Acórdão do Tribunal da Relação de Guimarães

Processo: 1292/24.5T8VCT.G1
Relator: JOSÉ CRAVO
Descritores: HOMEBANKING
MOVIMENTOS NÃO AUTORIZADOS
VISHING
Nº do Documento: RG
Data do Acordão: 30-10-2025
Votação: UNANIMIDADE
Texto Integral: S
Meio Processual: APELAÇÃO
Decisão: APELAÇÃO IMPROCEDENTE
Indicações Eventuais: 2ª SECÇÃO CÍVEL
Sumário:

I – O preceituado no art. 640º do CPC em conjugação com o que se dispõe no art. 662º do mesmo diploma legal permite ao Tribunal da Relação julgar a matéria de facto.
II – Assentando o entendimento da apelante numa factualidade que não logrou ver provada e cuja reapreciação igualmente não logrou ver alterada, revela-se inquinado o desfecho do recurso.
III – O Decreto-Lei n.º 91/2018, de 12/11, que transpôs para a ordem jurídica nacional a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, regula, além do mais, as operações conhecidas por homebanking, que fazem parte da designação genérica de "convenção de giro" associada ao contrato de depósito bancário.
IV – Nos termos deste quadro legislativo, para se isentar da responsabilidade de pagamento ao seu cliente dos valores respeitantes a movimentos que este não autorizou, deve o banco demonstrar que existiu fraude ou incumprimento dos deveres do cliente, a título de dolo ou de negligência grosseira.
V – O que, *in casu*, se não verificou, pois, pese embora de relevo, a falta de cuidado evidenciada não deve ser qualificada como negligência grosseira por, apesar de tudo, não se poder considerar que o apelado tenha praticado um erro imperdoável, ou uma desatenção ou incúria inexplicáveis, caracterizadores da mesma.

Decisão Texto Integral:

Acordam na Secção Cível do Tribunal da Relação de Guimarães

*

1 – RELATÓRIO

AA e **BB**, intentaram a presente acção declarativa sob a forma de processo comum[1], contra **Banco 1..., SA**, melhor identificados nos autos, peticionando, a final, a condenação do R. a reembolsar os AA. na quantia de € 16.998,00, com acréscimo de juros de mora à taxa legal de 10%, desde 11-01-2023 até efectivo e integral pagamento, e a pagar, a título de indemnização por danos não patrimoniais, quantia não inferior a € 5.000,00, igualmente acrescida de juros de mora à taxa legal desde 11-01-2023 até efectivo e integral pagamento.
Alegam, em síntese, que são titulares de uma conta de depósitos à ordem junto do Banco R., desde ../../2020, data em que aderiram aos serviços de "homebanking" e "mobilebanking".
Acontece que no dia 11-01-2023, o A. marido recebeu uma chamada no seu telemóvel, de alguém que se identificou como funcionário do Banco R., e que lhe indicou o seu nome e morada completos, solicitando confirmação de se manterem actualizados tais dados, para efeitos de validação da chamada. Depois disso, o Autor foi questionado acerca da realização de movimentos com o cartão de débito, designadamente nesse mesmo dia, e foi imediatamente informado da necessidade de proceder ao desbloqueio da sua conta bancária, e no seguimento deste telefonema, o A. recebeu várias mensagens escritas (SMS) no seu telemóvel em que o remetente era identificado por Banco 1..., referentes à reposição do "homebanking" e acesso aos canais digitais.

Pelas 12h49 desse mesmo dia, o A. marido dirigiu-se a uma caixa multibanco para efectuar um levantamento em numerário e uma consulta de movimentos da sua conta, tendo constatado que haviam sido efectuadas operações bancárias, que não foram por si executadas nem ordenadas, e que consistiram na mobilização da conta a prazo para a conta a ordem do montante de € 16.000,00, transferência, no valor de € 9.998,00 e "MB pagamento", no montante de € 7.000,00, que foram efectuadas sem o seu consentimento ou autorização.
O A., ainda nesse dia, reportou a situação ocorrida ao Banco, após lhe ter sido exigida a realização da participação criminal, mas até agora não lhe deu qualquer resposta.
Mais, alegam que em resultado dos factos descritos, os AA. sofreram abalo emocional, inquietações e transtornos, por se verem privados de uma boa parte das suas poupanças.

*

Citado, o R. deduziu contestação.
Alega, em síntese, que as operações e movimentos a débito realizados foram autenticadas através de elementos de "posse", "conhecimento" e "inerência", devidamente registadas e contabilizadas, não tendo sido afectadas por quaisquer avarias técnicas ou deficiências do serviço prestado.
Mais, alega que os AA. actuaram com culpa porque descuraram as recomendações de segurança do seu conhecimento no manuseamento do serviço de "homebanking", designadamente acederam ao serviço através da pesquisa em motores de busca, ingressando em páginas da internet falsas, nas quais era solicitada a introdução da senha ("password" completa, em vez de apenas três posições aleatórias do código alfanumérico, definido e conhecido apenas pelos mesmos), não tendo a situação sido o resultado de nenhuma anomalia, deficiência ou vicissitude, pontual ou permanente, total ou parcial, que tivesse afectado os sistemas informáticos do Banco 1....

*

Findos os articulados, foi realizada a audiência prévia.
Foi proferido despacho saneador, seguido do despacho de fixação do objecto do litígio e enunciação dos temas de prova.

*

Realizou-se a audiência de julgamento de acordo com o formalismo legal, conforme resulta da respectiva acta.

*

Foi, de seguida, proferida sentença, que decidiu nos seguintes termos:

Pelo exposto, decide-se julgar a presente acção parcialmente procedente e, em consequência:
5.1. Condena-se o Réu a reembolsar os Autores da quantia de € 16.998,00 (dezasseis mil novecentos e noventa e oito euros), acrescida de juros de mora à taxa legal, acrescida de uma sobretaxa de 10% a contar de 11/01/2023 até efectivo e integral pagamento;
5.2. Condena-se o Réu a pagar aos Autores, a título de indemnização por danos não patrimoniais, a quantia de € 2.000,00 (dois mil euros), acrescida de juros de mora à taxa legal, acrescida de uma sobretaxa de 10% a contar de 11/01/2023 até efectivo e integral pagamento.
Custas por Autores e Réu, na proporção do decaimento (art.º 527º, nº 1 e 2 do CPC).

Registe e notifique.

*

Inconformado com essa sentença, apresentou o R. **Banco 1..., SA** recurso de apelação contra a mesma, cujas alegações finalizou com a apresentação das seguintes conclusões:

A. O aqui recorrente não se conforma com a decisão proferida pelo tribunal *a quo*, reputando-a infundada: i. Tanto no que concerne à decisão sobre a matéria de facto, e, ii. mormente quanto à aplicação que faz do direito aos factos, como se procurará demonstrar de seguida.
B. O tribunal *a quo* considerou provada matéria de facto, alguma [muita mesmo] com respaldo nas declarações tomadas, exclusivamente, aos ora recorridos, em particular o impetrante AA.
C. O tribunal *a quo* diz ter alicerçado "(…) *a sua convicção no acervo documental junto aos autos em conjugação com o depoimento das testemunhas CC, DD, enteados do Autor marido, EE (investigador de irregularidades do Banco 1...), FF (Bancária no Banco 1...), GG (Director de Canais e qualidade do Banco 1...), e, ainda, ponderando as declarações de parte do Autor marido, tudo analisado à luz das regras da experiência comum e normalidade social.*"
D. Contudo, há factos essenciais para uma correta aplicação do Direito no caso concreto que não foram considerados, devendo-se, aparentemente, a uma deficiente análise da prova produzida, com inegável esquecimento do importante ***princípio da aquisição processual***, que impunha ao tribunal recorrido ter considerado provado importantes factos trazidos a juízo por testemunha que – nos seus dizeres – contribuiu para a formação da respetiva "*convicção judiciária*".
E. Foi produzida prova testemunhal pelo recorrente que exige modificação da matéria de facto provada, de modo a fazer-lhe constar factos essenciais.
F. O tribunal recorrido considerou provado que: *Nesse contacto telefónico, a pretexto de proceder ao desbloqueio de uma ordem de pagamento, solicitaram-lhe o fornecimento do Código OTP, enviado por SMS para o seu telemóvel pelo Banco Réu, o que Autor marido partilhou*.
G. Ficou por constar, a respeito deste código OTP, um aspeto assaz importante, diríamos mesmo derradeiro para permitir concluir e afirmar que o recorrido AA foi grosseiramente negligente no manuseamento do instrumento de pagamento em causa e das suas credenciais.
H. Inexplicavelmente, nenhuma menção consta referida ao teor da mensagem ***SMS***, enviada para o telemóvel do recorrido AA, contendo o referido OTP, não obstante o recorrente ter logrado fazer prova de que a mensagem SMS enviada continha, suficientemente explícito: *(i.) a que fim se destinava o OTP; (ii.) a advertência de que se o recorrido AA não tivesse desencadeado uma operação que justificasse o seu envio e a correlativa receção que contactasse imediatamente o Banco 1...; e (iii.) que o Banco 1... nunca solicita códigos por telefone*.
I. Tal prova obteve-se pelo depoimento da testemunha FF, quando questionada pelo mandatário do aqui recorrente sobre se tinha conhecimento do registo de mensagens SMS enviadas pelo Banco 1... para o telemóvel do recorrido AA esclareceu: "***Sim, por volta dessa hora*** *[a hora indicada pelo recorrido AA da receção da chamada*

