Supremo Tribunal de Justiça
Processo nº 1284/24.T8BRG.G1.S1

Relator: FERREIRA LOPES
Sessão: 19 Novembro 2025
Votação: UNANIMIDADE
Meio Processual: REVISTA
Decisão: NEGADA A REVISTA

PHARMING **HOMEBANKING** **OPERAÇÃO BANCÁRIA**

RESPONSABILIDADE BANCÁRIA

RESPONSABILIDADE PELO RISCO **ÓNUS DE PROVA**

NEGLIGÊNCIA GROSSEIRA **CULPA** **DADOS DE PAGAMENTO**

DIRETIVA COMUNITÁRIA **RECURSO DE REVISTA**

Sumário

(art. 663º, nº7, do CPC)
O risco inerente à utilização e funcionamento dos serviços de pagamentos electrónicos feitos no âmbito de contrato de homebanking recai sobre o Banco, o qual para se eximir dessa responsabilização, nos termos dos arts. 113º, nº3 e 115º do DL nº 91/2008 de 12.11, tem o ónus de provar a existência de fraude, dolo ou negligência grosseira do utilizador dos serviços de pagamento (ordenante).

Texto Integral

Acordam no Supremo Tribunal de Justiça

Sapatarias Gomes Carneiro, Ld.ª, com sede na Rua 1, n.º ..., 4730-..., Vila de Prado, Braga, propôs a presente acção declarativa de condenação sob a forma de processo comum contra o **Novo Banco, SA**, com sede na Avenida 1, n.º ... 1250-..., Lisboa, 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 Novo Banco, 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 na qual nega qualquer responsabilidade no sucedido, 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, pela improcedência da ação.

Realizado o julgamento, foi proferida sentença que julgou a acção improcedente e absolveu o Réu do pedido.

A Autora interpôs recurso da sentença e com sucesso, pois que a Relação de Guimarães, por acórdão de 02.04.2025, julgou a apelação procedente, revogou a sentença e condenou o Réu no pedido.

É a vez do Banco interpor recurso de revista, pugnando pela revogação do acórdão e repristinação da decisão de 1ª instância, tendo formulado as seguintes **conclusões:**

1. O Tribunal da Relação de Guimarães concedeu provimento ao recurso apresentado pela Autora, revogando a sentença proferida em primeira instância que julgou a acção improcedente, por não provada, e absolveu o Recorrente do pedido, decisão com a qual o Recorrente não se conforma

2. A decisão proferida pelo Mmo. Juiz *a quo* de primeira instância não merece qualquer censura, não se aceitando os fundamentos da sua revogação, devendo o acórdão proferido ser revogado, repondo-se a decisão proferida pela douta sentença, nos seus exactos termos.

3. O douto acórdão recorrido não dá razão à ora Recorrida quanto à resposta dada ao ponto 33 dos factos dados como provados, e ao ponto 47 dos factos não provados, mantendo neste ponto a decisão proferida em primeira instância.

4. No que diz respeito ao ponto 34 dos factos provados, o Tribunal considera que cabe razão à aí apelante, substituindo a sua redação pela seguinte:

"34. 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 actualização daquele site."

5. Com base nos mesmos factos provados da sentença da primeira instância, sendo que a alteração do ponto 34 não é sequer referida na fundamentação, os Venerandos Desembargadores chegam à conclusão oposta à do Mmo Juiz de primeira instância.

6. O Acórdão da Relação de Guimarães veio considerar que "*Não há na actuação da autora, uma falta indesculpável, que só uma pessoa especialmente negligente, descuidada e incauta deixaria de observar*". Os factos em que o Tribunal se estribou para chegar a esta conclusão, acima transcritos, deveriam conduzir à decisão oposta à que tomaram os Venerandos desembargadores, que concluíram:

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.

8. Não pode a Recorrente conformar-se com esta decisão, pois é evidente que a conclusão tem que ser precisamente no sentido oposto, como bem decidiu o MMo Juiz de primeira instância, concluindo que "*nenhuma responsabilidade pode ser assacada ao réu, tendo sido o gerente da autora quem não cumpriu de forma deliberada as obrigações previstas no art. 110º, n.º 1, al. a) e 2 do RJSPME. Ademais, considerando que o gerente da autora forneceu seis vezes as coordenadas do cartão matriz e os códigos de validação das operações fornecidos por chamada telefónica, para um fim diferente daqueles a que se destinam essas credenciais – atualização do site – depois de terem sido emitidos alertas de fraude pelo banco réu, designadamente em setembro e outubro de 2023, não pode deixar de se considerar que atuou com desatenção inexplicável e incúria indesculpável, quetraduzem umerroimperdoável. Significa, nessa medida,queatuoucom* ***negligência grosseira****." (negrito nosso)*

9. Os bancos, ao recorrerem a sistemas financeiros digitais que possibilitam um elenco de transacções a poderem ser operadas por essa via, passam a ter um dever acrescido de zelar, dentro daquilo que é exigível e até possível, pela integridade e segurança do património dos seus utilizadores.

