.

Decisão Texto Integral:

Acordam na 3ª Secção Cível do Tribunal da Relação de Guimarães

I. Relatório (feito com base no da decisão apelada).

EMP01..., Ld.ª, NIPC ...52, com sede na rua ..., ..., ..., ..., propôs a presente acção declarativa de condenação sob a forma de processo comum contra o Banco 1..., SA, NIPC ...16, com sede na Avenida ..., ..., ..., ..., pedindo a condenação deste a pagar-lhe a quantia de € 104.994,00, acrescida de juros comerciais contados à taxa legal em vigor, desde a citação e até efectivo e integral pagamento.
Alegou, para o efeito, em síntese, que foi retirada, sem autorização, das suas contas e através do serviço *homebanking* do Banco 1..., SA, a quantia global de € 124.992,00; que apenas lhe foi devolvida a quantia de € 19.998,00, recusando-se aquela instituição bancária a restituir-lhe o remanescente em falta - € 104.994,00; que o réu, enquanto depositário daquele valor, deverá proceder à respetiva restituição, na medida em que é responsável pela falha informática do seu sistema que foi atacado e penetrado por agentes desconhecidos maliciosos, com a intenção de furtar.

*

O réu deduziu contestação, no âmbito da qual, refutou qualquer avaria técnica ou qualquer outra deficiência do serviço efectuado por si, alegando que foi a autora que, não tendo respeitado as normas de segurança relativas àquele serviço, permitiu a realização das transferências da quantia de € 124.992,00 por terceiros.
Concluiu, deste modo, pela improcedência da ação e consequente absolvição do pedido.

*

Foi proferido o despacho saneador, no âmbito do qual foi identificado o objeto do litígio e foram enunciados os temas da prova.

*

Realizado o julgamento, foi proferida sentença, com o seguinte dispositivo:
*"**IV. DECISÃO.***
*Termos em que e face ao exposto, julgando a ação improcedente, por não provada, o Tribunal absolve o réu Banco 1... SA do pedido. **
Custas da ação a cargo da autora – art. 527º, nº 1, do C.P.C.
Registe e Notifique.".*

*

Inconformada com esta decisão, a autora dela interpôs recurso e formulou, a terminar as respectivas alegações, as seguintes conclusões (que se transcrevem):
"CONCLUSÕES:
[…]

*

Contra-alegou a ré, terminando com as seguintes conclusões, que igualmente se transcrevem:
[…]

*

O recurso foi admitido como de apelação, a subir imediatamente, nos próprios autos e com efeito devolutivo.

*

Colhidos os vistos legais, cumpre decidir.

*

II. Questões a decidir.

Sendo o âmbito dos recursos delimitado pelas conclusões das alegações do recorrente – arts. 635.º, n.º 4 e 639.º, n.ºs 1 e 2 do Código de Processo Civil (doravante, abreviadamente, designado por CPC) –, ressalvadas as questões do conhecimento oficioso que ainda não tenham sido conhecidas com trânsito em julgado, as questões que se colocam à apreciação deste Tribunal consistem em saber:
1. da impugnação da matéria de facto;
2. da procedência da acção.

*

III. Fundamentação de facto.

Os factos que foram dados como provados na sentença sob recurso são os seguintes:
"1. A autora exerce a sua atividade na área da sapataria, vendendo calçado.
2. O réu dedica-se à atividade bancária.
3. A autora é titular de três contas bancárias sediadas no Banco 1..., SA.
4. A autora, na pessoa do seu gerente, utiliza as referidas contas bancárias, para os movimentos de dinheiro necessários ao exercício da sua atividade.
5. No dia 17.12.2013, a autora aderiu aos canais diretos (vulgo canais digitais) disponibilizados pelo réu aos seus clientes.
6. À referida adesão foi associado o número de telemóvel ...84 para segurança adicional.
7. A adesão aos canais diretos tem subjacente a entrega ao cliente dos seguintes códigos e coordenadas de segurança:
. Código Secreto (PIN) – pessoal, único e intransmissível, composto por seis dígitos numéricos para, juntamente com o número de adesão, aceder aos canais diretos;
. Cartão de Acesso – o designado "cartão matriz", pessoal, único e intransmissível, do qual consta o número de adesão e uma chave alfanumérica necessária para validar as operações efetuadas por meio dos canais diretos;
. Código de Validação de Operação – código de autenticação único, que constituiu a segurança adicional, enviado por SMS ou, alternativamente, por chamada de voz, composto por seis dígitos, não alterável nem reutilizável (one time password), gerado no momento e enviado por notificação para o telemóvel configurado para a receção destes códigos.
8. No ano 2023, as contas bancárias tituladas pela autora sediadas na instituição bancária réu dispunham de acesso online.
9. Esse acesso online apenas poderia ser completado por três pessoas: o gerente, AA, o seu pai, BB, e CC, funcionária da autora há cerca de 18 anos.
10. O acesso online de CC só lhe permite preparar ou dar ordem para pagamentos

que só serão finalizados ou executados após ordem de um dos outros dois titulares da conta da empresa.
11. No dia 15 de novembro de 2023, CC, como habitualmente fazia no quotidiano, entrou na conta da autora através do seu aceso online e deu ordens de pagamento no site do banco, que aguardavam a ordem de execução por parte de um dos outros titulares da conta.
12. O AA faz os acessos à conta bancária unicamente pelo seu computador, utilizado exclusivamente por si, munido de antivírus atualizado.
13. No dia 15 de novembro de 2023, pelas 18 horas, o AA, ligou o computador para aceder ao site online do banco réu para confirmar e assinar os pagamentos que a CC havia preparado previamente.
14. E efetuou o login nos canais digitais com o número de adesão ...63, com a inserção correta e à primeira tentativa das credenciais de segurança - código secreto de 6 dígitos.
15. E entrou no site online do banco réu.
16. Poucos minutos depois, apareceu no ecrã uma caixa de texto com o logotipo do Banco 1..., SA.
17. Essa caixa de texto configurava a representação de uma página web igual à do réu.
18. Nessa caixa de texto constava a informação que o site estava em atualização e que demoraria alguns minutos a ficar concluída, aparecendo um contador de percentagem.
19. Durante este processo, apareceu uma nova caixa a pedir as coordenadas do cartão matriz para que pudesse concluir eficazmente a atualização, sendo que a imagem através da qual eram pedidos estes dados, era exatamente igual à fornecida habitualmente pelo website do réu.
20. O AA introduziu os códigos do cartão matriz seis vezes (tantas quantas lhe foram solicitadas).
21. Por cada uma das seis vezes, foi gerada uma "one time password push notification" enviada para o número de telemóvel associado à adesão (...84), conforme se discrimina:

22. Em todas as notificações "push" recebidas pelo gerente da autora no telemóvel, fez-se referência à confirmação de operações iniciadas no Banco 1... online, sendo as mesmas referentes a transferências internas, pagamentos de serviços ou transferências urgentes ou de grandes montantes.
23. O gerente da autora não confirmou as operações via notificação "push".
24. E, em todas as seis vezes, recebeu, no telemóvel associado à adesão, uma chamada da linha de apoio do banco, proveniente do número ...00, fornecendo o código de validação - "one time password".
25. As chamadas da linha de apoio do réu fornecendo o código de validação foram recebidas às 18:32h, 18:41h, 18:46h, 18:51h, 19:00h e 19:05h.
26. E o gerente da autora acionou os seis códigos de validação recebidos.
27. O gerente da autora contactou a linha de apoio ao cliente do banco, através do

número ...00, sem ter sido atendido por um assistente, uma vez que, apesar do acionamento dos códigos de validação fornecidos, a conclusão da atualização estava demorada.
28. Dada a falta de tempo no momento do sucedido e face ao não desenvolver da atualização do Banco 1..., o gerente da autora acabou por desligar o computador.
29. Na manhã seguinte, o gerente da autora apercebeu-se, através de informação transmitida pela funcionária CC, que tinham sido realizadas diversas transferências de duas contas da sociedade, para destinatários de origem desconhecida.
30. Na sessão do dia anterior, foram realizadas as seguintes operações:
. Pelas 18:33 horas, execução de transferência urgente ou grandes montantes com o número de pedido ...19, no valor de € 19.998,00, da conta ...81 para o IBAN ...84;
. Pelas 18:42 horas, execução de transferência urgente ou grandes montantes com o número de pedido ...17 no valor de € 49.998,00 da conta ...72 para o IBAN ...44;
. Pelas 18:47 horas, execução de transferência urgente ou grandes montantes com o número de pedido ...19, no valor de € 14.998,00, da conta ...72 para o IBAN ...23;
. Pelas 18:52 horas, execução de transferência interna com o número de pedido ...57, no valor de € 19.998,00 da conta ...72 para o IBAN ...23;
. Pelas 19:01 horas, execução de pagamento de serviços com o número de pedido ...38, no valor de € 10.000,00, da conta ...72, para Entidade ...83 – Easypay e a Referência ...62;
. Pelas 19:06 horas, execução de transferência interna com o número de pedido ...50, no valor de € 10.000,00, da conta ...72 para o IBAN ...23.
31. Cada uma das operações referidas em 30 foram autenticadas com recurso à inserção correta, e à primeira tentativa, das seguintes credenciais de segurança (autenticação forte):
. Três posições aleatórias do cartão matriz; e
. Código de seis dígitos recebido via chamada de voz no número de telemóvel associado à adesão da autora (one time password).
32. E foram registadas e contabilizadas.
33. As transferências não foram efetuadas por avaria técnica ou qualquer outra deficiência do serviço efetuado pelo réu.
34. A autora não manteve o computador utilizado no acesso aos canais digitais a salvo de software malicioso que foi acionado quando o seu gerente acedeu ao site online do réu no dia 15 de novembro de 2024, abrindo-se uma janela fraudulenta por cima da página fidedigna da instituição bancária e que remeteu para a necessidade de realizar uma atualização daquele site.
35. No dia 16.11.2023, na sequência do relatado pelo gerente da autora, a linha ... do réu bloqueou o acesso aos canais digitais da autora.
36. No dia 17.11.2023, o gestor de conta do Banco 1..., SA, DD cancelou o acesso a esses mesmos canais.
37. Após o conhecimento de que as operações bancárias não eram reconhecidas pela autora, o réu encetou de imediato todos os procedimentos considerados adequados com vista a tentar minimizar o prejuízo alegado pela autora.
38. Da realização daqueles procedimentos, resultou apenas a devolução à autora da quantia de € 19.998,00 no dia 04 de dezembro de 2023.
39. A autora apresentou queixa crime relativamente às operações efetuadas não reconhecidas por si, dando origem ao inquérito que corre termos sob o n.º 3362/23...., no DIAP- secção de Vila Verde. 40. A autora, no dia 21 de novembro de 2023, pelo punho do seu mandatário, através de carta registada com aviso de receção, interpelou o réu no sentido de este assumir a responsabilidade pelo sucedido, pagando-lhe a quantia que lhe foi subtraída.
41. Tal missiva foi recebida, mas o réu, em resposta, transmitiu à autora que declinava qualquer responsabilidade pelo sucedido.
42. O réu alerta os seus clientes com medidas de segurança que os mesmos devem tomar para prevenir a ocorrência de práticas fraudulentas.

43. O réu emitiu em setembro de 2023 o seguinte alerta de segurança:
- IMAGEM -

44. O réu emitiu em outubro de 2023 o seguinte alerta de segurança:
- IMAGEM -
45. Os alertas de segurança são emitidos aquando do login nos canais diretos e no sitio da internet do réu, disponível em:
[…]
46. O réu nunca solicitou ou solicita a inserção de credenciais pessoais dos clientes para a concretização de qualquer atualização do seu sitio da internet.".

*

Foram dados como não provados os seguintes factos:
"47. O sistema informático do réu foi atacado e penetrado por agentes desconhecidos, com a intenção de furtar.".