telefónica, no dia 11.01.2023] ***terá sido enviado um SMS com o intuito, neste caso, de associar… ativar a aplicação mobile* - [5m:36s – 5m:51s da sessão de julgamento realizada no dia 18.02.2025]**." O mesmo foi atestado pela testemunha EE, asseverando que às 11h:52m foi enviado um OTP para o telemóvel do recorrido AA para instalação da aplicação móvel **[22m:37s – 23m:44s da sessão de julgamento realizada no dia 28.01.2025]**.
J. A primeira das testemunhas referidas acrescentou saber que esse SMS foi enviado para o telemóvel do recorrido AA (e que este reconhece ter recebido) por volta das 11h:52m do dia 11.01.2023 **[5m:55s – 5m:59s da sessão de julgamento realizada no dia 18.02.2025]**.
K. Questionada sobre o teor da mensagem SMS esclareceu: "*a mensagem alerta para o facto de estar a ser realizada uma operação através dos canais digitais*" e um alerta de segurança para o caso de o cliente não reconhecer tal operação contactar o Banco 1... **[8m:45s – 8m:51s da sessão de julgamento realizada no dia 18.02.2025] e que**, continha um código [OTP] para ser **introduzido** e **não facultado** a ninguém **[7m:47s – 8m:23s da sessão de julgamento realizada no dia 18.02.2025]**
L. Extrai-se deste depoimento – com muito assinalável relevância – que o recorrido AA recebeu e partilhou um SMS que continha advertências expressas da sua ***finalidade*** ["(…) *estava a ser realizada uma operação nos canais digitais do Banco 1...* (…)"], do ***modo de utilização*** [introdução nos canais digitais do Banco 1... e não a sua partilha] e do ***procedimento a adoptar*** caso não reconhecesse (ou se lhe parecesse estranho) ter recebido aquela mensagem SMS com o OTP [contactar o Banco 1...].
M. Deste modo, pelo depoimento da testemunha FF exigia-se constar dos **factos provados** não apenas que: [***ee)***] ***Nesse contacto telefónico, a pretexto de proceder ao desbloqueio de uma ordem de pagamento, solicitaram-lhe o fornecimento do Código OTP, enviado por SMS para o seu telemóvel pelo Banco Réu, o que Autor marido partilhou,* COMO AINDA: *não obstante constar dessa mensagem SMS a menção de que o envio e a receção dessa mensagem e do Código OTP tinham na sua origem uma operação que tinha sido desencadeada pelo cliente nos canais digitais do Banco 1..., que se destinava a ser introduzido nesses canais digitais e que caso não reconhecesse tal operação devia contactar o Banco 1...***.
N. No âmbito do RJSPME competia ao aqui recorrente, enquanto ***prestador de serviços de pagamento***, provar os seguintes factos paralisantes da pretensão que lhe dirigiram os recorridos [***o*** ou ***os*** ordenantes, para efeitos das respetivas previsões normativas]: ***(i.)*** Que as perdas resultantes de operações de pagamento não autorizadas, foram devidas ao **incumprimento** de uma ou mais das obrigações previstas e contratadas, nomeadamente a utilização do instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização [artigos 110.º e 114.º do RJSPME]; (ii.) Que houve **negligência grosseira** do ordenante [artigo 115.º do RJSPME]; (iii.) 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*** prestado pelo Banco 1....
O. Da matéria de facto dada como provada pelo tribunal *a quo*, não

surgem elencados os seguintes factos: ***(i.)*** **incumprimento** de uma ou mais das obrigações previstas e contratadas, nomeadamente a utilização do instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização; ***(ii.)*** 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*** prestado pelo Banco 1....
P. A testemunha EE esclareceu minuciosamente como se processou o ataque de ***phishing*** [à margem dos sistemas informáticos do aqui recorrido, impedindo-o evitá-lo e debelá-lo] a alguns clientes (incautos e incumpridores das prescrições de utilização de instrumentos de pagamento como o homebanking, das recomendações de segurança periodicamente divulgadas e até de elementares e costumeiras regras de navegação na Internet e de segurança) do Banco 1..., no mês de dezembro de 2022.
Q. Esclareceu também a testemunha EE, a respeito da autenticação das operações realizadas, no dia 11.01.2023, através da aplicação móvel que: "(…) ***existem dois elementos de autenticação; o primeiro é o token …ou seja a partir do momento em que o cliente introduz o código que recebeu para autorizar aquele equipamento a transacionar é gerada esta chave de segurança que garante ao banco que o equipamento que está ser utilizado em cada transação*** (…)"; "***essa chave móvel é um elemento de posse***" (…) "***o segundo elemento pode ser biometria […] ou um PIN, um desenho padrão***" – ou seja, elementos de ***posse***, ***inerência*** ou ***conhecimento*** **[9m:17s – 10m:55s da sessão de julgamento realizada no dia 28.01.2025]**.
R. Asseverou também, e ainda, a testemunha EE que as transações reclamadas pelos aqui recorridos foram devidamente autenticadas, contabilizadas, registadas e que nenhum problema ou vicissitude afetou os sistemas informáticos, com base nos quais, foram processadas e consumadas **[37m:35s – 38m:51s da sessão de julgamento realizada no dia 28.01.2025]**.
S. Destarte, em função da prova produzida pelo Banco 1..., mediante a mobilização do testemunho de EE forçoso era considerar provado que: [***tt)***] ***As transações reclamadas pelos Autores nos presentes autos – consubstanciando operações de pagamento – foram autenticadas, contabilizadas e devidamente registadas, e não foram afetadas por qualquer avaria técnica ou por outra deficiência relacionada com o serviço de pagamento prestado pelo Banco 1...***.
T. Assim, deve o facto constante da al. ***ee)*** da matéria de facto provada, constante da sentença recorrida ser reformulado (pela sua ampliação), nos seguintes termos: [***ee)***] ***Nesse contacto telefónico, a pretexto de proceder ao desbloqueio de uma ordem de pagamento, solicitaram-lhe o fornecimento do Código OTP, enviado por SMS para o seu telemóvel pelo Banco Réu, o que Autor marido partilhou, não obstante constar dessa mensagem SMS a menção de que o envio e a receção dessa mensagem e do Código OTP tinham na sua origem uma operação que tinha sido desencadeada pelo cliente nos canais digitais do Banco 1..., que se destinava a ser introduzido nesses canais digitais e que caso não reconhecesse tal operação devia contactar o Banco 1...***.
U. Complementarmente, pelas mesmas razões, aos factos provados, constantes da sentença recorrida, deverá ser acrescentado, por

provado, o seguinte facto: ***As transações reclamadas pelos Autores nos presentes autos – consubstanciando operações de pagamento – foram autenticadas, contabilizadas e devidamente registadas, e não foram afetadas por qualquer avaria técnica ou por outra deficiência relacionada com o serviço de pagamento prestado pelo Banco 1...***.
V. A conduta do recorrido AA foi a única causa do sucedido, não só porque acedeu de modo diverso do prescrito ao serviço de ***homebanking***, ingressando em páginas contrafeitas, (às quais nunca teria acedido caso tivesse cumprido as obrigações e procedimentos acordados com o aqui recorrido no contrato ***quadro celebrado***), e nas quais digitou – facultando o acesso a terceiros – o seu ***username*** e – sem poder deixar de se fazer notar a enorme censura que isso envolve – digitando a totalidade dos carateres da sua **password**.
W. Ao agir como agiu facultou a terceiros as duas credenciais [***username*** e ***password***] do instrumento de pagamento [homebanking], permitindo-lhes, no dia **11.01.2023**, acederem ao ***homebanking*** do recorrido AA, ainda que confinados apenas à consulta de alguns dados (nomeadamente o contacto telefónico e movimentos a crédito e a débito registados na conta à ordem associada).
X. Com base nesse conhecimento, esses terceiros contactaram o recorrido AA, intitulando-se funcionários do Banco 1..., e partilhando-o movimentos recentemente realizados, que consultaram, simultaneamente espoletaram o processo de instalação da aplicação móvel [***app mobile Banco 1...***], e para cuja consumação careciam de um código OTP que era automaticamente enviado, através de mensagem SMS, para o telemóvel do recorrido AA.
Y. Lograram obtê-lo sob o pretexto de que era necessário para desbloquear o cartão de débito do recorrido AA, o mesmo que utilizara instantes antes.
Z. Descurando os mais elementares deveres de cuidado a observar neste "***tipo de coisas***", ignorando o teor dessa mensagem SMS que lhe foi enviada, e com claras exortações que o deviam ter demovido de proceder como procedeu, permitindo afirmar ter, com isso, atuado com manifesta e inegável ***negligência grosseira***, o recorrido AA facultou o código OTP.
AA. Em situação fáctica com enorme semelhança considerou a Relação de Coimbra que ***o utilizador do serviço de pagamento, ao informar terceiro dos dados da sua password e do código OTP, agiu com negligência grosseira, uma vez que o resultado era previsível para qualquer pessoa normalmente diligente, que se encontrasse na mesma situação*** (Ac. tirado no processo 8/23.8T8SAT.C1 em 25.03.2025).
BB. As normas do RJSPME em matéria de operações de pagamento não autorizadas constituem previsões especiais de responsabilidade civil, às quais são aplicáveis, no necessário a fazer proceder o instituto, as normas de responsabilidade civil comuns, constantes dos artigos 483.º e ss do Código Civil.
CC. Sobre a culpa do ordenante é mister não olvidar o auxílio interpretativo que nos é proporcionado pelo **Considerando 72** da Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25.11.2015, afirmando, apenas, em nosso entender a necessidade de reconhecimento de uma maior intensidade do juízo de censura ético-jurídica (inerente ao conceito de ***culpa***, entendida como a exigibilidade

