jurisprudência.pt

Tribunal da Relação de Guimarães
Processo nº 141/23.6T8VVD. G1

Relator: ANTÓNIO BEÇA PEREIRA
Sessão: 11 Junho 2025
Número: RG
Votação: UNANIMIDADE
Meio Processual: APELAÇÃO
Decisão: APELAÇÃO IMPROCEDENTE

RESPONSABILIDADE BANCÁRIA **HOMEBANKING**

NEGLIGÊNCIA GROSSEIRA

Sumário

1. Na negligência grosseira o agente atua sem o mais elementar senso comum, de modo manifestamente descuidado e imprudente, omitindo infundadamente precauções ou cautelas que num particular contexto são objetivamente básicas.
2. Atua com negligência grosseira o cliente de uma instituição bancária que, no âmbito do homebanking, recebeu um telefonema, que acreditou ser do seu banco, informando-o que "alguém estaria a tentar aceder à sua conta bancária", que a seguir recebe duas mensagens de texto no seu telemóvel, com a indicação de proveniência desse banco, dizendo-lhe "para confirmar a aprovação de pagamento com cartão ao comerciante EMP01... no valor de 2.800,00 EUR, introduza o código ...67" e "para confirmar levantamento MBWAY introduza o código ...70" e que, sem mais, introduz estes códigos e quando no seu serviço de homebanking o banco avisa os utilizadores, além do mais, que «existem tentativas de "Phishing" que recorrem a um esquema fraudulento de mensagens SMS e chamadas telefónicas supostamente em [seu] nome» e para terem "cuidado com SMS e telefonemas fraudulentos supostamente em [seu] nome".

Texto Integral

Acordam no Tribunal da Relação de Guimarães

I
AA instaurou a presente ação declarativa, que corre termos no Juízo Local Cível de Vila Verde, contra a Banco 1... S.A., formulando os pedidos de:

"*i. Ser a Ré condenada a restituir à Autora a quantia de € 2,900.00 (dois mil e novecentos euros), acrescida de juros de mora, à taxa de 4%, vencidos que se computam hoje em € 28.92 (vinte e oito euros e noventa e dois cêntimos), e os vincendos até à data do efetivo e integral ressarcimento;*
ii. Ser a Ré condenada a pagar à Autora a título de indemnização por danos morais, a quantia nunca inferior a € 3,000.00 (três mil euros), acrescida de juros de mora à taxa legal em vigor a contar da citação até efetivo e integral pagamento."
Alegou, em síntese, que foi movimentada da sua conta bancária a quantia de 2.900,00 € e que "*o serviço home banking prestado pela a aqui Ré, é da sua inteira responsabilidade e que, por isso mesmo, deve a Ré assumir os riscos de uma provável intrusão no sistema informático, da sua propriedade.*"
A ré contestou dizendo, em suma, que "*cumpriu integralmente todas as obrigações contratuais a que se vinculou perante a A., sendo que, os alegados danos só ocorreram por culpa única e exclusiva da A. inexistindo, como tal, qualquer obrigação de indemnizar*".

Realizou-se a audiência de julgamento e após foi proferida sentença em que se decidiu:
"*Em face do exposto e nos termos das disposições legais supra citadas, julga-se a presente ação integralmente improcedente, por não provada e, em consequência, absolve-se a ré de todos os pedidos formulados pela autora.*"

Inconformada com esta decisão, dela a autora interpôs recurso findando a respetiva motivação, com as seguintes conclusões:
1. Como supra se revelou, não pode a Recorrente conformar-se com a sentença recorrida.
2. Em caso de operação de pagamento não autorizada, a responsabilidade do prestador de serviços de pagamento encontra-se plasmada no artigo 114.º, n.º 1 do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (doravante, RJSPME).
3. Veja-se neste sentido o Acórdão do Tribunal da Relação de Lisboa, de 20/02/2024, processo n.º 6029/23.3T8LSB.L1-7, "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, provar que (i) a