*

IV. Do objecto do recurso.

1. Da impugnação da matéria de facto.

Verificando-se que a recorrente indica quais os factos que pretende que sejam decididos de modo diverso, bem como os meios probatórios que na sua óptica o impõe(m), podemos concluir que cumpriu o ónus estabelecido no art. 640.º do CPC.
Resulta das conclusões da apelante que esta não concorda com a resposta aos pontos 33.º e 34º dos factos dados como provados e com a resposta ao ponto 47º, dos factos dados como não provados.
Entende que este último deve ser dado como provado, que o ponto 33 deve ser dado como não provado e que no que ao ponto 34º diz respeito, deve considerar-se como não escrita a seguinte passagem: "*A autora não manteve o computador utilizado no acesso aos canais digitais a salvo de software malicioso".*
Tais factos têm a seguinte redacção:
"33. As transferências não foram efetuadas por avaria técnica ou qualquer outra deficiência do serviço efetuado pelo réu.
34. A autora não manteve o computador utilizado no acesso aos canais digitais a salvo de software malicioso que foi acionado quando o seu gerente acedeu ao site online do réu no dia 15 de novembro de 2024, abrindo-se uma janela fraudulenta por cima da página fidedigna da instituição bancária e que remeteu para a necessidade de realizar uma atualização daquele site.
47. O sistema informático do réu foi atacado e penetrado por agentes desconhecidos, com a intenção de furtar.".
No que ao ponto 33º dos factos provados e 47º dos não provados diz respeito, invoca a apelante que nos casos em que os Bancos permitem que hackers penetrem o sistema informático existe uma presunção de culpa aplicada à ré, com base nos artigos 796.º e 799.º, nº1 do Cód. Civil, consignando que o artigo 799º, nº1 refere que "*incumbe ao devedor provar que a falta de cumprimento ou o cumprimento defeituoso da obrigação não procede de culpa sua.",* o que faz com que o facto 47.º tivesse de ser dado por provado, já que era de presumir-se e tal presunção não foi ilidida e o 33.º por não provado.
Cremos não caber-lhe razão.
Desde logo, porque não põe a apelante em causa a prova em que se baseou o Tribunal a quo, para dar tais dados factos como provado e não provado. Ou seja, não indica ou esclarece porque razão, em seu entender a presunção não foi ilidida.
A tal acresce que, ainda que não tivesse sido ilidida a presunção, tal não levaria, sem mais, a que se considerasse provado o ponto 47º dos factos não provados e não provado o ponto 33º dos factos provados, pois que ambos contêm matéria de facto que vai além da mera presunção de culpa, razão pela qual é de improceder a

impugnação nesta parte.

Já no que à impugnação do ponto 34º dos factos provados diz respeito, entendemos caber razão à apelante, quando afirma que o segmento formulado na negativa no facto provado n.º 34.º "*A autora não manteve o computador utilizado no acesso aos canais digitais a salvo de software malicioso"* é conclusivo.
De facto, como a apelante bem afirma, tal deveria resultar de uma realidade que "a priori" permitisse formular esse juízo, teria de haver um facto prévio de onde se pudesse extrair tal conclusão. Para que o Tribunal a quo pudesse afirmar que o computador não foi mantido *"a salvo de software malicioso"* teria de ter factos de suporte, alegados e provados, que demonstrassem essa afirmação.
Para se poder afirmar que um dado equipamento não está seguro, é necessário saber quais os factos concretos que permitem extrair essa conclusão de falta de segurança.
Assim, tal segmento textual contém em si um juízo de valor sobre a segurança do computador, ou seja, uma verdadeira valoração de factos, uma conclusão.

Sucede contudo que, lida a contestação, se verifica que o réu alegou nos pontos 12º e 13º da mesma, o seguinte:
"12.º Em data não concretamente apurada, mas certamente em momento anterior à concretização das transferências que a A. agora alega não reconhecer, o legal representante clicou, através do computador habitualmente utilizado para aceder aos canais digitais do R., numa hiperligação maliciosa ou recebeu no computador material com vírus, que comprometeu a segurança daquele equipamento.
13.º Ao clicar – indevidamente – nos referidos links, o legal representante permitiu que aquele computador ficasse infectado com software malicioso (vulgo malware)."
Estes são os factos subjacentes a tal conclusão, e que não constam nem dos factos provados, nem dos não provados, podendo agora, este Tribunal, avaliar a prova produzida, para concluir pela sua prova ou não prova.
E quanto à prova de tal factualidade, não podemos deixar de concordar com a apelante, quando afirma que nenhuma se fez.
É que, como bem afirma, as declarações da única testemunha que foi considerada pelo Tribunal a quo quanto a esta matéria (EE), foram abstractas, teóricas, proferidas por alguém que não conhece o gerente da autora e que não conhece o computador deste, não tendo assim um conhecimento directo sobre os factos em causa.
Ouvido o seu depoimento, o que se verifica é que a testemunha em causa, adianta apenas possibilidades do que poderá ter sucedido, não afirmando, de forma peremptória e explicada o que efectivamente sucedeu.
A testemunha não tem qualquer conhecimento directo ou contemporâneo dos factos, aventando a possibilidade de infecção por vírus malaware, que não sabe como aconteceu ou até se aconteceu.
Por outro lado, temos como provado no ponto 12 que o gerente da autora faz os acessos à conta bancária unicamente pelo seu computador, utilizado exclusivamente por si e munido de antivírus actualizado.
Face a tal, e à mingua de outra prova, os factos alegados em 12 e 13 da contestação terão de ser dados como não provados, e consequentemente a sua conclusão.
Nesta medida, o ponto 34º dos factos provados, passa a ter a seguinte redacção:
"34º Foi accionado software malicioso quando o gerente da autora acedeu ao site online do réu no dia 15 de novembro de 2024, abrindo-se uma janela fraudulenta por cima da página fidedigna da instituição bancária e que remeteu para a necessidade de realizar uma atualização daquele site.".