de adotar comportamento diverso do concretamente acolhido).
DD. Opomo-nos, por isso, àquela conceção que teima em ver na negligência grosseira referida no RJSPME uma falha palmar, que impressiona, intolerável, mas antes devendo ser encarada como uma "***maior censurabilidade***".
EE. Mesmo aos olhos de tal conceção é inevitável classificar a conduta do recorrido AA como grosseiramente negligente.
FF. O recorrido AA ***(i.)*** acedeu – semanas antes do sucedido – ao ***homebanking*** do recorrente em manifesto incumprimento dos procedimentos de acesso (pela inscrição direta no browser / barra de endereços de ...); ***(ii.)*** facultou a sua password completa (em vez das habituais três posições aleatórias); ***(iii.)*** é contactado por putativo trabalhador do recorrente Banco 1... que lhe diz que o seu cartão de débito está bloqueado (o mesmo que usou instantes antes para pagar o abastecimento de combustível do seu carro); e que para o efeito precisava de um código [OTP] que ia receber no seu telemóvel constante de uma mensagem SMS; ***(iv.)*** leu essa mensagem – necessariamente -, ignorou as exortações e advertências que a mesma continha (que era uma operação que havia sido iniciada nos canais digitais, se não a reconhecesse que contactasse o Banco 1... e que o código OTP era para ser inserido – não partilhado) e, não obstante isto tudo, forneceu o código OTP.
GG. Tudo isto com indiferença pelas divulgações periódicas do recorrente sobre boas práticas e procedimentos a adotar no manuseamento dos serviços de banca digital.
HH. O recorrido AA violou as mais elementares obrigações [*palmares* mesmo] de um normal utilizador de serviços de pagamento: facultou a terceiros os dados da sua ***password*** e o código OTP recebido, ainda que advertido da causa do seu envio, e de outras menções de alerta, sem poder negar ter previsto o resultado dessas condutas.
II. O tribunal *a quo* parece ter ignorado um aspeto crucial, denunciando uma convicção pessoal do julgador – infundada e até algo "*preconceituosa*" – de que os recorridos [na sua qualidade de consumidores] merecem tratamento e proteção especiais no relacionamento com empresas como o recorrente, ainda que tal prefigure uma preconceção dos recorridos como sujeitos dotados de alguma incapacidade, incompatível com o critério do homem médio e, no caso, do utilizador de serviços digitais e de serviços de pagamento, de quem são exigidos especiais conhecimentos, deveres e comportamentos.
JJ. As transações reclamadas pelos recorridos foram realizadas mediante mecanismos de autenticação forte, mediante recurso a fatores de autenticação de duas das três espécies legalmente determinadas, significando isso que, para o aqui recorrente, provinham dos recorridos (em particular do recorrido AA), bastando ao aqui recorrente assegurar-se, como fez, de que as transações contestadas pelos recorridos, provinham de ordens suas.
KK. A instalação da ***app mobile Banco 1...*** apenas foi possível mediante a introdução do ***username*** e da ***password*** (completa) de exclusivo conhecimento do recorrido AA (competindo-lhe a correspondente obrigação de manter confidenciais tais dados: n.º 2 do artigo 110.º do RJSPME).
LL. A conclusão desse processo de instalação da ***app mobile do Banco 1...*** culminou – e apenas assim possível – com a introdução do código OTP remetido para o telemóvel que o recorrido AA indicara ao

aqui recorrente para esse efeito, aquando da celebração do contrato de disponibilização do serviço de ***homebanking***, tudo fazendo crer que tinha provindo de ordem sua, sem que nada permitisse crer o contrário.
MM. Sem razão para tal, ignorando - ou querendo ignorar - que as ordens geradas pela dita aplicação móvel também lhes são atribuídas (ao recorrido AA no caso), dado envolverem elementos de autenticação de duas das três espécies legalmente exigíveis: ***(i.)*** Posse: correspondente à chave que é gerada pela introdução do OTP; ***(ii.)*** Conhecimento ou inerência: correspondendo à solução adotada pelo cliente na utilização da app mobile no seu telemóvel (acedendo-lhe mediante a introdução de um código ou de um dado biométrico).
NN. Com particular relevância deu o tribunal *a quo* como provado que o recorrido AA acedeu ao ***homebanking*** do Banco 1... de modo diverso daquele que lhe impunha o contrato celebrado com o recorrente, que introduziu a totalidade da sua ***password***, e até que partilhou o código OTP que lhe foi remetido por mensagem SMS para o seu telemóvel, permitindo que terceiros instalassem a aplicação móvel do Banco 1..., associada a conta à ordem dos recorridos, em dispositivo que controlavam.
OO. A partir do momento da adesão ao serviço de ***homebanking*** o recorrido AA passou a autorizar o Banco 1... a realizar as operações ordenadas, através daquele meio eletrónico, desde que introduzidas as necessárias credenciais de utilização, não só movimentos a débito, como ainda a instalação da aplicação móvel.
PP. Da aceitação pelos recorridos desta disciplina negocial, no âmbito do serviço de ***homebanking*** acordado com o recorrente extraem-se duas evidências: o Banco 1... obrigou-se a manter sob rigorosa confidencialidade as Chaves de Acesso; e por seu turno os recorridos obrigaram-se a guardar sob segredo, o ***username, a password*** e os ***OTP's***, como ainda a assegurar que a sua utilização é feita exclusivamente pelos próprios e a prevenir o seu uso abusivo por parte de terceiros.
QQ. A situação identificada nestes autos corresponde, sem sombra de dúvida, a um cenário de ***phishing*** e ***vishing***, na medida em que o recorrido AA, ao aceder ao serviço de ***homebanking*** do aqui recorrente de modo totalmente diverso daquele que contratualmente lhe era imposto, e contrário às generalizadas recomendações de segurança, acabou por ingressar numa página de ***Internet*** contrafeita, onde partilhou as suas credenciais, permitindo a terceiros realizar diversas iniciativas, como se tratassem do próprio.
RR. O Banco 1... logrou provar que o sucedido resultou de ato que culposamente lhes é imputável, com particular censura pela forma grosseira como incumpriram deveres a que se encontravam adstritos, logrando ilidir a presunção de culpa constante do n.º 1 do artigo 799º do Código Civil, e demitindo-se de qualquer responsabilidade.
SS. Assim sendo, "***nestes caso[s], é o cliente quem suporta as perdas resultantes de operações de pagamento efectuadas em execução de ordens dadas através do sistema de homebanking por terceiros, a quem, por actuação gravemente negligente, facultou os códigos e chaves necessários a que tais ordens fossem identificadas como tendo sido dadas por si***."
TT. Tal é, efetivamente, a melhor solução de Direito aplicável aos factos provados nos presentes autos, tal como corrobora o sentido decisório impresso nas seguintes decisões: **Ac. do TRE de**

12/04/2018 [destacando-se das respetivas conclusões que: ***O comportamento do autor que tendo acedido a uma página eletrónica ilícita convencido de que se tratava da página da entidade bancária, forneceu, a solicitação do sistema, além do número de identificação e do código PIN, a totalidade das coordenadas do cartão matriz, mostra-se adequando a viabilizar a e realização por terceiros de operações de pagamento não autorizadas; A atuação do autor, ao inserir a totalidade das coordenadas inscritas no cartão matriz em páginas semelhante à do serviço de homebanking da Ré, configura negligencia grave***"; **Ac. do TRG de 25/11/2013** [destacando-se das respetivas conclusões que: ***No contrato coligado de depósito bancário e de serviços de acesso via internet à sua movimentação e a outros serviços disponibilizados pela ré, entidade bancária esta tem o dever de protecção e informação, na sua execução continuada; O aderente tem de cumprir um conjunto de deveres conexos com a segurança do seu sistema informático e uso da chave de acesso concedida pela ré, não a fornecendo a terceiros. A entidade bancária cumpre o seu dever de protecção e informação colocando no seu site toda a informação disponível sobre segurança, que os utentes têm o dever de consultar, para se prevenirem de fraudes. Age com culpa o utente que fornece todo o seu conteúdo do cartão matriz perante uma solicitação numa página idêntica à do banco, uma vez que contraria toda a lógica do sistema de segurança que não pode ser desconhecida por parte do utilizador]***; **Ac. do TRE de 12/12/2013** [destacando-se das respetivas conclusões que: ***Provando a Ré que a Autora fez uma utilização imprudente, negligente e descuidada desse serviço, revelando a terceiros, na internet, os seus códigos pessoais de acesso ao serviço, bem como dos elementos necessários para a confirmação/validação da operação bancária, não lhe é exigível o pagamento das quantias por eles indevidamente movimentadas]***; **Ac. do TRE de 25/06/2015** [destacando-se das respetivas conclusões que: ***Age com culpa o utente que fornece todo o conteúdo do cartão matriz perante uma solicitação numa página idêntica à do banco, uma vez que contraria toda a lógica do sistema de segurança que não pode ser desconhecida por parte do utilizados (…). A Ré ao provar a culpa da Autora na transmissão da totalidade dos dados do seu cartão matriz a terceiros e, consequentemente, o seu incumprimento do contrato de homebanking por violação das mais elementares regras de segurança impostas pelo mesmo, ilidiu a presunção de culpa prevista no art. 799º nº 1 do Código Civil, que sobre si impendia, pelo que não é responsável pela movimentação das contas bancárias de forma fraudulenta.***"

Nestes termos, e nos mais de Direito a suprir doutamente por V. Exa., deve a presente APELAÇÃO ser julgada procedente, por integralmente provada e:

i. Alterar a matéria de facto provada nos termos acima peticionados; e

ii. Revogar a decisão proferida pelo tribunal a quo substituindo-a por outra que considere ter o recorrido AA atuado com manifesta negligência grosseira, cumprindo-lhe, por isso, suportar o risco envolvido e as transações que diz não ter autorizado, sem nada poder reclamar do aqui recorrente Banco 1....

*

Foram apresentadas contra-alegações pelos AA. **AA** e **BB**, que se encontram finalizadas com a apresentação das seguintes conclusões:

1. A argumentação expendida pelo Recorrente nas suas alegações carece de sustentação factual e jurídica, revelando uma incompreensão ou desconsideração dos princípios que regem a responsabilidade das instituições financeiras em matéria de serviços de pagamento e segurança digital.
2. Isso mesmo é de tal forma tão evidente que o Banco Réu/ Recorrente optou por não impugnar uma série de factos dados como provados que estabelecem a sua responsabilidade e fazem soçobrar a sua tese de negligência grosseira dos Autores.
3. Conforme devidamente provado em primeira instância, e que o Recorrente não consegue infirmar, o Autor marido foi induzido em erro através de anúncios patrocinados em motores de busca (como Google e Microsoft Bing), que o direcionaram para uma página falsa do Banco 1... [alíneas o), p), q) da matéria de facto provada na sentença].
4. Esta circunstância, por si só, já demonstra a falha do Banco 1..., aqui Recorrente, em proteger os seus clientes de esquemas de phishing amplamente divulgados e que, como o próprio Banco reconhece, afetavam vários dos seus clientes desde meados de dezembro de 2022 [alínea o) da matéria de facto provada].
5. A sofisticação do esquema não se esgotou no phishing: o Autor marido foi subsequentemente alvo de uma chamada telefónica (vishing) de um indivíduo que se identificou como funcionário do Banco 1... [alínea bb) da matéria de facto provada].
6. O mais grave, e que inutiliza por completo a tese da "negligência grosseira" do Recorrido, é que este indivíduo possuía dados pessoais e bancários sensíveis do Autor (nome completo, morada, e até mesmo um movimento recente com o cartão de débito [alínea cc) da matéria de facto provada]).
7. Esta posse de informações confidenciais, que só poderiam ter origem em falhas de segurança ou vulnerabilidades exploradas no sistema do Banco 1..., foi determinante para criar uma falsa sensação de legitimidade e confiança no Autor [alínea dd) da matéria de facto provada].
8. Foi sob esta premissa de confiança, habilmente construída pelos "meliantes" (assim apelidados na sentença) com base em informações que deveriam estar seguras, que o Autor marido, a pretexto de "desbloquear uma ordem de pagamento", foi solicitado a fornecer um código OTP (One-Time Password) [alínea ee) da matéria de facto provada].
9. A entrega deste código não pode ser qualificada como negligência grosseira, mas sim como o resultado de uma manipulação psicológica sofisticada, onde a vítima foi levada a crer que estava a interagir com o seu próprio banco para resolver um problema.
10. A jurisprudência tem sido unânime em considerar que a negligência grosseira, para efeitos de exclusão da responsabilidade do prestador de serviços de pagamento, exige uma conduta de extrema gravidade, que se aproxima do dolo, ou seja, uma total e manifesta indiferença pelas regras de segurança.
11. O Banco 1..., como prestador de serviços de pagamento, tem um dever acrescido de segurança e proteção dos fundos dos seus clientes, conforme estabelecido no Decreto-Lei n.º 91/2018, de 12 de

novembro (Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica), que transpõe a Diretiva (UE) 2015/2366 – PSD2.
12. A inação do Banco 1... face à campanha de fraude em massa, que o próprio reconhece, e a falha em proteger os dados dos seus clientes que foram utilizados para legitimar a fraude, são fatores determinantes para a sua responsabilidade e afastam qualquer alegação de negligência grosseira por parte dos Recorridos.
13. A pretensão do Recorrente de ampliar a alínea ee) com a frase "não obstante constar dessa mensagem SMS a menção de que o envio e a receção dessa mensagem e do Código OTP tinham na sua origem uma operação que tinha sido desencadeada pelo cliente nos canais digitais do Banco 1..., que se destinava a ser introduzido nesses canais digitais e que caso não reconhecesse tal operação devia contactar o Banco 1..." constitui uma clara inovação factual, sem qualquer suporte na prova produzida em primeira instância.
14. O vishing, meticulosamente desenhado, incluiu a menção de dados pessoais e movimentos bancários reais do Autor [alínea cc) da matéria de facto provada], assim criando uma convicção de legitimidade e confiança que suplantou qualquer alerta genérico contido na mensagem SMS.
15. Quanto à proposta de aditamento do facto "tt) As transações reclamadas pelos Autores nos presentes autos - consubstanciando operações de pagamento - foram autenticadas, contabilizadas e devidamente registadas, e não foram afetadas por qualquer avaria técnica ou por outra deficiência relacionada com o serviço de pagamento prestado pelo Banco 1..." é inútil para a decisão da causa e, pior, constitui uma conclusão de direito disfarçada de facto.
16. O facto de as operações terem sido "autenticadas" não ilide a responsabilidade do Banco se a autenticação foi obtida por meios fraudulentos e se o Banco não provar a negligência grosseira do cliente, o que, como já se demonstrou, não conseguiu fazer (arts. 113.º do DL n.º 91/2018).
17. As operações foram "autenticadas" precisamente porque os "meliantes" obtiveram as credenciais e o OTP através de um esquema fraudulento sofisticado, que explorou falhas na segurança do Banco (acesso a dados pessoais) e a sua inação perante a campanha de fraude, e não por uma negligência grosseira do seu cliente.
18. Posto isto, não tem qualquer razão o Banco Recorrente ao insurgir-se contra a valoração que foi feita pelo Tribunal quanto ao depoimento das testemunhas FF e EE, a qual consta de forma exata da motivação da sentença, que supra se transcreveu.
19. A sentença recorrida, ao contrário do que o Banco 1... alega, não se limita a acolher as declarações do Autor AA, antes contém uma análise cruzada e conjugada de todos os elementos de prova disponíveis, desde logo dos documentos (as condições gerais do serviço, o Guia de Ativação dos Canais Digitais, os registos das operações bancárias, e o comprovativo da participação criminal), das testemunhas (cujo depoimento não foi posto em causa), bem como das presunções judiciais e das regras da experiência (a atuação sofisticada dos "meliantes" e a vulnerabilidade no sistema do Banco).
20. Acresce que a credibilidade que o depoimento das testemunhas mereceu para o Tribunal de primeira instância não é sequer minimamente abalada no recurso.
21. No julgamento da matéria de facto, os poderes da segunda instância estão delimitados pelos artigos 662.º, n.º 1, e 640.º, n.º 1, al.

b), do CPC, pelo que a decisão da primeira instância só poderá ser alterada se a prova produzida impuser objetivamente (e não apenas permitir) decisão diversa.
22. *In casu*, numa apreciação conjugada de todos os meios probatórios, a decisão da matéria de facto surge de forma lógica, racional e consentânea com as regras da experiência, não merecendo, por isso, qualquer reparo.
23. Ao exposto soma-se que do simples confronto do recurso interposto com a douta sentença proferida, resulta evidente que o Banco 1... optou por não impugnar uma série de factos cruciais que estabelecem a sua responsabilidade e fazem soçobrar decisivamente a sua tese de negligência grosseira dos Autores, desde logo os factos provados sob as alíneas o), p), q), x), cc), dd), ii), oo) e pp).
24. Ao não impugnar o julgamento destes factos, o Banco 1... permitiu que os mesmos se tornassem inalteráveis no processo, vinculando o Tribunal da Relação, e, por si só, são suficientes para sustentar a condenação independentemente da discussão sobre a eventual negligência do Autor, fazendo improceder o recurso (arts. 635.º, n.º 4, e 640.º do CPC).
25. A sentença de primeira instância aplicou corretamente o regime jurídico da responsabilidade dos prestadores de serviços de pagamento, consagrado no referido Decreto-Lei n.º 91/2018, de 12 de novembro (Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica), que transpõe para a ordem jurídica interna a Diretiva (UE) 2015/2366 (PSD2).
26. Deste regime legal flui que o prestador de serviços de pagamento está obrigado a assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao seu utilizador, devendo proporcionar um sistema de segurança eficaz e impeditivo de uma utilização abusiva por parte de terceiros.
27. Nos termos do artigo 113.º do referido diploma legal, o ónus da prova de que o utilizador agiu de forma fraudulenta ou com negligência grosseira recai sobre o prestador de serviços de pagamento, o que o Banco Réu/Recorrente não logrou demonstrar.
28. A responsabilidade do Banco 1... decorre, ainda, da sua falha em garantir a segurança dos seus sistemas e em proteger os seus clientes de forma eficaz – apesar de ter conhecimento da campanha de phishing e vishing que estava a afetar os seus clientes, não implementou medidas suficientes para a combater ou para alertar os seus clientes de forma clara e inequívoca, que não se bastam com meros avisos genéricos.
29. A utilização de dados pessoais e bancários dos Recorridos pelos “meliantes”, para legitimar a chamada telefónica, revela igualmente uma falha na segurança dos dados do Banco e uma vulnerabilidade que o mesmo deveria ter acautelado.
30. A jurisprudência tem sido consistente na atribuição de responsabilidade aos bancos em situações de fraude eletrónica, especialmente quando se verifica que a sofisticação do esquema fraudulento ultrapassa a capacidade de discernimento do utilizador comum e quando o banco não demonstra ter adotado todas as medidas de segurança exigíveis.
31. No caso dos autos, estão em causa três operações, que os Autores não executaram nem autorizaram, como o Banco Réu e Recorrente bem sabe por lhe ter sido, por diversas vezes e formas, comunicado [facto provado sob a alínea gg)].

32. Não raras vezes, os clientes bancários são alvo de ciberataques, sob a forma de phishing ou das suas variações designadas de smishing e vishing, mas, mesmo nestes casos, em que as vítimas contribuem de alguma forma para a utilização dos seus dados por terceiros dos seus dados, tal, só por si, não é suficiente para que se possa considerar a conduta como grosseiramente negligente.
33. Nas mais das vezes, as vítimas limitam-se a atuar perante o que tudo indicava ser proveniente do Banco de que são clientes, do mesmo canal emissor do qual já tinham recebido outros e-mails, SMSs e chamadas telefónicas de absoluta fidedignidade, inexistindo, por isso, um erro imperdoável, uma desatenção inexplicável ou uma incúria indesculpável.
34. Assim sendo, impende sobre o Banco Réu, enquanto prestador desse serviço, a responsabilidade pelo reembolso das quantias que foram objeto das operações não autorizadas (art. 114.º, n.º 1, do DL n.º 91/2018).
35. Ademais, as instituições de crédito como o Banco Recorrente são responsáveis pela boa gestão e pela proteção das enormes quantias monetárias depositadas junto das mesmas pelos seus clientes, devendo assegurar a fiabilidade dos serviços de acesso à distância, nomeadamente pela utilização da internet, e a confidencialidade dos dados dos seus clientes (Decreto-Lei n.º 298/92, de 31/12).
36. E assim sendo, a mais alta jurisprudência tem decidido de forma unívoca que a movimentação fraudulenta por terceiro de um depósito bancário, tal como o risco de extravio ou dissipação dos respetivos valores, não é oponível ao depositante, que a ela foi alheio, independentemente de culpa do depositário, que, aliás, sempre se presumiria (arts. 796.º e 799.º do CC).
37. Em face do exposto, o Banco Réu/Recorrente é contratualmente responsável perante os Autores e, tendo faltado culposamente ao cumprimento de obrigações que sobre si impendiam, responde por todos os prejuízos causados, incluindo a título de danos não patrimoniais (arts. 483.º, 496.º e 798.º do CC).
38. Os danos não patrimoniais só poderão ser ressarcidos pela atribuição de uma quantia que puna a conduta e, de certo modo, rasure a memória do acontecimento, tendo em conta não só a sensibilidade como a condição socioeconómica de lesado e lesante, nomeadamente pelo recurso a juízos de equidade (arts. 564.º e ss. do CC).
39. Assim sendo, têm os Autores direito a ser compensados pelo Banco 1... pelos danos não patrimoniais que a sentença julgou provados e que o Recorrente nem sequer colocou em causa [factos provados sob as alíneas qq) e rr)].
40. Tudo visto, e face ao exposto, a douta decisão proferida não merece a censura que o Réu/Recorrente lhe aponta, nem enferma de qualquer nulidade, irregularidade, insuficiência, contradição ou erro, motivo pelo qual deve ser mantida.