10.Esta circunstância não pode, contudo, invalidar aqueles que são os cuidados mínimos exigíveis a qualquer utilizador que retira também inúmeros benefícios deste tipo de serviços online.

11.Os contratos de homebanking encontram a sua disciplina e enquadramento jurídico no referido Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, do qual resulta um conjunto de deveres impostos tanto ao prestador dos serviços como ao seu utilizador, e cuja violação é geradora de responsabilidade civil.

12.O contrato de homebanking é um contrato-quadro que, acessoriamente ao contrato de abertura de conta, permite e disciplina a relação bancária à distância, nomeadamente através da página Web dos bancos na internet.

13.Por via domesmo, obancoobriga-sea disponibilizarmeios eletrónicos fiáveis necessários à comunicação à distância, a mantê-los em regular funcionamento, e a fornecer dispositivos de segurança personalizados de modo a assegurar o acesso exclusivo do cliente à sua conta bancária, obrigando-se o cliente, que tem uma mera faculdade de utilizar o sistema, a, caso exerça tal faculdade, fazê-lo de acordo com determinadas regras que visam assegurar a fiabilidade das comunicações.

14.Ora, nos termos do disposto no art.º 110.º n.º 1, al. a) do referido regime, o utilizador de serviços de pagamento com direito a utilizar um instrumento de pagamento deve utilizar o instrumento de pagamento de acordo com as condições gerais que regem a sua emissão eutilização, as quais têm de ser objectivas, não discriminatórias eproporcionais,

15.Sendo que, nos termos do n.º 2 do mesmo artigo, esclarece-se que 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.

16.Quer por via legal, quer por via contratual, a Recorrida encontrava-se obrigada a manter a confidencialidade e a preservar a segurança das suas credenciais de acesso aos canais

directos disponibilizados pelo Recorrente, bem como das credenciais necessárias à validação das operações a efectuar por aquela via.

17.Atendendo a que o legal representante da Recorrida cedeu tais elementos a terceiros, é manifesto que tal comportamento consubstancia uma violação grave das obrigações legais e contratuais assumidas aquando da adesão, independentemente do contexto em que tal sucedeu, não podendo deixar de, no caso concreto, ser especialmente censurável que o legal representante da Recorrida não tenha atentado minimamente no teor das **seis notificações push** que recebeu no seu telemóvel, que nem sequer abriu, sendo certo que só depois de expedidas estas foram realizadas as chamadas com indicação do código.

18.Ao longo de mais de 30 minutos o legal representante da Recorrida recebeu pedidos de inserção de códigos para uma alegada actualização de página e, seguindo as instruções, forneceu os códigos recebidos, por seis vezes!

19.O art.º 113.º do D.L. 91/2018, regula a prova de autenticação e execução da operação de pagamento, dispondo no respectivo n.º 1 que "*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*."

20.Nos termos desta norma, recai sobre o banco prestador do serviço o risco das falhas e do deficiente funcionamento do sistema, impendendo ainda sobre o mesmo o ónus da prova de que a operação de pagamento não foi afectada por avaria técnica ou qualquer outra deficiência.

21.O Recorrente, na qualidade de prestador do serviço de pagamento, provou cabalmente que as operações em causa (quer as transferências, quer as compras com cartão) foram autenticadas, devidamente registadas e contabilizadas, não tendo sido afetadas por qualquer espécie de avaria técnica ou qualquer outra deficiência do serviço por si prestado, o que resultou corroborado pelo depoimento da testemunha AA.

*22.*Dispõem ainda os números 3 e 4 da mesma norma o seguinte: *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, incluindoo prestadordoserviçodeiniciaçãodopagamento, se forcasodisso, 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*

23. A ocorrer a divulgação dos elementos de segurança e códigos de acesso pelo utilizador, é permitido ao Banco ilidir a presunção que sobre o mesmo recai, afastando a sua culpa ou demonstrando mesmo a culpa do cliente pela deficiente utilização daqueles meios, designadamente, alegando e provando que o cliente beneficiário violou o contrato, divulgando, por qualquer via, dados pessoais, secretos e intransmissíveis relativos ao seu acesso, em benefício de terceiros.

24.Com efeito, há um comportamento censurável do cliente se este fornecer a terceiros informação confidencial, tendo o Banco que provar que a utilização do serviço homebanking por parte do cliente ocorreu com total desrespeito pelas condições acordadas, nomeadamente quanto à segurança e confidencialidade.