operação de pagamento foi devidamente autenticada (art.º 113.º, n.º 1, do Decreto-lei n.º 91/2018, de 12.11), (ii) não foi afetada por qualquer avaria técnica ou por outra deficiência relacionada com o serviço de pagamento por si prestado (Artigo 114.º, n.º 9), mas ainda que (iii) o utilizador dos serviços de pagamento (ordenante) atuou de forma fraudulenta ou incumpriu de forma deliberada uma ou mais das suas obrigações decorrentes do artigo 110.º ou que atuou com negligência grosseira (art.º 113.º, n.º 3 e n.º 4)".
4. E o Acórdão do Tribunal da Relação do Porto, de 16/05/2023, proc. n.º 659/22.8T8PNF.P1, "a entidade bancária só não será responsabilizada pelas perdas, sofridas pelo cliente, decorrentes de operações fraudulentas sobre a conta deste, no âmbito do homebanking, se alegar e provar que o dano resultou de atuação dolosa ou grosseiramente negligente do utilizador do serviço".
5. Relativamente à autenticidade da operação de pagamento, considerando que o atual artigo 113.º, n.ºs 1 e 3 corresponde ao revogado artigo 70.º, n.ºs 1 e 2 do DL n.º 317/2009, importa fazer menção à doutrina de Carolina França Barreira, Homebanking: A Repartição dos Prejuízos Decorrentes de Fraude Informática.
6. No que concerne à negligência grosseira, esta ocorre quando o grau de reprovação ultrapassa a mera censura que merece a simples imprudência, irreflexão ou o impulso leviano, quando é alcançado um elevado grau de desleixo e incúria, onde não são observadas as regras elementares de prudência e de diligência minimamente exigíveis, correspondendo ao erro imperdoável, à desatenção e incúria indesculpável, à chamada culpa grave, vistos em confronto com o comportamento comum das pessoas.
7. A negligência grosseira diz respeito ao comportamento que nunca seria adotado pela generalidade dos utilizadores dos serviços de pagamento colocados perante as concretas circunstâncias do caso.
8. Ora, atento os factos dados como provados sob os números 5, 6, 7, 8, 9, 10, 11, 14, 15, 17, 18, 23 e 26 supra descritos, não age de forma grosseiramente negligente a pessoa que, no âmbito do homebanking, fornece os seus dados confidenciais na sequência do recebimento de uma chamada ou de uma mensagem, que tudo indicava ser proveniente da Recorrida (como provado nos autos), pelo mesmo canal emissor através do qual já tinha recebido outras chamadas e outras mensagens.
9. Ainda que a Recorrente tenho fornecidos os códigos para levantamento MBWAY e para aprovação de pagamento com cartão, tal não é suficiente para se considerar que a sua conduta foi grosseiramente negligente e que a sua atuação assume um elevado grau de descuido e censurabilidade, tendo em conta que a Recorrente limitou-se a atuar perante uma chamada e várias

mensagens que tudo indicava serem provenientes da Recorrida, visto que já tinha recebido outras, verdadeiras e fidedignas, nunca tendo desconfiando tratar-se de outro emitente que não a Recorrida.
10. A Recorrente acreditou que se tratava real e efetivamente de uma chamada e de mensagens da autoria dos serviços da Recorrida.
11. Toda esta situação não é suscetível de chamar a atenção da Recorrente no sentido de a levar a desconfiar da proveniência da chamada e das mensagens, não lhe sendo censurável a introdução dos dados solicitados, nem esses factos são suficientes para provar que, ao introduzi-los, a Recorrente tenha atuado de forma diferente do que seria exigível ao utilizador comum nestas circunstâncias concretas.
12. Considerando a idade, grau de conhecimento e a vulnerabilidade que a Recorrente está exposta, não seria expectável que a mesma diligenciasse de forma diferente, pelo que o comportamento da Recorrente não pode ser qualificado como grosseiramente negligente.
13. Com efeito, a Recorrente forneceu os seus dados/informações (confidenciais) àquela que acreditava ser a sua instituição bancária, visto que recebeu a indicação por parte da instituição (sendo, na verdade, um terceiro) de que alguém estaria a tentar aceder à sua conta bancária, bem como lhe foi dito, também pelo terceiro que se estava a fazer passar pela instituição, que iriam proceder à realização de operações bancárias, tendo esta de lhe fornecer os códigos que iria receber no seu telemóvel.
14. In casu, a Recorrida, que deve proteger os interesses dos seus clientes, deveria ter bloqueado as operações efetuadas, ou pelo menos, a transferência bancária no valor de € 2.800,00 (dois mil e oitocentos euros), visto que era uma operação bastante acima da média, tendo em consideração todas as transações/movimentações já efetuadas pela Recorrente e, como não o fez, todas as transferências deveriam poder ser canceladas no prazo de pelo menos 24 horas.
15. Também a Recorrida deve bloquear temporariamente transferências efetuadas para contas abertas recentemente ou localizadas noutros países com elevada incidência de fraudes, até que as próprias transações sejam investigadas ou reclamadas num prazo razoável.
16. Na verdade, ainda que resulte provado que a Recorrida publica no seu site público várias informações relativas a burlas e esquemas fraudulentos, todos desconhecem se esses esquemas/burlas estão realmente a ser evitados e em que quantidade, isto é, se basta informar os clientes através do seu site/aplicação para que tudo isto possa ser evitado e, na eventualidade de não o ser, se se pode imputar a responsabilidade aos clientes mediante negligência grosseira e não à própria instituição financeira.