TERMOS EM QUE DEVE SER NEGADO PROVIMENTO AO RECURSO INTERPOSTO PELO RÉU, CONFIRMANDO-SE INTEGRALMENTE A DOUTA DECISÃO PROFERIDA, COM O QUE FARÃO V. EXAS. A ESPERA E COSTUMADA JUSTIÇA!

*

A Exmª Juiz *a quo* proferiu despacho a admitir o recurso interposto,

providenciando pela sua subida a este Tribunal.

*

Facultados os vistos aos Exmºs Adjuntos e nada obstando ao conhecimento do objecto do recurso, cumpre apreciar e decidir.

*

2 – **QUESTÕES A DECIDIR**

Como resulta do disposto no art. 608º/2, *ex vi* dos arts. 663º/2, 635º/4, 639º/1 a 3 e 641º/2, b), todos do CPC, sem prejuízo do conhecimento das questões de que deva conhecer-se *ex officio*, este Tribunal só poderá conhecer das que constem nas conclusões que, assim, definem e delimitam o objecto do recurso.

Consideradas as conclusões formuladas pelo apelante, este pretende que:

I. - se altere a matéria de facto:
- quanto ao decidido no facto dado como provado em **ee)**, cuja redacção deve ser alterada (conclusão **T.**);
- quanto ao novo ponto a aditar ao elenco dos factos provados: o ponto **tt)** (conclusão **U.**);
II. - se reaprecie a decisão de mérito da acção (conclusões **V.** e ss.).

*

3 – OS FACTOS

Factos provados
a) O Banco 1... é uma instituição de crédito, registada junto do Banco de Portugal, habilitado a prosseguir todas as operações de banca universal, designadamente a recepção de depósitos, a prestação de serviços de pagamento e a emissão de moeda electrónica.
b) Exerce a sua actividade comercial em todo o território nacional, quer através da sua rede de balcões, quer através dos canais digitais que disponibiliza aos seus clientes, de acordo com práticas recomendadas, designadamente em matéria de cibersegurança.
c) Em matéria de banca digital disponibiliza aos seus clientes serviços de movimentação remota das respectivas contas através da página de "homebanking" e de aplicação digital "app mobile Banco 1...".
d) É recorrentemente recomendado pelo Banco 1... aos seus clientes que o acesso ao serviço "homebanking" ocorra a partir do acesso ao sítio da internet ... e que a instalação (download) da app ocorra a partir das lojas (stores) oficiais presentes em dispositivos móveis.
e) Os Autores são titulares de uma conta bancária de depósitos à ordem junto do Banco R., com o nº ...03, a que corresponde o IBAN ...36.
f) Os AA. procederam à abertura da referida conta em 10/01/2020, na Loja correios... de ....
g) Naquela ocasião, o Autor marido aderiu também a um cartão de débito, a ser-lhe remetido posteriormente, recebendo uma carta PIN com o nº ...17.
h) Por sugestão do funcionário do Banco R., os Autores viriam a aderir aos serviços de "homebanking" e "mobilebanking", designados de canais digitais, depois de lhes ter sido assegurado que os mesmos eram de uma grande comodidade e fiabilidade, sendo providos de um eficaz sistema de segurança.
i) A adesão a tais serviços foi formalizada pela assinatura dos Autores

de documentos já elaborados prévia e unilateralmente pelo Réu, cujo conteúdo não lhes foi lido e explicado.
j) No âmbito do acesso ao serviço "homebanking" do Banco 1... definiram as respectivas credenciais (username e password), não sendo estas conhecidas do Banco 1....
k) Para adesão e manuseamento do serviço de "homebanking" o Autor AA indicou junto do Réu o número de telemóvel ...72 para o qual, seriam enviados códigos (OTP´s), para fins diversos, nomeadamente, autenticação de determinadas operações.
l) O serviço de homebanking permite aos Autores movimentar, remotamente, fundos depositados junto do Réu, obrigando-se este, por sua banda, a disponibilizá-los, quando tal lhe seja solicitado pelos depositantes, segundo ordens transmitidas pelos modos de autenticação previstos.
m) Consta das condições gerais do serviço (cláusula 2.3.) o seguinte: "1) *Para aceder ao serviço o Cliente deverá utilizar o sítio da internet ....pt e cumprir os procedimentos estabelecidos pelo Banco para o efeito*.
n) Consta da cláusula 5.1 das condições gerais do serviço o seguinte: Para evitar o uso fraudulento dos Canais Digitais, o Cliente deverá:
(i) *Manter o(s) PIN secreto(s)*;
(ii) *Não permitir a utilização dos seus Códigos de Segurança por terceiros, ainda que seus mandatários*;
(iii) *Memorizar o(s) PIN, abstendo-se de os anotar*;
(iv) *Não guardar nem registar o(s) PIN, de uma forma que possa ser inteligível ou em local acessível a terceiros*;
(v) *Não registar os códigos PIN em algo que guarde ou transporte conjuntamente com o referido cartão*;
(vi) *Evitar enviar os seus dados pessoais e Códigos de Segurança via correio electrónico uma vez que os dados enviados por esta via circulam sem protecção*;
(vii) *Não introduzir os seus dados pessoais e Códigos de Segurança em qualquer página da internet, com excepção da página do Banco*;
(viii) *Verificar cuidadosamente o teor do SMS da Segurança Adicional, só o devendo introduzir no Homebanking, no Mobilebanking, caso esteja seguro da autenticidade da mensagem*;
(ix) *Alterar periodicamente os PIN´s secreto(s)*; e
(x) *Consultar com regularidade os movimentos realizados em conta de modo a detectar e reportar os mesmos prontamente ao Banco*.
n) Constava, igualmente, do Guia de Activação dos Canais Digitais fornecido com o número de utilizador provisório disponibilizado aos Autores aquando da adesão ao serviço, o seguinte: "*O Banco 1... nunca solicita a sua palavra-passe, seja através de email/sms, telefone ou por qualquer outro meio. Não confie em mensagens de e-mail supostamente enviadas pelo Banco 1..., solicitando elementos de carácter pessoal e/ou confidencial, como por exemplo as suas credenciais de acesso ou o número de telemóvel. Utilize e mantenha actualizado um programa antivírus para proteger o seu computador de ataques, esquemas e mensagens de correio electrónico maliciosos; Mantenha o sistema operativo, bem como outros programas do seu computador (e.g.browser), actualizados; aplique as actualizações de segurança disponibilizadas pelos devidos fornecedores de software; Sempre que suspeite que as suas credenciais de acesso possam estar comprometidas, não hesite em alterá-las de imediato ou pedir o seu bloqueio através do serviço telefónico.*"

o) A partir do início da segunda quinzena do mês de Dezembro de 2022, vários clientes do Réu foram afectados por uma prática, promovida e executada por terceiros não identificados, que consistia em contratar anúncios publicitários junto de entidades que administram e exploram motores de busca na internet (Google e Microsoft Bing), de acesso universal.
p) Qualquer cliente que introduzisse num dos sobreditos motores de busca a expressão “homebanking Banco 1...”, ou outra idêntica, encontraria nos lugares cimeiros dos resultados dessa pesquisa um dos mencionados anúncios, criando-lhe a convicção de que ao aceder-lhes estaria a aceder à página da internet do Banco 1....
q) Porém, ao aceder a tais anúncios, estava o cliente, a ingressar, numa página da internet falsa, com um endereço diferente da página de acesso ao homebanking do Banco 1..., artificiosamente criada por esses terceiros, com o intuito de se apropriarem de dados (máxime credenciais de instrumentos de pagamento), para lograrem, posteriormente, realizar operações de pagamento, em particular transferências a débito e pagamentos).
r) Logo no acesso inicial a essas páginas de internet falsas, eram solicitados aos clientes os seguintes dados “username” (nome de utilizador) e “password” (senha pessoal – código alfanumérico definido pelo cliente), tendo lhes sido solicitada a introdução de todos os caracteres da password, quando no acesso regular ao serviço de homebanking não é introduzida pelo registo de todos os caracteres que a compõe, mas apenas a introdução de algumas posições aleatórias.
s) Na posse destes dois elementos (username e password) do cliente, os terceiros conseguiram iniciar o processo de instalação da app mobile Banco 1..., em dispositivo que controlavam.
t) Iniciado o processo de instalação da App mobile Banco 1... foi automaticamente gerada uma One Time Password (OTP), com uma validade temporal muito reduzida (escassos minutos), a qual não pode ser partilhada.
u) Esse OTP foi automaticamente enviado por SMS para o telemóvel do cliente que está indicado junto do Réu.
w) Esses terceiros não identificados solicitavam aos clientes que introduzissem a referida OTP na página de internet falsa que haviam criado para esse efeito, tendo esses clientes partilhado esse código, com os mencionados terceiros.
v) A disponibilização do OTP pelos clientes a esses terceiros, permitiu-lhes concluir o processo de instalação da app mobile Banco 1... num dispositivo sob o seu controlo e, desse modo, ordenar movimentos a débito nas contas.
x) Em data não concretamente apurada, mas seguramente entre 15/12/2022 e 11/01/2023, o Autor marido pesquisou, através de um motor de busca de acesso universal, pelo site do Banco 1... e acedeu a um dos resultados exibidos que não correspondia à página oficial da internet (.... Pt).
y) De seguida foi redirecionado para uma página da internet falsa na qual introduziu o nome de utilizador (username) e a senha (password completa), no processo de autenticação para acesso ao serviço homebanking.
z) Actuando deste modo, facultou a terceiros, os meios necessários para que procedesse à instalação da app mobile Banco 1... (num equipamento móvel sob controlo desses terceiros, com um IP com