25.Ora, por reporte ao caso em apreço, temos queocomportamentodogerenteda Recorrida ao ceder a terceiros seis vezes e ao longo de mais de meia hora os códigos que recebeu, não atentando sequer no conteúdo das seis mensagens que recebeu no seu telemóvel configura uma situação e negligência grosseira apta a, de acordo com o disposto no art.º 113.º, n.º 4 do D.L. 91/2018, afastar a presunção de culpa que recai sobre a Recorrente.

26.Os deveres de segurança não são impostos somente ao banco, incumbindo também ao utilizadorpreservara eficáciadosdispositivosdesegurança, sejam eles cartõesbancários ou credenciais de acesso a canais digitais, devendo o utilizador fazer uso do instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização, bem como comunicar atempadamente qualquer utilização não autorizada.

27.Quanto à análise da responsabilidade do utilizador dos serviços de pagamento, in casu, o Recorrente, estabelece o art.º 115.º do D.L. nº 91/2018,

as seguintes regras:

“1 - 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 € 50,00;

(…)

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 110º, caso em que não são aplicáveis os limites referidos no nº 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 € 50,00. (…)”

28. Da análise do preceito em causa, resulta que é elemento essencial para aferir da imputação da responsabilidade, a apreciação da conduta do ordenante, apreciando-se da verificação de negligência grosseira.

29.No caso concreto, trata-se de um dever de diligência particularmente disseminado, na medida em que a vulgarização dos sistemas de pagamento eletrónico e de acesso aos canais digitais implicou uma informação generalizada da população nos cuidados a ter naquela utilização.

30. Atualmente, a utilização de serviços de homebanking, assim como o recurso a cartões bancários, e é de tal forma usual, que são do comum conhecimento os riscos e cuidados necessários em tais utilizações.

31.Acresce que, como se disse, o gerente da Recorrida é utilizador habitual dos canais directos desde a data da adesão (17.12.2013), sendo, por isso, frequentemente confrontado com alertas para não ceder os seus dados a terceiros e para atentar no teor das notificações recebidas.

32.Com efeito, o Recorrente divulga frequentemente campanhas de sensibilização junto dos seus clientes utilizadores dos canais directos, assim como alertas de segurança, com os quais aqueles são confrontados aquando do acesso aos canais directos.

33.Para além do que acima se expôs, o dever de diligência que impende sobre a Recorrida, resulta da própria lei e das cláusulas contratuais geralmente utilizadas pelas instituições bancárias, como se verifica no caso concreto, sendo ainda promovido este conhecimento generalizado pelo próprio Banco de Portugal.

34.Neste sentido, dificilmente se justifica que o utilizador de serviços de homebanking e de outros meios de pagamento incumpram os referidos deveres, que se encontram necessária e intrinsecamente presentes no homem médio, minimamente cumpridor e normalmente diligente.

35.Acresce ainda que se trata de um dever de fácil cumprimento, sem exigências de maior, bastando que se omita a divulgação a terceiros, seja presencial, seja telefónica ou digitalmente, das credenciais pessoais, pelo que o seu incumprimento se revela particularmente censurável.

36.Não se pode deixar de fazer a analogia com a divulgação a terceiros do código PIN (vd. Acórdão do Supremo Tribunal de Justiça, de 02.03.2010, proferido no processo nº 29371/03.5TJLSB.S1).

37.À semelhança do PIN utilizado para os cartões bancários, também os códigos de acesso ao homebanking, assim como as credenciais pessoais para a validação das operações, são elementos pessoais e intransmissíveis, em relação aos quais a Recorrida se obrigou a manter a segurança e confidencialidade, pelo que o supra exposto tem plena aplicação ao caso concreto.

38.Ora, tomando como bitola a diligência exigida ao homem médio minimamente zeloso, é manifesto que o gerente da Recorrida, com o comportamento supra descrito, infringiu os mais elementares deveres de cuidado que lhe eram exigidos, enquanto utilizador dos canais digitais disponibilizados pelo Recorrente, conforme factos provados 14 a 16, 20, 21, 22, 23, 24, 25 e 26.

39.Assim, a realização das operações apreço ficou a dever-se à actuação culposa e gravemente negligente da Recorrida, na pessoa do seu gerente, incumprindo o dever de segurança econfidencialidadequelheincumbia e, comotal, éresponsávelpela totalidade das perdas que sofreu.

40.O comportamento da Recorrida configura uma situação de negligência grosseira que, nos termos conjugados do disposto nos artigos 113.º, n.º 4 e 115.º, n.ºs 3 e 4 do D.L. 91/2018, afasta a responsabilidade do Recorrente,

fazendo recair sobre a Recorrida o encargo decorrente das operações em causa.

41.Assim, como ficou demonstrado, e não é posto em causa no Acórdão recorrido, todos os passos que consubstanciam o acesso novobanco online e a execução das subsequentes operações (transferências) ocorreram dentro da normalidade técnica, não padecendo de qualquer vício do sistema, e menos ainda que se possa imputar ao Recorrente.