*

Considerando as alterações introduzidas na decisão relativa à matéria de facto, a factualidade (provada) a atender para efeito da decisão a proferir é a que consta do ponto III, com as referidas alterações.

*

2. Cabe agora verificar se deve a sentença apelada ser revogada.
Não foi posta em causa pelas partes a subsunção efectuada pelo tribunal *a quo* da situação dos autos, ao Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RJSPME), aprovado pelo Decreto-Lei n.º 91/2018, de 12 de Novembro.
Tal diploma procedeu à transposição para a *"ordem jurídica interna da Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno (segunda Diretiva de Serviços de Pagamento), que procedeu a uma revisão do enquadramento jurídico europeu em matéria de serviços de pagamento.*", como é referido no preâmbulo do referido Decreto-Lei n.º 91/2018, de 12 de Novembro.
O Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RJSPME) regula o acesso à actividade das instituições de pagamento e a prestação de serviços de pagamento, bem como o acesso à actividade das instituições de moeda eletrónica e a prestação de serviços de emissão de moeda eletrónica (art. 1.º, n.º 1) e, nos termos do disposto no art. 3.º, n.º 1, é aplicável à actividade das instituições de pagamento com sede em Portugal e das respectivas sucursais, agentes e terceiros aos quais sejam subcontratadas funções operacionais, bem como à prestação de serviços de pagamento em Portugal pelas entidades legalmente habilitadas, nos termos previstos no n.º 3 do referido art. 3.º.
No caso dos autos, e considerando a factualidade que se apurou, não restam dúvidas de que é correcto o enquadramento legal efectuado na sentença apelada, ao aplicar o RJSPME, sendo a autora/apelante a utilizadora de serviços de pagamento e o banco réu, o prestador de serviços de pagamento (cfr. arts. 2.º, als. aa), pp), vv) e eee) e art. 4.º do referido regime jurídico).
Desse diploma, relevam para o caso dos autos, as seguintes disposições:
Artigo 110.º (Obrigações do utilizador de serviços de pagamento associadas aos instrumentos de pagamento):
"1 - O utilizador de serviços de pagamento com direito a utilizar um instrumento de pagamento deve:
a) Utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização, as quais têm de ser objetivas, não discriminatórias e proporcionais; e
b) 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.
2 - Para efeitos da alínea a) do número anterior, o utilizador de serviços de pagamento deve tomar todas as medidas razoáveis, em especial logo que receber um instrumento de pagamento, para preservar a segurança das suas credenciais de segurança personalizadas.".
Artigo 111.º (Obrigações do prestador de serviços de pagamento associadas aos instrumentos de pagamento):
"1 - O prestador de serviços de pagamento que emite um instrumento de pagamento deve:
a) Assegurar que as credenciais de segurança personalizadas do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento, sem prejuízo das obrigações do utilizador do serviço de pagamento estabelecidas no artigo anterior;
b) Abster-se de enviar instrumentos de pagamento não solicitados, salvo quando um instrumento deste tipo já entregue ao utilizador de serviços de pagamento deva ser substituído;
c) Garantir a disponibilidade, a todo o momento, de meios adequados para permitir ao utilizador de serviços de pagamento proceder à comunicação prevista na alínea b) do n.º 1 do artigo 110.º ou solicitar o desbloqueio nos termos do n.º 4 do artigo 108.º;