17. Impende sobre a Recorrida um dever de se pautar por um critério de diligência no interesse e segurança nas aplicações dos seus clientes, tal como é disposto no artigo 75.º do DL n.º 298/92, de 31 de dezembro e também um dever de assegurar níveis de competência técnica e garantir condições adequadas, eficientes e de qualidade aos seus clientes, nos termos do artigo 73.º do mesmo diploma.
18. Pois bem, o terceiro que se fez passar pela Recorrida apenas o conseguiu fazer com sucesso em virtude da vulnerabilidade no acesso ao sistema informático da Recorrida.
19. Segundo o Acórdão do Tribunal da Relação de Lisboa, Processo n.º 15455/20.9T8LSB.L1-6, "resulta das boas regras de conduta impostas por lei aos bancos (arts. 73.º a 75.º do RGICSF) que os serviços de pagamento presenciais ou eletrónicos prestados aos seus clientes, deve ser, não só de qualidade e eficiente, mas também serviço seguro…". "Ao prestador dos serviços bancários cabe, pois, por lei, assegurar a qualidade e segurança do sistema que permita movimentar a conta apenas a quem tem legitimidade, depositando, levantando ou transferindo fundos. O risco de funcionamento deficiente ou inseguro do sistema de prestação de serviços de pagamento ou transferência localiza-se, portanto, na esfera do seu prestador, a quem incumbe a responsabilidade por operações não autorizadas pelo cliente nem devidas a causa imputável ao cliente".
20. Não é concebível que a Recorrente, que confiou na sua instituição bancária, isto é, a Recorrida, tenha de arcar com as consequências (no caso financeiras), provenientes da incapacidade da Recorrida de assegurar a intangibilidade de terceiros que criam programas falsos para enganar os clientes das instituições financeiras, como sucedeu com a Recorrente, aliás, vicissitudes essas que lhe são inteiramente arredadas e alheias à sua responsabilidade.
21. Como resulta dos factos dados como provados sob os números 5, 6, 7, 8, 9, 10, 11, 14, 15, 17, 18, 23 e 26, não se pode imputar à Recorrente um comportamento grosseiramente negligente, porquanto foi a mesma induzida em erro.
22. A negligência que eventualmente se pode imputar pela conduta da Recorrente é, quanto muito, uma negligência inconsciente e leve, nunca grave ou grosseira.
23. Não estamos, claramente, perante uma chamada culpa grave nem tão pouco um erro imperdoável, desatenção ou incúria indesculpável.
24. Pelo exposto, deve o presente recurso ser julgado procedente e ser a sentença recorrida revogada e substituída por outra que condene a recorrida no pagamento da quantia de € 2.900,00 (dois mil e novecentos euros),

acrescida de juros de mora vencidos e vincendos, à taxa legal de 4%, até à data do efetivo e integral ressarcimento, e a título de indemnização por danos não patrimoniais, a quantia nunca inferior a € 3.000,00 (três mil euros), acrescida de juros de mora à taxa legal em vigor a contar da citação até efetivo e integral pagamento.
A ré contra-alegou sustentado a improcedência do recurso.
As conclusões das alegações de recurso, conforme o disposto nos artigos 635.º n.º 4, 637.º n.º 2 e 639.º n.os 1 e 2 do Código de Processo Civil[1], delimitam os poderes de cognição deste Tribunal e, considerando a natureza jurídica da matéria versada, as questões a decidir consistem em saber se a ré agiu com negligência grosseira e se, na negativa, deve ser julgado procedente o pedido.

II
1.º
Estão provados os seguintes factos:
1. No dia 24 de novembro de 2016, a autora e a ré celebraram um acordo designado "*Contrato de Adesão ao Serviço ...*".
2. No âmbito do acordo referido em 1), a ré facultou à autora o serviço ... através de quatro canais distintos: telefone, internet, mobile e SMS, e ativou as funcionalidades Cash-advance, MB NET, transferências internacionais, pagamento cartão de crédito extra património, requisição de cheques, operações de bolsa e fundos, mobilização de depósitos e acesso base.
3. Por via do acordo referido em 1), a autora passaria a conseguir aceder à sua conta bancária através do seu telemóvel ou de um computador através de acesso à internet e esses serviços ficaram associados às contas bancárias de que a autora é titular, abertas na ré, designadas conta ... com o n.º ...00 e conta ... com o n.º ...27. 4. A partir da celebração do acordo referido em 1), a ré atribuía à autora um cartão matriz de coordenadas acompanhado de um código e de um elemento de identificação ambos secretos.
5. No dia 09.11.2022, a autora recebeu no seu telemóvel várias chamadas telefónicas com indicação do número ...90.
6. O número de telefone ...90 pertence à ré.
7. Cerca das 13:13 horas do dia 09.11.2022, após três tentativas de chamada com indicação do número ...90, a autora atendeu o telefone e então foi-lhe referido que alguém estaria a tentar aceder à sua conta bancária.
8. Cerca das 13:13 horas, a autora recebeu, o seu telemóvel, uma mensagem de texto com indicação de proveniência de "Banco 1..." dizendo "*Para confirmar Associação de Dispositivo ao contrato, introduza o código ...05*", tendo-lhe sido posteriormente pedido o código nela inscrito.
9. Nas circunstâncias temporais referidas em 7), a autora encontrava-se a