42.O sistema do Recorrente não sofreu qualquer ataque que tivesse permitido a terceiros aceder à conta bancária da Recorrida e executar as transferências em causa, tendo este disponibilizado um serviço capaz e actuado com a diligência devida.

43.As operações contestadas pela Recorrida foram efectuadas à primeira tentativa, o que significa que as credenciais pessoais que permitiram o acesso à aplicação (número de adesão e PIN), assim como a autenticação através da "one time password", foram correctamente introduzidas, circunstância que isenta o Recorrente de qualquer responsabilidade.

44.Uma vez que a Recorrida cedeu a terceiros as suas credenciais de segurança, estamos perante um flagrante caso de violação das obrigações de confidencialidade, guarda e preservação da segurança daquelas credenciais, as quais decorrem do art.º 110.º do D.L. 91/2018, de 12 de Novembro.

45.Ao contrário do que conclui o acórdão recorrido, tendo em conta a forma como tais credenciais foram dadas a terceiro, temos que qualificar tal comportamento como conduta culposa e gravemente negligente da Recorrida.

46.O Tribunal da Relação interpretou e aplicou mal o direito, impondo-se que à questão a decidir se responda nos mesmos termos que a sentença proferida em primeira instância, ou seja: "*Nenhuma responsabilidade pode ser assacada ao réu, tendo sido o gerente da autora quem não cumpriu de forma deliberada as obrigações previstas no art. 110º, n.º 1, al. a) e 2 do RJSPME. Ademais, considerando que o gerente da autora forneceu seis vezes as coordenadas do cartão matriz e os códigos de validação das operações fornecidos por chamada telefónica, para um fim diferente daqueles a que se destinam essas credenciais – atualização do site – depois de terem sido emitidos alertas de fraude pelo banco réu, designadamente em setembro e outubro de 2023, não pode deixar de se considerar que atuou com desatenção inexplicável e incúria indesculpável, que traduzem um erro imperdoável. Significa, nessa medida, que atuou com negligência grosseira.*" Contra alegou a Recorrida, com as

seguintes conclusões:

*

Contra alegou a Recorrida pugnando pela improcedência do recurso e confirmação do acórdão, apresentando as seguintes conclusões:

1. O presente recurso, interposto pelo Novo Banco, S.A. (Recorrente), deve ser julgado integralmente improcedente, uma vez que o douto Acórdão do Tribunal da Relação de Guimarães, de 02-04-2025, ao revogar a sentença da 1.ª instância condenar o Recorrente, alicerçou-se numa correta e exaustiva análise da prova e doDireitoaplicável,especialmentedoRegimeJurídicodosServiçosdePagamento e da Moeda Eletrónica (RJSPME).

2. O Tribunal da Relação corretamente reavaliou e alterou a matéria de facto, especificamente o Ponto 34.º dos factos provados, ao considerar que o segmento "Aautoranãomanteveocomputadorutilizadonoacessoaoscanaisdigitaisasalvo de software malicioso" era conclusivo e desprovido de suporte factual, assentandoseapenasemdepoimentoabstratoeteóricodatestemunhadoBanco (AA)semconhecimentodiretodosfactosoudocomputadorem questão.

3. O Tribunal da Relação valorou adequadamente a prova que demonstrou que o gerente da Autora utilizava o seu computador exclusivamente para acesso bancário, munido de antivírus atualizado, e que o informático BB não detetou malware nainspeção realizadano dia seguinteaos factos.

4. A douta decisãorecorrida distinguiu acertadamente a fraude por"pharming",naqualogerentedaAutorafoiinduzidoemerroporumajanelafraudulentaidên página oficial do Banco e que aparentava ser um processo deatualização do site.

5. A Recorrida (Autora) não agiu com negligência grosseira, conforme o conceito densificado pelo Tribunal da Relação, que exige uma falta de cuidado "indesculpável", uma "desatenção inexplicável" ou uma "incúria inaceitável" que uma pessoa medianamente diligente nunca adotaria nas circunstâncias concretas.

6. O Tribunal da Relação ponderou adequadamente que o gerente da Autora, ao receber chamadas da linha de apoio oficial do Banco (n.º .....00), que forneciam os códigos de validação ("*one time password*"), tinha motivos razoáveis

paraconfiarnalegitimidadedasoperações,mesmoquenãotivesseconfirmadoas notificações "push", dado que a alternativa de validação por voz, proveniente de
númerooficial,éumprocedimentopermitidoedisponibilizadopeloprópriоBanco.

7. A falha do Recorrente Novo Banco em alertar os seus clientes para esta forma específica de fraude ("pharming"), ou em integrar o valor da transferência
naschamadasdevalidaçãoporvoz,contrariaoseudeverdeasseguraraseguрançado serviço e de prestar informação clara e apelativa sobre as novas formas de intrusão,o que o torna responsável pelo prejuízo.