d) Facultar ao utilizador do serviço de pagamento, a pedido deste, os meios necessários para fazer prova, durante 18 meses após a comunicação prevista na alínea b) do n.º 1 do artigo 110.º, de que efetuou essa comunicação ou solicitou o desbloqueio nos termos do n.º 4 do artigo 108.º;
e) Impedir qualquer utilização do instrumento de pagamento logo que a comunicação prevista na alínea b) do n.º 1 do artigo 110.º tenha sido efetuada.
2 - O prestador de serviços de pagamento assegura que a comunicação a que se refere a alínea c) do n.º 1 é efetuada a título gratuito, cobrando apenas, e se for caso disso, os custos diretamente imputáveis à substituição do instrumento de pagamento.
3 - O risco do envio ao utilizador de serviços de pagamento de um instrumento de pagamento ou das respetivas credenciais de segurança personalizadas corre por conta do prestador do serviço de pagamento.".
Artigo 112.º (Comunicação e retificação de operações de pagamento não autorizadas ou incorretamente executadas):
"1 - O utilizador do serviço de pagamento obtém do prestador de serviços de pagamento a retificação de uma operação de pagamento não autorizada ou incorretamente executada que dê origem a uma reclamação, nomeadamente ao abrigo dos artigos 130.º e 131.º, se comunicar a operação ao prestador de serviços de pagamento logo que dela tenha conhecimento e sem atraso injustificado, e dentro de um prazo nunca superior a 13 meses a contar da data do débito.
2 - Sempre que, relativamente à operação de pagamento em causa, o prestador do serviço de pagamento não tenha prestado ou disponibilizado as informações a que está obrigado nos termos do capítulo ii do presente título iii, não é aplicável o prazo máximo referido no número anterior.
3 - Em caso de intervenção de um prestador do serviço de iniciação do pagamento, o utilizador de serviços de pagamento obtém a retificação do prestador de serviços de pagamento que gere a conta, nos termos dos n.os 1 e 2 do presente artigo, sem prejuízo do disposto nos n.os 5 a 9 do artigo 114.º e nos artigos 130.º e 132.º.".
Artigo 113.º (Prova de autenticação e execução da operação de pagamento):
"1 - Caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, ou alegue que a operação não foi corretamente efetuada, incumbe ao respetivo prestador do serviço de pagamento fornecer prova de que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência do serviço prestado pelo prestador de serviços de pagamento.
2 - Se a operação de pagamento tiver sido iniciada através de um prestador do serviço de iniciação do pagamento, recai sobre este último o ónus de provar que, no âmbito da sua esfera de competências, a operação de pagamento foi autenticada e devidamente registada, e não foi afetada por qualquer avaria técnica ou por outra deficiência relacionada com o serviço de pagamento por si prestado.
3 - Caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, a utilização do instrumento de pagamento registada pelo prestador de serviços de pagamento, incluindo o prestador do serviço de iniciação do pagamento, se for caso disso, não é necessariamente suficiente, por si só, para provar que a operação de pagamento foi autorizada pelo ordenante, que este último agiu de forma fraudulenta, ou que não cumpriu, com dolo ou negligência grosseira, uma ou mais obrigações previstas no artigo 110.º.
4 - Nas situações a que se refere o número anterior, o prestador de serviços de pagamento, incluindo, se for caso disso, o prestador do serviço de iniciação do pagamento, deve apresentar elementos que demonstrem a existência de fraude, de dolo ou de negligência grosseira da parte do utilizador de serviços de pagamento.".
Artigo 114.º (Responsabilidade do prestador de serviços de pagamento em caso de operação de pagamento não autorizada):
"1 - Sem prejuízo do disposto no artigo 112.º, 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.
2 - O prestador de serviços de pagamento do ordenante 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.
3 - Sempre que haja lugar ao reembolso do ordenante, o prestador de serviços de pagamento do ordenante deve assegurar que a data-valor do crédito na conta de pagamento do ordenante não é posterior à data em que o montante foi debitado na conta.
4 - No caso previsto no número anterior, o prestador de serviços de pagamento do ordenante, se for caso disso, repõe a conta de pagamento debitada na situação em que estaria se a operação de pagamento não autorizada não tivesse sido executada.
5 - Caso a operação de pagamento seja iniciada através de um prestador do serviço de iniciação do pagamento, o prestador de serviços de pagamento que gere a conta 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.
6 - O prestador de serviços de pagamento que gere a conta não está obrigado ao reembolso no prazo previsto no número anterior se o prestador do serviço de iniciação do pagamento lhe der conhecimento de que tem motivos razoáveis para suspeitar de atuação fraudulenta do ordenante e de que comunicou por escrito esses motivos às autoridades judiciárias nos termos da lei penal e de processo penal.
7 - Sempre que haja lugar ao reembolso ao ordenante, o prestador de serviços de pagamento que gere a conta deve, se for caso disso, repor a conta de pagamento debitada na situação em que estaria se a operação de pagamento não autorizada não tivesse sido executada.
8 - Se o prestador do serviço de iniciação de pagamento for responsável pela operação de pagamento não autorizada, deve indemnizar imediatamente o prestador de serviços de pagamento que gere a conta, a pedido deste, pelos danos sofridos ou pelos montantes pagos em resultado do reembolso ao ordenante, incluindo o montante da operação de pagamento não autorizada.
9 - Nos casos a que é aplicável o disposto no n.º 2 do artigo 113.º, recai sobre o prestador de serviços de iniciação do pagamento o ónus de provar que, no âmbito da sua esfera de competência, a operação de pagamento foi autenticada e devidamente registada, e não foi afetada por qualquer avaria técnica ou por outra deficiência relacionada com o serviço de pagamento por si prestado.
10 - Sempre que o ordenante não seja imediatamente reembolsado pelo prestador de serviços de pagamento, e não tenham sido detetados motivos razoáveis que constituam fundamento válido de suspeita de fraude, ou essa suspeita não tenha sido comunicada, por escrito, à autoridade judiciária nos termos da lei penal e de processo penal, são devidos ao ordenante juros moratórios, contados dia a dia desde a data em que o utilizador de serviços de pagamento tenha negado que autorizou a operação de pagamento executada, até à data do reembolso efetivo da mesma, calculados à taxa legal, fixada nos termos do Código Civil, acrescida de 10 pontos percentuais, sem prejuízo do direito à indemnização suplementar a que haja lugar.".
Artigo 115.º (Responsabilidade do ordenante em caso de operação de pagamento não autorizada):
"1 - Em derrogação do disposto no artigo 114.º, 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.
2 - O disposto no n.º 1 do presente artigo não se aplica caso:
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.
3 - 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 das obrigações previstas no artigo 110.º, caso em que não são aplicáveis os limites referidos no n.º 1.
4 - Havendo 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.
5 - Se o prestador de serviços de pagamento do ordenante não exigir a autenticação forte do ordenante, este não deve suportar quaisquer perdas relativas a operação de pagamento não autorizada, salvo se tiver agido fraudulentamente.
6 - Caso o beneficiário ou o seu prestador de serviços de pagamento não aceite a autenticação forte do cliente, reembolsa os prejuízos financeiros causados ao prestador de serviços de pagamento do ordenante.
7 - Após ter procedido à comunicação a que se refere a alínea b) do n.º 1 do artigo 110.º, o ordenante não deve suportar quaisquer consequências financeiras resultantes da utilização de um instrumento de pagamento perdido, furtado, roubado ou abusivamente apropriado, salvo em caso de atuação fraudulenta.
8 - Se o prestador de serviços de pagamento não fornecer meios apropriados que permitam a comunicação, a qualquer momento, da perda, furto, roubo ou da apropriação abusiva de um instrumento de pagamento, conforme requerido pela alínea c) do n.º 1 do artigo 111.º, o ordenante não fica obrigado a suportar as consequências financeiras resultantes da utilização desse instrumento de pagamento, salvo nos casos em que tenha agido de modo fraudulento".
Como afirma 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 online na página www.cije.up.pt/revistared), nas situações em que ocorram prejuízos em resultado de operações não autorizadas, antes da notificação ao banco que providencia o serviço ou instrumento de pagamento através de meios electrónicos, a apreciação *"do comportamento do utilizador do serviço de home banking revela-se um fator da maior importância uma vez que é a partir dele que descobrimos quem irá suportar as perdas resultantes de operações fraudulentas"*.
Assim, em todas as situações não imputáveis a título de negligência grave ao utilizador do serviço, 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, supra transcritos) 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 (cfr. Carolina França Barreira, 'Home banking (…), pp. 47/48).
Já nas situações de negligência grosseira do utilizador do serviço, é este quem