trabalhar e assustada, acedeu à aplicação ... para verificar o saldo da sua conta bancária e foi advertida para encerrar essa aplicação no telemóvel para dessa forma conseguir evitar uma alegada burla.
10. Após, a autora recebeu uma nova mensagem de texto no seu telemóvel com a indicação de proveniência "*Banco 1...*" com o seguinte conteúdo "*para confirmar a aprovação de pagamento com cartão ao comerciante EMP01... no valor de 2.800,00 EUR, introduza o código ...67*".
11. Após, a autora recebeu uma nova mensagem de texto no seu telemóvel com a proveniência "*Banco 1...*" com o seguinte conteúdo "*Para confirmar levantamento MBWAY introduza o código ...70*".
12. Após nova consulta à sua conta bancária através da aplicação no seu telemóvel, a autora verificou que a quantia de € 1.800,00 que possuía na sua conta poupança ... n.º ...27 tinha migrado para a sua conta bancária n.º ...00 tendo esta, em altura anterior a este episódio, cerca de € 1.200,00.
13. A operação bancária referida em 11) culminou com a retirada de € 100.00 da conta bancária da autora.
14. Ao consultar o seu saldo bancário, a autora apercebeu-se que as quantias referidas em 10) e em 13) tinham sido subtraídas dessa conta bancária.
15. Cerca das 20:40 horas do dia 09.11.2022, a autora contactou a linha de apoio da ré de forma a expor e a tentar perceber o sucedido por os movimentos bancários terem sido realizados sem a sua intenção.
16. A informação prestada pelo operador da ré através da chamada telefónica referida em 15) apontou a responsabilidade da subtração das quantias monetárias à autora.
17. Aquando da chamada telefónica referida em 7), a autora acreditou que estaria a ser contactada pela ré.
18. Perante a situação referida em 16), no dia 11.11.2022, a autora tentou obter informações junto do balcão da ré, sito no Largo ..., em ..., balcão onde se encontra sediada a sua conta bancária, foi-lhe confirmada a transferência dos montantes referidos em 10) e em 13) e a autora requereu o cancelamento desses movimentos bancários, tendo-lhe sido informado que não era possível cancelar esses movimentos por esses montantes já terem sido creditados em conta que a ré não conseguia descortinar.
19. A autora apresentou reclamação por escrito no balcão da ré identificado em 18).
20. Em resposta à reclamação referida em 19), em 17.11.2022, a ré enviou um e-mail à autora por via do qual concluiu que os débitos referidos em 10) e em 13) eram "*da responsabilidade do cliente*".
21. Por carta datada de 18.11.2022, a ré respondeu à reclamação da autora, informando que "*o pedido de regularização não foi aceite, considerando o*