8. Nos termos do Art. 113.º do RJSPME, o ónus da prova de que a operação não foi afetadapor avaria técnica ou deficiência do serviço, e de que o utilizador agiu com doloounegligênciagrosseira, recai sobre o prestador de serviços de pagamento (o Banco).

9. O Recorrente não logrou provar a negligência grosseira do gerente da Autora, falhando assim em afastar a sua responsabilidade pelos danos, uma vez que o risco inerente à utilização e funcionamento dos serviços de pagamento recai sobre o prestador de serviços.

10. O Tribunal da Relação, ao condenar o Novo Banco, S.A. a repor a quantia indevidamente transferida, agiu em estrito cumprimento dos princípios e normas
doRJSPME,quevisamprotegeroutilizadoremsituaçõesdefraudeemquenãohaja dolo ou negligência grosseira imputável ao cliente.

11. Foi a Recorrente Novo Banco que incorreu numa conduta grosseira e indesculpavelmente negligente já que as chamadas de voz realizadas pelo Novo Banco contém uma grosseira falha de segurança, pois as mesmas não fazem qualquer menção ao valor concreto da transferência que o Cliente está a
validaremcadamomento,factoqueoTribunaltemdeconhecerporserdeumagravidade extrema num momento em que existem tantas fraudes deste jaez

12. Ocomportamento alternativoexigidoao Bancoeraqueachamadadevoz fina realizada para o Cliente validar a operação dissesse “para validar a suatransferênciadeEuros:XXXXX,porfavordigiteocódigoYYYY”,poisseassimfosse, nesta “última portagem”, o gerente da Autora teria a possibilidade de saber que não tinha feito nenhuma transferência da quantia de Euros: XXXXX e, por conseguinte, tinha a possibilidade de parar a operação, não digitando o código

final

13. Se o Novo Banco tivesse acautelado o procedimento descrito na conclusão anterior o gerente da Autora, ao receber a chamada de voz do Novo Banco, teria a oportunidade de perceber que havia uma fraude em curso, pois o montante da transferência não era o por si pretendido, pelo que deve o Tribunal consolidar que o NovoBanco incorre em comportamento dúplice, pois, se por umlado diz que faz alertasaosseusclientesacercadoaumentodecasosdefraude,poroutroladonão investe namelhoria do nível desegurança das operações.

14. Tanto é verdade o referido nas conclusões anteriores que esse é justamente o procedimento que já ocorre quando a validação é feita através de mensagem SMS, em que se faz menção ao montante concreto da transferência que se está a fazer.

Objecto da revista:

Saber se a apropriação por terceiros depositado em contas da Autora ocorreu por culpa da própria, *rectius*, do seu gerente quando acedeu ao site do Réu.

Fundamentação.

"**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 Novo Banco, 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, CC, o seu pai, DD, e EE, funcionária da autora há cerca de 18 anos.*

10*. O acesso online de EE 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, EE, 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 CC 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 CC, ligou o computador para aceder ao site online do banco réu para confirmar e assinar os pagamentos que a EE havia preparado previamente.*

14*. E efetuou o login nos canais digitais com o número de adesão 6779063, 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 Novo Banco, 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 CC 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 Novo Banco 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 Novo Banco, 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 EE, 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 PT50 ...;

. 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 PT...;

. 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 PT50 ...;

. 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 PT50 ...;

. 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 ....3 – 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 PT....

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 efectuadas por avaria técnica ou qualquer outra deficiência do serviço efetuado pelo réu.*

34. *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.”* (redacção dada pela Relação).

35. *No dia 16.11.2023, na sequência do relatado pelo gerente da autora, a linha NBnetwork do réu bloqueou o acesso aos canais digitais da autora.*

36. *No dia 17.11.2023, o gestor de conta do Novo Banco, SA, FF 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 3362/23.8JABRG, 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:*

44. O réu emitiu em outubro de 2023 o seguinte alerta de segurança:

***45**. Os alertas de segurança são emitidos aquando do login nos canais diretos e no sitio da internet do réu, disponível em:*

. https://www.novobanco.pt/seguranca;

. https://www.novobanco.pt/seguranca/alertas-fraude.

***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.".*

Foi dado como **não provado**:

a). O sistema informático do réu foi atacado e penetrado por agentes desconhecidos, com a intenção de furtar."

O direito.

A questão a decidir consiste em saber se a Autora pode reclamar do Réu o ressarcimento do prejuízo ocasionado por terceiros que de forma fraudulenta se apropriaram de dinheiro depositado em duas contas por si titulados no banco réu.