suporta 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 50,00€ (art. 115º, nº 4 do RJSPME).
O banco (prestador do serviço) suporta os prejuízos causados pelas debilidades dos sistemas de pagamento que disponibiliza aos seus clientes sempre que as perdas não tenham sido potenciadas por negligência grosseira destes.
Aqui cabe ao banco provar que a operação de pagamento foi devidamente autenticada e, uma vez feita esta prova, compete-lhe ainda provar a contribuição do cliente para os prejuízos ocorridos e o grau de culpa subjacente ao seu comportamento (cfr. Carolina França Barreira, 'Home banking (…), pp. 37 e 62/63).
Caso o não faça, ou seja, caso não prove que o cliente utilizador contribuiu com negligência grave para a ocorrência de operações de pagamento não autorizadas, então deverá o banco suportar a totalidade dos prejuízos (cfr. o Ac. da Relação do Porto de 18.04.2023, in www.dgsi.pt).
No caso dos autos, temos que o banco réu logrou demonstrar que as operações efectuadas não se deveram a avaria técnica ou qualquer outra deficiência do serviço prestado por si (cfr. ponto 33 dos factos provados).
Mais se provou que as operações em causa não foram autorizadas, pese embora tenham sido autenticadas com credenciais de acesso da autora e com a utilização do sistema de autenticação forte do cliente.
Provando-se ainda que as operações realizadas foram autenticadas, registadas e contabilizadas.
Contudo, como já referido, das normas acima transcritas resulta que, no caso de realização de operações de pagamento não autorizadas sobre a conta do cliente através da utilização de serviço de homebanking, com recurso a fraude informática e/ou burla, o banco apenas vê afastada a sua responsabilidade pelos danos sofridos pelo utilizador de serviços de pagamento se alegar e provar que o dano em causa se deveu a actuação dolosa ou negligência grosseira do utilizador do serviço.
Ou seja, o risco inerente à utilização e funcionamento dos serviços de pagamento recai sobre o prestador de serviços, cabendo a este, para se eximir dessa responsabilização, não só provar que a operação de pagamento foi devidamente autenticada (art. 113.º, n.º 1), mas ainda que o utilizador dos serviços de pagamento (ordenante) actuou de forma fraudulenta ou incumpriu de forma deliberada uma ou mais das suas obrigações decorrentes do artigo 110.º ou que actuou com negligência grosseira (art. 113.º, n.º 3 e n.º 4) (cfr. neste sentido, entre outros, o Ac. da Relação de Évora de 24.09.2020, ou o Ac. da Relação do Porto de 12.10.2023, ambos in www.dgsi.pt).
Entende a autora/apelante que não actuou com negligência grosseira, contrariamente ao que foi o entendimento da decisão apelada.
Há que verificar então se estamos perante uma situação em que se possa qualificar a actuação da autora/apelante como grosseiramente negligente.
Considerando que o conceito de negligência grosseira não é densificado no RJSPME, deve buscar-se o mesmo na disciplina geral do direito civil.
A determinação da diligência exigível é feita em abstracto, ie, confrontando a actuação do agente no caso concreto com a actuação que uma pessoa média – o '*bonus pater familias*' – nessa concreta situação teria, e não com a diligência habitual do autor da conduta negligente.
É o que resulta do disposto no art. 487º, n.º 2, do Cód. Civil: "*A culpa é apreciada, na falta de outro critério legal, pela diligência de um bom pai de família, em face das circunstâncias de cada caso".*
Henrique Sousa Antunes, in Comentário ao Código Civil, Direito das Obrigações, UCP, pág. 302 e 303, afirma que *"uma classificação de origem romana distingue as situações de desleixo ou imprudência (negligência) entre culpa grave ou lata, leve e levíssima.(…) A falta de diligência do bom pai de família constitui a culpa leve. A inobservância do cuidado que apenas uma pessoa com diligência acima da média*

revelaria constitui uma culpa levíssima. É culpa grave a atuação que configure uma diligência inferior àquela «que até os homens medianamente negligentes adotam»(Vaz Serra)”.
Também Inocêncio Galvão Telles, in Direito das Obrigações, 6ª edição, pág. 349 e 350, nos diz que *“quer a culpa grave, quer a culpa leve correspondem a condutas que uma pessoa normalmente diligente – o bonus pater familias – se absteria. A diferença entre elas está em que a primeira só por uma pessoa particularmente negligente se mostra susceptível de ser cometida. A culpa grave apresenta-se como uma negligência grosseira (…)”.*
Ou, como se afirma no Ac. da Relação do Porto de 10.01.2023, disponível in www.dgsi.pt: *“um acto qualificável como negligência grosseira, no âmbito da utilização de um sistema bancário electrónico de pagamentos, corresponde a um erro imperdoável, a uma desatenção inexplicável, a uma incúria inaceitável, por referência ao comportamento do comum das pessoas, mesmo daquelas que são pouco diligentes”*.
Assim, para que se considere um acto qualificável como negligência grosseira, é de exigir um nível de falta de cuidado mais elevado, um descuido ou desmazelo inadmissível para qualquer pessoa colocada naquela situação.
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 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 (cfr. Ac. da Relação do Porto de 18.04.2023, acima citado).
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.
Ou seja, quando estivermos perante um 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 (cfr. Ac. da Relação do Porto de 18.04.2023, acima citado).
Como se afirma no Ac. da Relação do Porto de 13.10.2016, in jurisprudência.pt: *“O pharming é uma modalidade de fraude pela qual o utilizador é redirecionado pelo programa de navegação (browser) instalado no seu computador para uma página falsa, em tudo semelhante à verdadeira, quando digitaliza o endereço correto do serviço de banca on-line. Esta modalidade pode ser dirigida, não só a um computador pessoal mas a um servidor DNS (Domain Name System), sendo apelidado de “DNS poisoning”. Neste caso, será atingido um enorme número de utilizadores que digitem o endereço (URL) correto da página de C1…, que automaticamente, por alteração do endereço armazenado no DNS, são redirecionados para a página falsa. É, no essencial, o acesso direto a uma página que, sendo falsa, se pensa ser verdadeira, que carateriza o pharming.*”.
Enquanto o *phishing* consiste no envio de mensagens de correio electrónico, aparentemente provindas da entidade bancária prestadora do serviço, com a finalidade de obtenção de dados confidenciais que permitam ao terceiro aceder ao serviço de pagamento electrónico.
Ambas as técnicas (técnicas fraudulentas que atingem o serviço de *home banking*) *“supõem que o pirata informático tenha acesso à conta de um determinado cliente de um banco através do sistema de banca eletrónica, permitindo-lhe transferir os fundos*