cliente responsável pelo(s) movimento(s) apresentados".
22. A autora apresentou uma participação criminal junto da Guarda Nacional Republicana, no Posto Territorial ..., a qual foi autuada com NUIPC 003356/22.....
23. Com os movimentos referidos em 10) e em 13), a autora ficou com dificuldades em pagar as suas despesas mensais.
24. Com a privação das quantias referidas em 10) e em 13), a autora sentiu angustia.
25. No dia 09.11.2022, a autora acedeu à aplicação ... através do seu telemóvel com o n.º ...73, para o que teve de proceder à sua autenticação.
26. Depois de aceder à aplicação ..., pelas 13:13 horas, a autora efetuou a associação do seu dispositivo móvel ao acordo referido em 1), operação exigida por razões de segurança e essa associação só é operada depois de a autora introduzir o código SMS Token que lhe foi remetido para o seu telemóvel, no caso, o código ...05, código que a autora introduziu e que permitiu a associação desse equipamento móvel ao contrato referido em 1).
27. Após a autora efetuar o procedimento referido em 26), foi transferido o saldo no valor de € 1.800,00 de uma aplicação para a conta de depósitos à ordem, ambas tituladas pela autora, a fim de provisionar a conta de depósitos à ordem associada ao seu cartão.
28. Pelas 13:36 horas desse dia, foi efetuada uma compra online no valor de € 2.800,00 e para o seu pagamento foi utilizado o cartão bancário da autora, com indicação do número, titularidade e código do cartão.
29. Por razões de segurança e para validação da operação referida em 28), a ré exige o acesso à ..., o que pressupõe a sua autenticação mediante a inserção do número de contrato e código pessoal secreto e, depois de autenticado o acesso da autora à ..., foi validado o movimento referido em 10) e em 28) com a confirmação e inserção do código SMS Token remetido por SMS para o telemóvel da autora associado ao acordo referido em 1), tendo a autora fornecido a terceiro esse código ...67, o que permitiu a validação dessa operação.
30. Após a operação referida em 29), a autora acedeu novamente, através do seu telemóvel, à aplicação ..., autenticando-se e então, através da aplicação MBWAY, foi ordenada a emissão de um código para permitir a outrem o levantamento, junto de uma qualquer ATM, da quantia de € 100,00, para cuja validação foi exigida pela ré a introdução de um código SMS Token enviado por SMS para o telemóvel da autora e a autora forneceu a outrem o código ...70, o que permitiu a validação dessa operação.
31. Perante a autenticação no serviço ... pela autora e validação das operações referidas em 29) e em 30) com a introdução dos respetivos códigos SMS

Token, a ré recebeu instrução para realização dessas operações bancárias.
32. Os SMS token referidos em 29) e em 30) foram enviados para o telemóvel da autora com a indicação concreta dos movimentos a que se destinavam e do valor das operações que se pretendia confirmar nos termos referidos em 10) e em 11).
33. As operações referidas em 29) e em 30) foram autenticadas e validadas, registadas e contabilizadas sem terem sido afetadas por avaria técnica ou por qualquer outra deficiência de funcionamento dos serviços da ré.
34. O contacto telefónico referido em 5) não foi efetuado pela ré.
35. Os movimentos referidos em 29) e em 30) só foram concretizados por a autora ter rececionado dois distintos SMS com o respetivo código SMS Token, mensagem que indicava que se destinava à confirmação dos movimentos referidos em 10) e em 11), indicava a sua natureza e valor e esses movimentos concretizaram-se por a autora ter fornecido a outrem aqueles códigos permitindo a confirmação dessas operações, a que acresceu a prévia fidelização do seu equipamento.
36. As operações referidas em 29) e em 30) não teriam sido concretizadas se a autora não tivesse fornecido a terceiro os códigos SMS Token referidos em 35).
37. Do acordo referido em 1) consta que "*a adesão ao serviço ... foi precedida da entrega das* "*Recomendações de Segurança e Utilização do ... através da internet*", *cujo teor leu e entendeu*".
38. A ré tem publicado, desde data não concretamente apurada, no seu site público (Banco 1....pt) a seguinte informação:
"*Existem tentativas de* "*Phishing*" *que recorrem a um esquema fraudulento de mensagens SMS e chamadas telefónicas supostamente em nome da Banco 1..., passíveis de comprometer a privacidade e a segurança dos nossos Clientes.*
Os destinatários deste esquema fraudulento recebem chamadas telefónicas com suposta origem na Banco 1.... O burlão alega que existem operações fraudulentas para cancelar e para tal recolhe do cliente dados pessoais e confidenciais, os quais concretizam a fraude.
Nos telefonemas, os burlões apresentam-se falsamente como colaboradores da Banco 1..., procuram recolher códigos de autorização para validação ilícita de operações bancárias em nome dos Clientes vítimas do esquema fraudulento.
Desconfie de mensagens/chamadas que não solicitou. Nunca forneça dados confidenciais e bancários em resposta a mensagens (ex. SMS, e-mail) ou telefonemas fraudulentos, mesmo que possam parecer ter origem supostamente na Banco 1....
Lembre-se sempre:
Não aceda à Banco 1... através de links em mensagens de email, SMS,