Decorre da matéria de facto que a Autora, titular de três contas bancárias no banco réu, e desde Dezembro de 2013 com acesso aos canais directos (vulgo canais digitais), disponibilizados pelo réu aos seus clientes, em 15.11.2023 quando o seu gerente acedeu ao site online do Réu, foi accionado software malicioso, com a abertura de "uma janela fraudulenta por cima da página fidedigna da instituição bancária", ocasião em que foram efectuadas seis transferências de duas contas da sociedade, no valor total de €124.992,00, para destinatários desconhecidos.

A sentença de 1ª instância julgou a acção improcedente por ter considerado que o gerente da Autor agiu com negligência grosseira, decisão revertida pelo acórdão recorrido que condenou o banco réu no pedido.

É contra esta decisão que reage o banco réu com os fundamentos supra referidos.

Vejamos.

O acesso *on line* para realização de operações bancárias, designado por homebanking consiste num serviço prestado pelo Bancos através do qual dá

ao cliente a possibilidade de efectuar operações bancárias via internet, nomeadamente consultas, pagamentos, subscrição de produtos financeiros e transferências.

Na definição do art. 2º, al. m) do Regime do Sistema de Pagamentos (RSP) aprovado pelo DL nº 317/2009 de 30/10, (que transpôs a Directiva 2007/64/CE de 13/11, o contrato de homebanking, como "contrato-quadro", é "*um contrato de prestação de serviços de pagamento que rege a execução futura de operações de pagamento individuais sucessivas e que pode enunciar as obrigações e condições para a abertura de um conta de pagamento*."

Este contrato tem obtido forte incremento e adesão, pelas inegáveis vantagens que propicia: para o cliente, proporciona-lhe um acesso rápido e continuado (sem limitações de horários) e cómodo (sem deslocações aos balcões) às suas contas e desse modo, a realização de operações bancárias; para o banco, permite-lhe agilizar os serviços e optimizar a gestão dos seus recursos humanos, com a inerente diminuição de custos.

O DL nº 91/2018, de 12.12, que transpôs a Directiva (EU) 2015/2366, é o diploma que atualmente regula o Regime Jurídico dos Serviços de Pagamento e da Moeda Electrónica (RJSPME) sendo um dos seus objectivos primordiais, como consta do respectivo preâmbulo, *"a protecção e segurança dos consumidores na utilização desses serviços de pagamento (...). A segurança dos pagamentos electrónicos afigura-se como uma aspecto fundamental para assegurar a protecção dos utilizadores e a promoção adequada do desenvolvimento do comércio electrónico."*

As obrigações do utilizador e do prestador de serviços de pagamento associados aos instrumentos de pagamento constam dos arts. 110º e 111º daquele diploma, que na parte que interessa dispõem o seguinte:

Art. 110º:

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 objectivas, não discriminatórias e proporcionais;

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 de instrumento de pagamento.

2. (…).

Art. 111º:

1. O prestador de serviços de pagamento que emita um instrumento de pagamento deve:

a) Assegurar que as credenciais de segurança personalizadas 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;

(…).

Art. 113º, sob a epígrafe *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 correctamente efectuada, incumbe ao respectivo prestador do serviço de pagamento fornecer a prova de que a operação foi autenticada, devidamente registada e contabilizada e que não foi afectada por avaria técnica ou qualquer outra deficiência do serviço prestado pelo prestador de serviços de pagamento.*

2. (…)

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 art. 110º.

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 utilizar de serviços de pagamento.

Quanto às responsabilidades decorrentes de operações de pagamento não autorizadas – nos termos consagrados nos arts. 114º e 115º – ela é de imputar ao prestador do serviço se vier a comprovar-se que a mesma não foi autorizada e não se verificar o incumprimento de nenhuma das obrigações que são impostas ao utilizador em caso de perda, roubo, apropriação abusiva de instrumento de pagamento ou quebra de confidencialidade dos dispositivos de segurança personalizados, respectivamente.

As operações de pagamento fraudulentas, por não autorizadas pelo titular da conta, mais frequentes são designadas por *phishing* e *pharming*.

O *phishing* pode ser definido como a fraude praticada através do envio de mensagens de correio electrónico, que provêm aparentemente do banco prestador do serviço, tentando obter dados confidenciais que permitam o acesso ao serviço de pagamento electrónico; no *pharming*, é adulterado o próprio nome de domínio de ume entidade financeira, redirecionando o utilizar para um site falso, que constitui um espécie de clonagem da real pagina da entidade visada. Isto é, sempre que o utilizador digita no teclado o endereço correcto da entidade bancária, é conduzido de forma automática para a página forjada, com as mesmas características gráficas e estéticas da verdadeira. (cf. *Maria Raquel Guimarães, "A fraude no comércio Electrónico: O problema da Repartição do Risco por Pagamentos Fraudulentos in Infracções Económicas e Financeiras, Estudos de Criminologia e Direito, Coimbra Editora,* 2013, e acórdão do STJ de 14.12.2016, P. 1063/12).