aí inscritos a débito para outras contas. Este acesso não autorizado é conseguido, tanto no phishing, como no pharming, através da utilização das chaves de acesso a este serviço bancário que o próprio cliente do banco forneceu, ainda que inadvertidamente, ao criminoso através da internet." (Cfr. Carolina França Barreira, 'Home banking (…), p. 25).
No caso dos autos, estamos perante uma situação que em tudo nos leva a concluir pela verificação de pharming, pois que quando a autora pretendeu utilizar o serviço (aceder ao site do réu para movimentar valores), surgiu-lhe uma janela, em tudo semelhante à página verdadeira do banco réu, onde era afirmado que estava a decorrer uma actualização.
Com efeito, provou-se que no dia 15 de Novembro de 2023, pelas 18 horas, o AA, ligou o computador para aceder ao site online do banco réu para confirmar e assinar os pagamentos que a CC havia preparado previamente.
Efetuou o login nos canais digitais com o número de adesão ...63, com a inserção correta e à primeira tentativa das credenciais de segurança - código secreto de 6 dígitos.
E entrou no site online do banco réu.
Poucos minutos depois, apareceu no ecrã uma caixa de texto com o logotipo do Banco 1..., SA.
Essa caixa de texto configurava a representação de uma página web igual à do réu.
Nessa caixa de texto constava a informação que o site estava em atualização e que demoraria alguns minutos a ficar concluída, aparecendo um contador de percentagem.
Durante este processo, apareceu uma nova caixa a pedir as coordenadas do cartão matriz para que pudesse concluir eficazmente a atualização, sendo que a imagem através da qual eram pedidos estes dados, era exatamente igual à fornecida habitualmente pelo website do réu.
O AA introduziu os códigos do cartão matriz seis vezes (tantas quantas lhe foram solicitadas).
Por cada uma das seis vezes, foi gerada uma "*one time password push notification"* enviada para o número de telemóvel associado à adesão (...84), conforme se discrimina:
- IMAGEM -

Em todas as notificações "push" recebidas pelo gerente da autora no telemóvel, fez-se referência à confirmação de operações iniciadas no Banco 1... online, sendo as mesmas referentes a transferências internas, pagamentos de serviços ou transferências urgentes ou de grandes montantes.
O gerente da autora não confirmou as operações via notificação "push".
E, em todas as seis vezes, recebeu, no telemóvel associado à adesão, uma chamada da linha de apoio do banco, proveniente do número ...00, fornecendo o código de validação - "*one time password*".
As chamadas da linha de apoio do réu fornecendo o código de validação foram recebidas às 18:32h, 18:41h, 18:46h, 18:51h, 19:00h e 19:05h.
E o gerente da autora accionou os seis códigos de validação recebidos.
Considerando tal factualidade, entendemos que, o cidadão comum, colocado naquela situação, facilmente cairia no logro em que caiu o gerente da autora, convencido de que não lhe estavam a ser pedidos mais do que elementos necessários à actualização em curso.
Com efeito, no caso, o gerente da autora utilizou o computador que sempre utiliza, devidamente protegido por anti-vírus.
Por outro lado, a solicitação das coordenadas do cartão matriz, foram para que pudesse concluir eficazmente a actualização que aparentemente estava em curso, sendo que a imagem através da qual eram pedidos estes dados, era exactamente igual à fornecida habitualmente pelo website do réu.

Assim, tal solicitação surgiu dissimulada no momento em que o gerente da autora ia iniciar as suas operações e, aparentemente, no âmbito da página daquele servidor. Nada fazia crer ao gerente da autora que a página onde veio a introduzir as coordenadas do cartão matriz, não fosse o próprio endereço eletrónico/site do banco. Donde, não poder concluir-se que a actuação do gerente da autora, até esse momento, se traduza num erro indesculpável, em que nenhuma pessoa medianamente sagaz e cuidadosa incorreria.
Por outro lado, o facto de o gerente da autora não ter confirmado as operações via notificação "push", também não pode relevar para a conclusão de uma actuação grosseiramente negligente, considerando que, como resultou provado no ponto 7 dos factos provados, a *"adesão aos canais diretos tem subjacente a entrega ao cliente dos seguintes códigos e coordenadas de segurança:*
…
. Código de Validação de Operação – código de autenticação único, que constituiu a segurança adicional, enviado por SMS ou, alternativamente, por chamada de voz, composto por seis dígitos, não alterável nem reutilizável (one time password), gerado no momento e enviado por notificação para o telemóvel configurado para a receção destes códigos". (sublinhado nosso), e a verdade é que, para além das mensagens "push", o gerente da autora também recebeu, logo de seguida, em todas as seis vezes, no telemóvel associado à adesão, uma chamada da linha de apoio do banco, proveniente do número ...00, fornecendo o código de validação - *"one time password".*
Ou seja, sendo alternativa a possibilidade de receber o código de validação de operação, por sms, ou por chamada de voz, e tendo as chamadas de voz ocorrido cerca de 1 minuto depois de cada uma das sms, não pode considerar-se que o comportamento do gerente da autora, ao não confirmar as operações via notificação "push", mas antes utilizando os códigos que lhe foram fornecidos por via telefónica, proveniente da linha de apoio do banco réu, se traduza num erro indesculpável, em que nenhuma pessoa medianamente sagaz e cuidadosa incorreria.
É que, para além de tudo o resto, as chamadas efectuadas foram provenientes da linha de apoio do banco réu, o que se mostra suficiente para que o gerente da autora pudesse confiar não ser necessário a confirmação das operações via notificação "push", mas antes, através do accionamento dos códigos que lhe foram fornecidos por via telefónica.
A tal acresce que, a técnica de *pharming* é mais difícil de ser detectada do que o *fishing*. Com ela, as páginas fraudulentas são muitas vezes iguais às páginas do banco e identificadas como ligações seguras, pelo que, a censura que se possa atribuir ao utilizador poderá ser aqui bem diferente da que se exerce nas situações de *fishing*.
Acresce ainda que, os alertas de segurança emitidos pelo banco réu, não versavam sobre situação idêntica à que ocorreu nos autos.
E, como se afirma no Ac. da Relação do Porto de 13.10.2016, já acima citado: *"Não é rigorosamente cindível o que constitui o sistema informático interno do Banco servidor e o conjunto do sistema que permite a utilização do serviço de homebanking, já que aquele conta necessariamente com os meios de acesso que os clientes têm que utilizar, como sejam computadores e telemóveis. Sendo estes indispensáveis, o serviço depende de todos eles. A acção fraudulenta aproveita-se não apenas da debilidade dos terminais que o cliente utiliza e da maior ou menor ingenuidade de cada um, mas também das insuficiências que ainda vão persistindo no sistema informático bancário para a prevenir e eliminar.*
Não obstante saber-se que as novas tecnologias têm contribuído para melhorar progressivamente o seu funcionamento, é do conhecimento geral o surgimento de novas formas de contaminação dos serviços de C1… por fishing e pharming, surpreendendo os servidores e os clientes nas mais diversas ocasiões.
Estão, por isso, os prestadores do serviço adstritos a prestar de forma apelativa e