endereços gravados nos "Favoritos" ou no "Histórico", nem através de anúncios ou outros resultados de pesquisas internet.
Digite sempre o endereço ... no seu browser, e confirme o certificado digital da Banco 1.... Proteja-se online e preserve as suas credenciais e os seus dados pessoais.
Suspeite da origem e do teor de mensagens e chamadas não solicitadas, e nunca forneça dados confidenciais e bancários em resposta às mesmas. Se adequado, contacte diretamente a entidade em causa através de um meio de contacto confiável.
Para sua proteção, não aceda a links enviados por SMS ou e-mail.
Suspeite sempre de links e ficheiros em mensagens eletrónicas. Um email, um SMS ou uma notificação nas redes sociais, cuja origem lhe pareça familiar, pode ter propósitos fraudulentos!
Suspeite sempre de mensagens que lhe peçam qualquer ação ou interação urgente. Não responda, não clique nos links nem abra anexos dessas mensagens.
Nunca valide a adesão a serviços ou operações bancárias que não solicitou, nem forneça incautamente, num qualquer esquema fraudulento quaisquer dados de validação que lhe sejam eventualmente dirigidos por SMS ou por outra via".
39. Desde agosto de 2008, a ré apresenta, sistematicamente, aos clientes sob a forma de janela do tipo *pop up*, na página de autenticação do serviço (página de login), informação de segurança, alertando os clientes para os riscos de fraude de que os mesmos podem ser alvo.
40. Os utilizadores da ... têm recomendações na página de login, não sendo possível fazer login sem fechar essa janela, com a seguinte mensagem: "*Cuidado com SMS e telefonemas fraudulentos supostamente em nome da Banco 1...*" e "*Nunca clique em hiperligações (links) enviados por SMS com origem num contacto desconhecido e nunca responda a SMS a solicitar os seus dados pessoais. Antes de validar uma operação, confira sempre os dados enviados na mensagem SMS, nomeadamente montante e destinatário*".
41. A ré publica ainda as seguintes recomendações de segurança na página de autenticação da ... que são apresentadas em cada login:
"*A Banco 1... não envia SMS a simular transações*"; "*Quando recebe um SMS é porque é real. Se não foi registada por si, é FRAUDE*"; "*Para evitar fraudes digite sempre ...*".
42. No âmbito do acordo referido em 1), a autora e a ré acordaram que "*para o Nível de serviço contratado está(ão) previsto(s) o(s) seguinte(s) Elemento(s) de Validação de movimentação de contas: Matriz e SMS Token*".
43. A ré mantém alertas de segurança constantes dirigidos aos seus clientes

através das conhecidas páginas *pop up* que os obriga a ler, sob pena de bloqueio e interrupção da ação pretendida.
44. O sistema informático da ré dispõe de vários níveis de Firewall, sistemas de prevenção de intrusão monitorizados 24 horas por dia, 7 dias por semana, sistemas de antivírus.
45. No dia 15.11.2022, a ré efetuou um crédito no montante de € 2.800,00 na conta bancária da autora, correspondente ao reembolso provisório que a ré efetua quando analisa reclamação referente a movimentos com cartão.
46. No dia 18.11.2022, a ré efetuou o débito do montante de € 2.800,00 na conta bancária da autora por ter concluído pela sua responsabilidade na realização desse movimento, o que foi comunicado à autora através da carta referida em 21).
47. Das Condições Gerais de Abertura de Conta e Prestação de Serviços do acordo referido em 1) consta, designadamente que:
- "*Os elementos de identificação e de validação são pessoais e intransmissíveis, devendo apenas ser do exclusivo conhecimento do titular*" (cláusula 48.º, n.º 1 das condições gerais);
- "*O titular obriga-se a garantir a segurança dos elementos de identificação e de validação, bem como a sua utilização estritamente pessoal e intransmissível, designadamente não entregando nem permitindo a sua utilização por terceiro, ainda que seu procurador ou mandatário; não os revelando nem, por qualquer forma, os tornando acessíveis ao conhecimento de terceiros*" (cláusula 48.º, n.º 2, alíneas a) e b) das condições gerais);
- "*Salvo estipulação escrita das partes em contrário, quando admissíveis, qualquer ordem não poderá ser revogada depois de recebida pela Banco 1…*" (cláusula 53.º, n.º 4 das condições gerais);
- "*O titular deverá respeitar as recomendações e orientações de segurança relativas à utilização do …, e, em especial, quando admissíveis, as aplicáveis aos pagamentos a realizar através da Internet, incluindo as que lhe são disponibilizadas previamente à subscrição da proposta de adesão ao …, bem como as que, em cada momento, lhe forem divulgadas pela Banco 1…*" (cláusula 54.º das condições gerais).
2.º
Como disse a Meritíssima Juiz, e é aceite pelas partes, "*a presente ação, tal como vem definida pelo pedido e pela causa de pedir, assenta na responsabilidade da ré pela violação dos deveres contratuais e, por essa razão, enquadra-se no âmbito da responsabilidade civil contratual, visando apurar se a ré é responsável pela restituição das quantias saídas da conta bancária da autora por via do serviço homebanking por si disponibilizado.*"
Atendendo aos considerandos acerca do *homebanking* e ao enquadramento