No caso, e como decidiu o acórdão recorrido, a Autora foi vítima de *pharming* e não de *phishing*, porquanto não resulta dos autos que lhe tivessem sido sacados os códigos pessoais através de qualquer mensagem de correio electrónico o tipo *spam.*

Conjugando o que dispõem os nºs 1, 3 e 4 do art. 113º do RJSPME, resulta que a prova efectuada pelo banco de que a operação de pagamento foi autenticada, devidamente registada e contabilizada, não prova, por si só, que a operação de pagamento foi autorizada pelo ordenante (nem que este último agiu de forma fraudulenta, ou que não cumpriu, com dolo ou negligência grosseira, uma ou mais obrigações previstas no art. 110º), incumbindo ao banco réu (prestador de serviços) fazer a prova da existência de fraude, de dolo ou de negligência grosseira da parte do utilizador dos serviços de pagamento.

Uma leitura conjugada das disposições supra transcritas, decorre, em síntese, que a entidade bancária, no caso da 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, 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.

Do regime de responsabilidade do ordenante em caso operação de pagamento não autorizada prevista no art. 115º, nºs 3 e 4, conjugada com o regime de prova de autenticação e execução da operação de pagamento previsto no art. 113º, nºs, 1, 3 e 4, do RJSPME, resulta assim que o risco inerente à utilização do sistema 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. 113º, nº1), mas ainda que o utilizador dos serviços de pagamento actuou de forma fraudulenta ou incumpriu de forma deliberada uma ou mais das suas obrigações decorrentes do art.110º ou que actuou com negligência grosseira (art. 113º, nºs 3 e 4). (cfr. o acórdão da Relação do Porto de 12.10.2023, P. 3728/21, que vimos seguindo de perto, o acórdão do STJ de 14.12.2016, P.1063/12, que embora proferido no âmbito do DL 317/2009, ainda com interesse considerando que o actual art. 113º, nºs 1 e 3, corresponde ao art. 70º, nºs 1 e 2 daquele diploma, e os acórdãos do STJ de 12.12.2023 P. 9240/20, e da Relação de Lisboa de 20.02.2024, P. 6029/23, consultáveis em www.dgsi.pt

Estando fora de questão que o gerente da Autora tenha agido de forma *fraudulenta* ou que incumpriu de forma *deliberada qualquer das obrigações* decorrentes do art. 110º, importa saber se a sua actuação pode ser qualificada como *negligência grosseira*.

Negligência, todos o sabemos, significa a inobservância de deveres de cuidado, de diligência ou perícia exigíveis para evitar o dano.

Já a negligência grave ou grosseira, corresponde à falta grave e indesculpável, consistente na omissão dos deveres a que está adstrito que só uma pessoa especialmente desleixada, descuidada e incauta deixaria de observar.

O DL nº 91/2018, não define "*negligência grosseira*". Todavia, no Considerando 72 da Directiva (EU) 2015/2366, afirma-se o seguinte:

"Para avaliar a eventual negligência ou negligência grosseira cometida pelo utilizador dos serviços de pagamento, deverão ser tidas em conta todas as circunstâncias. Os elementos de prova e o grau da alegada negligência deverão ser avaliados em termos de direito nacional. Todavia, embora o conceito de negligência implique uma violação do dever de diligência, a negligência grosseira deverá significar mais do que mera negligência, envolvendo uma conduta que revela um grau significativo de imprudência; por exemplo, conservar as credenciais utilizadas para autorizar uma operação de pagamento, num formato que seja aberto e facilmente detectável por terceiros."

Para Maria Raquel Guimarães, citada no acórdão do STJ de 17.06.2025, P. 25239/19, "*a actuação gravemente negligente do utilizador de um instrumento de pagamento pressupõe que este adopta um comportamento que o utilizador médio, razoavelmente informado e esclarecido, não adoptaria. (...).*

Não se pode qualificar a conduta de quem fornece credenciais de segurança em resultado de uma prática fraudulenta como gravemente negligente, quando essas práticas fraudulentas são levadas a cabo porque um grande número de pessoas é ludibriado através delas e não apenas as extremamente descuidadas ou incautas; e para um conduta poder ser qualificada como grosseiramente negligente ela não pode ser susceptível de ser levada a cabo por um número significativo de homens médios."

O acórdão de 12.12.2023, supra citado, decidiu:

"Não constitui negligência grosseira a actuação de um utilizador de um serviço de homebanking que, em resposta à solicitação feita por uma sms, identificada como do banco prestador do serviço, acede a um site aí indicado, em tudo igual à página oficial do seu serviço, usando isso o seu número de utilizador e PIN e fornecendo também os números do cartão matriz, com a finalidade de activar o serviço que estava inactivo conforme por duas vezes o banco informara.