origem em .../..., instalação essa que não foi concluída numa primeira fase, por razões concretas que não se lograram confirmar.
aa) Entre os dias 10/01/2023 e 11/01/2023, esses terceiros não identificados, na posse das credenciais correspondentes ao username e password do Autor marido, lograram aceder ao homebanking do Banco 1....
bb) No dia 11/01/2023, pelas 11h51, o Autor marido recebeu uma chamada no seu telemóvel com o nº ...72, com origem no nº ...73, de alguém que se identificou como funcionário do Banco.
cc) No início de tal chamada telefónica, o interlocutor do Autor indicou-lhe o seu nome e morada completos, solicitando confirmação sobre a realização de um movimento com o cartão de débito nessa manhã, num posto de abastecimento, no montante de € 50,00, factos que o Autor confirmou.
dd) Com a indicação desses dados pessoais e de movimentos concretos registados na sua conta à ordem, o interlocutor criou a convicção no Autor marido de que falava com algum funcionário do Banco 1....
ee) Nesse contacto telefónico, a pretexto de proceder ao desbloqueio de uma ordem de pagamento, solicitaram-lhe o fornecimento do Código OTP, enviado por SMS para o seu telemóvel pelo Banco Réu, o que Autor marido partilhou.
ff) Na posse desse código OTP concluíram com sucesso a instalação da App mobile Banco 1... num equipamento, com IP localizado em Portugal.
gg) Em acto contínuo, nesse mesmo dia 11/01/2023, foram realizados os seguintes movimentos, através da App mobile Banco 1... instalada em dispositivo dominado por esses terceiros:
- Mobilização da conta a prazo para a conta à ordem da conta ...48 para a conta ...03), no montante de € 16.000,00 – 11h56m;
- Transferência intrabancária da conta ...03 para a conta ...02, no valor de € 9.998,00 – 11h57m;
- Pagamento de serviços para a entidade “...30” e referência “...78”, no montante de € 7.000,00 – 11h58m.
hh) O Autor marido tomou conhecimento dessas operações, nesse mesmo dia, pelas 12h49, quando se dirigiu ao Multibanco, na cidade ..., onde ia almoçar, e efectuou um levantamento de € 80,00 em numerário e uma consulta de movimentos.
ii) Tais operações não foram por si executadas nem ordenadas, tendo sido realizadas contra a sua vontade, sem a sua autorização ou consentimento.
jj) O Autor dirigiu-se a um balcão do Banco R. na cidade ..., a fim de reportar o sucedido.
kk) Ali chegado, recebeu da funcionária do Banco Réu que o atendeu a confirmação de que tais movimentos teriam sido efectivamente realizados, pela mobilização de montantes depositados numa conta de depósitos a prazo dos Autores para a sua conta à ordem, a partir da qual se seguiram duas saídas de dinheiro – uma por transferência bancária e outra por pagamento MB.
ll) Por não ter efectuado tais movimentos, o Autor pretendeu desencadear junto do Banco R. os procedimentos de averiguações e os necessários para fazer reverter tais operações, mas foi-lhe transmitido que para o efeito era necessário previamente apresentar uma participação criminal.
mm) O Autor deslocou-se ao Posto Territorial ... da Guarda Nacional

Republicana, o da área da sua residência, onde apresentou a competente denúncia criminal dos factos, no mesmo dia 11/01/2023, pelas 15h29, dando origem ao NUIPC 104/23.1 JABRG.
nn) Munido do comprovativo da participação criminal, dirigiu-se ao balcão da Loja correios... de ..., para efectivar o reporte da situação, o que fez pelas 17h25 desse mesmo dia.
oo) Acto contínuo, às 17h27, o Autor recebeu mensagens escritas (sms) no seu telemóvel, do Banco 1..., dando-lhe nota do bloqueio de acesso aos canais digitais e do processo relacionado com o seu cartão de débito.
pp) Não obstante o tempo entretanto decorrido e as sucessivas diligências efectuadas pelos Autores, o Banco R. permanece sem dar qualquer resposta efectiva ao sucedido, estando aqueles privados dos referidos € 16.998,00, desde o dia 11/01/2023.
qq) Devido à situação, os Autores sofreram abalo emocional, inquietações e transtornos.
rr) Viram-se privados de uma parte das suas poupanças, o que lhes causou um estado de preocupação e angústia, ante a possibilidade de não reaverem o seu dinheiro.
ss) O Autor marido era frequente utilizador do serviço homebanking.

*

Factos não provados

a) A concretização das operações referidas, aconteceu por falha grave do sistema de segurança implementado pelo Banco R.
b) Os Autores sempre cumpriram todas as recomendações de segurança conhecidas e nunca facultaram a terceiros, ainda que inadvertidamente ou contra a sua vontade, os seus dados de acesso à conta bancária pelos canais digitais disponíveis.
c) O Banco Réu enviou nos dias 17 e 18 de Novembro de 2022, a toda a carteira de clientes, entre eles os Autores, um email com o assunto "Esteja sempre seguro com o Banco 1..., com as seguintes advertências:
"*Aceda directamente ao browser e certifique-se de que a ligação é segura*"
"(…) *não partilhe nenhum tipo de dados confidenciais*"
"*No Banco 1... nunca lhe pedimos que partilhe os seus dados de login ou códigos de segurança por e-mail, SMS, Whatsapp ou telefone*".
d) A página falsa acedida pelo Autor marido, nas circunstâncias referidas nas als. x), y) e z) dos factos provados continha elementos muito pouco semelhantes à webpage ... .pt., designadamente diferenças gráficas visíveis e com um procedimento de autenticação diverso daquele que o Banco proporciona.
e) Era do conhecimento dos Autores que nunca era solicitada a introdução completa da senha (password) com inscrição de todos os caracteres, mas apenas posições aleatoriamente selecionadas pelo sistema, bem como nunca devida ser partilhado qualquer código de autenticação (OTP).

*

Motivação

Na consideração da factualidade provada e não provada, o tribunal alicerçou a sua convicção no acervo documental junto aos autos em conjugação com o depoimento das testemunhas CC, DD, enteados do Autor marido, EE (investigador de irregularidades do Banco 1...), FF

(Bancária no Banco 1...), GG (Director de Canais e qualidade do Banco 1...), e, ainda, ponderando as declarações de parte do Autor marido, tudo analisado à luz das regras da experiência comum e normalidade social.
É pacífico e evidente que as descritas operações a débito executadas na conta bancária dos Autores não foram por estes realizadas, e foram realizadas por terceiros desconhecidos, atráves de actuação fraudulenta, sem conhecimento nem autorização dos Autores. Quanto ao "*modus operandi*" que permitiu essa actuação ilícita, foi fundamental o depoimento da testemunha EE, Investigador de irregularidades do Banco 1..., que descreveu, de modo circunstanciado, e pormenorizado o procedimento adoptado pelos terceiros desconhecidos para lograrem os seus intentos.
Explicou que o processo fraudulento iniciou-se com a criação de várias páginas (falsas) semelhantes ao site oficial do Banco 1... (quantificou 10 páginas identificadas), mas que apresentavam diferenças visíveis, designadamente quanto ao modo de acesso (no caso das páginas falsas surgia de imediato o login, enquanto que na página verdadeira era necessário digitar num botão que redirecionava os clientes para a página de login), e a introdução da password (nas páginas falsas era necessário introduzir a password completa, enquanto que na página genuína só era solicitada a introdução de algumas posições aleatórias), acessíveis através do motor de busca, e que os utilizadores ao clicarem no link respectivo eram redirecionados para as referidas páginas falsas, onde estes introduziam as suas credenciais de acesso ao homebanking – username e password –, na convicção que o estavam a fazer no site fidedigno. Através deste esquema, os meliantes obtiveram as credenciais de acesso dos clientes que lhes permitia aceder ao homebanking e consultar as contas e dados pessoais, como aconteceu no caso do Autor marido.
Referiu, ainda, que no caso do Autor, foi detectado que no dia 15/12/2022 foi instalada a aplicação num equipamento com IP em ..., mas conseguiram prevenir a perda de recursos financeiros, através do bloqueio do acesso aos canais digitais e desassociação do equipamento onde havia sido instalada a App. Houve um contacto com o cliente para aferir se detectava algum movimento suspeito na sua conta bancária, o qual confirmou que não.
Na posse dos dados recolhidos na primeira fase, numa segunda fase, telefonaram para o Autor, socorrendo-se de informações relativas a dados pessoais verdadeiros e movimentos bancários concretos realizados por este, com a finalidade de credibilizar a chamada. Durante a chamada, iniciaram a instalação da app mobilebanking em dispositivo no seu controlo, e a pretexto de ser necessário desbloquear o seu serviço, solicitaram-lhe o código de OTP, que entretanto, foi enviado pelo Banco 1... para o telemóvel do Autor marido, durante o processo de instalação da App. O Autor marido forneceu esse código, permitindo, assim, a conclusão do processo de instalação. Com a app instalada e com as credenciais que já tinham obtido na primeira fase, conseguiram realizar as operações a débito da conta do cliente.
Mais, esclareceu que a mensagem que o cliente recebeu quando foi iniciado o processo de instalação da App mobile pelos meliantes, não foi a que consta no doc- nº 4 com a petição inicial, tendo referido que tais mensagens foram recebidas pelo cliente posteriormente à execução dos movimentos, sendo que a explicação plausível, é que o