jurídico do mesmo decorrente dos artigos 108.º, 110.º, 111.º, 113.º, 114.º e 115.º do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (Decreto-Lei 91/2018, de 12 de novembro) que figuram na decisão recorrida, é inútil estar aqui a repetir o que aí já foi dito.
O tribunal *a quo* afirmou, e as partes também aceitaram esse segmento, que "*a instituição bancária, enquanto prestador do serviço, suporta os prejuízos causados pelas debilidades dos sistemas de pagamento que disponibiliza aos seus clientes sempre que tais perdas não tenham sido causadas por negligência grosseira destes*".
E a ré veio a ser absolvida por se ter entendido "*que a realização das operações bancárias supra referidas no montante global de € 2.900,00 apenas pode ser imputada à autora a título de negligência grosseira*".
Mas a autora discorda e defende que dos "*factos dados como provados sob os números 5, 6, 7, 8, 9, 10, 11, 14, 15, 17, 18, 23 e 26 supra descritos,* [resulta que] *não age de forma grosseiramente negligente*". Por isso, a ré deve ser condenada "*no pagamento da quantia de € 2.900,00* (…)*, e a título de indemnização por danos não patrimoniais,* [n]*a quantia nunca inferior a € 3.000,00* (…)*, acrescida*[s] *de juros de mora*".
Contrapõe a ré afirmando que "*perante esta factualidade entendeu a Meritíssima Juiz a quo - e muitíssimo bem, a nosso ver - que o comportamento da Autora aí descrito consubstanciava uma negligência grosseira*".
Vejamos.
A "*culpa em sentido estrito ou negligência* (…) *consiste no simples desleixo, imprudência ou inaptidão*"[2]; "*na omissão da diligência exigível do agente*"[3]. E "*quer a culpa grave (que também se diz culpa lata) quer a culpa leve correspondem a condutas de 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 suscetível de ser cometida. A culpa grave apresenta-se como uma negligência grosseira* (…)*. A culpa levíssima, essa seria a que apenas uma pessoa excecionalmente diligente conseguiria evitar.*"[4]
Ora, "*a negligência grosseira, correspondendo a uma culpa grave, pressupõe que a conduta do agente – porque gratuita e de todo infundada – se configure como altamente reprovável, à luz do mais elementar senso comum.*"[5] Há nela uma "*omissão dos deveres de cuidado que só uma pessoa especialmente negligente, descuidada e incauta deixaria de observar*"[6]. Na verdade, na negligência grosseira encontramos um "*elevado grau de inobservância do dever objetivo de cuidado e de previsibilidade da verificação do dano ou do perigo, configurando uma omissão fortemente indesculpável das precauções*

ou cautelas mais elementares"[7]. Em suma, na negligência grosseira o agente atua sem o mais elementar senso comum, de modo manifestamente descuidado e imprudente, omitindo infundadamente precauções ou cautelas que, num particular contexto, são objetivamente básicas.
E, "*desde que a lei não estabeleça outro critério, a culpa será apreciada, em face das circunstâncias de cada caso, pela diligência de um bom pai de família ou homem médio («in abstracto»)*"[8], contendo o n.º 2 do artigo 799.º, no âmbito da responsabilidade contratual, "*uma remissão para o artigo 487.º n.º 2, estabelecendo a unidade do critério da apreciação da culpa em todo o sistema da responsabilidade civil, seja de natureza extraobrigacional ou obrigacional.*"[9]
Voltando ao nosso caso, vemos que a autora recebeu um telefonema e "*acreditou que estaria a ser contactada pela ré*". Então, sob a alegação de que "*alguém estaria a tentar aceder à sua conta bancária*", depois de receber a mensagem descrita no facto 8, a autora recebeu uma nova mensagem de texto no seu telemóvel «*com a indicação de proveniência "Banco 1…" com o seguinte conteúdo "para confirmar a aprovação de pagamento com cartão ao comerciante EMP01… no valor de 2.800,00 EUR, introduza o código …67*"» e mais uma «*com a proveniência "Banco 1…" com o seguinte conteúdo "Para confirmar levantamento MBWAY introduza o código …70*"» e satisfez esses pedidos.
Aceitando que a autora se convenceu de que a ré a estava a avisar de que "*alguém estaria a tentar aceder à sua conta bancária*", a questão que se coloca é a de saber se é razoável supor que essa intromissão na sua conta seria evitada com a "*aprovação de* [um] *pagamento com cartão ao comerciante EMP01… no valor de 2.800,00 EUR*" e com um "*levantamento MBWAY*".
Muito fracamente, não se descortina uma razão minimamente aceitável para admitir que a aprovação do pagamento e do levantamento que estava a ser pedido à autora pudesse evitar que alguém acedesse à sua conta bancária; não se vê qualquer nexo causal entre o que lhe foi solicitado e este fim.
As mensagens dos factos 10 e 11 são absolutamente claras. Elas dizem expressamente que, sendo satisfeitas, se concretizaria um pagamento e um levantamento MBWAY. Como poderia a autora pensar que, por essa via, estava a impedir que alguém acedesse à sua conta bancária?
Para além disso, a autora era utente do serviço de homebanking da ré há cerca de oito anos. E nesse período teve oportunidade de ter conhecimento dos alertas da ré mencionados nos factos 38 a 43, dos quais se destaca a informação de que «*Existem tentativas de "Phishing" que recorrem a um esquema fraudulento de mensagens SMS e chamadas telefónicas supostamente em nome da Banco 1…*» e o aviso para ter "*Cuidado com SMS e*