A negligência grosseira, merecedora de reprovação pelo mais elementar senso comum por configurar uma falta indesculpável na omissão dos deveres a que está obrigado, não se verifica quando a lesada, com a atenção que lhe era exigida e de que era capaz nas circunstâncias do caso, não se pôde opor aos artifícios de complexidade electrónica que lhe foram colocados por terceiros que se fizeram passar com aparente credibilidade pelos serviço do banco, solicitando a resolução de um problema que, efectivamente, em momento

anterior e por duas vezes, o banco informara dever ser resolvido."

No caso em apreciação, passou-se o seguinte:

No dia 15.11.2023, o gerente do Autora entrou no site online do banco réu para completar e assinar uns pagamentos que a sua funcionária havia preparado, momento em que apareceu no ecrã uma caixa de texto com o logotipo do Novo Banco, SA com a informação de que o site estava em actualização e que demoraria alguns minutos a ficar concluída;

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;

Tal ocorreu por ter sido accionado software malicioso quando o gerente da autora acedeu ao site online do réu, 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;

O CC 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);

- Em todas as notificações "push" recebidas pelo gerente da autora no telemóvel, fez-se referência à confirmação de operações iniciadas no Novo Banco 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.

- O gerente da autora acionou os seis códigos de validação recebidos.

Não pode afirmar-se à luz da factualidade apurada que o gerente da Autora forneceu voluntariamente os seus códigos a terceiros: fê-lo em resposta a uma solicitação que surgiu numa caixa de texto, *"exatamente igual à fornecida habitualmente pelo website do réu*", durante uma alegada actualização do site do NB e para que "a actualização pudesse ser eficazmente concluída".

O cidadão com bons conhecimentos de informática provavelmente estranharia que actualização do site necessitasse das coordenadas do cartão matriz, mas nada na matéria de facto indica que o gerente da Autora fosse uma pessoa com aquele tipo de competências.. Não há, por conseguinte, negligência grave e grosseira.

Também nos parece que do facto de não ter confirmado as seis mensagens, através de notificações *"push"* (que constituem alertas) enviadas para o número de telemóvel associado à adesão, em que se fazia referência à confirmação de operações iniciadas no Novo Banco, cada uma delas enviada 2 minutos antes de cada uma das transferências, se possa deduzir que agiu com negligência grosseira.

É que as notificações push, em que se pedia que confirmasse as operações, foram seguidas, um minuto depois, do código de validação enviado para o telemóvel associado à adesão.

Concorda-se com a Relação que a este propósito referiu:

"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."

Do facto de se ter provado "que o réu nunca solicitou ou solicita a inserção de credenciais pessoais dos clientes para a concretização de qualquer atualização do seu sitio da internet", sem que se tenha provado que Réu alertou os seus clientes para o risco de fraude com mensagens de falsas actualizações do site, não indicia que o gerente da Autora violou grosseiramente um alerta de segurança,

Os alertas feitos em Setembro e Outubro de 2023, alertando para o cuidado a ter com mensagens referindo "*instalação de complemento de segurança*" ou alerta para "*falsos sms e chamadas telefónicas fraudulentas*" – nada referiam para o risco de fraude como o que afectou a Autora.

Resta dizer que o facto de "*os computadores do Banco não terem sido alvo de qualquer quebra de segurança informática, nem o seu sítio institucional alvo de intrusão ou outra violação (...) não isenta da responsabilidade o banco recorrente porque esta responsabilidade não resulta da violação de qualquer culpa sua, mas sim de um comportamento da recorrida que pudesse ser julgado fraudulento ou grosseiro. O risco corre por conta do recorrente, tendo por fundamento o art. 796, nº1, do CCivil, apenas poderia ser afastado se tivesse ficado demonstrada a culpa da autora e neste caso a culpa da autora teria de corresponder a culpa grosseira, por nos termos da Directiva transposta, a isenção de responsabilidade do banco apenas ocorrer em caso de actuação fraudulenta ou negligência grosseira*", como decidiu o supra citado acórdão do STJ de 12.12.2023.

Em suma, a matéria de facto provada não permite concluir que o gerente da Autora quando acedeu ao site do Banco réu no dia 15.11.2023, actuou com negligência grosseira, pelo que as perdas resultantes das operações de pagamento não realizadas e autorizadas por si, correm por conta do Banco, como decidiu o acórdão recorrido.

Com o que improcedem na totalidade as conclusões do Recorrente.

Decisão.

Pelo exposto, nega-se a revista e confirma-se acórdão recorrido.

Custas pelo Recorrente.

Lisboa, 19.11.2025

José Maria Ferreira Lopes

Maria dos Prazeres Pizarro Beleza

Fátima Gomes