Autor se tivesse apercebido do engano em que caiu e tivesse redefinido a sua password. As mensagens que recebeu com o Código OTP que possibilitou a conclusão da instalação da App foram recebidas em momento temporal anterior. Concretizou, ainda, que os movimentos na conta bancária do Autor foram concretizados através da App que os terceiros conseguiram instalar.
Reconheceu que os serviços de segurança do Banco não foram suficientemente rápidos a detectar a operação fraudulenta de forma a permitir-lhes reverter a operação. Se tivesse sido imediatamente detectada a operação poderia ser possível bloquear a transferência para a conta "mula". A este respeito, resulta da factualidade provada que apesar do Autor ter, de imediato, contactado o Banco logo que se apercebeu dos movimentos fraudulentos, este só iniciou os procedimentos após a apresentação da participação criminal que o Banco exigiu que fosse efectuada previamente, como confirmou a testemunha FF.
Admitiu que depois deste ataque cibernético foram revistos os limites das transferências diárias para contas de titulares diferentes que passaram de € 10.000,00 para € 5.000,00.
As testemunhas FF (funcionária do Banco Réu) e GG (Director de Canais e qualidade do Banco), confirmaram o procedimento fraudulento e o "*modus operandi*" dos meliantes através do qual foram obtidas as credenciais do cliente e concretizados os movimentos na sua conta bancária, nos moldes descritos pela testemunha EE. Ambas as testemunhas confirmaram que o Banco disponibiliza aos seus clientes informação de sensibilização para a possibilidade de ocorrerem acções fraudulentas, alertando-os para a necessidade de assumirem comportamentos preventivos, mas não especificaram, em concreto, que informações e alertas foram remetidos para os clientes.
De realçar, que não foram apresentados quaisquer documentos que comprovem o envio de um email para os Autores no teor identificado nos art.ºs 57º e 58º da contestação, embora tal documento tenha sido protestado juntar.
A testemunha FF, confirmou, ainda, a necessidade de uma participação criminal prévia para que fosse despoletado qualquer procedimento por parte do Banco.
Ambas as testemunhas esclareceram, ainda, que o ciberataque não vulnerabilizou a página do Banco, nem os respectivos sistemas de segurança, tendo ocorrido à margem desses sistemas.
Por seu turno, as testemunhas CC e DD, confirmaram o estado anímico em que os Autores ficaram na sequência dos factos.
Os documentos juntos pelos Autores, provam que estes estavam na posse das condições gerais de abertura de conta e utilização dos serviços, designadamente através dos canais digitais, a sua adesão a esses serviços (ficha de adesão a produtos e serviços e condições particulares), e que igualmente lhes foi fornecido o "guia de activação dos canais digitais", onde consta para além do mais o procedimento de activação do serviço homebanking Banco 1..., a activação da APP Banco 1... e execução das operações (doc. nº 1), pelo que se considera que não podiam desconhecer as condições de utilização do serviço. O documento de registo das chamadas onde consta o contacto fraudulento (doc. nº 2 e 3) e nos docs. nºs 5 e 6 os talões comprovativos dos movimentos.

[transcrição dos autos].

*

4 – FUNDAMENTAÇÃO DE Facto e de DIREITO

Apreciemos as questões suscitadas nas conclusões formuladas pelo apelante.
E fazendo-o, começamos pelas questões relativas à impugnação da matéria de facto.

I) Da alteração da matéria de facto

Alegando ter sido deficiente a análise da prova produzida, diverge o apelante **R. Banco 1..., SA** da decisão da matéria de facto provada, pretendendo a reformulação *pela sua ampliação* do ponto **ee)** e o aditamento de um novo facto: o ponto **tt)**.
Indica o sentido da decisão e os elementos de prova em que fundamenta o seu dissenso, indignando-se com o facto do Tribunal *a quo* não ter considerado toda a prova produzida, antes se tendo respaldado *nas declarações tomadas, exclusivamente, aos ora recorridos, em particular o impetrante AA*.
Mostram-se, assim, cumpridos todos os ónus impostos pelo art. 640º do CPC.
Cumpre, pois, apreciar.

O art. 662º do actual CPC regula a reapreciação da decisão da matéria de facto de uma forma mais ampla que o art. 712º do anterior Código, configurando-a praticamente como um novo julgamento.
Assim, a alteração da decisão sobre a matéria de facto é agora um poder vinculado, verificado que seja o circunstancialismo referido no nº 1, quando *os factos tidos como assentes, a prova produzida ou um documento superveniente impuserem decisão diversa*.
A intenção do legislador foi, como fez constar da "Exposição de Motivos", a de reforçar os poderes da Relação no que toca à reapreciação da matéria de facto.
Assim, mantendo-se os poderes cassatórios que permitem à Relação anular a decisão recorrida, nos termos referidos na alínea c), do nº 2, e sem prejuízo de se ordenar a devolução dos autos ao tribunal da 1ª. Instância, reconheceu à Relação o poder/dever de investigação oficiosa, devendo realizar as diligências de renovação da prova e de produção de novos meios de prova, com vista ao apuramento da verdade material dos factos, pressuposto que é de uma decisão justa.
As regras de julgamento a que deve obedecer a Relação são as mesmas que devem ser observadas pelo tribunal da 1ª. Instância: tomar-se-ão em consideração os factos admitidos por acordo, os que estiverem provados por documentos (que tenham força probatória plena) ou por confissão, desde que tenha sido reduzida a escrito, extraindo-se dos factos que forem apurados as presunções legais e as presunções judiciais, advindas das regras da experiência, sendo que o princípio basilar continua a ser o da livre apreciação das provas, relativamente aos documentos sem valor probatório pleno, aos relatórios periciais, aos depoimentos das testemunhas, e agora inequivocamente, às declarações da parte – cfr. arts. 466º/3 e 607º/4 e 5 do CPC, que não contrariam o que acerca dos meios de prova se dispõe nos arts. 341º a 396º do CC.
Deste modo, é assim inequívoco que a Relação aprecia livremente todas as provas carreadas para os autos, valora-as e pondera-as,

recorrendo às regras da experiência, aos critérios da lógica, aos seus próprios conhecimentos das pessoas e das coisas, socorrendo-se delas para formar a sua convicção.
Provar significa demonstrar, de modo que não seja susceptível de refutação, a verdade do facto alegado. Nesse sentido, as partes, através de documentos, de testemunhas, de indícios, de presunções etc., demonstram a existência de certos factos passados, tornando-os presentes, a fim de que o juiz possa formar um juízo, para dizer quem tem razão.
Como dispõe o art. 341º do CC, as provas têm por função a demonstração da realidade dos factos.
E, como ensina Manuel de Andrade, aquele preceito legal refere-se à prova "*como resultado*", isto é, "*a demonstração efectiva* (…) *da realidade dum facto – da veracidade da correspondente afirmação*".
Não se exige que a demonstração conduza a uma verdade absoluta (objectivo que seria impossível de atingir) mas tão-só a "*um alto grau de probabilidade, suficiente para as necessidades práticas da vida*"[2].
Quem tem o ónus da prova de um facto tem de conseguir "*criar no espírito do julgador um estado de convicção, assente na certeza relativa do facto*", como escreve Antunes Varela[3].
O julgador, usando as regras da experiência comum, do que, em circunstâncias idênticas normalmente acontece, interpreta os factos provados e conclui que, tal como naquelas, também nesta, que está a apreciar, as coisas se passaram do mesmo modo.
Como ensinou Vaz Serra "*ao procurar formar a sua convicção acerca dos factos relevantes para a decisão, pode o juiz utilizar a experiência da vida, da qual resulta que um facto é a consequência típica de outro; procede então mediante uma presunção ou regra da experiência, ou de uma prova de primeira aparência*"[4].
Ou seja, o juiz, provado um facto e valendo-se das regras da experiência, conclui que esse facto revela a existência de outro facto.
O juiz aprecia livremente as provas e decide segundo a sua prudente convicção acerca de cada facto – cfr. art. 607º/5 do CPC, cabendo a quem tem o ónus da prova "*criar no espírito do julgador um estado de convicção, assente na certeza relativa do facto*", como refere Antunes Varela[5].
Se se instalar a dúvida sobre a realidade de um facto e a dúvida não possa ser removida, ela resolve-se contra a parte a quem o facto aproveita, de acordo com o princípio plasmado no art. 414º do CPC, que, no essencial, confirma o que, sobre a contraprova, consta do art. 346º do CC.
De acordo com o que acima ficou exposto, cumpre, pois, reapreciar a prova e verificar se dela resulta, com o grau de certeza exigível para fundamentar a convicção, o que o apelante pretende neste recurso.

*

Como já referido supra, pretende o apelante a alteração da matéria de facto provada, com a reformulação de um ponto e o aditamento de outro.

*

Passemos, então, aos aludidos factos, começando pela pretendida alteração da matéria de facto provada quanto ao ponto a reformular.
Além de outros, a Meritíssima Juiz *a quo* considerou provado que:
ee) Nesse contacto telefónico, a pretexto de proceder ao desbloqueio de uma ordem de pagamento, solicitaram-lhe o fornecimento do Código OTP, enviado por SMS para o seu telemóvel pelo Banco Réu,

o que Autor marido partilhou.
Motivando tal decisão, o tribunal consignou o já supra transcrito, que aqui se dá por reproduzido, a fim de evitar repetições.
Com o que discorda o apelante, propondo a seguinte redacção, ***para permitir concluir e afirmar que o recorrido AA foi grosseiramente negligente no manuseamento do instrumento de pagamento em causa e das suas credenciais***:
ee) Nesse contacto telefónico, a pretexto de proceder ao desbloqueio de uma ordem de pagamento, solicitaram-lhe o fornecimento do Código OTP, enviado por SMS para o seu telemóvel pelo Banco Réu, o que Autor marido partilhou*, não obstante constar dessa mensagem SMS a menção de que o envio e a receção dessa mensagem e do Código OTP tinham na sua origem uma operação que tinha sido desencadeada pelo cliente nos canais digitais do Banco 1..., que se destinava a ser introduzido nesses canais digitais e que caso não reconhecesse tal operação devia contactar o Banco 1...*.
Entendendo os apelados terem sido *fatores determinantes para a sua* (do R.) *responsabilidade e afastam qualquer alegação de negligência grosseira por parte dos Recorridos*, a *inação do Banco 1... face à campanha de fraude em massa, que o próprio reconhece, e a falha em proteger os dados dos seus clientes que foram utilizados para legitimar a fraude*. Pelo que, a pretensão do Recorrente de ampliar a alínea **ee)**, *constitui uma clara inovação factual, sem qualquer suporte na prova produzida em primeira instância*.
Quid iuris?