clara, pelas formas mais adequadas, especialmente na própria página do serviço, através de caixas que o cliente deve fechar para prosseguir na ação desejada, as informações necessárias a prevenir o logro de cada um. Não basta avisar que há fraude no serviço C1…; deve ser explicitada cada uma das formas utilizadas pelos hackers e o modo como o cliente deve evitar o engano.
O cliente não deve ser surpreendido com uma forma nova e desconhecida de intrusão e recolha abusiva e eficaz de dados, sem revelação de códigos pessoais e outros elementos secretos, se o Banco já a conhecia e não a anunciou adequadamente na página do serviço ao longo do tempo em que é sabido estar a ser utilizada por hackers.
A prevenção do prejuízo emergente daquele tipo de ações é uma campanha que compete aos Bancos realizar de modo a que chegue rápido e eficazmente aos seus clientes de C1….".
Assim, resulta para nós claro, dos factos provados, que a autora não agiu deliberadamente em prejuízo do réu e que forneceu os referidos dados convencida de que o fazia a pedido do serviço de homebanking do réu, para concluir as actualizações que pensava estarem em curso.
Não há na actuação da autora, uma falta indesculpável, que só uma pessoa especialmente negligente, descuidada e incauta deixaria de observar.
E, só a violação deliberada do dever de sigilo dos dados pessoais e intransmissíveis ou a negligência grosseira da autora permitiriam o afastamento da responsabilidade o Banco.
Ora, como se afirma no Ac. da Relação de Lisboa de 11.04.2019, in dgis.pt: "*… o legislador faz recair sobre o banco a prova de que as operações de pagamento não foram efectuadas por avarias técnicas ou quaisquer outras deficiências, não bastando, para o efeito, socorrer-se do registo da operação de molde a demonstrar que ela foi autorizada pelo ordenante, tendo ainda de demonstrar que o cliente agiu de forma fraudulenta, ou não cumpriu deliberadamente ou por negligência grave algumas das suas obrigações previstas no artº 67º do DL 242/2012.*
A opção pelo afastamento do ónus da prova a cargo do consumidor quanto ao mau funcionamento do sistema informático de homebanking, resulta da circunstância de ser o prestador de serviços de homebanking quem tem maior facilidade em demonstrar a versão factual que lhe aproveita, ou seja, a de que a utilização fraudulenta do serviço de homebanking por parte de terceiros não se deveu ao mau funcionamento do sistema informático.
No fundo, o legislador entendeu que o prestador de serviços é quem está em melhores condições, do que qualquer outro (incluindo o consumidor), para trazer a factualidade demonstrativa do modo como as coisas se passaram. E é assim, porque o funcionamento do "sistema informático" homebanking "pertencente à sua esfera de risco", funcionando como critério suplementar de distribuição do ónus da prova, ou, melhor dizendo, ao "círculo de vida" em que o facto se produz: é a consagração da denominada teoria das esferas de risco, que preconiza uma ligação umbilical entre o ónus da prova e a dicotomia obrigações de meios/obrigações de resultado. (Cf. Hugo Luz dos Santos, "Plaidoyer por uma distribuição dinâmica do ónus de prova…", cit., pág. 21 e segs.)."
Entendemos pois, que não pode ser qualificada a actuação do gerente da autora como negligência grosseira, concluindo-se assim, pela revogação da decisão proferida quanto à responsabilidade do banco, e consequente obrigação de repor o montante transferido indevidamente da conta da autora, no valor de €104.944,00 (€ 104.994,00 - €50,00).
Procede, pois, a apelação.

*

VI. Decisão.

Perante o exposto, acordam as Juízes que constituem este colectivo da 3ª Secção

Cível do Tribunal da Relação de Guimarães em julgar procedente a apelação, em consequência do que revogam a sentença apelada, condenando o réu a repor o montante transferido indevidamente da conta da autora, no valor de €104.944,00. Custas da acção e da apelação, por autora e réu, na proporção dos respectivos decaimentos.

*

Guimarães, 2 de Abril de 2025

Assinado electronicamente por:
Fernanda Proença Fernandes
Anizabel Sousa Pereira
Elisabete Moura Alves
(O presente acórdão não segue na sua redacção as regras do novo acordo ortográfico, com excepção das “citações/transcrições” efectuadas que o sigam)