telefonemas fraudulentos supostamente em nome da Banco 1…".
Neste contexto, a conduta da autora é manifestamente reprovável à luz do mais elementar senso comum, havendo nela uma omissão dos deveres de cuidado que só uma pessoa especialmente negligente, descuidada e imprudente deixaria de observar; há no comportamento da autora uma manifesta omissão de precauções ou cautelas básicas.
Perante a realidade com que se deparou, se, mesmo assim, ainda admitia, com maior ou menor probabilidade, que a ré a podia estar a avisar para um perigo de intromissão na sua conta, tendo-lhe sido solicitada a colocação de códigos para um pagamento e um levantamento, o mínimo que o bom senso e a prudência impunham era que a autora tomasse a iniciativa de contactar os serviços daquela e, estando absolutamente segura de que era com ela que estava a falar, esclarecesse a situação.
Neste cenário o homem médio não teria, sem mais, como fez a autora, correspondido ao que foi pedido nas mensagens.
E não esqueçamos que as operações em causa "*não teriam sido concretizadas se a autora não tivesse fornecido a terceiro os códigos SMS Token*".
Por conseguinte, tal como decidiu o tribunal *a quo*, a autora agiu com negligência grosseira, o mesmo é dizer que a ré não pode ser responsabilizada pela movimentação dos 2.900,00 €, nem tão pouco por danos não patrimoniais que a autora possa ter sofrido.
Duas palavras finais a propósito do que a autora afirma nas conclusões 14.ª e 15.ª.
Em primeiro lugar, nada se provou quanto à média "*de todas as transações/ movimentações já efetuadas pela Recorrente*", pelo que, independentemente do mais, não se pode afirmar que a "*transferência bancária no valor de € 2.800,00* (…) *era uma operação bastante acima da média*". Acresce que, objetivamente, 2.800,00 € não é um valor elevado.
Em segundo lugar, também não se provou que os 2.800,00 € foram transferidos "*para contas abertas recentemente ou localizadas noutros países com elevada incidência de fraudes*".

III
Com fundamento no atrás exposto julga-se improcedente o recurso, pelo que se mantém a sentença recorrida.

Custas pela autora.
Notifique.

António Beça Pereira

Maria dos Anjos Nogueira
Joaquim Boavida

[1] São deste código todos os artigos mencionados adiante sem qualquer outra referência.
[2] Almeida Costa, Direito das Obrigações, 5.ª Edição, pág. 468.
[3] Antunes Varela, Das Obrigações em Geral, Vol. I, 5.ª Edição, pág. 525.
[4] Galvão Telles, Direito das Obrigações, 7.ª Edição, pág. 354.
[5] Ac. STJ de 24-2-2010 no Proc. 747/04.2 TTCBR.C1.S1. Neste sentido veja-se Ac. STJ de 16-12-2010 no Proc. 2732/07.3TBFLG.G1.S1, ambos em www.gde.mj.pt.
[6] Ac. STJ de 13-12-2007 no Proc. 07S3655, www.gde.mj.pt.
[7] Ac. STJ de 19-10-2005 no Proc. 05S1918, www.gde.mj.pt.
[8] Almeida Costa, Direito das Obrigações, 5.ª Edição, pág. 470. Neste sentido veja-se Antunes Varela, Das Obrigações em Geral, Vol. I, 5.ª Edição, pág. 528, Galvão Telles, Direito das Obrigações, 7.ª Edição, pág. 354 e Henrique Sousa Antunes, Comentário ao Código Civil, Direito das Obrigações, Das Obrigações em Geral, Universidade Católica, 2024, pág. 301.
[9] Maria da Graça Trigo e Rodrigo Moreira, Comentário ao Código Civil, Direito das Obrigações, Das Obrigações em Geral, Universidade Católica, 2024, pág. 1111.