Ora, revisitada a respectiva prova produzida, o que fizemos, consultando os documentos juntos aos autos e ouvindo as gravações da prova obtida no decurso da audiência de julgamento, especialmente as declarações de parte do A. AA e o depoimento da testemunha EE (Investigador de irregularidades do Banco 1...), não se logrou adquirir convicção diferente daquela obtida pelo Tribunal da 1ª instância. Mesmo sem a mais valia que representa a imediação, não nos ficaram quaisquer dúvidas quanto à credibilidade atribuída à prova produzida e elencada tal como consta na motivação quanto aos factos em questão, pelo Tribunal *a quo* na sentença recorrida. Não se podendo acompanhar a arguição do recorrente de que não havia sido considerada toda a prova produzida, antes se tendo respaldado *nas declarações tomadas, exclusivamente, aos ora recorridos, em particular o impetrante AA*, pois, como já melhor resultava da motivação, *quanto ao "modus operandi" que permitiu essa actuação ilícita, foi fundamental o depoimento da testemunha EE, Investigador de irregularidades do Banco 1..., que descreveu, de modo circunstanciado, e pormenorizado o procedimento adoptado pelos terceiros desconhecidos para lograrem os seus intentos*. Sendo que nada de novo trouxe o recorrente que não tivesse sido ponderado e escrutinado, para além da sua versão e interpretação no que concerne a esta concreta questão, pois o acrescento que pretende e a maneira encontrada de a redigir, não passam de um juízo conclusivo e opinativo, sem suporte na prova produzida. Lembrando-se que o facto de as operações terem sido "autenticadas" pelo utilizador, não ilide a responsabilidade do Banco se a autenticação foi obtida por meios fraudulentos e se o Banco não provar a negligência **grosseira** do cliente (vd. art. 113.º do DL n.º 91/2018, de 12-11). O que não conseguiu fazer, pois as operações foram "autenticadas" como

resultado da intromissão abusiva de terceiros, que obtiveram as credenciais e o OTP através de um esquema fraudulento sofisticado, que explorou falhas na segurança do Banco (acesso a dados pessoais) e a sua inação perante a campanha de fraude, e não por uma negligência grosseira do seu cliente. Decorrendo, pois, a responsabilidade do Banco 1... da sua falha em garantir a segurança dos seus sistemas e em proteger os seus clientes de forma eficaz – apesar de ter conhecimento, como apurado em **o)**, da campanha de *phishing* e *vishing* que estava a afetar os seus clientes, não implementou medidas suficientes para a combater ou para alertar os seus clientes de forma clara e inequívoca, não sendo suficiente meros avisos genéricos. Também a utilização de dados pessoais e bancários dos Recorridos por terceiros, para legitimar a chamada telefónica, revela igualmente uma falha na segurança dos dados do Banco e uma vulnerabilidade que o mesmo deveria ter acautelado. Acompanhando-se a tendência da jurisprudência para responsabilizar o banco em situações em que a fraude é muito sofisticada e o banco falha em implementar medidas de segurança adequadas, pois há um reconhecimento de que o utilizador comum pode ter dificuldade em identificar esquemas complexos, o que aumenta a responsabilidade do banco. A decisão judicial dependerá sempre da análise caso a caso das medidas de segurança adoptadas pelo banco e do grau de diligência do cliente.
Verifica-se, pois, reiterando, que o recorrente nada de novo trouxe sobre esta matéria, pretendendo tão só que seja feita uma valoração diferente e subjectiva – assente essencialmente no seu próprio entendimento – daquela efectuada pelo Tribunal *a quo*.
Resultando evidente nos autos, que na motivação da decisão sobre a matéria de facto, o tribunal recorrido elencou de forma clara e exaustiva os seus argumentos, que aqui se dão por reproduzidos, a fim de evitar mais repetições. Sendo que, na decisão da matéria de facto, cuidou o decisor de esclarecer o caminho que seguiu na ponderação de toda a prova, esclarecendo o relevo de uma e de outra, bem como a conjugação feita.
Logo, porque todos os elementos convocados pelo tribunal *a quo* constam do processo e foram devidamente ponderados, entende-se nada haver aqui a corrigir, decidindo-se pela improcedência da impugnação quanto à alteração desta matéria de facto.

*

Passemos, agora, ao pretendido aditamento de um novo ponto ao elenco dos factos provados, com fundamento no depoimento da testemunha HH e com o seguinte teor:
tt) As transações reclamadas pelos Autores nos presentes autos – consubstanciando operações de pagamento – foram autenticadas, contabilizadas e devidamente registadas, e não foram afetadas por qualquer avaria técnica ou por outra deficiência relacionada com o serviço de pagamento prestado pelo Banco 1....
Com o que não discordam os recorridos, por entenderem ser *inútil para a decisão da causa e, pior, constitui uma conclusão de direito disfarçada de facto*.
Quid iuris?

Diga-se, desde já, terem razão os recorridos. Com efeito, o aditamento do ponto em causa constituiria uma inutilidade para a decisão da causa, não só porque ninguém o questionou, como o seu conteúdo

resulta já disperso na demais factualidade assente - cfr. pontos **gg)** e ss. -, achando-se pressuposto, encerrando, pois, matéria conclusiva.
Tal como já supra mencionado, o facto de as operações terem sido "autenticadas" pelo utilizador, não ilide a responsabilidade do Banco se a autenticação foi obtida por meios fraudulentos e se o Banco não provar a negligência grosseira do cliente (vd. art. 113.º do DL n.º 91/2018, de 12-11). O que ocorreu, *in casu*.
Como assim, sem mais considerações, improcede esta pretensão do recorrente.

*

II. - <u>Da reapreciação da decisão de mérito da acção</u>

Fixada a matéria de facto, que não sofreu qualquer alteração depois de se ter examinado a sua reapreciação conforme pretendido na apelação, levando em conta as conclusões do recurso, passemos, agora, à também pretendida reapreciação da decisão de mérito da acção.
Ora, atendendo a que a matéria de facto não sofreu qualquer alteração, prejudicada fica desde logo essa reapreciação da decisão em conformidade com a pretendida alteração da matéria de facto.
Efectivamente, mantendo-se o quadro factual julgado provado e não provado pelo Tribunal *a quo*, ter-se-á de manter, igualmente, a decisão jurídica da causa nos seus precisos termos, uma vez que se mostra adequada e correcta face à factualidade apurada e aos normativos aplicáveis, nada havendo a apontar à sua fundamentação, que aqui se dá por reproduzida, a fim de evitar repetições.
Não tendo a apelante colocado em causa a aplicação do direito aos factos, antes defendendo decisão diversa em função da alteração da matéria de facto que pretendia com o recurso, impugnação que improcedeu.
Implicando, pois, a reapreciação pretendida pela recorrente, o acolhimento da pretendida alteração da matéria de facto, que representava a sua visão dos factos, mas que não se apurou após instrução e julgamento da causa.
Verificando-se que as partes celebraram contratos de depósito e, coligados com estes, contratos de prestação de serviços, no âmbito do qual os apelados aderiram ao serviço de pagamentos eletrónicos ou à distância, também denominado homebanking, da apelante.
É sobre este contrato de prestação de serviços de pagamento que regula o Decreto-Lei nº 91/2018 de 12-11.
No âmbito desse contrato o apelado foi vítima de *vishing* – forma de *phishing* realizada através de *fraude verbal para levar as pessoas a fornecer dados pessoais ou bancários.*
Assentando o principal ponto de discórdia do recorrente na questão da qualificação da negligência do A. como grosseira, temos que, à luz das circunstâncias concretas que foram analisadas e, em face daquele que tem sido o excurso jurisprudencial em circunstâncias semelhantes, acompanhamos o entendimento de que a culpa que aqui se verificou foi uma culpa relevante, mas que não alcançou o mais exigente nível da negligência grosseira para o qual, a falta de cuidado deve ser escandalosa e o desleixo inadmissível, assim apreensível de modo generalizado[6]. Não vemos que, *in casu*, se tenha alcançado tal patamar. Pese embora de relevo, a falta de cuidado evidenciada não deve ser qualificada como negligência grosseira por, apesar de tudo, não se poder considerar que o apelado tenha praticado um erro

imperdoável, ou uma desatenção ou incúria inexplicáveis, caracterizadores da mesma. Lembrando-se que a inação do Banco 1... face à campanha de fraude em massa, que o próprio reconhece, e a falha em proteger os dados dos seus clientes que foram utilizados para legitimar a fraude, são factores determinantes para a sua responsabilidade e afastam qualquer alegação de negligência grosseira por parte dos Recorridos. Isto porque, as operações foram "autenticadas" como resultado da intromissão abusiva de terceiros, que obtiveram as credenciais e o OTP através de um esquema fraudulento sofisticado, que explorou falhas na segurança do Banco (acesso a dados pessoais) e a sua inação perante a campanha de fraude, e não por uma negligência grosseira do seu cliente.
Chegando-se à mesma conclusão do Tribunal *a quo*, que *dos factos provados resulta claro que os movimentos bancários não decorreram de uma actuação fraudulenta do Autor marido. Também não resulta que tenha ocorrido incumprimento doloso das suas obrigações. Afigura-se-nos que apesar do Autor marido não ter observado todas as recomendações e advertências que lhe foram transmitidas pelo banco Réu, tal incumprimento não se reconduz a negligência grosseira prescrita no art.º 113º, nºs 3 e 4 do RJSPME.*
Com efeito, para a responsabilização do utilizador do serviço não basta a negligência simples (ou culpa leve), é preciso negligência grosseira, uma falta de cuidado extremamente grave.
Não merece, assim, a sentença do Tribunal *a quo* qualquer reparo, pois assenta em operações intelectuais válidas e justificadas e com respeito pelas normas processuais atinentes à prova.

*

5 – SÍNTESE CONCLUSIVA (art. 663º/7 CPC)

…

*

6 – DISPOSITIVO

Pelo exposto, acordam os Juízes desta secção cível em julgar a presente apelação improcedente, assim se confirmando a decisão recorrida.
Custas pelo recorrente.
Notifique.

*

Guimarães, 30-10-2025

(José Cravo)
(Afonso Cabral de Andrade)
(Joaquim Boavida)

[1] Tribunal de origem: Tribunal Judicial da Comarca de ..., V.Castelo - JL Cível - Juiz ...
[2] *In* "Noções Elementares de Processo Civil", págs. 191 e 192.
[3] *In* "Manual de Processo Civil", Coimbra Editora, pág. 420.
[4] *In* B.M.J. nº 112, pág. 190.
[5] Obra supracitada.
[6] [6] Neste sentido, vd. Ac. da RL de 20-02-2024, prolatado no Proc. nº 25052/20.3T8LSB.L1-7 e acessível *in* www.dgsi.pt.